MAX-PLANCK-INSTITUT FÜR QUANTENOPTIK

Entanglement Properties of Quantum States and Quantum Operations

Barbara Kraus

MPQ 282

January 2003

Max-Planck-Institut für Quantenoptik
85740 Garching, Bundesrepublik Deutschland

Entanglement Properties of Quantum States and Quantum Operations

Dissertation

zur Erlangung des akademischen Grades:

Doktor rer. nat.

an der
Naturwissenschaftlichen Fakultät
der
Leopold-Franzens-Universität Innsbruck eingereicht von

Mag. rer. nat. Barbara Kraus

im Januar 2003

durchgeführt am Institut für Theoretische Physik
der Universität Innsbruck bei

Univ. Prof. Dr. J. Ignacio Cirac

Preface

This Thesis summarizes the work that I have been doing during the last three years. I spent the first two of them at the University of Innbruck, Austria and the last one at the Max–Planck–Institute of Quantum Optics in Garching, Germany.

This work is concerned with Quantum Information Theory, which is a very young research field that combines classical information theory with quantum mechanics. One of the main difference between quantum mechanics and classical mechanics is that in quantum mechanics we have the superposition principle. This states that if a system can be in two different states, $|0\rangle$ and $|1\rangle$, then it can also be prepared (as long as superselection rules do not forbid this) in a superposition $\alpha|0\rangle + \beta|1\rangle$. This principle, when applied to two or more subsystems, gives rise to the phenomenon called entanglement. In entangled states, particles can be correlated in a very special form that cannot be explained via classical mechanics, which does not include the superposition principle. Note that any state describing a system composed of several subsystems which contains these kind of correlations, i.e. which is entangled (non–separable), cannot be created locally; that is, using local operations and classical communication. Entanglement, one of the main features in Quantum Information Theory, has several fundamental implications and opens a door to many useful applications. Entangled states can be used, for instance, to send secret messages from one location to another, spatially separated one. This process is the basis of quantum cryptography. The communication protocols used so far are based on some code which is difficult (using classical tools) to decipher. However, they are not proven to be secure. Using entangled states it is also possible to teleport a (unknown) quantum state form one place to a spatially separated location. Another important advantage of Quantum Information is that it allows a speed–up in computation. There exist some algorithms for which it was proven that they can be executed much faster by quantum computers, i.e. computers which are based on the principles of quantum mechanics, than by classical computers.

Form these applications of Quantum Information it becomes clear that

one of the most important issues in Quantum Information Theory is to study the entanglement properties of quantum states. One of the main tasks is to solve the so–called separability problem, which is the characterization of entanglement of mixed states. Despite the effort put into this fundamental problem, which lies at the heart of Quantum Information Theory, it is far from being solved. An even more difficult problem is the quantification of entanglement of multipartite states. So far, a classification of multipartite states according to their entanglement properties has been presented, but there exists neither a criterion to decide to which class a given multipartite state belongs to, nor a computable measure of entanglement for all these different kinds of entanglement. Another fundamental problem in Quantum Information Theory is to decide how useful a given state is for the purposes mentioned above. In particular, whether a state can be transformed into a maximally entangled state, using only local operations and classical communication. This question constitutes the so–called distillability problem.

In recent years a new topic in the research in Quantum Information Theory has been identified, namely the study of the entanglement properties of physical actions. The relevance of this problem is given by the fact that physical actions are the ones that are responsible for creating and manipulating entanglement. Thus, if we want to understand the role of entanglement in Quantum Information Theory, we should also be able to characterize and quantify the physical actions in this respect.

This Thesis is mainly concerned with the two fundamental problems of separability and distillability and with the characterization of physical actions according to their entanglement properties. It is divided into three main parts.

In the first part of this Thesis we introduce some basic concepts which will be used throughout.

The second part of this Thesis deals with the entanglement properties of quantum operations transforming states in a finite dimensional as well as infinite dimensional Hilbert space. We characterize the quantum operators acting on a finite dimensional Hilbert space according to their entangling properties [23]. The formalism developed there allows us to show that it is possible to implement non–local quantum operations using a small amount of entanglement. We also study two–qubit unitary operators [94]. We determine how much entanglement can be created by such an operator when acting on a separable state describing a system composed of two qubits. We also investigate how auxiliary systems might be used to increase the amount of entanglement produced. On the other hand, we investigate continuous variable systems. We concentrate on the so–called Gaussian states, which are present, e.g., in the experiments using linear optics. We investigate interac-

tions which leave a Gaussian state Gaussian and are assisted by *fast* local operations [98]. We analyze which interactions (Hamiltonians and gates) can be simulated in the given setup. Furthermore, we determine the optimal strategy to create/increase the entanglement contained in a two–mode Gaussian state using some given interaction. Analogously, we analyze the optimal ways to produce squeezing, a quantity which is relevant for continuous variable systems.

In the third and last part of this Thesis we investigate quantum states according to their entanglement properties. We study the separability as well as the distillability problem described above. We derive computable necessary and sufficient conditions for separability for low rank density operators describing a system composed of one qubit and a N–level system, and sufficient conditions for separability for arbitrary such states [95]. The main idea there is to prove that the separability problem can be reformulated in terms of polynomial equations. On the other hand, we investigate entanglement witnesses, which are operators that allow us to distinguish between separable and entangled states [106, 107]. We show how those operators can be optimized; that is, how to construct out of a given entanglement witness one which detects the presence of entanglement in an optimal way. Furthermore, we present a canonical form for the so–called non–decomposable entanglement witnesses. We also characterize the states which allow us to determine the border between separable and entangled states, the so–called "edge states". Those methods, developed in order to solve the separability problem for bipartite systems, can easily be generalized to the multipartite case. As applications of those methods we study the entanglement properties of multipartite symmetric states, which are states that are invariant under exchange of any pair of particles. On the other hand, we investigate the quantum correlations contained in some particular examples of three–qubit states. Although, the results and methods derived here are quite powerful, there is no general solution to the problem of separability for quantum states in a finite dimensional Hilbert space. The situation is different in the case of Gaussian states. There the separability problem of bipartite Gaussian states has been solved by presenting an operational criterion [57]. Moreover, the separability problem of three–mode tripartite Gaussian states has also been solved [58]. Easily computable criteria that classify the quantum states according to their separability properties have been derived [58]. We present these results and give a physical interpretation of the criterion of bipartite separability. After that, we study the distillation problem for multipartite quantum states in a finite dimensional Hilbert space. We show that the notion of entanglement witnesses can be employed to characterize distillable as well as activatable states, which are states that can be distilled, consuming

some "weak" entangled state [97]. It should be stressed that this is not only a reformulation of the problem, but gives a new insight into the distillation properties of states, as demonstrated by some non–trivial applications.

Contents

Part I

Basic concepts

The goal of this part of the Thesis is two–fold. On the one hand, we want to review the basic concepts of Quantum Information Theory. On the other hand, we introduce the notation used throughout this Thesis.

This Thesis will deal with either quantum states describing a system composed of two or more subsystems or quantum operations acting on such systems. We denote the subsystems by the capital letters A, B, C, *etc.* throughout this Thesis. As common in Quantum Information Theory we call the persons holding these systems *Alice, Bob, Charly, etc.*, respectively. The Hilbert space of system X will be denoted by $\mathcal{H}_X$ and its dimension by d_X or d_x. We denote by $\mathcal{B}(\mathcal{H})$ the Hilbert space of linear operators acting on a finite dimensional Hilbert space, $\mathcal{H}$, with the scalar product $(A, B) = \mathrm{tr}(A^\dagger B)$. Furthermore, we use capital Greek letters for joint states of at least two systems, e.g. $|\Psi\rangle_{AB}$ denotes a state of systems A and B. Small Greek letters are used for states describing one subsystem, e.g. $|\phi\rangle_A$, if not stated otherwise. We omit the subscripts whenever the system to which a state, a Hilbert space, *etc.* belongs is clear. We denote by $|0\rangle, |1\rangle$ *etc.* the computational basis. We define the Pauli operators as

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = i \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1}$$

and denote by $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. If it is not clear which system an operator is acting on, we specify it with either a sub– or superscript, e.g. $\vec{\sigma}_A$ or σ_x^A. The identity operator acting on a n–dimensional Hilbert space will be denoted by $\mathbb{1}_n$.

This part of the Thesis is divided into two chapters. Chapter 1 is devoted to quantum states. First of all, we consider finite dimensional Hilbert spaces. We introduce the notion of Schmidt decomposition and entanglement measures for pure states. Then we consider the more realistic situation of mixed states. We discuss the problem of separability and review some known results concerning it. In particular we introduce the notion of entanglement witnesses and positive maps there. We also define the problem of distillation in this section. The last part of Chapter 1 is concerned with states belonging to an infinite dimensional Hilbert space. In particular, we consider *Gaussian states*, which are states that occur in current experiments using linear optics. In fact, those states comprise essentially all the experimentally realizable continuous variable (CV) states. We review also for Gaussian states some measures of entanglement and squeezing, a quantity which does not have a counterpart in the case of finite dimensional Hilbert spaces, but is relevant for continuous variable systems.

Chapter 2 is concerned with quantum operations. Again, we distinguish between operators acting on finite– and infinite dimensional Hilbert spaces.

We introduce the notion of completely positive maps, which is the mathematical description of the most general physically implementable operation. After that we consider the evolution of Gaussian states under symplectic transformations.

Chapter 1

Quantum states

1.1 Pure states

A pure state, $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \ldots \mathcal{H}_Z$, describing the state of a system composed of several subsystems is called entangled if it cannot be prepared using only local operations and classical operations (LOCC). Mathematically stated: A state is entangled if it cannot be written as a product state, i.e if it cannot be decomposed as $|\phi\rangle_A |\psi\rangle_B \ldots |\chi\rangle_Z$. In the case of pure states it is very simple to decide whether a given state is entangled or not, in which case it is called separable. One only has to determine the reduced density operator,

$$\rho_X = \mathrm{tr}_{\text{all but } X}(\rho), \tag{1.1}$$

where $\rho = |\Psi\rangle\langle\Psi|$ is the density operator corresponding to the pure state $|\Psi\rangle$. Then the state is a product state if and only if (iff) ρ_X is pure [iff $\mathrm{tr}(\rho_X) = 1$] for all subsystems X. Note that it is much more difficult to decide whether a mixed state is separable or not. In fact, this problem, known as the separability problem is still open for the general case. In Sec. 1.2.1 and Sec. 1.3.2 we investigate the separability properties of quantum states and introduce different methods to characterize them (Chapter 7). In the case of bipartite, and tripartite 1–mode Gaussian States (Sec. 1.3) the separability problem is completely solved as we will see in Sec. 7.2.

Let us now turn back to pure states, in particular to the case of a pure state describing a system composed of two subsystems. The aim of the following two sections is to analyze how entangled such a state is. We review some measures of entanglement and recall the properties that should naturally be fulfill by them. For the purpose of quantifying entanglement we introduce first of all the notion of Schmidt decomposition, which provides us a helpful form of decomposing any pure bipartite state.

1.1.1 Schmidt decomposition

A pure state $|\Psi\rangle$, describing the state of two particles, A and B, always has a *Schmidt decomposition* in the form:

$$|\Psi\rangle = \sum_{k=1}^{m} c_k |\phi_k\rangle_A |\psi_k\rangle_B , \tag{1.2}$$

where $m = \min\{\dim(\mathcal{H}_A), \dim(\mathcal{H}_B)\}$ and $\langle\phi_k|\phi_l\rangle = \langle\psi_k|\psi_l\rangle = \delta_{kl}$ $\forall k, l = 1, \ldots, m$. The real and positive coefficients c_k, which are the square roots of the eigenvalues of the reduced density operator, $\rho_A = \mathrm{tr}_B(|\Psi\rangle\langle\Psi|)$ [or $\rho_B = \mathrm{tr}_A(|\Psi\rangle\langle\Psi|)$] (1.1) are called Schmidt coefficients . We will choose them in decreasing order, i.e. $c_1 \geq c_2 \ldots \geq c_m$.

A state is maximally entangled if the $m = \min\{\dim(\mathcal{H}_A), \dim(\mathcal{H}_B)\}$ Schmidt coefficients are all equal. The Bell basis is an example of a basis consisting out of maximally entangled pure states of two qubits, It is defined as

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{1.3}$$

Later on we also make use of the so–called magic basis [67], which is defined in the same way as the Bell-basis except for some global phases. We will denote the elements of this basis by

$$\begin{aligned} |\Phi_1\rangle &= |\Phi^+\rangle, \quad |\Phi_2\rangle = -i|\Phi^-\rangle, \\ |\Phi_3\rangle &= |\Psi^-\rangle, \quad |\Phi_4\rangle = -i|\Psi^+\rangle. \end{aligned} \tag{1.4}$$

1.1.2 Entanglement measures

We review here some measures of entanglement for pure states. One entanglement measure is the so–called *concurrence* [155], C. It is defined as

$$C(|\Psi\rangle) = |\langle\Psi|\sigma_y \otimes \sigma_y|\Psi^*\rangle|, \tag{1.5}$$

where σ_y is one of the Pauli operators defined in (1). Writing $|\Psi\rangle$ in the magic basis (1.4), i.e. $|\Psi\rangle = \sum_k \mu_k |\Phi_k\rangle$ we get

$$C(|\Psi\rangle) = |\sum_k \mu_k^2|. \tag{1.6}$$

There exist other measures of entanglement which are better expressed in terms of the Schmidt coefficients (1.2) of the state.

The *Entropy of Entanglement* is defined as follows:

$$E_E(|\Psi\rangle) \equiv S(\rho_{red}) = -\mathrm{tr}[\rho_{red}\log_2(\rho_{red})] = -\sum_{k=1}^{m} c_k^2 \log_2(c_k^2), \tag{1.7}$$

where ρ_{red} denotes the reduced density operator of either system A or B (1.1) and the c_k's denote the Schmidt coefficients of $|\Psi\rangle$. This measure, also called the von Neumann entropy of the reduced state, has a well defined meaning: given n copies of a state $|\Psi\rangle$ then one can produce, using only local operations and classical communication, $nE_E(|\Psi\rangle)$ maximally entangled states and vice versa (in the limit $n \to \infty$) [5].

Another useful measure is the *Schmidt number* [116], which we will denote by E_S. It is the number of Schmidt coefficients which are different than zero minus one.

There is another set of measures, the so–called *Entanglement Monotones*, which arises in the context of allowed modification of entangled states under local operations [149, 114]. They are defined as

$$E_n(|\Psi\rangle) = \sum_{k=n}^{m} c_k^2, \tag{1.8}$$

for $n = 1, ..., m-1$.

We will also use the so–called 2–Entropy (related to the 2–Rènyi entropy) of the reduced density operator [81]. It is defined as

$$E_R(|\Psi\rangle) \equiv S_R(\rho_A) = 1 - \mathrm{tr}(\rho_A^2) = 1 - \sum_{k=1}^{m} c_k^4, \tag{1.9}$$

where again ρ_A denotes the reduced density operator of $|\Psi\rangle\langle\Psi|$ and c_k the Schmidt coefficients of $|\Psi\rangle$. In the following we will call this measure the *Rènyi entanglement* .

Properties

A state describing two qubits contains two Schmidt coefficients at most, c_1, c_2, where $c_2 = \sqrt{1 - c_1^2}$. Thus, its entanglement is completely determined by one parameter, c_1. All the measures of entanglement are monotonic functions of each other and, therefore, equivalent. Note further that two states describing two qubits which are equally entangled can always be transformed into each other using local unitary operators. In higher dimensions (m-level systems) the entanglement measures are no longer monotonic functions of each other.

Let us denote now by $|\Psi\rangle$ and $|\Psi'\rangle$ two states describing two m-level systems. Then it might happen that for some measure $|\Psi\rangle$ is more entangled than $|\Psi'\rangle$, whereas for some other measure it is the other way around.

Let us here summarize some of the properties which have to be satisfied by any measure of entanglement, E [73]:

(a) Invariance under local unitary operators, U_A, U_B:

$$E(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger) = E(\rho). \tag{1.10}$$

(b) Monotonicity under local operations: Suppose that Alice makes a measurement on her qubit and she obtains with probability p_k the state σ_k. Then the entanglement cannot increase on average, i.e:

$$E(\rho) \geq \sum_k p_k E(\sigma_k). \tag{1.11}$$

(c) Convexity: The entanglement decreases if we discard some information, i.e.

$$E\left[\sum_k p_k \rho_k\right] \leq \sum_k p_k E(\rho_k) \tag{1.12}$$

Note that (c) implies that for every mixed state ρ there exists a pure state $|\Psi\rangle$ such that $E(\rho) \leq E(|\Psi\rangle\langle\Psi|)$. This is the reason why we only have to consider pure states to prove some statements in this Thesis (Sec. 4.2.2).

Now we briefly summarize some useful properties of the particular measures of entanglement mentioned in the previous subsection. Let us start with the properties of the concurrence, C, assuming that we have two qubits in the state $|\Psi\rangle = \sum_k \mu_k |\Phi_k\rangle$, where the $|\Phi_k\rangle$ form the magic basis (1.4):

(i) $C(|\Psi\rangle) = 1$ iff $\mu_k^2 = e^{i\delta}|\mu_k|^2$ $(k = 1, \ldots, 4)$. This means that a state, written in the magic basis is maximally entangled iff its coefficients are real, except for a global phase.

(ii) $C(|\Psi\rangle) = 0$ iff $|\Psi\rangle$ is a product state iff $\sum_k \mu_k^2 = 0$.

These two properties imply that if $|\Phi\rangle$ and $|\Phi^\perp\rangle$ are real in the magic basis (and therefore they are maximally entangled) then the state $(|\Phi\rangle \pm i|\Phi^\perp\rangle)/\sqrt{2}$ is a product state.

Let us also review some properties of the Entropy of Entanglement, E_E, the Schmidt number, E_S, the entanglement monotones E_n, and the Rènyi entanglement, E_R, for arbitrary states of two m–level systems:

(1) A maximally entangled state, $|\Psi\rangle$ of two $m-$level systems has m Schmidt coefficients, which are all $1/\sqrt{m}$. Thus $E_E(|\Psi\rangle) = \log_2(m)$, $E_S(|\Psi\rangle) = m-1$, $E_n(|\Psi\rangle) = (m-n)/m$, $(n = 1, \ldots, m-1)$ and $E_R(|\Psi\rangle) = 1-1/m$.

(2) A product state can be written as $|\Psi\rangle = |\phi\rangle_A |\psi\rangle_B$, thus it has only one Schmidt coefficient, which is equal to 1. And so $E_E(|\Psi\rangle) = E_S(|\Psi\rangle) = E_n(|\Psi\rangle) = E_R(|\Psi\rangle) = 0$ $(n = 1, \ldots, m-1)$.

1.2 Mixed states

It is impossible to create, maintain, or manipulate pure entangled states under laboratory conditions, since any system is subjected to the effects of external noise and interactions with the environment. These effects turn pure states into mixed states. And so the *pure state entanglement* is transformed into *mixed state*, or *noisy entanglement*. Since most of the applications in Quantum Information are based on entanglement, [49, 10, 6, 50, 136, 4, 116] one is especially interested in characterizing quantum states according to their nonlocal properties. In particular one wants to know whether and how a given state can be produced or manipulated using only local operations and classical communication (LOCC). And so, the main questions of interest are

- *Is a given mixed state entangled, i.e is it impossible to create it using LOCC, or is it separable and can be produced locally?* Finding an answer to this question is the well known *separability problem.*
- *Can a given mixed state be used for purposes such as quantum teleportation, quantum communication, etc., where pure maximally entangled states are required?* In other words, is it possible to transform using LOCC (in the asymptotic limit) N copies of the state into a maximally entangled state? This problem is known as the *distillation problem.* There is another, very similar problem, which is called the *activation problem.* There the parties share some additional "very weak" entangled state, which they might use to distill entanglement.

The aim of this section is to give the mathematical definitions of all these problems and to review some known results concerning them.

1.2.1 The separability problem

The separability problem is the characterization of mixed entangled states. It is a highly nontrivial problem and has not been accomplished so far. In

fact, the apparently innocent question: *Is a given state entangled and does it contain quantum correlations, or is it separable, and does not contain any quantum correlations?* will, in general, be very hard (if not impossible!) to answer. In this section we summarize some known results concerning the problem of separability. In particular we will introduce a method for solving this problem. It is based on positive maps and so–called entanglement witnesses. Later, in Sec. 7.1.2, we will show how these entanglement witnesses and the corresponding positive maps can be optimized. Let us now consider the bipartite case and then generalize the problem as well as the methods to solve it to multipartite systems.

Bipartite case

Mathematically, bipartite mixed state entanglement can be described as follows. A density operator $\rho \geq 0$ acting on a finite Hilbert space $H = H_A \otimes H_B$ describing the state of two quantum systems A and B is called separable [151] (or not entangled) if it can be written as a convex combination of product vectors; that is, in the form

$$\rho = \sum_k p_k |e_k, f_k\rangle\langle e_k, f_k|, \tag{1.13}$$

where $p_k \geq 0$, and $|e_k, f_k\rangle \equiv |e_k\rangle_A \otimes |f_k\rangle_B$ are product vectors. Conversely, ρ is nonseparable (or entangled) if it cannot be written in this form. Physically, a state described by a separable (nonseparable) density operator ρ can always (never) be prepared locally.

For low dimensional systems [118, 71] there exist operationally simple necessary and sufficient conditions for separability. In fact, in $H = \mathbb{C}^2 \otimes \mathbb{C}^2$ and $H = \mathbb{C}^2 \otimes \mathbb{C}^3$ the Peres–Horodecki criterion [118, 71] establishes that ρ is separable iff its *partial transpose* is positive[1]. Where the partial transpose of an operator O with respect to system A; in an orthonormal basis $\{|k\rangle\}_{k=1}^N \in H_A$, is defined as

$$O^{T_A} = \sum_{k,k'=1}^{N} \langle k|O|k'\rangle_A |k'\rangle_A\langle k|. \tag{1.14}$$

One can analogously define the partial transpose of O with respect to B in a given basis, O^{T_B}. Partial transposition fulfills the following useful property

$$\mathrm{tr}_X(O^{T_X} Y) = \mathrm{tr}_X(O Y^{T_X}), \tag{1.15}$$

[1]Note that in the case of two qubits, it was even possible to derive a closed expression for the entanglement of formation, that is the entanglement which is needed to create the state [155].

for any subsystem X. We say that a positive operator has a positive partial transposition (PPT) if $\rho^{T_A} \geq 0$. Note that this property is basis independent, and that $\rho^{T_A} \geq 0$ iff $\rho^{T_B} \geq 0$[2].

It can be easily seen that all separable operators (independent of the dimension of the Hilbert space) have a positive[3] partial transpose. In other words, a states whose partial transpose is non–positive semidefinite (in the following a NPPT state) is always entangled. The converse is, however, not true in general. That is, there are positive partial transpose operators which are nonseparable (PPTES) [75, 11, 29]. Thus, the separability problem reduces to finding whether density operators with positive partial transpose are separable or not.

Several necessary conditions for separability, of density operators acting on a finite dimensional Hilbert space, have been formulated in the recent years. Werner [151] formulated a criterion based on the analysis of a local hidden variable model and on the positivity of the mean value of the flipping operator. The Horodeckis [83] obtained a criterium in the form of inequalities for the so called α-entropies. in Ref. [71] they also established the connection between separability and the theory of positive maps [138, 157]. A necessary and sufficient condition for separability has been expressed in terms of these maps, as we will see below. Later on [75, 70], a sufficient criterion for a state to be PPT entangled was given. It is the so–called *range criterion* [75]:

Lemma 1.1 *[75] (Range Criterion) If a bipartite state ρ is separable then there exists a set $\{|e_i, f_i\rangle\}$ such that span $\{|e_i, f_i\rangle\} = R(\rho)$ and span $\{|e_i^*, f_i\rangle\} = R(\rho^{T_A})$*[4].

This criterion gave rise to the first examples of PPTES. After that, a systematic method of constructing entangled states with positive partial transpose, based on the existence of unextendible basis of product vectors was formulated [11, 29, 140, 9, 82].

In Sec. 7.1.1 we use this criterion to derive computable necessary and sufficient conditions for separability for density operators supported on $\mathbb{C}^2 \otimes \mathbb{C}^N$, which have low rank [95]. The idea is to subtract from a PPT state, ρ, projectors onto product vectors [108, 105] in such a way that the resulting state and its partial transpose remain positive semi–definite. If after several steps the remainder, δ, vanishes then one has obtained a decomposition (namely the convex combination of the states which were subtracted) into product

[2]Note that partial transposition depends on the used basis, but the eigenvalues do not.
[3]In the following we will sometimes call a positive semidefinite operator simply positive.
[4]$R(X)$ denotes the range of the operator X acting on $\mathcal{H}$, i.e. $R(X) = \{|\Phi\rangle \in \mathcal{H} : \exists\, |\Psi\rangle \in \mathcal{H}$ such that $X|\Psi\rangle = |\Phi\rangle\}$.

vectors of the state, ρ (1.13). In this case one has proven that the state is separable. If one does not end up with zero, one obtains a state which has the property that for all product vectors $|e,f\rangle$ and $\epsilon > 0$, $\delta - \epsilon|e,f\rangle\langle e,f|$ is not positive or does not have a positive partial transpose. Using Lemma 1.1 it can be shown that[5] this state is entangled. This states lie on the boundary between the PPTE and NPPT states. We call them "edge" states. In order to characterize those states we use the following criterion [75, 95]:

Criterion: A PPTE state δ is an "edge" state iff there exists no $|e,f\rangle \in R(\delta)$ s.t. $|e^*,f\rangle \in R(\delta^{T_A})$[5].

Note that the edge states violate the range criterion of separability (Lemma 1.1) in an extreme manner [75, 95]. They are of special importance since they are responsible for the entanglement contained in PPTES's. As explained above we have:

Proposition 1.1 *Every PPTES ρ is a convex combination*

$$\rho = (1-p)\rho_{sep} + p\delta, \tag{1.16}$$

of some separable state, ρ_{sep}, and an edge state, δ.

Note that in the decomposition (1.16) the weight p can be chosen to be minimal [i. e. there exists no decomposition of type (1.16) with a smaller p (see Appendix E.1 and [106])]. This decomposition will become important when we study the separability properties of PPT states (Sec. 7.1). In particular, it provides us with a simple method to construct edge states in arbitrary dimensions, and a separability check (see [95] and Sec. 7.1).

Multipartite case

A density operator ρ describing the state of $N > 2$ particles, $A, \ldots, Z$ can contain many kinds of entanglement, due to the different possibilities for the particles to be entangled to each other. In Ref. [39] a classification of mixed multipartite states according to their separability properties has been given. The idea is to group the N particles into $m \leq N$ subsets. Each of the m subsets is considered as a single particle. The separability properties of those m–partite states define the different classes. Let us, as an example consider the simplest case of three qubits. We need to distinguish the following five classes[6] [39]:

[5] See Sec. 7.1.1 for further explanation

[6] As mentioned already, we denote by $|\phi\rangle_X$ an unnormalized state corresponding to the Hilbert space $\mathcal{H}_X$, for any subset of particles, X. If the system to which the state belongs to is clear, we omit the subscript.

- *Fully inseparable states* are not separable with respect to any bipartite splitting. An example would be the GHZ–state, $1/\sqrt{2}(|000\rangle + |111\rangle)$.

- *1–qubit biseparable states* are separable with respect to one bipartite splitting, but inseparable with respect to the other two. For instance a state which can be written as $\rho = \sum_i |a_i\rangle_A \langle a_i| \otimes |\phi_i\rangle_{BC} \langle \phi_i|$, but is not separable with respect to the other, $B - AC$ and $C - AB$, splittings. An example would be $|0\rangle_A |\Phi^+\rangle_{BC}$, where $|\Phi^+\rangle$ is one of the Bell–states (1.3).

- *2–qubit biseparable states* are separable with respect to two bipartite splittings but non–separable with respect to the third splitting[7].

- *3–qubit biseparable states* are separable with respect to all bipartite splittings but cannot be written as a convex combination of product states of the form $|a\rangle_A |b\rangle_B |c\rangle_C$[7].

- *Fully separable states* are states which can be written as $\rho = \sum_i |a_i\rangle_A \langle a_i| \otimes |b_i\rangle_B \langle b_i| \otimes |c_i\rangle_C \langle c_i|$. An example would be $|000\rangle$.

In Sec. 7.2.2 we apply this characterization to three–mode Gaussian states and present an operational criterion to decide to which class a state belongs to. In the finite dimensional case however, this problem is still open.

Throughout this Thesis we call fully separable a state which is separable with respect to any grouping or, equivalently, for $m = N$. Note that this state can be prepared, using only LOCC, out of a product state, e.g. $|0,\ldots,0\rangle$, i.e it can be written as

$$\rho = \sum_i |a_i\rangle_A \langle a_i| \otimes \ldots \otimes |z_i\rangle_Z \langle z_i| , \tag{1.17}$$

where $|x_i\rangle_X$ belongs to the Hilbert space of particle X. States which are separable with respect to a bipartite splitting are called biseparable. We call a state, ρ, Y–PPT if its partial transpose with respect to system Y is a positive semidefinite operator. Otherwise we call it Y–NPPT. If a state has a positive (non–positive) semidefinite partial transpose with respect to all systems then we call it simply PPT (NPPT). If we consider, for instance, only two systems, we have $\rho^{T_B} = (\rho^{T_A})^T$ and therefore ρ is A-NPPT iff it is B-NPPT; we call such a state NPPT.

[7] For an example see [39]

Entanglement witnesses and positive maps

Entanglement witnesses (EWs) are observables which allow us to distinguish between entangled and separable states. Due to an isomorphism [84] between linear operators and linear maps, one can construct to any EW the corresponding positive map (PM) and vice versa. The PM is also capable to detect entangled states, as we will see [71].

Entanglement witnesses for bipartite systems

We call an operator $W = W^\dagger$ acting on $H = H_A \otimes H_B$ an EW if [71, 140, 139]:

(I) $\langle e, f|W|e, f\rangle \geq 0$ for all product vectors $|e, f\rangle$;

(II) has at least one negative eigenvalue (i.e. is not positive);

(III) $\mathrm{tr}(W) = 1$.

The first property (I) implies that $\mathrm{tr}(W\rho) \geq 0$ for all ρ separable. Thus, any $\rho \geq 0$, for which $\mathrm{tr}(W\rho) < 0$ is nonseparable. In that case we say that W *detects* ρ. Property (II) implies that every EW detects something. In particular it detects the projector on the subspace corresponding to the negative eigenvalues of W. The third property (III) is just a normalization condition. We will need it in Sec. 7.1.2 in order to compare the action of different EWs [8].

The importance of EWs is due to the following theorem [71]:

[8] This normalization condition expresses the fact that if W fulfills (I–II), and λ is a positive number, then λW also fulfills (I–II), so that we can always normalize W to have (III). Given an operator satisfying (I) and (II) we can always define $W' = W/\mathrm{tr}(W)$, so that it fulfills both properties as well and detects the same operators as W. This follows from the fact that $\mathrm{tr}(W)$ must be strictly positive since if we take the trace in an orthonormal basis of product vectors, using (I) we have that $\mathrm{tr}(W) \geq 0$. If $\mathrm{tr}(W) = 0$ then we would have that $\langle e, f|W|e, f\rangle = 0$ for all product vectors; since we can always construct a complete set of operators $\{|e_i, f_i\rangle\langle e_i, f_i|\}$ out of product vectors in the space of the operators acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, this immediately implies that $W = 0$, which contradicts (II). This set of operators can be constructed as follows. Let us consider a Hilbert space $\mathcal{H}_A$ of dimension d_a and an orthonormal basis $\{|k\rangle\}_{k=1}^{d_a}$. We define the states $|\Psi^r_{k,k'}\rangle = (|k\rangle + |k'\rangle)/\sqrt{2}$ and $|\Psi^i_{k,k'}\rangle = (|k\rangle + i|k'\rangle)/\sqrt{2}$ for $k < k'$ and the projectors on these states $A_k = |k\rangle\langle k|$, $A^r_{k,k'} = |\Psi^r_{k,k'}\rangle\langle\Psi^r_{k,k'}|$, and $A^i_{k,k'} = |\Psi^i_{k,k'}\rangle\langle\Psi^i_{k,k'}|$. The set $S_A = \{A_k, A^r_{k,k'}, A^i_{k,k'}, k = 1, \ldots, d_a, k' = k+1, \ldots, d_a\}$ is complete in the space of operators acting on $\mathcal{H}_A$. This can be easily shown by noting that $|k\rangle\langle k'| = A^r_{k,k'} + iA^i_{k,k'} - (1+i)(A_k + A_{k'})/2$ for $k \neq k'$. We can do the same construction for $\mathcal{H}_B$ and obtain a set S_B. The set composed of tensor products of all elements of S_A with S_B is complete in the space of operators acting on $\mathcal{H}_A \otimes \mathcal{H}_B$.

Theorem 1.1 *(Separability criterion) [71] A state $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is entangled iff there exists an EW, W such that*

$$\mathrm{tr}(\rho W) < 0, \tag{1.18}$$

i.e. iff there exists an EW which detects it.

Let us here present the proof of this theorem, since it gives an insight into the problems of separability and entanglement witnesses.

Proof: We define A as the real space generated by hermitian operators in $\mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$. The set of separable states is convex and closed in A. On the other hand, the set including only the point ρ is convex, closed and compact. Thus, there exists a real functional f on A and a real number α such that $f(\rho) < \alpha \leq f(\tilde{\rho})\ \forall \tilde{\rho}$ separable (Hahn–Banach Theorem [121]). As A is a real Hilbert space the real functional f can be represented as $f(\rho) = tr(\rho W)$, where $W \in A$. We define $\tilde{W} = W - \alpha\mathbb{1}$. Then we have $f(\rho) = tr(\rho W) = tr(\rho\tilde{W}) + \alpha$. Using the inequality above we have: $tr(\rho\tilde{W}) + \alpha < \alpha$ and therefore $tr(\rho\tilde{W}) < 0$. Whereas $\alpha \leq f(\tilde{\rho}) = tr(\tilde{\rho}\tilde{W}) + \alpha$ and therefore $tr(\tilde{\rho}\tilde{W}) \geq 0\ \forall\tilde{\rho}$ separable. ■

Depending on the states which are detected by the EW one distinguishes between decomposable and non–decomposable EWs.

A EW is called decomposable if it can be written as

$$W = P + Q^{T_A}, \tag{1.19}$$

where P and Q are positive semidefinite operators. Note that, first of all the class of decomposable EW is very simple to characterize and second that a decomposable EW is only able to detect the entanglement of a NPPT state. The reason for this is simply, $\mathrm{tr}(\rho W) = \mathrm{tr}(\rho P) + \mathrm{tr}(\rho^{T_A} Q)$[9], which is for any PPT state a sum of positive numbers and therefore positive. Thus, decomposable EWs do not allow us to distinguish between separable and PPTE states. For this purpose we need non–decomposable EWs, that is EWs which cannot be written as in Eq. (1.19). In Sec. 7.1.2 we will show that an EW is non–decomposable iff it detects a PPTES.

Entanglement witnesses for multipartite systems

We call an operator, $W = W^\dagger$, acting on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \ldots \mathcal{H}_Z$ a N–partite EW (EW between the N parties) if the following properties are fulfilled

[9] We used property (1.15) of the partial transposition.

(i) $\langle a,\ldots,z|\, W\,|a,\ldots,z\rangle \geq 0 \quad \forall\, |a\rangle \in \mathcal{H}_A,\ldots,|z\rangle \in \mathcal{H}_Z$

(ii) W is not positive, i.e. W has at least one negative eigenvalue

(iii) $\mathrm{tr}(W) = 1$.

It can be easily seen that condition (i) ensures that $\mathrm{tr}(W\rho) \geq 0$ for any ρ fully separable (1.17). Thus, if for some density operator, ρ, and an EW[10], W, $\mathrm{tr}(W\rho) < 0$ then ρ must be (in one or another way) entangled. Note that if we are not interested in comparing EWs, we might call an hermitian operator an EW if it fulfills the properties (i) and (ii).

Analogously to the bipartite case (1.19) we define the decomposable EW (DEW), as the ones which can be written as

$$W = O_0 + O_1^{T_A} + \ldots O_N^{T_Z}, \tag{1.20}$$

where the operators O_i are positive semidefinite[11]. Again, it can be easily verified that those entanglement witnesses cannot detect any PPTES. On the other hand, non–decomposable EW (NDEW) cannot be written as (1.20).

Positive maps

Since there exists an isomorphism between EW and positive maps [84], the necessary and sufficient condition (Theorem 1.1) can also be states in terms of PMs. It turns out that PMs are even more powerful than EWs, in the sense that all the states detected by an EW are also detected by the corresponding PM.

Let us, first of all, review some of the definitions and properties of linear maps. We consider a linear, hermitian[12] map $\mathcal{E} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_C)$. We say that $\mathcal{E}$ is positive if for all $Y \in \mathcal{B}(\mathcal{H}_A)$ positive, $\mathcal{E}(Y) \geq 0$. Let us here also introduce the extensions of linear maps. Given $\mathcal{E} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_C)$, we define its extension $\mathcal{E}\otimes\mathbb{1}_B : \mathcal{B}(\mathcal{H}_A)\otimes\mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_C)\otimes\mathcal{B}(\mathcal{H}_B)$ according to $\mathcal{E}\otimes\mathbb{1}_B(\sum_i Y_i\otimes Z_i) = \sum_i \mathcal{E}(Y_i)\otimes Z_i$, where $Y_i \in \mathcal{B}(\mathcal{H}_A)$ and $Z_i \in \mathcal{B}(\mathcal{H}_B)$. A linear map is completely positive if all extensions are positive. The classification and characterization of positive (but not completely positive) maps is an open question (see, e.g. Ref. [157, 22] and Sec. 7.1.2).

[10] Whenever it is obvious from the context that we consider a N–partite EW, W, we might simply call it an EW.

[11] Consider, for instance, a bipartite DEW, W. It can be written as (1.20) $W = Q_0 + Q_1^{T_A} + Q_2^{T_B} = Q_0 + (Q_1 + Q_2^T)^{T_A} = Q_0 + \tilde{Q}_1^{T_A}$, with $\tilde{Q}_1 = Q_1 + Q_2^T, Q_0, Q_1, Q_2 \geq 0$, where we used that $Q_2^{T_B} = (Q_2^T)^{T_A}$.

[12] A map, $\mathcal{E}$ is called hermitian if $\mathcal{E}(A^\dagger) = [\mathcal{E}(A)]^\dagger$ for any $A \in \mathcal{B}(\mathcal{H})$.

An example of a positive (but not completely positive) map is transposition (in a given basis); that is, the map $\mathcal{E}_T$ such that $\mathcal{E}_T(Y) = Y^T$. The corresponding extension is the partial transposition (1.14). A map $\mathcal{E}$ is called decomposable if it can be written as $\mathcal{E} = \mathcal{E}_1 + \mathcal{E}_2\cdot\mathcal{E}_T$, where $\mathcal{E}_{1,2}$ are completely positive. If it cannot be written in this form, it is called non–decomposable.

One can relate linear maps with linear operators in the following way [84]. We will assume $d_A \equiv \dim(\mathcal{H}_A) \leq \dim(\mathcal{H}_C)$, but one can otherwise exchange $\mathcal{H}_A$ by $\mathcal{H}_C$ in what follows. Given $X \in \mathcal{B}(\mathcal{H}_A\otimes\mathcal{H}_C)$ and an orthonormal basis $O_A = \{|k\rangle\}_{k=1}^{d_A}$ in $\mathcal{H}_A$, we define the linear map $\mathcal{E}_X : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_C)$ according to

$$\mathcal{E}_X(Y) = \mathrm{tr}_A(X^{T_A}Y), \tag{1.21}$$

for all $Y \in \mathcal{B}(\mathcal{H}_A)$, where tr_A denotes the trace in $\mathcal{H}_A$ and the partial transpose is taken in the basis O_A. Similarly, given a linear map we can always find an operator X such that (1.21) is fulfilled, namely $X \propto \mathcal{E}_X\otimes\mathbb{1}_C(|\Psi\rangle\langle\Psi|)$, where

$$|\Psi\rangle = \sum_{k=1}^{d_A} |k\rangle_A \otimes |k\rangle_C. \tag{1.22}$$

For instance, the map, $\mathcal{E}_T$ (transposition in the basis O_A), corresponds to $T = (|\Psi\rangle\langle\Psi|)^{T_A}$, where the partial transposition is taken in the basis O_A.

Given a linear map $\mathcal{E}_X$, one can easily show the following relations:

(a) $\mathcal{E}_X$ is completely positive iff $X \geq 0$;

(b) $\mathcal{E}_X$ is positive but not completely positive iff X is an EW [except for the normalization condition (III)];

(c) $\mathcal{E}_X$ is decomposable iff X is decomposable.

Thus, the problem of studying and classifying PM is very much related to the one of EW. Furthermore, PM can be also used to detect entanglement [71]. Let us consider the extension $\bar{\mathcal{E}}_X \equiv \mathcal{E}_X \otimes 1 : \mathcal{B}(\mathcal{H}_A)\otimes\mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_C)\otimes\mathcal{B}(\mathcal{H}_B)$, where we take $d_B \equiv \dim(\mathcal{H}_B) = \dim(\mathcal{H}_C)$. Then we have that given $\rho \in \mathcal{B}(\mathcal{H}_A\otimes\mathcal{H}_B)$,

$$\mathrm{tr}(\rho X) = \langle\Psi|\bar{\mathcal{E}}_X(\rho)|\Psi\rangle, \tag{1.23}$$

where $|\Psi\rangle = \sum_{k=1}^{d_B} |k\rangle_C \otimes |k\rangle_B$. Thus, if an EW, W, detects ρ, then $\bar{\mathcal{E}}_W(\rho)$ is a non–positive operator. On the other hand, $\mathcal{E}_W(\rho_{sep}) = \sum_i p_i \mathcal{E}_W(|a_i\rangle\langle a_i|)\otimes|b_i\rangle\langle b_i| \geq 0$, for all $\rho_{sep} = \sum_i p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|$ separable. Consequently, $\rho \geq 0$ is entangled iff there exists a PM such that acting on ρ gives a non–positive operator. In that case we say that the PM "detects" ρ. It can be

easily seen that PMs are "more efficient" in detecting entanglement than EWs. The reason is that it may happen that $\bar{\mathcal{E}}_X(\rho)$ is non–positive but still $\mathrm{tr}(\rho X) \geq 0$. Analogously to EWs it is straightforward to generalize the notion of PMs to more than two systems.

1.2.2 The distillation and activation problems

A state shared between an arbitrary number of parties is called fully distillable if it is possible to transform via LOCC several copies of the state into a maximally entangled state shared between all the parties. The motivation of this definition is very clear. If two (or more) spatially separated parties share a maximally entangled state then they can use it for many quantum informational purposes, e.g. quantum communication [18, 49]. In realistic situation however, the parties will not share a pure entangled state, but rather a mixed state. The goal is then to use several copies of this state and transform them into a state which can then be used for the desired purpose. Thus, the operations which allow the parties to manipulate the state are restricted to local operations and classical communication.

A very related process is the one of *activation of entanglement*. There the parties are given some PPTES, in addition to the copies of their states. They can consume it in order to distill the entanglement included in their states.

Let us now state the problem mathematically. In the bipartite case, a state, $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, with $\dim(\mathcal{H}_X) = d_X$ for $X = A, B$, is called distillable if Alice and Bob can produce by LOCC a maximally entangled state

$$|\Phi_d\rangle = \sum_{k=1}^{d} |k,k\rangle\,, \tag{1.24}$$

with $d = \min(d_A, d_B)$.

It has been shown [70] that the problem of distillation of a state, ρ, can be formulated in the following way:

Lemma 1.2 *(Distillability) [70] A state, ρ, is distillable iff there exists a positive integer N and a state of the form*

$$|\Psi\rangle = |e_1, f_1\rangle + |e_2, f_2\rangle\,, \tag{1.25}$$

such that

$$\langle\Psi|\,(\rho^{\otimes N})^{T_A}\,|\Psi\rangle < 0, \tag{1.26}$$

where $\{e_1, e_2\}$ ($\{f_1, f_2\}$) are two (unnormalized) orthogonal vectors in $(\mathbb{C}^{d_A})^{\otimes N}$ [$(\mathbb{C}^{d_B})^{\otimes N}$].

This condition simply means that iff there exists a $\mathbb{C}^2 \otimes \mathbb{C}^2$ subspace, on which the projection of $\rho^{\otimes N}$ is NPPT, then the state is distillable. This can be understood as follows: if there exists such a subspace then Alice and Bob can distill a maximally entangled state in $\mathbb{C}^2 \otimes \mathbb{C}^2$ [72]. They can then use some of those distilled states to convert them, by LOCC, into a maximally entangled state in $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. On the other hand, a maximally entangled state in $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ can be converted into a maximally entangled state in $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Distillable states are called *free entangled* states in contrast to the *bound entangled* states, which cannot be transformed using LOCC (distilled) into a single pure entangled state of two qubits, even if two parties share an arbitrarily large supply of such states. Note that any PPTES is bound entangled. In the case of one qubit and a N–level system it was shown [72, 38] that all NPPT entangled states can be distilled into maximally entangled pure states by local operations. However, there exists a strong evidence that this is not true in general [38, 30]. That is, it seem that there exist NPPT states which cannot be distilled. Note that this would imply that the distillable entanglement [the quantity that measures how much entanglement can be distilled out of N copies (in the asymptotic limit)] is neither additive nor convex [131].

If a state is not distillable, then Alice and Bob might be still able to distill a maximally entangled state by LOCC, if they share, in addition to their copies of the state, a PPTES. The condition is then simply that several copies of ρ together with the PPTES are distillable.

The mathematical details as well as the generalization to more systems will be discussed in Chapter 8. There we will also show how the problem of distillation and activation can be related to the one of EWs (or, equivalent to PMs). This connection gives a new insight in the problem of distillation and activation.

1.3 Gaussian states

In quantum optics and in other scenarios described by continuous quantum variables, not all states on the infinite dimensional Hilbert space are equally accessible in current experiments. In fact, the set of *Gaussian states* comprises essentially all genuinely continuous variable (CV) states that can currently be prepared in the laboratories. This, and the mathematical simplicity of these states are the reasons why CV Quantum Information has so far considered almost exclusively Gaussian states. This section summarizes some results concerning those states.

We consider systems composed of n distinguishable infinite dimensional

subsystems, each with Hilbert space $\mathcal{H} = \mathrm{L}^2(\mathbb{R})$. These could be implemented quantum optically by different modes of the electromagnetic field, hence each of these subsystems will be referred to as a "mode". To each mode belong the two canonical observables $X_k, P_k, k = 1, \ldots, n$ with commutation relation $[X_k, P_k] = i$. Defining $R_{2k-1} = X_k, R_{2k} = P_k$, for $k = 1, 2, \ldots, n$, these relations are summarized as $[R_k, R_l] = -iJ_{kl}$, using the antisymmetric $2n \times 2n$ matrix

$$J_n \equiv \oplus_{k=1}^{n} J_1, \quad J_1 \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{1.27}$$

Whenever the dimension of the space on which J acts is clear, we will omit the index. As in Eq. (1.27) we will often use direct sum notation for matrices and vectors. That is, if $A \in M_{n,n}$ and $B \in M_{m,m}$, then $A \oplus B \in M_{n+m,n+m}$ is the $(n+m) \times (n+m)$ square matrix

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}. \tag{1.28}$$

Similarly, if $f_1 \in \mathbb{R}^n$ and $f_2 \in \mathbb{R}^m$ are two vectors, then $f_1 \oplus f_2 \in \mathbb{R}^{n+m}$ is a vector whose first n components are given by the entries of f_1 and the last m by those of f_2.

For continuous variable systems, it is convenient to describe the state ρ by its characteristic function

$$\chi_\rho(x) = \mathrm{tr}[\rho D(x)]. \tag{1.29}$$

Here $x = (q_1, p_1, \ldots q_n, p_n)$, with $q, p \in \mathbb{R}^n$ is a real vector, and

$$D(x) = e^{-i\sum_k (q_k X_k + p_k P_k)}, \tag{1.30}$$

is the displacement operator, also called Weyl operator. The characteristic function contains all the information about the state of the system, that is, one can construct ρ knowing χ [$\rho \propto \int \chi(x) D^\dagger(x) dx$]. Gaussian states are exactly those for which χ is a Gaussian function of the phase space coordinates x [112],

$$\chi_\rho(x) = e^{-\frac{1}{4} x^T \gamma x - i d^T x}, \tag{1.31}$$

where γ is a real, symmetric, strictly positive matrix, the *correlation matrix* (CM) , and $d \in \mathbb{R}^{2n}$ is a real vector, the *displacement*. A Gaussian state is completely determined by γ and d. Note that both, γ and d, are directly measurable quantities, their elements γ_{kl} and d_k are determined by the expectation values and variances of the operators R_k, via

$$d_k = \mathrm{tr}(\rho R_k), \tag{1.32}$$

and

$$\gamma_{kl} = 2\mathrm{Re}\{\mathrm{tr}[\rho(R_k - d_k)(R_l - d_l)]\}. \tag{1.33}$$

Note that the displacement of a (known) state can always be adjusted to $d = 0$ by a sequence of unitaries applied to individual modes, i.e. by local operations. This implies that d is irrelevant for the study of nonlocal properties and will be put to zero if not stated differently[13].

Not all real, symmetric, positive matrices γ correspond to the CM of a physical state. There are a number of equivalent ways to characterize physical CMs, which will all be useful in the following. We collect them in

Lemma 1.3 *(Correlation Matrices)*
For a real, symmetric $2n \times 2n$ matrix $\gamma > 0$ the following statements are equivalent:

$$\gamma \text{ is the CM of a physical state,} \tag{1.34a}$$

$$\gamma + J\gamma^{-1}J \geq 0, \tag{1.34b}$$

$$\gamma - iJ \geq 0, \tag{1.34c}$$

$$\gamma = S^T(D \oplus D)S, \tag{1.34d}$$

for S symplectic[14] and $D \geq \mathbb{1}$ diagonal.

Proof: (1.34*a*) $\Leftrightarrow$ (1.34*b*) see [112]; (1.34*a*) $\Leftrightarrow$ (1.34*c*) see [153]; (1.34*a*) $\Leftrightarrow$ (1.34*d*) see [53, Prop. 4.22].

Whenever we consider a bipartite splitting of the state (n modes at Alice's and m modes at Bob's side, which we call $n \times m$ case in the following) we might write the correlation matrix in the block form

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}. \tag{1.35}$$

Here A, B and C are $2n \times 2n$, $2m \times 2m$, and $2n \times 2m$ matrices, respectively. Note that A refers to the first system and B to second system. That is, when tracing for instance over the second system, the correlation matrix of the corresponding reduced density operator, ρ_A (1.1) is A. The matrix C describes the correlations between both systems and vanishes for pure product states.

[13] Note that analogously to the finite dimensional case, any measure of entanglement has to fulfill condition (a) in Sec. 1.1.2, which implies the statement.

[14] A linear transformation S on phase space is called *symplectic* if it preserves J, i.e. if $SJS^T = J$ holds (see Appendix A).

1.3.1 Pure states

A CM, $\gamma \in M_{2n,2n}(\mathbb{R})$ corresponds to a pure state iff $D = \mathbb{1}$ in Eq. (1.34d), i.e. iff $\det\gamma = 1$ (e.g. [112]). It is easy to see from (1.34d) that for pure states Ineq. (1.34b) becomes an equality and $\dim[\ker(\gamma - iJ)] = n$. It is clear from Eq. (1.34d) that for every CM γ there exists a pure CM γ_0 such that $\gamma_0 \leq \gamma$. This will allow us to restrict some proofs to pure CMs only. Note that for a pure $2n \times 2n$ CM γ it holds that $\mathrm{tr}\gamma \geq 2n$[15].

When considering pure two-mode states (1×1 case) only, we can always write their CM in the form [134]

$$\gamma = (S_1 \oplus S_2) \begin{pmatrix} \cosh(r)\mathbb{1} & \sinh(r)\sigma_z \\ \sinh(r)\sigma_z & \cosh(r)\mathbb{1} \end{pmatrix} (S_1^T \oplus S_2^T), \tag{1.37}$$

which we refer to as the *pure state standard form* of γ. Here, $S_{1,2}$ are local symplectic matrices, $r \geq 0$, and σ_z is the Pauli matrix defined in (1). The parameter r contains all information about the entanglement of the state, whereas S_1 and S_2 contain information about local squeezing. Given a CM γ in its block form (1.35), one can readily find its pure state standard form using the following procedure:

We have $S_k = O_k D_k O_k'$, where O, O' are rotations and $D_k = \mathrm{diag}(e^{r_k}, e^{-r_k})$ (Appendix A). The six matrices are determined as follows: $O_{1(2)}$ diagonalize $A(B)$. The rotations O_k' realize the singular value decomposition of $D_1^{-1} O_1^T C O_2 D_2^{-1}$. The two-mode squeezing parameter r is given by $\cosh r = \sqrt{\det(A)}$, while the squeezing parameters r_1, r_2 of S_k can be calculated by the trace of A and B, resp.: $\cosh 2r_1 = (\mathrm{tr}A)/(2\cosh r)$, $\cosh 2r_2 = (\mathrm{tr}B)/(2\cosh r)$.

An example of a pure state would be the two–mode squeezed state

$$|\Psi(r,\phi)\rangle = \frac{1}{\cosh(r/2)} \sum_{n=0}^{\infty} [\tanh(r/2) e^{2i\phi}]^n |n,n\rangle\,, \tag{1.38}$$

where $|n\rangle$ denote the Fock states here. Note that the decomposition presented in Eq. (1.38) is the Schmidt decomposition (1.1.1) of the state $|\Psi(r,\phi)\rangle$.

[15] This can be seen as follows. First note that if the statement is true for $n = 1$, then it is true for an arbitrary n, since the trace over n modes can be considered as n traces over one mode. Let us write the one–mode CM as

$$\gamma = \begin{pmatrix} a & c \\ c & b \end{pmatrix}, \tag{1.36}$$

where a, b, c are real, $a, b > 0$ and $ab \geq 1$. From $0 \leq (a-b)^2 = \mathrm{tr}(\gamma)^2 - 4ab$ follows the statement.

Since for $r \neq 0$ there exist more than two Schmidt coefficients the state $|\Psi(r,\phi)\rangle$ is for $r \neq 0$ entangled. Actually, for $r \to \infty$ we obtain that all the Schmidt coefficients of the state become equal, which implies that the state is maximally entangled. Note however, that $\lim_{r\to\infty} |\Psi(r,\phi)\rangle$, is an improper state, which means that it does no longer belong to the Hilbert space $L^2(\mathbb{R})$ ($\| \lim_{r\to\infty} |\Psi(r,\phi)\rangle \| = 0$). Using the definition (1.33) to determining for instance, the CM $\gamma(r)$ corresponding to $|\Psi(r,0)\rangle$ one finds that it is given by Eq. (1.37) with $S_1 = S_2 = \mathbb{1}$.

Measures of entanglement and squeezing

Let us first of all introduce some measures of entanglement and squeezing for pure bipartite states and then consider the problem for the more general case of mixed states. Recall that the CM γ contains all the information concerning the non–local properties (entanglement and squeezing) of the state.

Apart form the Entropy of Entanglement, i.e., the von Neumann entropy of the reduced state, as defined in (1.7), the *purity* of the reduced density matrix measures the entanglement. Note that it is in general no measure of entanglement, but for pure states, $|\Psi\rangle$ the purity

$$P(|\Psi\rangle) = \mathrm{tr}(\rho_{red}^2), \tag{1.39}$$

where ρ_{red} is the reduced density operator of either system A or B, decreases the more entangled $|\Psi\rangle$ is. Therefore we may use, e.g., the inverse square of the purity, i.e., $\mathcal{P}(|\Psi\rangle) = [\mathrm{tr}(\rho_{red}^2)]^{-2}$ to quantify how entangled a given pure state is.

In order to define the next measure of entanglement we have to introduce the notion of partial transposition for Gaussian states [133] . On phase space transposition corresponds to the transformation that changes the sign of all the p coordinates $(q_1, p_1, \ldots, q_n, p_n) \mapsto \Lambda(q_1, p_1, \ldots, q_n, p_n) = (q_1, -p_1, \ldots, q_n, -p_n)$ [133] and leaves the q's unchanged. For instance, the partial transpose in system A (one mode) transforms γ and d according to

$$(\gamma, d) \mapsto (\Lambda_A \gamma \Lambda_A, \Lambda_A d), \tag{1.40}$$

where

$$\Lambda_A = diag(1, -1) \oplus \mathbb{1}. \tag{1.41}$$

In the following Λ_X will denote the operator corresponding to the partial transposition of system X. Analog to the previous section, we call a state, corresponding to a CM γ, whose partial transpose is positive (non–positive), i.e. a state where $\Lambda_X \gamma \Lambda_X$ is a valid (not valid) CM (see Lemma 1.3) X–PPT (X–NPPT). A Gaussian states which is X–PPT (X–NPPT) with respect to

all (one) systems will be simply called PPT (NPPT). Note that we will also call the CM γ itself X–PPT or X–NPPT, respectively.

With that we can now introduce another measure of entanglement, the so–called *negativity* $\mathcal{N}$ [150]. It is defined as the absolute value of the sum of the negative eigenvalues of the partial transposed density operator, ρ^{T_A}. For Gaussian states this corresponds to the sum over all symplectic eigenvalues (Appendix A) of the CM corresponding to ρ^{T_A}, which are smaller than one[16]. The other interesting quantity that characterizes Gaussian states besides the entanglement is the *squeezing* inherent in the state, i.e., by how much the variance of some (passive-linearly transformed, i.e. transformed by a symplectic and orthogonal matrix) quadrature is reduced below the standard quantum limit. The reduced variance is given by the smallest eigenvalue $\lambda_{\min}(\gamma)$ of γ and we define the squeezing of a state with CM γ as the inverse of $\lambda_{\min}(\gamma)$

$$\mathcal{S}(\gamma) = \min\{\text{eig}(\gamma)\}^{-1} = [\lambda_{\min}(\gamma)]^{-1}. \tag{1.42}$$

In a situation like in Chapter 5 where only orthogonal operations are freely available, the squeezing of a state represents a valuable resource which can be used, e.g., for the creation of entanglement [154].

Let us now analyze the entanglement properties of a pure two–mode Gaussian state. As already mentioned after Eq. (1.37), the single parameter which characterizes the non-local properties of such a state is the two-mode squeezing parameter r. This automatically implies, similar to the two qubit case (Sec. 1.1.2) that any monotonic function of this parameter can be used to quantify the entanglement of pure two-mode Gaussian states and we are free to choose the most convenient one. Using the notation of Eq. (1.35) and Eq. (1.37) for a two–mode Gaussian state, γ we obtain for the reduced state $\gamma_A = A = \cosh(r) S_1 S_1^T$.

The von Neumann entropy is then given by $E(|\psi\rangle) = \cosh(r/2)^2 \log[\cosh(r/2)^2] - \sinh(r/2)^2 \log[\sinh(r/2)^2]$ [143].

The purity of the reduced state is given by $\det(A)$ as [130] $\mathcal{P}(|\Psi\rangle) \equiv E_p(\gamma) = \{\text{tr}[\rho_{\text{red}}(\gamma)^2]\}^{-2} = \det A = \cosh(r)^2$. As mentioned before, the determinant of a CM is one, iff the state is pure, which implies that $E_p(\gamma) = 1$ iff the state is not entangled, i.e., iff $r = 0$.

The negativity for a 1×1 Gaussian state (not necessarily pure!) with CM γ is given by the inverse of the smallest symplectic eigenvalue (Appendix A) of the partially transposed CM $\tilde{\gamma} = \Lambda_A \gamma \Lambda_A$, which can easily be calculated

[16] From Lemma 1.3 it can be seen that the symplectic eigenvalues of the CM corresponding to ρ^{T_A} which are smaller than one correspond to the negative eigenvalues of ρ^{T_A}.

[150] as

$$\mathcal{N}(\gamma) = \left[\min\{\text{sing.val.}\left(J_2^T \tilde{\gamma} J_2 \tilde{\gamma}\right)\}\right]^{-1/2}, \tag{1.43}$$

where $J_2 = J \oplus J$ is the symplectic matrix for two modes.

It was also shown in Ref. [154], that the negativity of a two-mode CM γ is bounded by $1/\sqrt{\lambda_1 \lambda_2}$, where λ_1, λ_2 are the two smallest eigenvalues of the γ.

The eigenvalues of the CM, $\gamma(r)$ corresponding to the two–mode squeezed state, $|\Psi(r,0)\rangle$ given in (1.38) are $\{e^r, e^{-r}\}$. Thus, the squeezing (1.42) of this state is $\mathcal{S}[\gamma(r)] = e^r$.

1.3.2 Mixed states

Analogously to the finite dimensional case, the question of separability is very easy to answer for pure states, as we have seen. It gets much more involved in the case of mixed states. We introduce in this section some known results concerning the problem of separability for Gaussian states.

Note that in contrast to the case of finite dimensional Hilbert spaces, the distillation problem for a general bipartite Gaussian state is solved. It was shown in Ref. [56] that a bipartite Gaussian state is distillable iff its partial transpose is no longer positive semidefinite, i.e the state is NPPT[17].

In Ref. [48, 52, 59] the problem of manipulation of Gaussian states has been studied. In particular, in Ref. [59, 52] the most general operations transforming Gaussian states to Gaussian states were studied. These operations are called Gaussian operations [59]. In Ref. [59] Giedke and Cirac proved that it is not possible to distill Gaussian states using Gaussian operations (see also [48]). This is a drawback for the experiments since commonly used linear optic devices (beam splitters, phase shifter and squeezer, *etc.*) belong to the class of Gaussian operations and can therefore not be used to distill the entanglement of Gaussian states.

The separability problem

A very important transformation for the study of entanglement is, as for states in finite dimensional Hilbert spaces, partial transposition [118, 71] (1.40). As explained in Sec. 1.2.1, transposition is an example of a positive but not completely positive map and therefore may reveal entanglement

[17] Recall that in the bipartite finite dimensional case this is only a necessary condition for a state to be distillable. There it is expected that there exist NPPT undistillable states [38, 30].

when applied to a part of an entangled system. Using the definition of partial transposition (1.40), the NPPT-criterion for inseparability [118, 71] (see Sec. 1.2.1) translates very nicely to Gaussian states:

Theorem 1.2 *(NPPT criterion)*
Let γ be the CM of a $1 \times n$ system, then γ corresponds to a inseparable state if and only if $\Lambda_A \gamma \Lambda_A$ is not a physical CM, i.e. if and only if

$$\Lambda_A \gamma \Lambda_A \not\geq iJ, \tag{1.44}$$

where $\Lambda_A = \Lambda \oplus \mathbb{1}$ is the partial transposition in A's system (1.41).

As mentioned already, we call the CM γ "NPPT" if (1.44) holds.

Proof: See [133] for $N = 1$ and [153] for the general case.

For states of at least two modes at both sides condition (1.44) is still sufficient for inseparability, but no longer necessary as shown by Werner and Wolf, who have considered a family of 2×2 entangled states with positive partial transpose [153]. In the same paper, it was shown that

Theorem 1.3 *(Separability of Gaussian States)*
A state with CM γ is separable iff there exist CMs γ_A, γ_B such that

$$\gamma \geq \gamma_A \oplus \gamma_B. \tag{1.45}$$

It is observed in Ref. [153] that if Ineq. (1.45) can be fulfilled, then the state with CM γ can be obtained by local operations and classical communication from the product state with CM $\gamma_p = \gamma_A \oplus \gamma_B$, namely by mixing the states (γ_p, d) with the d's distributed according to the Gaussian distribution $\propto \exp\left[-d^T(\gamma - \gamma_p)^{-1} d\right]$.

Note that while Theorem 1.3 gives a necessary and sufficient condition for separability, it is not a practical criterion, since to use it, we have to prove the existence or non-existence of CMs γ_A, γ_B. Instead, a criterion would allow to directly calculate from γ whether the corresponding state is separable or not (see Sec. 7.2.1 and Sec. 7.2.2). Theorem 1.3 and its extension to the 3-party situation are the starting point for the derivation of such a criterion for the general bipartite case (Sec. 7.2.1) and for the case of three-partite three-mode states $(1 \times 1 \times 1)$ (Sec. 7.2.2).

Chapter 2

Quantum operations

We analyze physical implementable operations acting on a finite as well as infinite dimensional Hilbert space. For the finite dimensional case we consider the most general physical operations. In the case of operators transforming density operators corresponding to a Gaussian state, we focus our attention to Gaussian unitary operators.

2.1 Completely positive maps

Any physical action can be mathematically described by a completely positive map (CPM). Recall that, a linear, hermitian map $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ is completely positive if the following is fulfilled (Sec. 1.2.1):

(i) $\mathcal{E}(\rho) \geq 0$ for all $\rho \geq 0$, i.e. $\mathcal{E}$ is a positive map (Sec. 1.2.1) and

(ii) the extension $\mathcal{E} \otimes \mathbb{1}_n : \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\bar{\mathcal{H}}) \to \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\bar{\mathcal{H}})$ is positive for all n, where the action of $\mathcal{E} \otimes \mathbb{1}_n$ on the state $\tilde{\rho} = \sum_k \rho_k \otimes \sigma_k$, with $\rho_k \in \mathcal{B}(\mathcal{H})$ and $\sigma_k \in \mathcal{B}(\bar{\mathcal{H}})$ is defined as $(\mathcal{E} \otimes \mathbb{1}_n)(\tilde{\rho}) = \sum_k \mathcal{E}(\rho_k) \otimes \sigma_k$.

In other words, a map is completely positive if all extensions $\bar{\mathcal{E}} = \mathcal{E} \otimes \mathbb{1}_n$ are positive. Condition (i) (positivity) simply means that whenever one acts with a physical operation on a physical state then the outcome must be physical (up to a proportionality constant). In particular the outcoming state must be a positive semi–definite operator. If one entangles the system with some other system and applies then a physical operation to only one of the subsystems then the outcome must again be physical [condition (ii)].

Note that any CPM can be written as

$$\mathcal{E}(\rho) = \sum_k O_k \rho O_k^\dagger, \tag{2.1}$$

where O_k are operators acting on $\mathcal{H}$. Note that maps which do not preserve the trace, i.e $\mathrm{tr}[\mathcal{E}(\rho)]$ is not necessarily one $\forall\rho$ with $\mathrm{tr}(\rho)=1$, correspond to physical actions which occur with certain probability.

Let $\mathcal{H}$ now be a composite Hilbert space of system A and B. We define separable CPMs similarly to the definition of separable density operators (1.17). That is, $\mathcal{E}$ is separable [120] if its action can be expressed in the form

$$\mathcal{E}(\rho)=\sum_{k=1}^{l}(O_k^A\otimes O_k^B)\rho(O_k^A\otimes O_k^B)^\dagger, \tag{2.2}$$

for some integer l and where O_k^A and O_k^B are operators acting on $\mathcal{H}_{A,B}$, respectively. Otherwise, we say that it is non–separable. Up to a proportionality constant, separable maps are those that can be implemented using local operations and classical communication only[1], i.e. useless for several tasks in Quantum Information.

It is straight forward to generalize the notion of CPMs to multipartite systems ($\mathcal{H}=\mathcal{H}_A\otimes\mathcal{H}_B\otimes\ldots\otimes\mathcal{H}_Z$). A CPM is then called *fully separable* if it can be, up to a proportionality constant, implemented locally, i.e. if it can be written as:

$$\mathcal{E}(\rho)=\sum_{k=1}^{l}(O_k^A\otimes O_k^B\ldots O_k^Z)\rho(O_k^A\otimes O_k^B\ldots O_k^Z)^\dagger, \tag{2.3}$$

where l is some finite number.

Note that these definitions allow us to reformulate the separability criterion [ρ is fully separable if it can be written as a convex combination of product sates (1.17)] as follows. A state, ρ, is fully separable iff there exists a fully separable map $\mathcal{E}$ such that $\rho\propto\mathcal{E}(|00\ldots0\rangle\langle00\ldots0|)$. In the following we will call a fully separable CPM simply separable if not stated otherwise.

2.2 Gaussian operators

As already mentioned, Gaussian operations are physical operations which transform Gaussian states to Gaussian states. in Ref. [59] Giedke and Cirac showed that the Gaussian operations are exactly those which can be performed on Gaussian states using linear optical elements (beam splitter, squeezer, *etc.*) and homodyne measurements. In that paper it is also shown how to characterize CPMs according to their entanglement properties using positive semidefinite operators. This can be viewed as a generalization of the characterization introduced in Ref. [23] (see Sec. 4.1.2) to operators acting on infinite dimensional Hilbert spaces. Note that this formalism enabled the authors to prove that it is not possible to distill Gaussian states using Gaussian operations. We will not introduce here the most general Gaussian operations, described by CPMs, but rather consider only the simplest case of Gaussian unitary operators.

[1]Note that this does not contradict the statement given in Ref. [9], in which it is shown that there are certain trace preserving separable completely positive maps that cannot be implemented locally with probability one.

2.2.1 Symplectic transformation

Let us first of all show how the CM, γ, and the displacement, d, corresponding to a Gaussian state, ρ, change under the evolution of a unitary operator, U. Using the definitions introduced in Sec. 1.3, we obtain for the characteristic function (1.29) of $U\rho U^\dagger$,

$$\chi_{U\rho U^\dagger}(x)=\mathrm{tr}[\rho U^\dagger D(x)U]=\mathrm{tr}(\rho e^{-i\vec{x}^T U^\dagger\vec{R}U}). \tag{2.4}$$

If there exists some matrix $S(t)$ such that $\vec{R}(t)=U^\dagger\vec{R(0)}U=S(t)\vec{R(0)}$, then the state remains a Gaussian state, since Eq. (2.4) reads in this case as

$$\mathrm{tr}[\rho e^{-i\vec{x}^T S(t)\vec{R(0)}}]=\mathrm{tr}[\rho e^{-i(S(t)^T\vec{x})^T\vec{R(0)}}]=\chi_\rho[S(t)^T\vec{x}]. \tag{2.5}$$

Thus the correlation matrix and the displacement transforms according to[2]

$$\gamma(t)=S(t)\gamma S(t)^T \tag{2.6}$$
$$d(t)=S(t)d. \tag{2.7}$$

Note that the commutation relations $[R(t)_k,R(t)_l]=[UR(0)_kU^\dagger,UR(0)_lU^\dagger]=-iJ_{kl}$ imply that $-iJ_{k,l}=[(S(t)R)_k,(S(t)R)_l]=\sum_{m,n}S_{k,m}S_{l,n}[R_m,R_n]$ which is fulfilled iff $SJS^T=J$, i.e. iff S is symplectic. The most general Gaussian unitary operator can be written as $U=e^{iG}$, where G is an hermitian operator which is quadratic in the operators X_k,P_k.

Let us, as an example, consider the time evolution corresponding to a two–mode quadratic Hamiltonian of the form

$$H=aX_1X_2+bP_1P_2+dX_1P_2+cP_1X_2. \tag{2.8}$$

[2]One could also use the Heisenberg equation, i.e. $dA/dt=i[H,A]$ for the mode operators (X_k,P_k) to obtain this result.

We are going to study this kind of interaction in Chapter 5. Let us use the notation

$$H = (X_1, P_1) K \begin{pmatrix} X_2 \\ P_2 \end{pmatrix} \quad \text{where} \quad K = \begin{pmatrix} a & d \\ c & b \end{pmatrix}. \tag{2.9}$$

Furthermore we denote by $s_1 = \sigma_1$, $s_2 = \text{sign}[\det(K)]\sigma_2$ [3] with $\sigma_1 \geq \sigma_2 \geq 0$ the singular values of K. We refer to the s_k as the *restricted singular values* of K.

For the quadratic interaction Hamiltonian (2.8) characterized by a matrix K as in Eq. (2.9) we obtain as solution of the Heisenberg equations for $\vec{R} = (X_1, P_1, X_2, P_2)^T$

$$\vec{R}(t) = e^{Mt}\vec{R}(0) = S(t)\vec{R}(0), \tag{2.10}$$

where

$$M = \begin{pmatrix} 0 & L \\ \tilde{L} & 0 \end{pmatrix}, \tag{2.11}$$

with

$$L = \begin{pmatrix} c & b \\ -a & -d \end{pmatrix} = J^T K, \text{ and } \tilde{L} = -JL^T J^T = J^T K^T. \tag{2.12}$$

Using the fact that $M^2 = -\alpha \mathbb{1}$, with $\alpha = -\det(L)$ we can easily re-express Eq. (2.10) and find

$$S(t) = \cosh(\sqrt{\alpha}t)\mathbb{1} + \sinh(\sqrt{\alpha}t)/\sqrt{\alpha}M. \tag{2.13}$$

Thus, every evolution generated by a Hamiltonian (2.8) is uniquely characterized by a symplectic transformation $S(t)$ of the form (2.13). Note that any such transformation can be written in its *standard form*

$$S(t) = \cosh(\sqrt{\alpha}t)(O_1 \oplus O_2) \begin{pmatrix} 1 & 0 & h_1 & 0 \\ 0 & 1 & 0 & -h_2 \\ h_2 & 0 & 1 & 0 \\ 0 & -h_1 & 0 & 1 \end{pmatrix} (O_1 \oplus O_2)^T, \tag{2.14}$$

where $O_1, O_2 \in SO(2, \mathbb{R})$ perform the restricted singular value decomposition of L, and $h_k = \tanh(\sqrt{\alpha}t)/\sqrt{\alpha}s_k$, where s_k are the restricted singular values of L, which clearly coincide with those of K.

[3] The sign function is defined as $\text{sign}(x) = \pm 1$ if $x \gtrless 0$ and $\text{sign}(x) = 0$ if $x = 0$.

Part II

Entanglement properties of quantum operations

Chapter 3

Introduction

As explained before, an important task in Quantum Information Theory is to characterizing and quantifying the entanglement properties of multipartite states (see Sec. 1 and Sec. III). In practice, these states are created by a physical action (or operation) involving the interaction between several systems. This suggests that the analysis of these operations with regard to the possibility of creating entanglement may play an important role in Quantum Information Theory.

This part of the Thesis is completely devoted to investigate the entanglement properties of quantum operators. We will distinguish between operators acting on a finite (Chapter 4) and infinite dimensional (Chapter 5) Hilbert spaces, since the mathematical tools needed in these two cases are completely different. In the finite dimensional case we characterize all operations according to their capability of entangling two systems (Sec. 4.1.4, [23]). We will show that and how it is possible to implement non–local operations using a small amount of entanglement. Then we determine the optimal way to entangle two systems using an arbitrary two–qubit gate (Sec. 4.2.2, [94]). In Chapter 5 we study operators acting on infinite dimensional Hilbert spaces. In particular we analyze Gaussian operators (Sec. 2.2, [98]). First of all, we study the problem of interaction simulation. That is, given some interaction (either in terms of a fixed unitary operation, or the evolution due to some non–local Hamiltonian) assisted by some local operations, we determine the interactions which can be simulated with it. This problem is of great experimental relevance if one wants for instance two system to interact according to some evolution (or gate), but the Hamiltonian (or gate) occurring in the experiment is a different one. After that we study also in the infinite dimensional case methods to create entanglement in a very efficient way. Efficient methods for the creation of squeezing are also derived.

Chapter 4

Operators acting on a finite dimensional Hilbert space

In this chapter we investigate the entanglement properties of operators acting on a finite dimensional Hilbert space. In Sec. 4.1 (see also [23]) we characterize all operations [physical actions or, mathematically, CPM (see Sec. 2.1)] according to their entanglement properties. We show which operations are able to create entanglement, starting form an initially separable state. The ones which are capable to produce entanglement are then classified according to the kind of entanglement (free or bound entanglement) that they can create. As an application of this formalism we show how to implement entangling operations using a small amount of entanglement. After that we determine in Sec. 4.2 the optimal way to create entanglement using an arbitrary two–qubit gate [94]. There we quantify the maximal amount of entanglement produced by these kind of operations, in contrast to Sec. 4.1 where we qualify it. To this end we show that an arbitrary two–qubit gate can be decomposed into a product of local operations, followed by a simple non–local operations and again local operations. This allows to reduce the number of parameters used to describe an arbitrary unitary two qubit operation (15) to three, for this problem relevant, parameters.

4.1 Characterization and Implementation

We determine which physical operations acting on two spatially separated systems are capable of producing entanglement. This goal is partly motivated by the recent spectacular experimental progress in the field, where several physical set–ups have been recognized to produce entangled states [111, 123]. Thus, some of the questions we analyze here can be stated as

follows: given a machine acting on two systems, can it create entanglement? If so, what kind of entanglement? The basic mathematical tool to answer these questions is the isomorphism introduced by Jamiołkowski [84] (see also Sec. 1.2.1). We will extend such an isomorphism to relate physical operations [equivalently, completely positive maps (CPM) $\mathcal{E}$ (Sec. 2.1)] on two systems and unnormalized states (positive operators E) acting on two other systems. This allows us to reduce the problem of the characterization of physical operations to the one of physical states, which has been extensively studied in recent years (see Sec. 1.2.1, Chapter 7, and references therein).

This relation between physical operations and states has a well defined physical meaning. In fact, from the isomorphism it follows naturally that given a physical operation $\mathcal{E}$ acting on two separated systems A and B initially disentangled (but entangled locally to some other ancilla systems) we can always obtain the corresponding state E as an outcome. What is even more surprising is that, starting from the state E we can always perform some local measurements such that for certain outcomes the state of systems A and B changes exactly as if we had applied the corresponding operation $\mathcal{E}$.

This last property will allow us to answer an intriguing question raised in the context of Quantum Information Theory. Let us assume that we have two qubits A and B at different locations and we want to apply some non–local operation. This situation raises, for example, in the context of distributed quantum computation [24], where non–local operations between different quantum computers are required. So far, it is known that one can use maximally entangled states and LOCC to perform that task as follows: we can teleport the state of A to the location of B, perform the operation locally, and then teleport the corresponding state back to A. In this process one has to consume two maximally entangled states (i.e. two ebits) apart from transmitting two classical bits in each direction [20, 21]. However, it is known that for some kind of operations (like the controlled–NOT gate) one can economize the resources, such that only one ebit is consumed [62]. In fact, all the operations that have been studied so far [20, 21, 62, 47, 26] require *an integer number of ebits*. We will show here that many operations require *a non–integer number of ebits*. In particular, if the operation can only entangle qubits weakly, the required number is much smaller than one. This automatically implies that many tasks in distributed quantum computation can be performed with a much smaller entanglement than the one required so far.

4.1.1 Isomorphism between completely positive maps and positive semidefinite operators

Let us consider two systems A and B at different locations, whose states are represented by vectors in the Hilbert space $\mathcal{H}_{A,B}$, respectively, both of dimension d. As explained in Sec. 2.1 any physical action on those systems is represented mathematically by a completely positive linear map $\mathcal{E}$ mapping the density operator ρ of those systems onto another positive operator $\mathcal{E}(\rho)$. For the sake of generality, we will in the following not impose that the map preserves the trace of ρ, since we may be interested in physical actions that occur with certain probability [129]. Let us here briefly recall the used notation and definitions introduced in Sec. I.

A density operators ρ is separable if it can be written as a convex combination of product state (1.17). Similarly, a CPM is separable ; if

$$\mathcal{E}(\rho) = \sum_{i=1}^{n} (O_i^A \otimes O_i^B)\rho(O_i^A \otimes O_i^B)^\dagger, \tag{4.1}$$

for some integer n and where O_i^A and O_i^B are operators acting on $\mathcal{H}_{A,B}$, respectively. Otherwise, we say that it is non–separable. Recall that, up to a proportionality constant, separable maps are those that can be implemented using only LOCC.

Our first goal is to determine when a given CPM is able to produce entangled states. From the definition of separable state and separable CPMs (4.1) it follows that if $\mathcal{E}$ and ρ are separable, then $\mathcal{E}(\rho)$ is also separable. This reflects the fact that by local actions one cannot create entanglement (Sec. 1.1.2).

Now, let us consider two systems, A and B, spatially separated, each of them composed of two particles ($A_{1,2}$, and $B_{1,2}$). Let us consider a CPM $\mathcal{E}$ acting on systems A_1 and B_1. We are interested in whether this CPM can create "non–local" entanglement between the systems A and B [1]. We define the operator $E_{A_1A_2,B_1B_2}$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ [where now $\mathcal{H}_A = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ and $\mathcal{H}_B = \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$, and $\dim(\mathcal{H}_{A_i}) = \dim(\mathcal{H}_{B_i}) = d$] as follows:

$$E_{A_1A_2,B_1B_2} = \mathcal{E}(P_{A_1A_2} \otimes P_{B_1B_2}). \tag{4.2}$$

Here, $P_{X_1X_2} = |\Phi\rangle_{X_1X_2}\langle\Phi|$ with

$$|\Phi\rangle_{X_1X_2} = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle_{X_1} \otimes |i\rangle_{X_2}, \tag{4.3}$$

[1]Note that we can always take instead of two particles $A_{1,2}$ a single one with more levels. This is why we are interested in what we call non–local entanglement between systems A and B, rather than intrinsic or local entanglement between $A_{1,2}$.

for $X = A, B$, and $S = \{|i\rangle\}_{i=1}^{d}$ an orthonormal basis. In the definition (4.2) the map $\mathcal{E}$ is understood to act as the identity on the operators acting on $\mathcal{H}_{A_2}$ and $\mathcal{H}_{B_2}$. The operator E has a clear interpretation since it is proportional to the density operator resulting from the operation $\mathcal{E}$ on systems A_1 and B_1 when both of them are prepared in a maximally entangled state with two ancillary systems, respectively.

On the other hand, we have

$$\mathcal{E}(\rho_{A_1B_1}) = d^4 \mathrm{tr}_{A_2A_3B_2B_3}(E_{A_1A_2,B_1B_2}\rho_{A_3B_3}P_{A_2A_3}P_{B_2B_3}). \tag{4.4}$$

This can be proved as follows. First, we can write $d^2\mathrm{tr}_{A_3B_3}(\rho_{A_3B_3}P_{A_2A_3}P_{B_2B_3}) = \rho^T_{A_2B_2}$, where T means transpose in the basis $S_{A_2} \otimes S_{B_2}$. Now, using (4.2) one can readily show that $\mathcal{E}(\rho_{A_1B_1}) = d^2\mathrm{tr}_{A_2B_2}(E_{A_1A_2,B_1B_2}\rho^T_{A_2B_2})$. Equation (4.4) has a very simple interpretation. It reflects the fact that if we have the state $E_{A_1A_2,B_1B_2}$ at our disposal, we can always produce the map $\mathcal{E}$ on any state of systems A_3 and B_3 by performing a joint measurement locally such that both systems A_2A_3 and B_2B_3 are projected onto the maximally entangled state (4.3). Of course, this will happen with certain probability. Below we will show how to implement CPMs with unit probability using this method.

4.1.2 Characterization according to entanglement properties

The relations (4.2) and (4.4) induce a one–to–one correspondence between CPM acting on tensor product spaces and positive operators. In fact, this correspondence can be viewed as an extension of the isomorphism introduced by Jamiołkowski [84] (see also Sec. 1.2.1) to tensor product spaces. Using these relation it is very easy to show that:

(i) $\mathcal{E}$ is separable iff $E_{A_1A_2,B_1B_2}$ is separable with respect to the systems (A_1A_2) and (B_1B_2). Thus, we can study the separability of CPM by studying the problem of separability of positive operators. This immediately implies that we can use all the results derived for the latter problem (see Sec. 7.1, [104], and reference therein).

(ii) $\mathcal{E}$ can create non–local entanglement between A and B iff $E_{A_1A_2,B_1B_2}$ is non–separable with respect to the systems (A_1A_2) and (B_1B_2). In particular, we can always obtain a state whose density operator is proportional to $E_{A_1A_2,B_1B_1}$ out of separable states by entangling our systems locally with ancillas[2].

[2]Note that operator E associated to operations like the swap is entangled, although

(iii) Let us assume that $E^{T_{A_1A_2}}_{A_1A_2,B_1B_2} \geq 0$, where $T_{A_1A_2}$ denotes transposition with respect to A_1 and A_2 in the basis S_A. Then, if $\rho^{T_{A_1}} \geq 0$ we have that $\mathcal{E}(\rho_{A_1B_1})^{T_{A_1}} \geq 0$. If additionally $E_{A_1A_2,B_1B_2}$ is entangled (i.e. bound entangled [3]), then we can always produce bound entangled states out of non–entangled states by using the map $\mathcal{E}$ (see ii). $\mathcal{E}$ is called PPT–preserving in this case.

(iv) If $\mathcal{E}$ corresponds to a unitary action, the corresponding operator has rank one, i.e. it can be written as $E = |\Psi\rangle\langle\Psi|$, where $|\Psi\rangle \in \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$ is a normalized state.

4.1.3 Illustrative examples

We illustrate some of the above results with some simple examples concerning qubits ($d = 2$). First, let us assume that $E_{A_1A_2,B_1B_2}$ is an entangled state with positive partial transposition. According to (i) the corresponding completely positive map $\mathcal{E}$ is nonseparable and according (iii) $[\mathcal{E}(\rho)]^{T_{A_1}} \geq 0$ for all ρ separable. But in this case, positive partial transposition is equivalent to separability ([118, 81] Sec. 1.2.1), and therefore $\mathcal{E}(\rho)$ is separable for all ρ separable. However, if we allow for input states that are locally entangled with ancillas, the final state will be (bound) entangled according to (ii). As for another example, we consider a family of phase gates of the form

$$U(\alpha_N) \equiv e^{-i\alpha_N \sigma_x^{A_1} \otimes \sigma_x^{B_1}}, \ \alpha_N \equiv \pi/2^N \tag{4.5}$$

where the σ's are Pauli operators (1). These gates are of the same kind as the ones used in the discrete Fourier transform [86]. The corresponding operator $E_{A_1A_2,B_1B_2} = |\psi_{\alpha_N}\rangle\langle\psi_{\alpha_N}|$, where

$$\begin{aligned} |\psi_{\alpha_N}\rangle \ = \ & \cos(\alpha_N)|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2} \\ & -i\sin(\alpha_N)|\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}, \end{aligned} \tag{4.6}$$

and $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and $|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$ are Bell states (1.3).

Let us now consider a basis of maximally entangled states of systems A_2A_3 (and B_2B_3) as $|\Phi_i\rangle = \mathbb{1} \otimes U_i|\Phi\rangle$, where U_i are a unitary operators and

such operator acting on two particles A_1, and B_1 cannot create non–local entanglement. However, this is not in contradiction with this statement since if we allow such particles to be locally entangled with some other two A_2 and B_2, respectively, the swap operation can indeed produce non–local entangled states.

[3] Recall that bound entangled states are non–separable states that cannot be distilled to maximally entangled states [75].

$|\Phi\rangle$ is defined in (4.3). If we perform a measurement in that basis and obtain $|\Phi_i\rangle_{A_2A_3}$ and $|\Phi_j\rangle_{B_2B_3}$ the state of our systems will be $\mathcal{E}(U_i \otimes U_j \rho_{A_1B_1} U_i^\dagger \otimes U_j^\dagger)$. Thus, we see that as a result of the measurement we either implement the CPM, $\mathcal{E}$, or local operations followed by the CPM. Below, we will show how to use this effect in order to perform arbitrary non–local unitary operations by using entangled states. We will restrict ourselves to the case of qubits, but our results can be easily generalized. We will first show how to perform gates of the form (4.5) with probability 1/2. If we fail, we will show that by using other entangled states and performing more measurements of the same kind, we can make the probability of success equal to one. Then we will show how we can use these results to implement $U(\alpha)$ for arbitrary α. Finally, we will show that any arbitrary unitary operation can be implemented using the method described above.

Let us start considering the gates $U(\alpha_N)$ (4.5). The amount of entanglement of the corresponding state $|\psi_{\alpha_N}\rangle$ (4.6) is given by its entropy of entanglement (1.7)

$$E(\psi_{\alpha_N}) = -x\log_2(x) - (1-x)\log_2(1-x), \tag{4.7}$$

where $x = \cos^2(\alpha_N) = \cos^2(\pi/2^N)$. On the one hand, $E(\psi_{\alpha_2}) = 1$, i.e. according to our discussion $U(\pi/4)$ is capable of creating 1 ebit of entanglement. On the other hand, $E(\psi_{\alpha_1}) = 0$, i.e. $U(\pi/2) = -i\sigma_x \otimes \sigma_x$ is a *local* gate. For $N \geq 2$, we have that $E(\psi_{\alpha_N})$ is monotonically decreasing with N. Note that for N sufficiently large, we can regard (4.5) as an infinitesimal transformation and use the results of Ref. [43] to show that the gate can optimally create an entanglement proportional to α_N. We will show that in that limit $U(\alpha_N)$ can be implemented with unit probability by using an average amount of entanglement also proportional to α_N, assisted by classical communication of approximately 2 bits in both directions.

We want to perform the gate on systems A_3B_3 and obtain the output state in systems A_1B_1. We assume that both systems A_1A_2 and B_1B_2 are in the state $|\psi_{\alpha_N}\rangle$ and we measure systems A_2A_3 and B_2B_3 in the Bell basis $|\Psi_{i_1,i_2}\rangle = \mathbb{1} \otimes \sigma_{i_1,i_2}|\Phi^+\rangle$, where $\sigma_{1,1} = \mathbb{1}, \sigma_{1,2} = \sigma_x, \sigma_{2,1} = \sigma_y$, and $\sigma_{2,2} = \sigma_z$. Note that all outcomes of the measurement are equally probable. If the outcome for A_2A_3 is $|\Psi_{i_1,i_2}\rangle$, we apply σ_{i_1,i_2} to A_1 and proceed analogously with B_2B_3. One can readily see that the resulting operation on A_1B_1 after this procedure will be: (i) $U(\alpha_N)$ if $i_1 = j_1$; (ii) $U(\alpha_N)^\dagger = U(-\alpha_N)$ if $i_1 \neq j_1$. Thus, with probability 1/2 we obtain the desired gate, whereas with probability 1/2 we apply $U(-\alpha_N)$ instead, and so we fail. In order to apply the desired gate with probability one, we proceed as follows. If we fail, we repeat the procedure but with systems A_1A_2 and B_1B_2 prepared in the

state $|\psi_{2\alpha_N}\rangle$. With a probability 1/2 we will succeed, and otherwise we will have applied $U(-\alpha_N)^3$ to the original state. We continue in the same vein; that is, in the k–th step we use systems A_1A_2 and B_1B_2 in the state $|\psi_{2^{k-1}\alpha_N}\rangle$ so that if we fail altogether we will have applied $U(-\alpha_N)^{2^{k-1}}$. For $k = N$ we have that $U(-\alpha_N)^{2^N-1} = -U(\alpha_N)$, and therefore even if we fail we will have applied the right gate, so that the procedure ends.

The total average entanglement which is consumed during this procedure is given by

$$\bar{E}[U(\alpha_N)] = \sum_{k=1}^{N} \left(\frac{1}{2}\right)^{k-1} E(\psi_{\alpha_{N-k+1}}) = \alpha_N f_N, \tag{4.8}$$

where

$$f_N = \frac{1}{\pi}\sum_{k=1}^{N} 2^k E(\psi_{\alpha_k}) < f_\infty = 5.97932. \tag{4.9}$$

In (4.8), the weight factor of $p_k = (1/2)^{k-1}$ gives the probability that the k–th step has to be performed. Thus, we obtain $\bar{E}[U(\alpha_N)] < \alpha_N f_\infty$. Due to the fact that in each step of this procedure one bit of classical communication in each direction is necessary [4], the average amount of classical communication is given by $2 - (1/2)^{N-2}$ bits.

4.1.4 Implementation using a small amount of entanglement

Although the procedure described above allows only to implement gates with "binary phases" $\alpha_N = \pi/2^N$, any gate $U(\alpha)$ with arbitrary phase α can be approximated with arbitrarily high accuracy by a sequence of gates of the form $U(\alpha_N)$, consuming on average $\bar{E} \leq f_\infty \alpha$ ebits of entanglement. Furthermore, this procedure allows to implement any arbitrary two–qubit unitary operation U. We can write any such operation as $U = e^{-iHt} = \lim_{n\to\infty}(\mathbb{1} - iHt/n)^n$, where H is a self–adjoint operator. We can thus apply infinitesimal gates $U_n = (\mathbb{1} - iHt/n)$ sequentially using an extension of the scheme described above. Note that after such an infinitesimal operation we can perform local operations without consuming entanglement. This allows us to restrict the form of the Hamiltonians to those that can be written as

$$H_0 = \sum_{k=x,y,z}^{3} \mu_k \sigma_k^A \otimes \sigma_k^B \equiv \sum_{k=1}^{3} H_k. \tag{4.10}$$

[4] In practice, only $(N-2)$ steps have to be performed, as it happens that the required operation in step $(N-1)$, $U(\pi/2)$, is a local operation which can be performed with certainty and without classical communication.

This can be viewed as follows. Any Hamiltonian can be written (except for a trivial constant) as

$$H = (\vec{\alpha}^T\vec{\sigma}_A)\otimes\mathbb{1}_B + \mathbb{1}_A\otimes(\vec{\beta}^T\vec{\sigma}_B) + \vec{\sigma}_A^T\gamma\vec{\sigma}_B. \tag{4.11}$$

Here $\vec{\alpha}$, $\vec{\beta}$, and γ are, respectively, two real vectors and a real matrix. If we apply infinitesimal local transformations in A and B with Hamiltonians $-\vec{\alpha}\cdot\vec{\sigma}^A$ and $-\vec{\beta}\cdot\vec{\sigma}^B$ respectively, this will be equivalent to having H with $\alpha = \beta = 0$. On the other hand, we can write γ in its singular value decomposition, i.e $\gamma = O_1\gamma_d O_2$, where O_1 and O_2 are special orthogonal matrices and γ_d is a positive diagonal matrix. The sorted singular values of γ (the diagonal elements of γ_d) will be denote by $\gamma_1, \gamma_2, \gamma_3$ ($\gamma_1 \geq \gamma_2 \geq |\gamma_3| \geq 0$). Applying the local unitary operators, U_A (V_B) and $U_A^\dagger$ ($V_B^\dagger$), before and after the evolution, such that $U_A^\dagger\vec{\sigma}_A^T U_A = \vec{\sigma}_A^T O_1^T$ ($V_B^\dagger\vec{\sigma}_B V_B = O_2^T\vec{\sigma}_B$), we find that the Hamiltonian is transformed into the standard form (4.10). Since the H_k commute, we have that the corresponding unitary operation is given by

$$\tilde{U}_n = e^{-iH_1 t/n}e^{-iH_2 t/n}e^{-iH_3 t/n}, \tag{4.12}$$

a sequence of operations of the form (4.5) for which we already have provided a protocol. The required amount of entanglement is therefore given by $\bar{E}_U = f_\infty t(\mu_1+\mu_2+\mu_3)$ ebits.

Using the results of Ref. [43], one can compare for small α_N (large N) the average amount of entanglement used up to implement the gate (4.5) with the maximal amount of entanglement which can be produced with help of a single application of the gate [5]. One finds that for $\alpha_N \to 0$ that the ratio $\bar{E}[U(\alpha_N)]/E_{\text{create}}[U(\alpha_N)]$ is given by ≈ 3.1268.

As an aside, let us mention that we have restricted ourselves here to the implementation of non–local unitary operations. In fact, with the formalism introduced here one can extend the analysis to non–unitary operations and even to the implementation of non–local measurements. All these results indicate that the entanglement properties of a physical operation $\mathcal{E}$ are directly related to the entanglement of the corresponding operator E.

4.1.5 Generalization to multi–partite systems

It is straight forward to generalize this formalism to multipartite systems. We consider a CPM, $\mathcal{E}$, acting on the N systems A_1,B_1 ..., Z_1. The corresponding Hilbert space is $\mathcal{H} = \mathcal{H}_{A_1}\otimes\mathcal{H}_{B_1}\otimes\ldots\otimes\mathcal{H}_{Z_1}$.

[5] As shown in Ref. [43], in the limit $\alpha_N \to 0$, the maximal amount of created entanglement is given by $E_{\text{create}}[U(\alpha_N)] = 1.9123\alpha_N$.

Then we have (Sec. 2.1) a CPM is separable (fully separable) if it can be written as $\mathcal{E}(\rho) = \sum_{k=1}^{l} (O_k^A \otimes O_k^B \dots O_k^Z)\rho(O_k^A \otimes O_k^B \dots O_k^Z)^\dagger$, where l is some finite number. A CPM, $\mathcal{E}$, is called Y–PPT–preserving if for all ρ Y–PPT, $\mathcal{E}(\rho)$ is Y–PPT. We call a CPM PPT–preserving, if it is Y–PPT–preserving for all systems Y.

We define the operator

$$E_{A_1,A_2,\dots,Z_1,Z_2} = \frac{1}{d^{2N}} \mathcal{E}(P_{A_1,A_2} \otimes \dots P_{Z_1,Z_2}), \tag{4.13}$$

where P_{X_1,X_2} is the projector onto the maximally entangled state (4.3). $E_{A_1,A_2,\dots,Z_1,Z_2}$ is acting on $\mathcal{H}_A \otimes \dots \otimes \mathcal{H}_Z$, with $\mathcal{H}_X = \mathcal{H}_{X_1} \otimes \mathcal{H}_{X_2}$ and $\dim(\mathcal{H}_{X_i}) = \dim(\mathcal{H}_{Y_i}) = d$, for $i = 1,2$ and $X, Y \in \{A, \dots, Z\}$. As before, the map $\mathcal{E}$ in Eq. (4.13) is understood to act as the identity on the operators in $\mathcal{B}(\mathcal{H}_2)$. Analogously to Eq (4.4) we have that,

$$\mathcal{E}(\rho_{A_1,\dots Z_1}) = \operatorname{tr}_{A_2,A_3\dots Z_2,Z_3}(E_{A_1,A_2,\dots Z_1,Z_2} \rho_{A_3\dots Z_3} P_{A_2,A_3} \otimes \dots P_{Z_2,Z_3}), \tag{4.14}$$

which can be also written as

$$\mathcal{E}(\rho_{A1,\dots Z_1}) = \operatorname{tr}_{A_2,\dots,Z_2}(E_{A_1,A_2,\dots Z_2,Z_2} \rho^T_{A_2,\dots Z_2}). \tag{4.15}$$

Analogously to the bipartite case we have

(p1) $\mathcal{E}$ is a fully separable CPM iff E is fully separable with respect to the systems $(A_1, A_2), \dots (Z_1, Z_2)$.

(p2) $\mathcal{E}$ can create entanglement iff E is entangled with respect to the systems $(A_1, A_2), \dots (Z_1, Z_2)$.

(p3) $\mathcal{E}$ represents a Y–PPT–preserving CPM iff E is Y–PPT.

Note that we can also generalize this isomorphism for CPM's of the form $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\bar{\mathcal{H}})$. Then the corresponding operator E is an element of $\mathcal{B}(\mathcal{H} \otimes \bar{\mathcal{H}})$.

4.1.6 Conclusions

In summary, we have shown that the problem of separability of non–local actions can be connected to the one for states via an isomorphism. The methods introduced here also allow to show how one can implement certain non–local operations if one shares a small amount of entanglement and is allowed to perform local operations and classical communication. These local

operations require, in principle, Bell measurement between the two particles in one location which may be difficult in practice. However, in experiments one can substitute these pairs of particles by a single one with more levels[6], which implies that only single particle operations are needed. Note that those measurements can then be easily performed with ions or atoms [123]. On the other hand, since with photons it is possible both to create entangled states and to perform Bell measurements (with certain probability) [14, 13] our method allows to perform probabilistic non–local gates between photons without having to use controlled non–linear interactions [36].

There are many other important applications of this powerful isomorphism. For instance, as shown in Ref. [36] it is possible to prove that non–local unitary operations can be purified, stored, or compressed. In Ref. [37] the isomorphism presented here has been used to characterize the equivalence classes of non–local operations. As we have seen it is straightforward to generalize the formalism to more than two systems [36]. It can be even generalized to operators acting on an infinite dimensional Hilbert space [59].

4.2 Optimal creation of entanglement using a two-qubit gate

We consider here a unitary operator, U_{AB}, acting on two qubits. The goal is to use this non–local interaction to create as much entanglement as possible, starting out with some product state of system A and B, $|\phi\rangle_A |\psi\rangle_B$ [94]. Note that we can clearly apply the formalism introduced in the previous section to decide whether the considered unitary operation is able to create entanglement or not (in the case of unitary operators it is particulary simple, because the corresponding positive semidefinite operator would be a pure state and as such it is known how to decide whether it is entangled or not). The results derived here give a characterization of two–qubit gates in terms of the amount of entanglement that they can produce (in contrast to the previous section we quantify not qualify the produced entanglement here). For example, we will determine which are the operators U_{AB} that can create maximally entangled states. While most of the results derived here are concerned with two qubits, we will also show that if we allow them to be initially (locally) entangled with some ancillas, one can obtain more entanglement, at least, for certain measures of entanglement.

This section is divided into three parts. In Section 4.2.1 we study unitary operators acting on two qubits. In general such an operator can be parame-

[6] See footnote [1] in page 44

terized in terms of 15 coefficients (plus a global phase). Thus, to study the maximum entanglement which can be produced in terms of all these parameters seems a formidable task. However, we will show that one can always decompose $U_{AB} = (U_A \otimes U_B)U_d(V_A \otimes V_B)$[7], where U_d has a special form that only depends on three parameters and the rest are local unitary operators. This implies that we can restrict ourselves to characterize operators of the form U_d. In Section 4.2.2 we determine how much entanglement can be produced by a general two–qubit gate acting on a product state of two qubits. We also find which of such states give rise to that amount of entanglement. In Section 4.2.3 we discuss the case where we allow the qubits to be initially entangled with ancillas. We will show that the solution to the problem depends on the measure of entanglement we use to quantify it. We will also give two examples in which this problem can be solved analytically for a particular measure of entanglement.

4.2.1 Unitary two–qubit operations

We consider an arbitrary unitary two–qubit operation U_{AB}. This operator is acting on a four dimensional Hilbert space and so one needs 15 parameters to describe it (plus a global phase). We show here that three parameters suffice to characterize its non–local properties. This fact, including some symmetry properties derived in Appendix B.1, will allow us to determine in the following sections the maximal amount of entanglement which can be created by an arbitrary unitary two–qubit operation.

Decomposition

Theorem 4.1 *(Decomposition of an arbitrary two-qubit unitary operation) For any unitary operator U_{AB} there exist local unitary operators, U_A, U_B, V_A, V_B, and a unitary operator U_d such that*

$$U_{AB} = U_A \otimes U_B U_d V_A \otimes V_B, \tag{4.16}$$

where

$$U_d = e^{-i\vec{\sigma}_A{}^T d \vec{\sigma}_B} \tag{4.17}$$

and d is a diagonal matrix.

[7]Note that the existence of such a decomposition has been independently proven by Khaneja and S. J. Glaser ([91]). Our proof will be, however, constructive.

We will denote the diagonal elements of d by $\alpha_x, \alpha_y, \alpha_z$. Note that any measure of entanglement is not changed by local unitary operators. Thus the entanglement created by U_{AB} is the same as the one created by $U_d V_A \otimes V_B$. And so the maximal amount of entanglement which can be produced by applying a general unitary, U_{AB} is the same as the one created by U_d. This means that we have to deal with unitaries which are determined by only 3 parameters, $(\alpha_x, \alpha_y, \alpha_z)$, instead of 15 parameters, which are used in order to describe a general unitary operator acting on two qubits.

Proof of the Theorem 4.1

Our prove will be constructive. Let us call a basis consisting of maximally entangled orthonormal states a maximally entangled basis. Furthermore, we use for this proof the subscript k if a definition or statement is true for $k = 1, \ldots, 4$, if not stated differently. Let us note first of all that $U_d = \sum_{k=1}^{4} e^{-i\lambda_k} |\Phi_k\rangle \langle\Phi_k|$, where $\{|\Phi_k\rangle\}$ denotes the magic basis (1.4), which can be easily shown.

Lemma 4.1 *For any maximally entangled basis $\{|\Psi_k\rangle\}$, there exist phases ζ_k and local unitaries U_A, U_B such that*

$$U_A \otimes U_B e^{i\zeta_k} |\Psi_k\rangle = |\Phi_k\rangle . \tag{4.18}$$

Proof: According to the discussion in Sec. 1.1.2 [see property (i) of maximally entangled states] we can always write $|\Psi_k\rangle = e^{\gamma_k} |\bar{\Psi}_k\rangle$, where $|\bar{\Psi}_k\rangle$ is real in the magic basis. Let us consider two different states, $|\bar{\Psi}_k\rangle$ and $|\bar{\Psi}_l\rangle$, then $1/\sqrt{2}(|\bar{\Psi}_k\rangle - i|\bar{\Psi}_l\rangle) = |e, f\rangle$ [Sec. 1.1.2 (ii)] and $1/\sqrt{2}(|\bar{\Psi}_k\rangle + i|\bar{\Psi}_l\rangle) = |\tilde{e}, \tilde{f}\rangle$, where $|e\rangle, |\tilde{e}\rangle \in \mathcal{H}_A$ and $|f\rangle, |\tilde{f}\rangle \in \mathcal{H}_B$. Note that $|e, f\rangle$ must be orthogonal to $|\tilde{e}, \tilde{f}\rangle$. This immediately implies that these vectors must give the Schmidt decomposition of both $|\bar{\Psi}_{k,l}\rangle$. Thus we can write

$$|\bar{\Psi}_1\rangle = \frac{1}{\sqrt{2}}(|e, f\rangle + |e^\perp, f^\perp\rangle) \tag{4.19a}$$

$$|\bar{\Psi}_2\rangle = \frac{-i}{\sqrt{2}}(|e, f\rangle - |e^\perp, f^\perp\rangle). \tag{4.19b}$$

Using the same arguments for $|\bar{\Psi}_{3,4}\rangle$ it is easy to determine that they can be written as

$$|\bar{\Psi}_3\rangle = \frac{-i}{\sqrt{2}}(e^{i\delta}|e, f^\perp\rangle + e^{-i\delta}|e^\perp, f\rangle) \tag{4.20a}$$

$$|\bar{\Psi}_4\rangle = \pm\frac{1}{\sqrt{2}}(e^{i\delta}|e, f^\perp\rangle - e^{-i\delta}|e^\perp, f\rangle) \tag{4.20b}$$

for some δ. In this case, choosing

$$U_A = |0\rangle\langle e| + |1\rangle\langle e^\perp| e^{i\delta}, \tag{4.21a}$$
$$U_B = |0\rangle\langle f| + |1\rangle\langle f^\perp| e^{-i\delta} \tag{4.21b}$$

and the phases ζ_k appropriately, we have (4.18) .■

Note that this first lemma implies that one can go from one maximally entangled basis to any other using only local unitaries, if one chooses the global phases appropriately.

Lemma 4.2 *Given a general unitary operator, U, then there always exist phases ϵ_k and two maximally entangled basis $\{|\Psi_k\rangle\}$ and $\{|\tilde{\Psi}_k\rangle\}$ such that*

$$U|\Psi_k\rangle = e^{i\epsilon_k}|\tilde{\Psi}_k\rangle. \tag{4.22}$$

Proof: We give a constructive proof. Let us denote by $\{|\Psi_k\rangle\}$ the eigenstates of U^TU, where U^T denotes the transpose of U in the magic basis and $e^{2i\epsilon_k}$ are the corresponding eigenvalues. Note that the eigenvectors of the symmetric operator U^TU are orthonormal and real, except for global phases. Thus, since we are working in the magic basis, they build a maximally entangled basis. Now we define $|\tilde{\Psi}_k\rangle$ as

$$|\tilde{\Psi}_k\rangle \equiv e^{-i\epsilon_k}U|\Psi_k\rangle. \tag{4.23}$$

Since the set $\{|\tilde{\Psi}_k\rangle\}$ also form an orthonormal basis, it remains to prove that its elements are real. In order to show that let us consider the eigenvalue equation, $(U^TU - e^{2i\epsilon_k}\mathbb{1})|\Psi_k\rangle = 0$. Multiplying it by $U^*e^{-i\epsilon_k}$ we get that $(e^{-i\epsilon_k}U - e^{i\epsilon_k}U^*)|\Psi_k\rangle = 0$, which is true iff $e^{-i\epsilon_k}U|\Psi_k\rangle$ is real. ■

With all that we are now in the position to show that any unitary operator can be decomposed into local operators and U_d as in Eq.(4.16). So let us now give the procedure to determine the unitary operators that appear there.

1) Calculate the eigensystem of the unitary, symmetric operator U^TU. Let us denote the eigenvalues by $e^{2i\epsilon_k}$ and the eigenstates by $|\Psi_k\rangle$. As proven in Lemma 4.2 the set of those states is a maximally entangled basis.

2) Choose V_A, V_B and the phases ξ_k, as explained in Lemma 4.1, such that

$$V_A \otimes V_B e^{i\xi_k}|\Psi_k\rangle = |\Phi_k\rangle. \tag{4.24}$$

3) Calculate

$$|\tilde{\Psi}_k\rangle = e^{-i\epsilon_k}U|\Psi_k\rangle. \tag{4.25}$$

Note that according to Lemma 4.2 the set of those states is also a maximally entangled basis.

4) Choose the eigenvalues of U_d, $e^{i\lambda_k}$ (note that this is equivalent to choose the diagonal elements of d) and the unitary operators U_A, U_B such that

$$U_A^\dagger \otimes U_B^\dagger e^{i(\lambda_k+\xi_k+\epsilon_k)}|\tilde{\Psi}_k\rangle = |\Phi_k\rangle, \tag{4.26}$$

which, according to Lemma 4.1, is always possible. It is simple to check that with these definitions we obtain the decomposition (4.16).

Periodicity and symmetry of the maximal amount of entanglement created by U_{AB}

In Appendix B.1 we show that when studying the maximum amount of entanglement created by a two-qubit gate we can restrict ourselves to the case where

$$\pi/4 \geq \alpha_x \geq \alpha_y \geq \alpha_z \geq 0. \tag{4.27}$$

This is due to the fact that the maximal amount of entanglement created by U_d is symmetric around $\pi/4$ and $\pi/2$–periodic in α_x, α_y and α_z.

As already mentioned, the operator U_d is diagonal in the magic basis, and therefore we can write

$$U_d = \sum_{k=1}^{4} e^{-i\lambda_k}|\Phi_k\rangle\langle\Phi_k|. \tag{4.28}$$

The phases λ_k are

$$\begin{aligned}\lambda_1 &= \alpha_x - \alpha_y + \alpha_z,\\ \lambda_2 &= -\alpha_x + \alpha_y + \alpha_z,\\ \lambda_3 &= -\alpha_x - \alpha_y - \alpha_z,\\ \lambda_4 &= \alpha_x + \alpha_y - \alpha_z.\end{aligned} \tag{4.29}$$

4.2.2 Two qubits

In this section we consider the following scenario. Alice and Bob have one qubit each. They want to entangle them by applying a given unitary operation U_{AB}. Their main goal is to find the best separable (pure[8]) input state that gives as much entanglement as possible. Note, according to our discussions in Sec. 1.1.2, all measures of entanglement are equivalent in this case. We choose here the concurrence defined in (1.5). We just have to find which states $|\phi\rangle_A, |\psi\rangle_B$ maximize the concurrence of the output state $U_d|\phi\rangle_A, |\psi\rangle_B$, where U_d is given in (4.17) with restrictions (4.27). We will call these states best input states. Writing the input and output state in the magic basis, $\{|\Phi_k\rangle\}_{k=1}^4$ (1.4), with the coefficients w_k, μ_k respectively, we apply the unitary operator U_d and obtain

$$\sum_k \mu_k |\Phi_k\rangle = U_d(|\phi\rangle_A |\psi\rangle_B) = \sum_k w_k e^{-i\lambda_k} |\Phi_k\rangle . \tag{4.30}$$

We want to maximize the concurrence of the output state, $C = |\sum_k \mu_k^2|$, where we have to make sure that the following conditions are satisfied:

(c1) $\sum_k |\mu_k|^2 = 1$, which is that the output state is normalized. Note that, since U_d is unitary this implies that the input state is normalized.

(c2) $\sum_k \mu_k^2 e^{2i\lambda_k} = 0$. This condition is due to the fact that the input state is a product state, which can be seen as follows. From Eq.(4.30) we see that $w_k = \mu_k e^{i\lambda_k}$, and according to Section 1.1.2 [property (ii) of product states] this last one is a product state iff the sum of the coefficients in the magic basis squared vanishes, which implies the above equation.

We can determine the maximum of the concurrence of the output state under the conditions (c1), (c2) by maximizing C^2 and imposing the above conditions in terms of Lagrange multipliers, i.e. we maximize

$$\begin{aligned} f(\mu_1 \dots \mu_4) = &\sum_{k,l} \mu_k^2 (\mu_l^*)^2 - 2\eta_1 (\sum_k |\mu_k|^2 - 1) \\ &-\eta_2 \sum_k \mu_k^2 e^{2i\lambda_k} - \eta_2^* \sum_k (\mu_k^*)^2 e^{-2i\lambda_k}, \end{aligned} \tag{4.31}$$

[8] Note that the maximum entanglement reached for pure states is always larger than the one reached by a mixed state. This can be seen as follows: let us write an arbitrary mixed state, ρ in its eigenbasis, i.e $\rho = \sum_k p_k |\Psi_k\rangle\langle\Psi_k|$. Using the convexity of any measure of entanglement, E, (1.12) we have that $E(\rho) \leq \max_{|\Psi_k\rangle} E(|\Psi_k\rangle)$. Thus it suffices to consider only pure states.

where η_1 is real. We find it convenient to denote $\sum_l (\mu_l^*)^2 = Ce^{i\gamma}$, $\eta_2 = |\eta_2|e^{i\epsilon}$, and $\mu_k = |\mu_k|e^{i\xi_k}$. We obtain

$$\mu_k \sum_l (\mu_l^*)^2 = \eta_1 \mu_k^* + \eta_2 \mu_k e^{2i\lambda_k} \quad \forall k. \tag{4.32}$$

Multiplying Eq (4.32) by μ_k, summing over k and using (c1) and (c2) we find that $\eta_1 = C^2$. And so we have, assuming that $C \neq 0$,

$$\mu_k (Ce^{i\gamma} - \eta_2 e^{2i\lambda_k})/C^2 = \mu_k^*. \tag{4.33}$$

One of the solutions to this equation is $\mu_k = 0$. To find the others we write Eq. (4.33) as

$$\left| 1 - \frac{|\eta_2|}{C} e^{i(2\lambda_k - \gamma + \epsilon)} \right| = C. \tag{4.34}$$

Let us distinguish now two cases, namely when η_2 is zero or not.

- $\eta_2 = 0$: From Eq. (4.34) it follows that $C = 1$. Using then Eq. (4.33) it is easy to see that $e^{2i\xi_k} = e^{-i\gamma} \forall k$. Thus all the coefficients have the same phase (except for the sign) and therefore the output state is, according to the discussions of Section 1.1.2 (i), a maximally entangled state. In order to obtain this state by applying U_d to a product state the conditions, (c1) and (c2) still have to be imposed. In Appendix B.2 we show that those conditions can be fulfilled iff $\alpha_x + \alpha_y \geq \pi/4$ and at the same time $\alpha_y + \alpha_z \leq \pi/4$. There, we also determine the best input state.

- $\eta_2 \neq 0$: In this case Eq. (4.34) can have at most two solutions for a fixed value of $|\eta_2|/C$. Thus, in order to fulfill (4.32) $\forall k$ at least two of the coefficients have to vanish[9]. Let us call the other two μ_k and μ_l. Then, in order to fulfill conditions (c1) and (c2) we have to satisfy $|\mu_k|^2 + |\mu_l|^2 e^{2i(\lambda_l + \xi_l - (\lambda_k + \xi_k))} = 0$ and the normalization condition. Thus $|\mu_k| = |\mu_l| = 1/\sqrt{2}$ and the difference between the two phases ξ_k and ξ_l is $\lambda_l - \lambda_k - \pi/2$. With all that it is now simple to determine that the largest reachable concurrence is

$$C = \max_{k,l} |\sin(\lambda_k - \lambda_l)|. \tag{4.35}$$

[9] Note that if two or more λ's are equal, this does not need to be necessary. However, we can discard this case since it has zero measure in the set of unitary operators, and obtain this result by imposing continuity.

Except for global phases the corresponding output state is $1/\sqrt{2}(|\Phi_k\rangle + i\,|\Phi_l\rangle\, e^{\lambda_k-\lambda_l})$ and the separable input state, which leads to this maximum is

$$\frac{1}{\sqrt{2}}(|\Phi_k\rangle + i\,|\Phi_l\rangle). \tag{4.36}$$

Note that the input state $1/\sqrt{2}(|\Phi_k\rangle - i\,|\Phi_l\rangle)$ (the corresponding output state would then be $1/\sqrt{2}(|\Phi_k\rangle - i\,|\Phi_l\rangle\, e^{\lambda_k-\lambda_l})$) leads to the same amount of entanglement.

Note that in case $\alpha_x \leq \pi/8$, we obtain that $C = \sin(\alpha_x + \alpha_y)$, which is directly related to the entanglement capability of the Hamiltonian of the form $\sigma_A^T d \sigma_B$ [43]. For higher values of α_x the result may not be directly related to that quantity.

In summary, we have shown here that if we apply U_d to a separable input state and calculate the maximum of the concurrence of the output state, then we find: If $\alpha_x + \alpha_y \geq \pi/4$ and $\alpha_y + \alpha_z \leq \pi/4$ then this maximum is equal to 1. Otherwise it is given by (4.35). In addition we determined the best input state in each of those two cases. Note that, since we were dealing with two–qubit states we could have taken, according to the discussions in Sec. 1.1.2, any other measure of entanglement to obtain the same result.

4.2.3 The role of auxiliary systems

We analyze now whether and how it would be possible to increase the amount of entanglement of the output state with the help of auxiliary systems. So, we consider the situation where Alice and Bob have two qubits each[10]. Let us denote the auxiliary qubits by A' and B'. We allow input states in which Alice and Bob's qubits are locally entangled, i.e. of the form $|\phi\rangle_{AA'}\,|\psi\rangle_{BB'}$. Then they apply a non–local unitary transformation, U_{AB} to the qubits A and B. The question is, then, for which $|\phi\rangle_{AA'}$ and $|\psi\rangle_{BB'}$ they are able to reach $\max_{|\phi\rangle_{AA'},|\psi\rangle_{BB'}} E(U_{AB}\otimes \mathbb{1}_{A'B'}\,|\phi\rangle_{AA'},|\psi\rangle_{BB'})$, where E denotes some measure of entanglement between Alice's two qubits and Bob's two qubits. In what follows we write again simply $|\phi\rangle$ ($|\psi\rangle$) instead of $|\phi\rangle_{AA'}$ ($|\psi\rangle_{BB'}$). On the other hand, according to Sec. 4.2.1, we can restrict ourselves to operators U_d of the form (4.17). For convenience we will call the input state where $|\phi\rangle$

[10]Note that since one of Alice's and one of Bob's subsystems (the one on which they apply the unitary operator) is a qubit, the state describing such a subsystem and an ancilla of arbitrary dimension can always be viewed as a state describing two qubits (it has at most two Schmidt coefficients).

and $|\psi\rangle$ are both maximally entangled, *local maximally entangled* and the one where both are product states, *local product state*.

The main difference to the previous section is that now the best input states depend on the measure of entanglement. To illustrate this fact we show that for some measures of entanglement the best input states are the ones where $|\phi\rangle$ and $|\psi\rangle$ are entangled. On the other hand, there are measures of entanglement for which a local product state is the best input state.

We also show that for some special class of U_d (where d has only one non vanishing element) the solution to our problem is independent of the measure of entanglement. In particular, we determine the maximal amount of created entanglement and the best input state for this case. Furthermore, for the class of U_d where all the diagonal elements of d are the same we will determine the maximum Rènyi entanglement (Sec. 1.1.2) as well as the best input state according to this measure of entanglement.

Dependence on the entanglement measure

Let us compare the answer to our problem for some of the measures of entanglement which we summarized in Sec. 1.1.2. According to some numerical examples we have that:

- Schmidt number: The best local maximally entangled states are always better than the best local product states. This can be easily understood since in the first case the maximum value which E_S can take is 3, whereas in the latter one it can be at most 1. Thus using this measure of entanglement the ancillas will in general increase the entanglement of the output state.

- Rènyi entanglement: We have checked that for this measure the best input states are always either local product states or local maximally entangled states. In particular, in the next subsection we will provide analytical results for some particular cases.

- Entanglement monotones: We have verified that there are unitary operators U_d for which local product states are the best input states, whereas for some other values the local maximally entangled states lead to the most entangled output state. But there also exist some U_d for which neither the local product states nor the local maximally entangled states are the best input states.

From these examples it becomes clear that it does not make much sense to ask for the best input state, if one does not specify according to which measure of entanglement.

Examples

Before we start with the examples let us make some general statement about the input state. It can always be written in the Schmidt decomposition (Sec. 1.1.1) as

$$|\phi\rangle_{AA'} = c_a |\phi_0\rangle_A |0\rangle_{A'} + s_a |\phi_0^\perp\rangle_A |1\rangle_{A'}, \tag{4.37a}$$

$$|\psi\rangle_{BB'} = s_b |\psi_0\rangle_B |0\rangle_{B'} + c_b |\psi_0^\perp\rangle_B |1\rangle_{B'}, \tag{4.37b}$$

where $c_a^2+s_a^2 = c_b^2+s_b^2 = 1$. This is due to the fact that local unitaries applied to A' and B' do not change the entanglement (and commute with U_d). Let us now treat two cases in which it is possible to determine the best input state for some measures of entanglement. The first one should be viewed as a very simple illustration, whereas the second one is much more involved.

Example 1

Let us consider the following simple unitary operator,

$$U_d = e^{-i\alpha S_x} = \cos(\alpha)\mathbb{1} - i\sin(\alpha)\sigma_x \otimes \sigma_x, \tag{4.38}$$

where $S_x = \sigma_x \otimes \sigma_x$. In this case it is fairly simple to determine the output state. It has at most 2 Schmidt coefficients and therefore the state can be viewed as a state describing two qubits. This implies, as discussed in Sec. 1.1.2, that all the measures of entanglement are equivalent when calculating the optimal states. We take E_E, the Entropy of Entanglement (1.7).

Let us define ρ_1 as the density operator whose off–diagonal elements are zero, whereas the diagonal elements are the same as the one of the state ρ. Using the fact that the von Neumann entropy is convex we have that $S(\rho_1) \geq S(\rho)$. Apart from that, since the problem is symmetric under exchanging system (AA') with (BB'), it is easy to verify that the states with $\sigma_x|\phi\rangle \propto |\phi^\perp\rangle$ and $\sigma_x|\psi\rangle \propto |\psi^\perp\rangle$ lead to the most entangled output state. Now, since the states $|\phi\rangle = |1\rangle, |\psi\rangle = |1\rangle$, as well as the states $|\phi\rangle = |\Phi^+\rangle, |\psi\rangle = |\Phi^+\rangle$ fulfill this condition, both, a local product state and a local maximally entangled state are the best input states. The maximal entropy of entanglement which can be obtained is then

$$\max E_E = -\cos(\alpha)^2 \log_2[\cos(\alpha)^2] - \sin(\alpha)^2 \log_2[\sin(\alpha)^2]. \tag{4.39}$$

Example 2

Here we determine the best input state, according to the Rènyi entanglement, corresponding to a unitary of the form

$$U_d = e^{-i\alpha(S_x+S_y+S_z)} = (\cos(\alpha)^3 - i\sin(\alpha)^3)\mathbb{1} - i\sin(\alpha)\cos(\alpha)e^{i\alpha}(S_x + S_y + S_z), \tag{4.40}$$

where $S_\beta \equiv \sigma_\beta \otimes \sigma_\beta$ $(\beta = x, y, z)$. Here we have used $[S_x, S_y] = [S_x, S_z] = [S_y, S_z] = 0$. In Appendix B.3 we show that, according to any measure of entanglement the best input state can always be written as

$$|\phi\rangle_{AA'} = c_a |0\rangle_A |0\rangle_{A'} + s_a |1\rangle_A |1\rangle_{A'} \tag{4.41a}$$

$$|\psi\rangle_{BB'} = s_b |0\rangle_B |0\rangle_{B'} + c_b |1\rangle_B |1\rangle_{B'}, \tag{4.41b}$$

where $s_a^2 + c_a^2 = s_b^2 + c_b^2 = 1$.

Let us start by proving that the best input state is either a local product state or a local maximally entangled state. Calculating the reduced density operator one finds that $\rho_A = \rho_1 \oplus \rho_2$ $(\mathrm{tr}(\rho_1\rho_2) = 0)$, where ρ_1, ρ_2 are 2×2-matrices which depend on s_a, s_b and α. It is straightforward to calculate $E_R(U_d|\phi\rangle|\psi\rangle) = S_R(\rho_A) = S_R(\rho_1) + S_R(\rho_2)$ and determine its maxima. One finds that either the local product states $(s_a^2, s_b^2 = 0, 1)$ or the local maximally entangled states $(s_a^2 = s_b^2 = 1/2)$ always lead to a maximum of the Rènyi entanglement. In the case of a local product state, it is easy to check that the best one is $|01\rangle$ (or equivalently $|10\rangle$[11]). Let us denote by $E_R^{\mathrm{m.e}}$ $(E_R^{\mathrm{p.s}})$ the Rènyi entanglement for a local maximally entangled input state (product state $|01\rangle$) respectively. We obtain

$$E_R^{\mathrm{m.e}}(\alpha) = \frac{3}{16}[3 - 2\cos(4\alpha) - \cos(4\alpha)^2] \tag{4.42a}$$

$$E_R^{\mathrm{p.s}}(\alpha) = \frac{1}{2}[1 - \cos(4\alpha)^2]. \tag{4.42b}$$

Comparing those two expressions we find that $\forall\alpha < \alpha_0$, where $\alpha_0 = \arccos(1/5)/4 \approx 0.109\pi$ the local product state is the best input state and otherwise the local maximally entangled state leads to the output state with the largest Rènyi entanglement. In Figure 4.1 we illustrate this result.

[11] Note that, due to the symmetry of the problem, the entanglement produced by the input state $|01\rangle$ has to be the same as the one produced by $|10\rangle$.

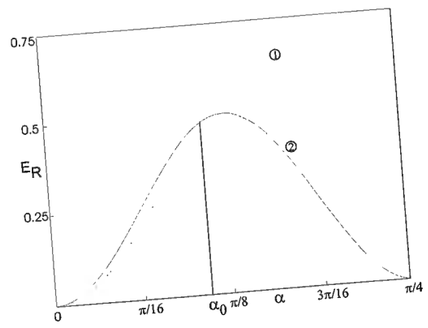

Figure 4.1: Rènyi entanglement for the local maximally entangled input state (1) and for the product state $|01\rangle$ (2)

4.2.4 Conclusions

We have determined the separable pure two–qubit states which have to be used in order to create as much entanglement as possible by applying a general two–qubit gate. Furthermore, we have shown which unitary operators are able to create a maximally entangled state. For all the other unitary operators we have given the maximal amount of entanglement which can be created by them [Eq.(4.35)]. Thus, the results derived in this section characterize arbitrary two qubit interactions in terms of the entanglement which they can produce. Furthermore we have shown that by using ancillas one has to specify which is the measure of entanglement to be maximized. We have given two examples of unitary operations for which it is possible to determine the maximal amount of some particular measure of entanglement.

Note that the derivations presented in this section have been useful for many other instances. They have been generalized to the case where the initial state is entangled (see [103]). Using the decomposition presented in Eq. (4.16), it was shown in Ref. [17] that any entangling two–qubit gate, assisted by one–qubit gates is universal for quantum computation. In Ref. [42] the optimal conversion of unitary operators was studied. In this paper it was shown, using (4.16), that there exist two classes of non–local two–qubit gates. It was demonstrated how the representatives of these classes can be deterministically converted into any operation of its class. In Ref. [148] the interaction cost of non–local gates, that is the minimal time of interaction required to perform the gate when assisting the process with fast local unitaries, was analyzed. In this case the decomposition of two–qubit gates presented here [(4.16)] was used to derive an analytic expression for

the interaction cost of any two–qubit unitary operation given any coupling Hamiltonian. In Ref. [147] the catalysis of non–local operations was studied. In particular, it was shown, using the decomposition (4.16), that and how entanglement can be used, without being consumed, to accomplish unitary operations that could not be performed without it. In [126] the thermalization process, which is the relaxation towards the thermal equilibrium of a system which is in contact with a reservoir was considered. A model in which the system is a qubit and reaches equilibrium after several successive two–qubit interactions, which are called thermalizing machines, with the reservoir was considered. The decomposition of two–qubit gates (4.16) was used to characterize the thermalizing quantum machines.

In Ref. [43] the following method of entanglement creation as studied. Two qubits are interacting with each other via some non–local Hamiltonian. The physical setup is such that it is possible to apply *fast* local operations to each of the qubits. The aim is to produce as much entanglement as possible starting from some initially entangled state. From the analysis it becomes clear why these intermediate local operations (which are itself not able to create entanglement) will increase the entanglement production. It was shown [43] that the optimal way to create entanglement is to increase at each infinitesimal time step the produced entanglement maximally. That is, the best method to create entanglement is to maximize at each point the entanglement rate[12]. In other words we have $E_{\max}(t) \equiv \int_{t_0}^{t} dt \Gamma_{E(t)}$, where $\Gamma_{E(t)}$ is the maximal rate produced by the interaction starting with some pure state, $|\Psi\rangle$ with entanglement E. In that paper it was shown that the optimal amount of entanglement included in the initial state[13] is independent of the interaction Hamiltonian. It was shown that the maximal amount of created entanglement can be written as a product of a function depending only on the choice of the entanglement measure and a function which depends on the Hamiltonian. Since the dependence of the Hamiltonian occurs only in this function it is called the *entanglement capability* of the Hamiltonian. The authors also determined the optimal input state. Depending on the considered experiment, i.e. if it is possible to apply fast local operations, or rather a fixed quantum gate is given, as we analyzed in Sec. 4.2, one has to choose the optimal way to create entanglement.

[12] In Chapter 5 we consider a similar situation for continuous variable systems. Note that there it is not true that the optimal method to create entanglement is to maximize at each time step, δt, the created entanglement (the entanglement rate).

[13] Recall that it is always possible to transform a pure two qubit state by local unitary operations to any other having the same amount of entanglement. Since in the setup considered here it is possible to apply local unitary operations at each time step, the relevant quantity here is the initial entanglement.

Chapter 5

Operators acting on an infinite dimensional Hilbert space (Gaussian operators)

In contrast to the previous chapter we consider here operators acting on an infinite dimensional Hilbert space. In particular, this chapter deals with Gaussian operations (Sec. 2.2) [98]. We consider two–mode pure Gaussian states and interaction Hamiltonians which preserve the Gaussian character and analyze the dynamics of entanglement and squeezing [98]. As we explain below, the problems studied here are all motivated by the experimental situation in which light gets entangled with an atomic ensemble via a Kerr–like interaction [100, 113, 119, 33]. We expect that the techniques developed in this chapter can be easily extended to address other related problems, like the one of entangling two atomic ensembles using light.

First of all we show which Hamiltonians can be simulated using a given interaction and how to do so optimally (Sec. 5.1). We also show which conditions have to be fulfilled in order to generate a general Gaussian operation. In Sec. 5.2.1 we determine the optimal rate of entanglement generation as well as of squeezing generation for arbitrary input states (Sec. 5.2). Finally, in Sec. 5.2.2 we give an optimal entanglement generation scheme for finite times, starting out from a product (unsqueezed) state.

Setup

We consider a continuous variable system composed of two one–mode systems coupled via some interaction Hamiltonian. The goal is to analyze which kind of evolutions we can achieve with such an interaction if certain instantaneous local operations can be applied at will. In particular, we study

optimal methods of creating or increasing the entanglement shared by the two modes.

The interaction Hamiltonian has the general form

$$H = aX_1X_2 + bP_1P_2 + cP_1X_2 + dX_1P_2 \tag{5.1}$$

where a, b, c and d are real parameters, and $X_{1,2}$ and $P_{1,2}$ are canonical operators for the first and second mode, respectively [1]. We use dimensionless units throughout this chapter. We assume that local operations, generated by the Hamiltonians

$$H_{\mathrm{loc},i} = g(X_i^2 + P_i^2), \tag{5.2}$$

can be applied instantaneously, where g is a real number that can be tuned at will [1]. These operations can neither change the entanglement nor the squeezing present in the state. Lastly, we assume that the initial state is pure and Gaussian.

Our choice of the Hamiltonian interaction as well as the instantaneous local operations is motivated by current experiments with atomic ensembles [128, 87, 101, 66]. In particular, to those set-ups in which an atomic ensemble interacts with two modes of the electromagnetic field [2] with different polarizations [100, 102, 35, 32]. If the atoms are sufficiently polarized along some given direction (say x) we can replace the total angular momentum operators describing the internal state of the atoms by canonical operators. That is (if the involved levels have spin $\pm 1/2$), $S_y \to X_1/\sqrt{N/2}$, $S_z \to P_1/\sqrt{N/2}$, $S_x \to N/2$, with $[X_1, P_1] \simeq i$ ($\hbar = 1$), and where N is the number of atoms. This approximation is valid as long as $|\langle S_x\rangle - N/2| \leq o(\sqrt{N})$ for all times [2]. Similarly, if the electromagnetic field is sufficiently polarized along some direction, we can substitute the Stokes operators by canonical ones, X_2 and P_2 [127].

For some atomic structures and off-resonant interactions, the Hamiltonian describing the interaction between the atomic ensemble and the light can be written as [100]

$$H_0 = aX_1X_2, \tag{5.3}$$

which is a particular case of Eq. (5.1); in the following we will put the coupling constant $a = 1$ when referring to H_0. In the same scenario, simple and fast local operations can be performed on the atoms and the electromagnetic field. For example, a magnetic field or a polarizer gives rise to the local

[1] Note that the Hamiltonians that we are considering here are not semi-bounded. However, this is not a problem since we are always considering initial states and times for which the real Hamiltonian can be locally approximated by these Hamiltonians.

[2] This is the case if the atomic ensemble is embedded in a ring cavity, for example. Note that for optically thick samples, the description may also be valid in free space.

Hamiltonians Eq. (5.2). Since the interaction between atoms and light is typically weak, with moderate magnetic fields the operations generated locally can be regarded as instantaneous. On the other hand, if the atoms and the light are completely polarized, the corresponding state in terms of our continuous variable description is the tensor product of two vacuum states, in particular it is a pure Gaussian state.

We emphasize that even though we have motivated our choices with some particular physical set-up, our description is applicable to other physical situations and our results apply to the general interaction Hamiltonian Eq. (5.1).

We consider the following general *strategy* for state or gate engineering which can be realized using the tools described above. Starting with a pure initial state, described by the density operator $\rho(0)$, we perform fast local operations $V_0 \otimes W_0$ on the state and we then let H act on it for a time t_1. Then we perform again local rotations, $V_1 \otimes W_1$ followed by the non–local interaction generated by H for a time t_2 and so on until $\sum_k t_k = t$. This yields to the total time-evolution operator

$$\mathcal{U}(t) = [V_n \otimes W_n]U(t_n)\cdots U(t_2)[V_1 \otimes W_1]U(t_1)[V_0 \otimes W_0], \qquad (5.4)$$

so that $\rho(t) = \mathcal{U}(t)\rho(0)\mathcal{U}(t)^\dagger$. Here $U(t) = e^{-iHt}$.

First, we want to analyze which $\mathcal{U}$ are achievable with this strategy. Second, for a given $\rho(0)$ we look for the best choice of n, $\{t_1, \ldots, t_n\}$, and the local operations $\{V_1 \otimes W_1, \ldots, V_n \otimes W_n\}$ in order to maximize the created entanglement/squeezing. We consider two different regimes. First, we choose $\sum_k t_k = \delta t \ll \tau(H)$ (the characteristic time of the interaction) so that we can expand all the U as well as $\mathcal{U}(t)$ in lowest order in t_k. Second, we choose t_k finite. In the following we refer to those two regimes as infinitesimal and finite respectively.

5.1 Simulation of interactions

In this section we characterize all the unitary evolutions which we can generate within the given setup. That is we define the set of unitary operators which can be written as (5.4). In the infinitesimal regime the problem is usually called *Hamiltonian simulation* , whereas for t finite it is usually called *gate simulation* .

The first part of this section is devoted to the infinitesimal regime, where we will in general derive the necessary and sufficient conditions for Hamiltonian simulation. In the second part we are concerned with the finite time regime. There we show that with (almost) any Hamiltonian H as in Eq. (5.1)

and the local operations corresponding to the Hamiltonians given in (5.2) it is possible to generate any unitary gate.

5.1.1 Hamiltonian simulation

Given two Hamiltonians H and H' of the form (5.1) we want to see the conditions under which H can simulate H'. That is, for a given sufficiently small t' we want to find out if it is possible to have

$$e^{-iH't'} = [V_n \otimes W_n]e^{-iHt_n}\cdots e^{-iHt_2}[V_1 \otimes W_1]e^{-iHt_1}[V_0 \otimes W_0]. \qquad (5.5)$$

with t_k small as well. If it is possible to choose $t \equiv \sum_k t_k = t'$ we say that H can simulate H' *efficiently.*

A central result in the theory of Hamiltonian simulation [8] states that an alternating sequence of manipulations and interactions as given in (5.5) is equivalent to a fictitious free evolution due to a certain effective Hamiltonian H_{eff}, i.e. produces a unitary transformation

$$\mathcal{U} = e^{-iH_{\text{eff}}t'}$$

and

$$\kappa H_{\text{eff}} = \sum_{i=1}^{n} p_k \left(\widetilde{V}_i^\dagger \otimes \widetilde{W}_i^\dagger\right) H \left(\widetilde{V}_i \otimes \widetilde{W}_i\right) \qquad (5.6)$$

where $\kappa := t'/t$, $t := \sum_{i=1}^n t_i$, the $p_k := t_k/t$ form a probability distribution and the $\widetilde{V}_i \otimes \widetilde{W}_i$ follow uniquely from the interspersed control operations $V_j \otimes W_j$ (and vice versa). Obviously one can in this way *simulate* an evolution due to a Hamiltonian H_{eff} by means of a given Hamiltonian H.

Eq. (5.6) has a clear interpretation: A protocol proceeding in infinitesimal time steps yields a mean Hamiltonian which is a weighted sum of locally transformed variants of the original Hamiltonian H. The so-called *simulation factor* κ is the ratio of simulated time t' and time of simulation t and, therefore, is a measure for the efficiency of the simulation. The case $\kappa \geq 1$ corresponds to the *efficient simulation.*

Necessary and sufficient condition

Concerning the bilinear interaction Hamiltonians, it is convenient to rewrite the Hamiltonian of Eq. (5.1) as follows [see Eq. (2.9)]

$$H = (X_1, P_1)K\begin{pmatrix} X_2 \\ P_2 \end{pmatrix} \quad \text{where} \quad K = \begin{pmatrix} a & d \\ c & b \end{pmatrix}. \qquad (5.7)$$

The action of a local rotation $V(\varphi) = \exp[-i(X^2+P^2)\varphi/2]$ on the canonical operators X and P can be expressed by

$$V\begin{pmatrix} X \\ P \end{pmatrix} V^\dagger = \bar{R}\begin{pmatrix} X \\ P \end{pmatrix} \quad \text{where}$$
$$\bar{R} = R(\varphi) = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \in SO(2,\mathbb{R}). \tag{5.8}$$

Thus we can associate to all local rotations V_i, W_i (5.2) real orthogonal 2×2 matrices $\bar{R}, \bar{S}\ldots$ with determinant $+1$. Consequently we have

$$(V\otimes W)\, H\, (V^\dagger \otimes W^\dagger) = (X_1, P_1)\bar{R}^T K \bar{S}\begin{pmatrix} X_2 \\ P_2 \end{pmatrix}. \tag{5.9}$$

Furthermore we use that for any matrix K as given in (5.7) there exists a singular value decomposition $K = OD\tilde{O}$ where $O, \tilde{O} \in O(2,\mathbb{R})$, $D = \mathrm{diag}(\sigma_1, \sigma_2)$ and the singular values $\sigma_1 \geq \sigma_2 \geq 0$ of K are unique. If we restrict ourselves on *special* orthogonal matrices we can still find matrices $R, S \in SO(2,\mathbb{R})$ such that

$$K = R\begin{pmatrix} s_1 & 0 \\ 0 & s_2 \end{pmatrix} S \tag{5.10}$$

and $s_1 = \sigma_1$, $s_2 = \mathrm{sign}[\det(K)]\sigma_2$ [3]. Without loss of generality we may always assume that

$$s_1 \geq |s_2|\,. \tag{5.11}$$

Then these two values are uniquely defined. As mentioned already, we call them the restricted singular values of K.

Assume now we want to simulate, in the above sense, some Hamiltonian H' by means of some other Hamiltonian H, both of the form (5.7). Let s_1, s_2 and s_1', s_2' denote their respective restricted singular values. Then we have the following result:

H can efficiently simulate H' iff

$$\begin{aligned} s_1 + s_2 &\geq s_1' + s_2' \\ s_1 - s_2 &\geq s_1' - s_2'. \end{aligned} \tag{5.12}$$

The proof is elementary but requires some effort in notation such that we postpone it to App. C.1.

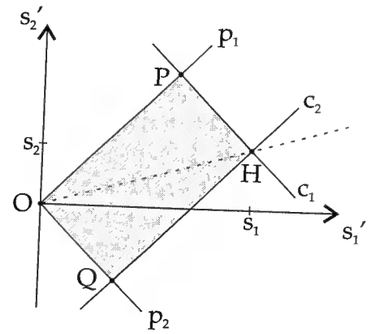

Figure 5.1: Illustration of the accessible region in the (s_1', s_2')-plane for the case $s_2 > 0$. Coordinates of relevant points: $H = (s_1, s_2)$, $P = \frac{s_1+s_2}{2}(1,1)$, $Q = \frac{s_1-s_2}{2}(1,-1)$. See text for explanation.

Discussion

Since the number of relevant parameters characterizing an interaction Hamiltonian is two, one can nicely illustrate the above result: The Fig. 5.1 illustrates the following geometrical relations: Point $H = (s_1, s_2)$ denotes the original general Hamiltonian. Lines p_1 and p_2 indicate the boundaries where $s_1' = \pm s_2'$ respectively and are due to premise $s_1' \geq |s_2'|$. Lines c_1 and c_2 stem respectively from the first and second inequality constituting the necessary and sufficient condition. The region of accessible Hamiltonians, i.e. points $H' = (s_1', s_2')$ is thus contained in the rectangle $OPHQ$. One can even visualize how this set deepens with increasing time of simulation by parameterizing $H(t) = (s_1 t, s_2 t)$. Thus, H moves outward on the dashed line while P and Q move on p_1 and p_2 respectively. It is therefore just a matter of time to reach any point in the quadrant enclosed by p_1 and p_2.

It is also quite instructive to consider certain special cases: (i) For $s_2 = s_1$ ($s_2 = -s_1$) the dashed line coincides with p_1 (p_2), respectively. This is a trivial case where we are confined to simulate locally equivalent variants of the original Hamiltonian (see App. C.1). Therefore, Hamiltonians whose restricted singular values are of equal modulus are nearly useless for the purpose of Hamiltonian simulation. (ii) For $s_2 = 0$ or, equivalently, $\det(K) = 0$ the picture gets symmetric with respect to the s_1'-axis. This symmetrization can be interpreted in terms of time efficiencies, as we shall explain in the following.

[3] (see footnote [3] on p. 38).

Based on the criterion above one can ask for time efficiencies and especially for *time optimal protocols*. Time optimal simulation is achieved if the simulation factor $\kappa = t'/t$ [see Eq. (5.6)] gets maximal. Without loss of generality we set $t' = 1$ such that $\kappa = 1/t$. Given now H and H' with restricted singular values s_1, s_2 and s_1', s_2' we can determine the minimal time of simulation as $t_{\min} := \min_t\{t : (s_1+s_2)t \geq (s_1'+s_2'), (s_1-s_2)t \geq (s_1'-s_2')\}$. We find

$$t_{\min} = \begin{cases} \frac{s_1'+s_2'}{s_1+s_2} & \text{if} \quad \frac{s_2'}{s_1'} \geq \frac{s_2}{s_1} \\ \frac{s_1'-s_2'}{s_1-s_2} & \text{if} \quad \frac{s_2'}{s_1'} < \frac{s_2}{s_1} \end{cases}. \tag{5.13}$$

Thus the efficiency of simulation depends strongly on whether $\text{sign}(s_2') = \text{sign}(s_2)$ or not, the last case being more time consuming. Only when $s_2 = 0$ [case (ii) above] it is equally expensive (in terms of costs of interaction time) to simulate either kind of Hamiltonians H' [$\text{sign}(s_2') \lesseqgtr 0$], a fact which is reflected in the above mentioned symmetrization. Correspondingly, the optimal time of simulation or, so to say, the *minimal interaction costs* [148] are in this case uniquely determined by

$$t_{\min} = (s_1' + |s_2'|)/s_1. \tag{5.14}$$

Application to X_1X_2-interaction

Let us outline some conclusions out of this result for the interaction $H = X_1X_2$. The restricted singular values of H are $s_1 = 1$ and $s_2 = 0$. Therefore we can efficiently ($\kappa = 1$, i.e. $t' = t$) implement all Hamiltonians H' whose restricted singular values fulfill

$$s_1' + |s_2'| \leq 1. \tag{5.15}$$

As an example as well as to give a basis for further results we shall consider here two kinds of well known unitary transformations: the *beam-splitter* operator

$$U_{\text{bs}}(t) := e^{-iH_{\text{bs}}t} \quad \text{where} \quad H_{\text{bs}} = X_1P_2 - P_1X_2 \tag{5.16}$$

and the *two-mode squeezer*

$$U_{\text{tms}}(t) := e^{-iH_{\text{tms}}t} \quad \text{where} \quad H_{\text{tms}} = X_1X_2 - P_1P_2. \tag{5.17}$$

The action of $U_{\text{bs}}(\pi/2)$ corresponds to swapping the states of the first and the second mode, i.e. it transforms $X_1, P_1 \to -X_2, -P_2$ and $X_2, P_2 \to X_1, P_1$. Note that the global phase thereby acquired by subsystem 1 can be corrected locally.

Application of $U_{\text{tms}}(t)$ squeezes the EPR modes $(X_1 + X_2)$ and $(P_1 - P_2)$ by a factor e^{-2t} and therefore also entangles the two systems, as we shall see.

In order to perform these operations by means of the X_1X_2-interaction we have to determine the restricted singular values of H_{bs} and H_{tms}. One finds for H_{bs} $s_1 = 1, s_2 = 1$ and for H_{tms} $s_1 = 1, s_2 = -1$. Since in both cases condition (5.15) is not met we cannot *efficiently* simulate these Hamiltonians. But nevertheless we can determine strategies for infinitesimal simulations being time optimal. The minimal time of simulation can be calculated using (5.14) and yields a maximal simulation factor $\kappa = 1/t_{\min} = 1/2$ for both, the beam-splitter and the squeezer. Thus, in order to implement $U_{\text{bs}}(t')$ we need at least a time $t = 2t'$ and to create squeezing by a factor $e^{-2t'}$ it will take a time $2t'$, i.e. to implement $U_{\text{tms}}(t')$ we need a time $t = 2t'$. Explicit simulation protocols can be constructed following App. C.1.

In summary, defining the matrices K and K' as in Eq. (5.7), as well as their respective restricted singular values $s_{1,2}$ and $s_{1,2}'$, we found the following results: (i) The Hamiltonian H can efficiently simulate H' if and only if

$$s_1 + s_2 \geq s_1' + s_2' \quad \text{and} \quad s_1 - s_2 \geq s_1' - s_2', \tag{5.18}$$

(ii) If it is not possible to simulate H' efficiently with H, then the minimal time needed to simulate the evolution corresponding to H' for the time t' is $t_{\min} := \min_t\{t : (s_1 + s_2)t \geq (s_1' + s_2')t', (s_1 - s_2)t \geq (s_1' - s_2')t'\}$.
Thus except for the cases $s_1 = \pm s_2$ every Hamiltonian of the form (5.1) can simulate all other Hamiltonians of that form (including the $s_1' = \pm s_2'$ case). In particular, with the Hamiltonian H_0 describing the atom-light interaction one can simulate every bilinear Hamiltonian (5.1) and can do so efficiently as long as $|s_1'| + |s_2'| \leq 1$. In this case, the interaction existing in the physical setup can be considered universal.

5.1.2 Gate simulation and state engineering

Until now we have focused on the regime of infinitesimal times in order to clarify which *unitary evolutions* we can simulate by means of the given interaction. We found that we can do so – more or less efficiently – for all evolutions governed by Hamiltonians of the form (5.7), but no more. This leaves open the question which *unitary operations* can in general, i.e., for finite times, be realized with a given interaction and local rotations.

As we show in the following, any interaction described by some Hamiltonian H where $s_1 \neq |s_2|$ together with local rotations is sufficient to realize *any unitary operation* of the form $\exp(iG)$, where G is a quadratic expression in the operators $\{X_1, P_1, X_2, P_2\}$. That is, any Gaussian unitary transformation of the two modes can be obtained. This implies, that any desired pure

Gaussian state can be "engineered" starting from any given (pure Gaussian) input state. In particular, the Hamiltonian H_0 allows to generate all unitary linear operations, which shows that $H, H_{\mathrm{loc},i}$ generate a set of universal linear gates for continuous variables smaller than the one given in Ref. [110].

As we show in App. C.2, any $U = \exp(-iG)$ can be decomposed as

$$\begin{aligned} U &= (V_5 \otimes W_5)\, U_{\mathrm{bs}}(t_5)\, (V_4 \otimes W_4) \times \\ &\quad \times U_{\mathrm{tms}}(t_4)\, (V_3 \otimes W_3)\, U_{\mathrm{bs}}(t_3)\, (V_2 \otimes W_2)\, U_{\mathrm{tms}}(t_2) \times \\ &\quad \times (V_1 \otimes W_1)\, U_{\mathrm{bs}}(t_1)\, (V_0 \otimes W_0)\,, \end{aligned} \tag{5.19}$$

where all $(V_i \otimes W_i)$ are local rotations, $U_{\mathrm{bs}}(t_i)$ is a beam-splitter and $U_{\mathrm{tms}}(t_i)$ a two-mode squeezing operation as defined in Eqs. (5.16) and (5.17). Since all Hamiltonians with $s_1 \neq |s_2|$ can be used to simulate beam-splitters and two-mode squeezers one can reach any desired unitary U and therefore also any desired Gaussian state.

Let us analyze some important applications of these results in the case of atomic ensembles interacting with light. They imply that with current experiments with atomic ensembles one can generate all unitary linear operations, as well as arbitrary Gaussian states. In particular, one can generate local squeezing operators for which $\tilde{H} = X_1^2 - P_1^2$ [which are not included among the Hamiltonians of the form (5.1) and therefore cannot be simulated infinitesimally by any of them] and therefore one can generate squeezing in the atomic system, light system or both independently (without performing measurements). On the other hand, one can use H_0 to generate the swap operator, which (in the Heisenberg picture) transforms

$$X_1 \leftrightarrow X_2, \quad P_1 \leftrightarrow P_2. \tag{5.20}$$

This operation can be generated in a finite time. Thus, one can use the interaction H_0 to realize a perfect interface between light and atoms, which allows to use the atomic ensemble as a quantum memory for light, as opposed to the case in Ref. [128] where this result is obtained in the limit of very strong interaction.

5.2 Creation of entanglement and squeezing

The problem that we consider now can be stated as follows. Let us assume that we have some initial pure two–mode Gaussian state and we have some

interaction described by the general Hamiltonian (5.1) and the local operations (5.2) at our disposal. We want to know how entanglement/squeezing can be created in an optimal way. We use the results derived in the previous section to find the optimal strategies both in the infinitesimal and finite regime.

Since all the Hamiltonians we are considering are at most quadratic in X and P, an initial Gaussian state will be Gaussian at all times (Sec. 2.2.1). Recall that this means that we can always fully describe it by its correlation matrix (CM) γ, with $\gamma_{kl} = 2\mathrm{Re}\{\mathrm{tr}[\rho(R_k - d_k)(R_l - d_l)]\}$ and its displacement d, with $d_k = \mathrm{tr}(\rho R_k)$, where $\vec{R} = (X_1, P_1, X_2, P_2)^T$ (Sec. 1.3).

As explained in Sec. 1.3.1 the displacements are of no importance concerning the entanglement and squeezing properties of the states and can be made zero by local displacement operations, which can be easily implemented in our physical set-up. Therefore we take $d_k = 0$ and are only concerned with the CM γ.

We will either use the block form (1.35)

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \tag{5.21}$$

with 2×2 matrices A, B, C or the pure standard form[4] (1.37)

$$\gamma = (S_1 \oplus S_2) \begin{pmatrix} \cosh(r)\mathbb{1} & \sinh(r)\sigma_z \\ \sinh(r)\sigma_z & \cosh(r)\mathbb{1} \end{pmatrix} (S_1^T \oplus S_2^T). \tag{5.22}$$

Recall that the matrix A (B) in (5.21) corresponds to the first (second) system and C, describing the correlations between both systems and vanishes for product states. Let us also recall here that $S_{1,2}$ [Eq. (5.22)] are local symplectic matrices and contain only the information about local squeezing. The two–mode squeezing parameter r contains all information about the non–local properties of the state.

As shown in Sec. 2.2.1 the CM evolves due to the interaction (5.1) according to $\gamma(t) = S(t)\gamma S(t)^T$, where $S(t) = e^{MT}$, with

$$M = \begin{pmatrix} 0 & L \\ \tilde{L} & 0 \end{pmatrix}, \tag{5.23}$$

with

$$L = \begin{pmatrix} c & b \\ -a & -d \end{pmatrix} = J^T K, \text{ and } \tilde{L} = -JL^T J^T = J^T K^T. \tag{5.24}$$

[4] Since all the states and operations we consider here are pure, γ corresponds always to a two–mode pure state. This is why we can write it at any step of our analysis as (5.22).

Note that for $0 \neq -\det(L) =: \alpha$ we have $\tilde{L} = \alpha L^{-1}$. As shown in Sec. 2.2.1 the symplectic matrix, $S(t)$ can be re–expressed as

$$S(t) = \cosh(\sqrt{\alpha}t)\mathbb{1} + \sinh(\sqrt{\alpha}t)/\sqrt{\alpha}M. \tag{5.25}$$

We can also write it in its standard form (2.14)

$$S(t) = \cosh(\sqrt{\alpha}t)(O_1 \oplus O_2) \begin{pmatrix} 1 & 0 & h_1 & 0 \\ 0 & 1 & 0 & -h_2 \\ h_2 & 0 & 1 & 0 \\ 0 & -h_1 & 0 & 1 \end{pmatrix} (O_1 \oplus O_2)^T, \tag{5.26}$$

where $O_1, O_2 \in SO(2,\mathbb{R})$ perform the restricted singular value decomposition of L, and $h_k = \tanh(\sqrt{\alpha}t)/\sqrt{\alpha}s_k$, where s_k are the restricted singular values of L, which coincide with those of K.

For the infinitesimal case, i.e., the evolution corresponding to $S(\delta t)$ for an infinitesimally short time step δt, we have

$$S(\delta t) = \mathbb{1} + \delta t M, \tag{5.27}$$

and the correlation matrix $\gamma(t)$ transforms to first order as

$$\gamma(t+\delta t) = \gamma(t) + \delta t[M\gamma(t) + \gamma(t)M^T]. \tag{5.28}$$

5.2.1 Optimal entanglement/squeezing rates

The goal of this section is to determine the optimal strategy for the generation of entanglement [squeezing] in an (infinitesimally) small time step δt. That is, given a pure Gaussian state ρ with CM γ and an interaction Hamiltonian H as in Eq. (5.1) we look for the best choice of the local rotations $V \otimes W$ such that $e^{-iH\delta t}(V \otimes W)\rho(V \otimes W)^\dagger e^{iH\delta t}$ is as entangled [squeezed] as possible. Stating this problem mathematically: We maximize the *entanglement [squeezing] rate*, that is the time-derivative of the chosen entanglement [squeezing] measures E [$\mathcal{S}$] under the time-evolutions obtainable in the given setting.

Entanglement rate

Given some entanglement measure E (Sec. 1.3.1). We use the obvious notation $E(t) \equiv E[\gamma(t)]$ when considering the time-evolution of E. Then, mathematically the goal is to maximize the *entanglement rate* [43]

$$\frac{dE}{dt} = \lim_{\delta t \to 0} \frac{E(t+\delta t) - E(t)}{\delta t}. \tag{5.29}$$

Since for the case of two modes in a pure state there is a single parameter that describes the entanglement [cf. Eq. (5.22)] all entanglement measures are monotonically dependent on each other (see also Sec. 1.3.1). This means that maximizing the rate (with respect to the evolution) corresponding to some measure of entanglement, say f is equivalent to maximize the rate corresponding to the von Neumann entropy of the reduced state (the canonical measure of entanglement for pure states, also called Entropy of Entanglement), E[5] (Sec. 1.3.1).

Let us choose the two–mode squeezing parameter r defined in (5.22), $E_0(\gamma) = r$ as measure of entanglement. In fact, E_0 is the log-negativity (see Sec. 1.3.1, [150]) of the Gaussian state. The entanglement rate is then simply given by

$$\Gamma_E = \left.\frac{dE_0}{dt}\right|_{t=0} = \lim_{\delta t \to 0} \frac{r(\delta t) - r}{\delta t}, \tag{5.30}$$

where $r \equiv r(0)$ is the entanglement of the initial CM γ.

In order to determine Γ_E we use the formula $\Gamma_{E_p} = \sinh(2r)\Gamma_E = 2\sqrt{-\det(A)\det(C)}\Gamma_E$, where Γ_{E_p} denotes the entanglement rate corresponding to the purity-related measure $E_p(\gamma) = \cosh(r)^2$ (Sec. 1.3.1).

Let H as in Eq. (5.7) be the given Hamiltonian. It generates an evolution given by the symplectic transformation $\bar{S}(\delta t)$, which we write in its standard form (5.26) as $\bar{S}(\delta t) := (\bar{O}_1 \oplus \bar{O}_2)S(\delta t)(\bar{O}_1 \oplus \bar{O}_2)^T$. Since local operations cannot increase the entanglement the only way in which the local control operations may help is to rotate the state by $\tilde{O}_1 \oplus \tilde{O}_2$ before applying H. Thus the best strategy yields a $\gamma(\delta t)$ that can be written as

$$\gamma(\delta t) = S(\delta t)(O_1 \oplus O_2)\gamma(O_1 \oplus O_2)^T S(\delta t)^T, \tag{5.31}$$

where we defined $O_i := \bar{O}_i^T \tilde{O}_i$ and omitted the irrelevant final local rotations coming from $\bar{S}(\delta t)$. Writing $\gamma(\delta t)$ in the form (5.21) and using Eq. (5.28) it is straight forward to determine the CM corresponding to the reduced state,

$$A(\delta t) = O_1 A O_1^T + \delta t(L_0 O_2 C^T O_1^T + \text{H.c.}), \tag{5.32}$$

where $L_0 = \text{diag}(s_2, -s_1)$ is determined by the Hamiltonian H, cf. Eq. (5.26) and Eq. (5.23). One quickly sees that $\det[A(\delta t)] = \det(A)[1 +$

[5] This can be seen as follows. For pure Gaussian states, as given in Eq. (5.22), $E(|\psi\rangle) = \cosh(r/2)^2 \log[\cosh(r/2)^2] - \sinh(r/2)^2 \log[\sinh(r/2)^2]$ [143]. Consider now any function $f(r)$ such that $E(f)$ is a monotonic function of f. Then we have $\max_H \left(\frac{dE}{dt}\right)\big|_{t_0} = \max_H[\left(\frac{dE}{df}\right)\big|_{t_0}\left(\frac{df}{dt}\right)\big|_{t_0}] = \left(\frac{dE}{df}\right)\big|_{t_0} \max_H \left(\frac{df}{dt}\right)\big|_{t_0}$. Since E is a monotonic function we have that $\left(\frac{dE}{df}\right)\big|_{t_0} > 0$, which implies that maximizing $\left(\frac{dE}{dt}\right)\big|_{t_0}$ with respect to the evolution is equivalent to maximize $\left(\frac{df}{dt}\right)\big|_{t_0}$ with respect to the evolution.

$2\delta t\,\mathrm{tr}(L_0 O_2 C^T A^{-1} O_1^T)]$, where we used the simple relation for 2×2 matrices: $\det(X+\delta t Y) = \det(X)[1+\delta t\,\mathrm{tr}(X^{-1}Y)] + o(\delta t^2)$ and the fact that A is symmetric and invertible.

For the entanglement rate corresponding to E_p we obtain $\Gamma_{E_p} = 2\det(A)\mathrm{tr}(L_0 O_2 C^T A^{-1} O_1^T)$. As mentioned before, we can from this easily determine the rate Γ_E corresponding to the two-mode squeezing parameter namely we have

$$\Gamma_E = \sqrt{\frac{\det(A)}{-\det(C)}}\mathrm{tr}(L_0 O_2 C^T A^{-1} O_1^T) = \mathrm{tr}(L_0 O_2 Y O_1^T), \tag{5.33}$$

where we have defined $Y := \sqrt{\det(A)/[-\det(C)]}C^T A^{-1}$.

Our aim is to maximize this expression with respect to the special orthogonal matrices O_1 and O_2. Note that $\det Y = -1$, which can be easily verified using Eq. (5.22). Therefore Y has the restricted singular values $e^l, -e^{-l}, l \geq 0$. Using that L_0 is diagonal it is straight forward to verify that the maximum of Eq. (5.33) is achieved when choosing O_1, O_2 such that they diagonalize Y such that $O_2 Y O_1^T = \mathrm{diag}(e^l, -e^{-l})$ yielding

$$\Gamma_{E,\mathrm{opt}}[\gamma(t), H] = s_1 e^l - s_2 e^{-l}. \tag{5.34}$$

The optimal choice for $\tilde{O}_i$ is

$$\tilde{O}_{i,\mathrm{opt}} = \bar{O}_i O_i, \tag{5.35}$$

with $\bar{O}_i$ given by $\bar{S}(\delta t)$. The best state to let H act on is thus $\gamma_{\mathrm{opt}} = (\tilde{O}_{1,\mathrm{opt}} \oplus \tilde{O}_{2,\mathrm{opt}})\gamma(\tilde{O}_{1,\mathrm{opt}} \oplus \tilde{O}_{2,\mathrm{opt}})^T$. Note that l which determines the singular values of Y can be easily determined by [6]

$$\begin{aligned}\cosh(2l) &= \frac{\det(A)}{-2\det(C)}\mathrm{tr}(A^{-2}CC^T) \\ &= \frac{1}{2}\mathrm{tr}[(S_1^T S_1)^{-1}\sigma_z S_2^T S_2 \sigma_z].\end{aligned} \tag{5.36}$$

Note that there is no divergence as $\det C \to 0$ as is seen by the second expression in Eq. (5.36).

[6] Note that the S_k's in Eq. (5.22) are uniquely defined only if γ is not a product state (i.e., iff $C \neq 0$), cf. [56] Given a product state with CM $\tilde{S}_1\tilde{S}_1^T \oplus \tilde{S}_2\tilde{S}_2^T$, the S_k are defined only up to local rotations $S_k = \tilde{S}_k O_k$. These O_k can be chosen such that $O_1(S_1^T S_1)O_1^T = \mathrm{diag}(\sigma_{1-}, \sigma_{1+})$ and $O_2(S_2^T S_2)O_2^T = \mathrm{diag}(\sigma_{2+}, \sigma_{2-})$, where $\sigma_{k+} = e^{r_k} \geq \sigma_{k-} = e^{-r_k}, r_k > 0$ are the singular values of $S_k^T S_k$. This local operation achieves the maximum $\cosh(r_1 + r_2)$ for the RHS in Eq. (5.36) as given by von Neumann's trace theorem [69].

Thus we see that the entanglement rate depends on the initial local squeezing of the two modes as well as the angle between the two locally squeezed quadratures, but it does not depend on the entanglement of the state. Rewriting $\Gamma_{E,\mathrm{opt}}$ as $(s_1 - s_2)\cosh l + (s_1 + s_2)\sinh l$ we see that some Hamiltonians can produce entanglement even if there is no local squeezing present in the state (which implies that $l = 0$), while others (notably the beam splitter with $s_1 = s_2 = 1$) cannot.

Note that the rate goes to infinity as local squeezing is increased, in contrast to the case of qubits. Given a CM γ, there are typically local rotations that enhance the entanglement rate.

From these results we conclude that if the goal is to create as much entanglement as possible it is more efficient to squeeze the state locally first (if possible) before using the interaction; in particular, the use of squeezed light [102] is advantageous compared to coherent light [35].

In summary, given an interaction Hamiltonian H corresponding to a matrix K and an initial state with CM γ the optimal state preparation by local rotations (before letting H act) can be understood as a two-step procedure. First transform γ locally such that $C^T A^{-1}$ is diagonal [restricted singular value decomposition, cf. Eq. (5.10)]. If K was already in its restricted singular value decomposition, we are done. Otherwise the second step of the state preparation can be viewed (in the Heisenberg picture) as the restricted singular value decomposition of K. Then the optimal entanglement rate (entanglement is measured by E_0) is given by Eq. (5.34) in terms of the singular values s_k of the Hamiltonian matrix K and the local squeezing parameter l of the given state γ.

In the Fig. 5.2 we compare the entanglement rates and the entanglement obtained for different strategies using the "natural Hamiltonian" H_0. As initial state we consider the product of the vacuum state in the first system and the squeezed vacuum in the second system, i.e.,

$$\gamma_{\mathrm{in}} = \mathbb{1}_2 \oplus \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}, \tag{5.37}$$

with squeezing parameter $r = 2.5$. We compare the strategy in which the rate of entanglement creation is optimized at each time to two simpler ones, namely to just apply the natural Hamiltonian H_0 or to simulate the two-mode squeezing Hamiltonian $H_{\mathrm{tms}} = X_1 X_2 - P_1 P_2$ using the optimal scheme of Sec. 5.1. The rate-optimization strategy leads in fact to a combination of the other two: one applies first the natural Hamiltonian for a finite time and then (when the "local squeezing" l has all been converted to two-mode squeezing) one simulates H_{tms}. Having initially local squeezing available

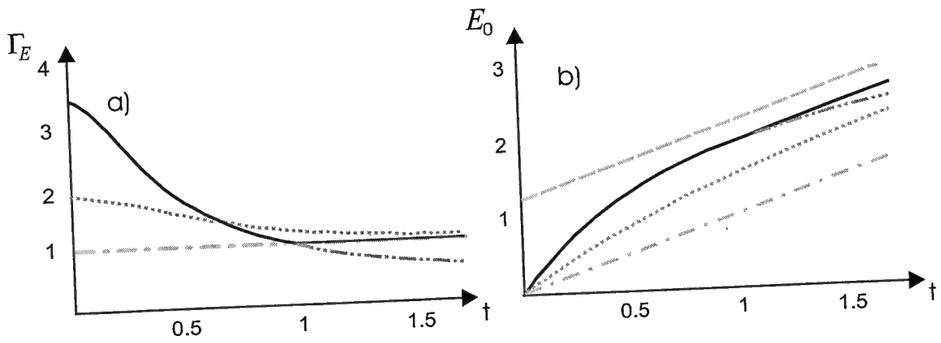

Figure 5.2: (a) The entanglement rate obtained for the squeezed state γ_{in} (5.37) as initial state and various strategies. The solid line represents the optimal-rate strategy derived in this section; the dotted line represents the rate obtained by simulating the two-mode squeezing Hamiltonian H_{tms}; the "dot–dot–dashed" line represents the rate obtained for the natural Hamiltonian $H_0 = X_1 X_2$. For the vacuum state as initial state we obtain the constant rate 1 (dashed line) (b) The entanglement created by the different strategies [same styles as in a) for the different scenarios]. The dashed line represents the upper bound Eq. (5.48).

clearly helps with entanglement generation: for an initial unsqueezed state the optimal rate is constant $\Gamma_E = 1$.

Fig. 5.2b shows that the optimization strategy can lead to noticeably more entanglement in the resulting state after finite time: when the entanglement rate is optimized at each point, more entanglement is produced than, e.g., with the interactions H_0 or H_{tms}. However, optimizing the rate is in general not the best strategy for the creation of entanglement, see Fig. 5.3.

Squeezing rate

As in the previous section we are given an interaction Hamiltonian of the form (5.1), an initial Gaussian state with CM γ, and we consider the case of infinitesimal interactions. Our goal is here to determine for each H and γ the strategy which maximizes the squeezing rate. We measure squeezing by $Q(\gamma) = \log[\mathcal{S}(\gamma)]$, where $\mathcal{S}$ was defined in Eq. (1.42) as the inverse of the

smallest eigenvalue of γ. The rate we are interested in is

$$\begin{aligned} \Gamma_S &= \frac{d}{dt} \log \mathcal{S}[\gamma(t)]\Big|_{t=0} \\ &= \frac{-1}{\lambda_{\min}(\gamma)} \lim_{\delta t \to 0} \frac{\lambda_{\min}[\gamma(\delta t)] - \lambda_{\min}(\gamma)}{\delta t}. \end{aligned} \tag{5.38}$$

Note that using the logarithm of $\mathcal{S}$ instead of $\mathcal{S}$ simplifies the formulas but since log is a monotonic function, maximizing the rate of $\log \mathcal{S}$ implies a maximal rate for $\mathcal{S}$ as well [7].

After applying the general strategy to the input state with CM γ we obtain $\gamma(\delta t)$ as in Eq. (5.28). Doing first order perturbation theory we find for the smallest eigenvalue $\lambda_{\min}[\gamma(\delta t)] = \lambda_{\min}(\gamma) + \delta t \hat{x}^T (M^T \gamma + \gamma M)\hat{x} = \lambda_{\min}[1 + \delta t \hat{x}^T (M^T + M)\hat{x}]$, where $\hat{x}$ is the normalized eigenvector corresponding to the smallest eigenvalue $\lambda_{\min}(\gamma)$ of γ. We obtain for the squeezing rate:

$$\Gamma_S = \frac{-1}{\lambda_{\min}(\gamma)} [\hat{x}^T (M^T + M)\hat{x}], \tag{5.39}$$

which is maximized when $-\hat{x}^T (M^T + M)\hat{x}$ is as large as possible. Note that

$$M^T + M \equiv \begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}, \tag{5.40}$$

where $N = \tilde{L} + L^T = J^T K^T + K^T J$, where J is the $SO(2)$–matrix of Eq. (1.27) and we have used the definitions (5.24) and (5.7). One quickly sees that $N = N^T$. Writing K in its restricted singular value decomposition $K = SK_0R$, where $S, R \in SO(2, \mathbb{R})$ and $K_0 = \text{diag}(s_1, s_2)$ as in Eq. (5.10), and using that R, S commute with J we see that $N = R^T (J^T K_0 + K_0 J) S^T = C_S(H) R^T J^T \sigma_z S^T$, where

$$C_S(H) = s_1 - s_2. \tag{5.41}$$

Note that the matrix $\tilde{O} := R^T J^T \sigma_z S^T$ is orthogonal with $\det(\tilde{O}) = -1$ and that we can obtain any such $\tilde{O}$ choosing $R, S \in SO(2, \mathbb{R})$, i.e., by the local operations applied to the initial state. Using the notation $\hat{x}^T = (\vec{x}_1^T, \vec{x}_2^T)$, where $\vec{x}_1, \vec{x}_2 \in \mathbb{R}^2$, we find $\Gamma_S = 2C_S(H)\vec{x}_1^T \tilde{O} \vec{x}_2 \leq 2C_S(H) \max_{\tilde{O}} |\vec{x}_1^T \tilde{O} \vec{x}_2| = 2C_S(H)\|\vec{x}_1\|\|\vec{x}_2\|$, which gives an upper bound

$$\Gamma_S \leq 2C_S(H)\|\vec{x}_1\|\|\vec{x}_2\|$$

[7] Note that this can be shown in exactly the same way as we showed that the entanglement rate can be maximized with respect to the evolution according to any measure of entanglement (see footnote [5] on p. 75).

for Γ_S. This maximum can be reached for $\tilde{O}_{\rm opt}$ such that $(-\tilde{O}_{\rm opt}\vec{x}_2)||\vec{x}_1$. Given γ (i.e., $\vec{x}_1, \vec{x}_2$) we can calculate $\tilde{O}_{\rm opt}$ with $\det \tilde{O}_{\rm opt} = -1$ which satisfies this condition. This then determines the optimal choice of $R, S \in SO(2,\mathbb{R})$, i.e. how to transform the initial state with CM γ before letting H act in order to maximize the squeezing rate. One simple choice yielding $\tilde{O} = \tilde{O}_{\rm opt}$ is $S = \mathbb{1}$, i.e. nothing has to be done on the second system and $R_{\rm opt} = J^T\sigma_z\tilde{O}^T_{\rm opt} \in SO(\mathbb{R},2)$. Thus, the optimal input state is given by $\gamma_{\rm opt} = (R^T_{\rm opt}\oplus\mathbb{1})\gamma(R_{\rm opt}\oplus\mathbb{1})$.

Summarizing this part, we found for the optimal squeezing rate:

$$\left.\frac{dS}{dt}\right|_{\rm opt} = \left.\frac{dS}{dQ}\right|_{Q(t)} g_S[\gamma(t)]C_S(H). \tag{5.42}$$

$C_S(H) = s_1 - s_2$ with s_i's are the restricted singular values of K (5.7), the only function which depends on H, is the *squeezing capability* of the Hamiltonian H, and

$$g_S(\gamma) = 2\|\vec{x}_1\|\|\vec{x}_2\| \leq 1, \tag{5.43}$$

quantifies how "squeezable" the state γ is by interactions of the type (5.1). Here $\hat{x}^T = (\vec{x}_1, \vec{x}_2)$, with $\vec{x}_1, \vec{x}_2 \in \mathbb{R}^2$ is the normalized eigenvector corresponding to the minimal eigenvalue of $\gamma(t)$.

The optimal CM to let H act on is $\gamma_{\rm opt} = (R^T_{\rm opt}\oplus\mathbb{1})\gamma(R_{\rm opt}\oplus\mathbb{1})$, where

$$R_{\rm opt} = J^T\sigma_z\tilde{O}^T \tag{5.44}$$

and $-\tilde{O}_{\rm opt}$ parallelizes $\vec{x}_1$ and $\vec{x}_2$. Note that the fact that $\hat{x}$ is normalized implies that $\Gamma_S \leq C_S(H)$ for any input state. Since we look at the logarithm of the squeezing this implies that $\frac{dS(\gamma)}{dt} \leq \mathcal{S}(\gamma)C_S(H)$.

5.2.2 Optimal entanglement generation from the vacuum state

Now we consider the situation in which we start with both modes in the vacuum state and we have a Hamiltonian H for a finite time (as well as instantaneous local operations). Since in practice, we are interested in creating the largest amount of entanglement when H acts for a *finite* total time t. Optimizing the rate of entanglement creation Sec. 5.2.1 at each time does lead to a local but not necessarily, as we saw, the global maximum of the entanglement at time t [94].

We now show how to employ the interaction H to create the most entanglement in a given time t. To this end, we make use of the squeezing of γ which was introduced in Eq. (1.42) as the inverse of the smallest eigenvalue

of γ. The squeezing of γ is known [154] to give an upper bound for the amount of entanglement of γ, with $\mathcal{N}(\gamma) \leq \mathcal{S}(\gamma)$, with $\mathcal{N}(\gamma)$ the negativity, given in (1.43). We proceed as follows: First we calculate the strongest squeezing that can be achieved after time t. This also gives an upper bound for the entanglement that can be obtained during this time. Then we point out a strategy that achieves the optimal squeezing and at the same time the strongest entanglement compatible with the given squeezing, thus being optimal on both counts.

The squeezing capability of a symplectic map S, i.e., the factor by which the squeezing in a CM can be increased by the application of S, is given by the inverse square of the smallest singular value of S, since $\mathcal{S}(S\gamma S^T) \leq [\sigma_{\rm min}(S)]^{-2}\mathcal{S}(\gamma)$. Here and in the following we use that for the smallest singular value of a product AB we have $\sigma_{\rm min}(AB) \geq \sigma_{\rm min}(A)\sigma_{\rm min}(B)$. Now consider the symplectic map $S(t)$ corresponding to the unitary evolution generated by an interaction Hamiltonian H after time t, cf. Eq. (5.25). The singular values of $S(t)$ can easily be calculated analytically. We need them only for small times to first order in t, in which case we find:

$$\sigma_\pm[S(t)] = \sqrt{1 \pm \frac{1}{2}(s_1 - s_2)t + o(t)^2}, \tag{5.45}$$

where s_1, s_2 are the restricted singular values of the matrix K [cf. Eq. (5.7)] corresponding to H.

Since $S(t) = S(t/2)S(t/2) = \Pi_{k=1}^N S(t/N)$ we see immediately that $(\sigma_{\rm min}[S(t)])^2 \geq e^{-(s_1-s_2)t}$, which implies that the squeezing capability of $S(t)$ is bounded by $e^{(s_1-s_2)t}$. Now consider a strategy as in Eq. (5.4), alternating the use of H for time t_k with local rotations $V_k \otimes W_k$. Note that the $t_k, k = 1, \ldots, N$, which sum to t, are not assumed to be infinitesimal. The time-evolution effected by this strategy is described by a symplectic map

$$S(t) = \Pi_k \tilde{S}_k, \tag{5.46}$$

where $\tilde{S}_k = O_k S(t_k) O'_k$ and O_k, O'_k are the local rotations corresponding to $V_k \otimes W_k$. Clearly, $\sigma_{\rm min}[S(t)] \geq \Pi_k e^{-(s_1-s_2)t_k/2} = e^{-(s_1-s_2)t/2}$. Hence $\mathcal{S}[S(t)S(t)^T] \leq e^{(s_1-s_2)t}$, i.e. we have an upper bound to the amount of squeezing that can be produced from an initially unsqueezed pure state by applying H for a total time t.

A strategy to achieve this optimum is the following: we choose the local rotations V_k, W_k as $\pi/2$-rotation in system 1 and $3\pi/2$ in system 2, the times t_k all equal, and consider the limit $t_k \to 0$. This corresponds to the situation considered in Sec. 5.1 and simulates the Hamiltonian related to $K' = (K + JKJ)/2$. Let $K = O_1\,\mathrm{diag}(s_1, s_2)O_2$, then we have

that $K' = 1/2\, O_1[\mathrm{diag}(s_1, s_2) + \mathrm{diag}(-s_2, -s_1)]O_2$, since rotations commute with J. That is, apart from local rotations the strategy, which simulates the two-mode squeezing Hamiltonian with an efficiency $(s_1 - s_2)/2$, which is the optimal factor according to Eq. (5.13). Letting H_{tms} act for a time $t' = t(s_1 - s_2)/2$ (using up an interaction time t) transforms the vacuum state into the two-mode squeezed state with CM

$$\gamma_{\mathrm{tms}}(t') = \begin{pmatrix} \cosh 2t'\mathbb{1} & \sinh 2t'\sigma_z \\ \sinh 2t'\sigma_z & \cosh 2t'\mathbb{1} \end{pmatrix}. \tag{5.47}$$

which saturates the bounds derived above, since $\mathcal{S}[\gamma_{\mathrm{tms}}(t')] = e^{(s_1-s_2)t}$.

Now we show that γ_{tms} in Eq. (5.47) is also the most entangled state that can be obtained after letting H act for a total time t. Using Eq. (1.43) for the negativity of a Gaussian state with CM $\gamma = S(t)S(t)^T$ (i.e. an arbitrary strategy applied to the vacuum state) we get

$$\mathcal{N}(\gamma) = [\mathcal{S}(J^T\tilde{\gamma}J\tilde{\gamma})]^{-1/2} \leq \mathcal{S}(\tilde{\gamma}) = \mathcal{S}(\gamma) = e^{(s_1-s_2)t}.$$

Since $\mathcal{N}[\gamma_{\mathrm{tms}}(t')] = e^{(s_1-s_2)t}$ the simulation of two-mode squeezing is the optimal strategy for both squeezing and entanglement generation. Note that even a rough approximation of the optimal strategy, i.e., a strategy consisting of just two or three steps already yields a marked improvement in generated squeezing and entanglement.

Up till now we have only considered the unitary evolution of the initial state. There are, however, further tools available in current experiments. There might be additional light modes (ancillas) in the vacuum state on which passive linear optical operations (described by orthogonal and symplectic transformations) as well as complete or partial homodyne measurements can be performed. In principle these might help to increase the entanglement in γ, but in the following we show that this is not the case. We consider the following general set-up: consider system with CM γ, ancilla systems in vacuum state i.e., $\gamma_{\mathrm{anc}} = \mathbb{1}$, linear passive interactions (described by a symplectic and orthogonal matrix O) between the system light mode and the ancillas (e.g. beam splitter between light and ancillary modes), such that the whole system is described by the CM $\gamma' = O^T(\gamma \oplus \gamma_{\mathrm{anc}})O$; clearly, $\mathcal{S}(\gamma') = \mathcal{S}(\gamma)$ and now we show that a Gaussian measurement does not increase $\mathcal{S}(\gamma)$: We write γ' as

$$\gamma' = \begin{pmatrix} A' & C' \\ C'^T & B' \end{pmatrix},$$

where the block matrix B' refers to the ancillary modes to be measured. Then the resulting state is described by the CM $\gamma_{\mathrm{out}} = A' - C'B'^{-1}C'^T$ [59]. Using

the following characterization of the smallest eigenvalues [68] it is straight forward to see that the measurement has reduced the squeezing of the state:

$$\begin{aligned} \mathcal{S}(\gamma_{out}) &= \min_{x\in\mathbb{C}^n}\left\{\frac{x^\dagger(A' - C'B'^{-1}C'^T)x}{x^\dagger x}\right\}^{-1} \\ &\leq \min_x\left\{\frac{x^\dagger(A' - C'B'^{-1}C'^T)x}{x^\dagger(\mathbb{1} + C'B'^{-2}C'^T)x}\right\}^{-1} \\ &= \min_x\left\{\frac{y^\dagger\gamma' y}{y^\dagger y} : y = \begin{pmatrix} x \\ -B'^{-1}C'^T x \end{pmatrix}\right\}^{-1} \\ &\leq \min_{y\in\mathbb{C}^{2n}}\left\{\frac{y^\dagger\gamma' y}{y^\dagger y}\right\} = \mathcal{S}(\gamma') \quad \blacksquare \end{aligned}$$

Consequently, unsqueezed ancilla systems and Gaussian measurements are of no help in increasing the squeezing or entanglement in a Gaussian state.

The preceding discussion does not completely solve the problem of optimal entanglement generation with a Hamiltonian H, since only one particular initial state (the vacuum) has been considered. If, e.g., the initial state of the light field is squeezed, we have seen in Sec. 5.2.1 that better rates can be achieved (see Fig. 5.2), which will translate into larger entanglement after finite times. The methods used above easily yield an upper bound for the entanglement that can be obtained from initially squeezed states: Consider an initial product state with squeezing e^{r_1} and e^{r_2} in systems 1 and 2 and let $r_1 \geq r_2$. By the same arguments as above, after H has acted for a time t the squeezing in the final state and the negativity are bounded by $e^{(s_1-s_2)t+r_1}$. We can find a better bound on the achievable entanglement drawing on results from Ref. [154], where it was shown that the negativity of a two-mode CM γ is bounded by $1/\sqrt{\lambda_1\lambda_2}$, where λ_1, λ_2 are the two smallest eigenvalues of the γ. This implies that

$$\mathcal{N}(\gamma_{\mathrm{out}}) \leq e^{(s_1-s_2)t+(r_1+r_2)/2}, \tag{5.48}$$

which yields the dashed curve in Fig. 5.2b. This bound is most probably not tight for $r_k \neq 0$, not even as $t \to \infty$.

One might think that in order to optimize the entanglement after some finite time t it always suffices to optimize the rate at each time as for the case of a vacuum input. For qubit systems this was indeed shown to be true [43]. In contrast, it does not hold for CV systems as the counterexample depicted in Fig. 5.3 shows: We start with a slightly entangled state with CM $\gamma_{\mathrm{in},2}$ which can be obtained from the two-mode squeezed state $\gamma_{\mathrm{tms}}(t_0/2)$ squeezing both X_1 and X_2 by $r_1 = r_2$. Then the "local squeezing parameter" l is zero and the optimal rate therefore $\Gamma_E = 1$. If t_0 is small and r_1, r_2 large

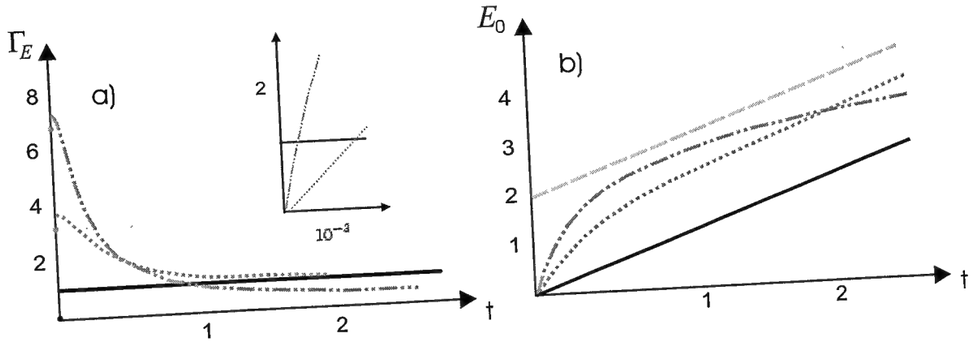

Figure 5.3: (a) The entanglement rate obtained for the initial state $\gamma_{\text{in},2} = S_{r_1,r_2}\gamma_{\text{tms}}(t_0/2)S^T_{r_1,r_2}$, where $S_{r_1,r_2} = \text{diag}(e^{r_1/2}, e^{-r_1/2}, e^{r_2/2}, e^{-r_2/2})$ and $r_1 = r_2 = 2, t_0 = 10^{-3}$. The solid line $\Gamma_E = 1$ is obtained with the strategy that optimizes the entanglement rate at each time; the dotted line represents the rate obtained for optimal simulation of H_{tms}; the "dot–dot–dashed" line represents the rate obtained for the natural Hamiltonian $H_0 = X_1X_2$. The inset shows that one has to "pay" with initial entanglement rates smaller than the optimal value of 1 to reach a state that allows for the large rates later on. (b) The entanglement created by the different strategies [same styles for different scenarios as in a)] and the upper bound Eq. (5.48).

it is possible to sacrifice some entanglement in order to "activate" the local squeezing thus enhancing the rate later on and obtaining significantly more entanglement at time $t \gg t_0$.

The difference to the qubit case is related to the fact that in the CV context not all local transformations are available and hence not all equally entangled states are locally equivalent.

In summary, we show that the optimal way to create entanglement in the finite regime is to apply local instantaneous operations flipping the X and P variables of both systems periodically after small times Δt. After a finite time t (and for $\Delta t \to 0$) this produces (up to local rotations) a two-mode squeezed state, which is both optimally squeezed and entangled. In particular, $Q(t) = (s_1 - s_2)t$ and $E_0(t) = (s_1 - s_2)t$.

We also show that it is not possible to increase the entanglement using Gaussian measurements during the evolution. We consider a system with CM γ and ancilla systems in vacuum state. We allow for linear passive interactions (described by a symplectic and orthogonal matrix O) between one system and the ancillas and show that a Gaussian measurement does

neither increase the squeezing nor the entanglement. This result implies that our method is optimal even if we allow for feedback, something which has been recently considered in the context of spin squeezing generation [141, 12].

For the case of atomic ensembles our result implies that there is a method to improve the entanglement generation in present experiments [66].

5.3 Discussion and conclusion

We have investigated how a quadratic interaction between two continuous variable systems (as it occurs naturally in certain quantum optical systems) can be optimally used to perform several quantum information tasks when certain simple local control operations (phase space rotations) can be implemented as well. First we have given necessary and sufficient conditions for the simulation of a Hamiltonian evolution given a fixed interaction and fast local rotations. In particular, we have shown that the naturally occurring Hamiltonian Eq. (5.3) allows to simulate all bilinear Hamiltonians and is in fact of the most versatile kind for this purpose. Moreover we have seen that almost all the Hamiltonians of the form (5.1) (and in particular H_0) allow to generate all symplectic transformations on two modes, i.e., the complete group $SP(2,\mathbb{R})$ can be generated starting from no more than the three Hamiltonians $H_0, H_{\text{loc},1}, H_{\text{loc},2}$.

With these results we have addressed the questions of optimal creation of entanglement and squeezing for a two–mode Gaussian state using a given interaction of the form (5.1) and local rotations of the form $H_{\text{loc},i} = g(X_i^2 + P_i^2)$, both of which are available in current experiments. For the case of small (infinitesimal) interaction times, we have determined the optimal strategy to increase entanglement or squeezing for any input state, i.e, we have derived the maximal entanglement and squeezing rates and determined the strategies which lead to these maxima. For the general case (finite interaction time) we have derived the optimal strategy for the creation of entanglement and squeezing starting with the vacuum state. We have also shown that (in contrast to qubit systems) for continuous variables optimizing the entanglement rate is not necessarily the best way to generate a finite amount of entanglement.

There are several interesting applications of our results for quantum information processing. In particular, we have seen that the beam splitter Hamiltonian $H_{\text{bs}} = X_1P_2 - P_1X_2$ can be simulated with an efficiency factor $1/2$ by H_0. When acting for a time $t = \pi$ the Hamiltonian H_{bs} generates the swap operation between the systems 1 and 2, thus performing the "write-in" and "read-out" operations needed when the atomic ensemble is to be used

as a *quantum memory* for the state of the light mode [93].

Another interesting application for atomic ensembles is enabled by the so-called spin-squeezed states [92] which have been prepared experimentally in settings similar to the one described in this section [66, 101]. It has been shown that these states allow for a significant increase in the precision of atomic clocks [135]. While the methods presented above show efficient ways to create squeezed atomic states (e.g., by using the interaction to create squeezing or entanglement optimally and then project the atoms into a pure squeezed state by measuring the light), it would also be interesting to find the *optimal* such procedure.

Note that the argument in Sec. 5.2.2 is easily adapted to similar circumstances. E.g., it was shown in Ref. [135] that the interaction between the atoms of a suitably prepared Bose-Einstein–condensate (BEC) can be described by the quadratic Hamiltonian $J_z^2 \approx P^2$, which can be used to drive the BEC into a spin squeezed state. By the same reasoning as in Sec. 5.2.2 we see that after an interaction time t a squeezing of e^t is the maximum achievable. This shows optimality of the procedure suggested in Ref. [135] (which employs effectively the so-called "two-axes counter-twisting" Hamiltonian).

In summary, we have investigated the capabilities of CV interaction Hamiltonians H. We have shown which other Hamiltonians can be simulated with such an H and the available control operations and how to do so efficiently. Then we have derived the optimal entanglement generation rates achievable with this Hamiltonian and given an optimal protocol for the generation of entanglement between the two modes for finite times.

Part III

Entanglement properties of quantum states

Chapter 6

Introduction

Apart from having fundamental implications [116], such as Bell's theorem or the existence of decoherence, entanglement is in the realm of several practical applications of Quantum Information [28]. An entangled state can be used for instance, to teleport a state of a particle to another particle [6], which is spatially separated from it. It was also shown how to use entangled states to send secret messages from one place to another [49]. In most of those proposals one needs pure maximally entangled states. In reality, however, the states which are produced in the laboratories are, due to the interaction with the environment, mixed. Despite of its importance, the entanglement properties of systems are far from being understood. In particular, we do not even know how to solve the following question: given two systems A and B in a state described by a density operator ρ, are those systems entangled? This question constitutes the so–called separability problem, and it represents one of the most important theoretical challenges of the emerging theory of Quantum Information.

Another important problem in Quantum Information Theory is to decide whether several copies of a state can locally be transformed into a maximally entangled state. This problem is known as the distillation problem. A similar problem is the one of activation of entanglement. There the spatially separated parties use some PPTES in order to distill the entanglement.

Recently increasing attention was paid to infinite dimensional systems, the so-called continuous quantum variables (CV). This interest was sparked mainly by the experimental realization of CV quantum teleportation [142, 15, 54]. Quantum Information with CV in general is mainly concerned with the family of Gaussian states, since these comprise essentially all the experimentally realizable CV states. Gaussian states occur in current experiments using linear optics.

In this chapter we investigate the entanglement properties of quantum

states, for both, the finite dimensional and the infinite dimensional case. The first part of this chapter is devoted to the separability problem. We derive necessary as well as sufficient conditions for separability of density operators acting on a finite dimensional Hilbert space [95, 106, 107]. For bipartite Gaussian states we derive a computable necessary and sufficient condition for separability [57]. In the three–partite, in particular the $1 \times 1 \times N$ case, we derive criterions which classify the states according to their separability properties [58]. In the last part of this chapter we analyze the distillability problem for multipartite systems [97]. We present a formalism which allows to connect the problem of distillation and activation to the one of entanglement witnesses.

Chapter 7

The separability problem

A significant amount of work in the field of Quantum Information Theory has been devoted to the separability problem during the last few years (see Sec. 1.2.1, Sec. 1.3, and for instance [31, 122, 74, 25, 115, 89, 46, 104] and references therein). One of the important tools to study this problem is partial transposition [118] (Sec. 1.2.1 and Sec. 1.3.1). It provides us with a necessary condition for a density operator to be separable. This condition turns out to be sufficient as well for two particular cases: (a) A and B are two qubits or one qubit and one qutrit [71]; (b) A and B are two modes in a Gaussian state [34, 133]. Thus, in these two cases the separability problem can be fully solved. However, for higher dimensional systems as well as in the case in which A and B consist of several modes in a joint Gaussian state, partial transposition alone does not provide a general criterion for separability. In both cases, examples of states which despite of being entangled satisfy the partial transposition criterion have been provided [75, 11, 153].

When going from two to more parties, current knowledge is even more limited. A classification of N-partite mixed states according to their separability properties has been given in Ref. [39, 40] (see also Sec. 1.2.1). But even for three qubits there is currently no general way to decide to which of these classes a given state belongs (see however [1, 39, 40]).

In this section we study several different methods for solving the separability problem. First of all we consider density operators acting on a finite dimensional Hilbert space. On the one hand, we derive necessary and sufficient conditions of separability for low and medium rank density operators supported on $\mathbb{C}^2 \otimes \mathbb{C}^N$ [95]. The idea is to subtract product vectors from the range of ρ keeping it and its partial transpose positive. On the other hand, we investigate entanglement witnesses (EWs), i.e. operators which allow us to distinguish between separable and entangled states, and the corresponding positive maps (Sec. 1.2.1). We study how to optimize EW, that is how to

construct out of a given EW one which detects the presence of entanglement in an optimal way. As an application of all those developed methods we investigate the separability properties of symmetric states, i.e. states which are invariant under exchanging particles. As another application we study three–qubit states. We construct three–partite edge PPTES.

The second part of this chapter is devoted to the separability problem of density operators describing a continuous variable system. We will derive a necessary and sufficient criterion of separability for all bipartite Gaussian states, which is easy to compute. On the other hand, we study the case of three spatially separated modes. In this case there are many possibilities for the modes to be entangled to each other. We will characterize all three–mode Gaussian states according to their separability properties ([39, 40]). Furthermore we give necessary and sufficient conditions for a state to belong to one class or the other. Again the conditions are simple to compute. We will also show that none of the classes is empty by providing examples for each of them. Using the separability criterion for the bipartite case we show how to generalize these results to the $1 \times 1 \times N$ case.

7.1 Finite dimensional Hilbert space

We study two different methods of solving the separability problem. On the one hand, we analyze the separability properties of density operators acting on $\mathbb{C}^2 \otimes \mathbb{C}^N$. There we use the method of subtracting projectors onto product vectors in order to derive necessary and sufficient conditions for low rank density operators and sufficient conditions for a general density operator. On the other hand, we use the approach of entanglement witnesses and positive maps to address the problem of separability for arbitrary states in a finite dimensional Hilbert space. We prove that an EW is non–decomposable iff it detects a PPTES. Furthermore, we show how to construct out of an arbitrary EW an optimal one. As we will see, for analyzing the separability properties of density operators we only need to characterize optimal EW.

7.1.1 $\mathbb{C}^2 \otimes \mathbb{C}^N$ composite quantum systems

As explained before, when studying the separability problem we can restrict ourselves to PPT states. The reason for this is that any NPPT state is entangled. In this section we analyze the separability properties of PPT state supported on $\mathbb{C}^2 \otimes \mathbb{C}^N$. The results derived here are based on the method of subtracting product vectors, developed in Ref. [108, 125, 146]. The idea of subtracting product vectors has been proven to be very useful to

determine a number of separability properties in the multiqubit case [39]. It allowed: i) to define unique optimal decomposition of mixed states in Hilbert space of arbitrary dimensions into a sum of separable and inseparable part; ii) to find minimal decompositions into product vectors of separable density operators acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$ (two qubits), and iii) to define a measure of entanglement in those systems.

In the present section, by studying the conditions under which we can subtract product vectors from ρ while keeping ρ and its partial transpose positive, we are able to find necessary and sufficient conditions for separability for low and medium rank density operators. We also give a sufficient condition for separability for general density operators. In particular we show in this section that if the rank of ρ equals N then it is separable, and that bound entangled states have rank larger than N. We also give a separability criterion for a generic density operator such that the sum of its rank and the one of its partial transpose does not exceed $3N$. If it exceeds this number we show that one can subtract product vectors until decreasing it to $3N$, while keeping the positivity of ρ and its partial transpose. This automatically gives us a sufficient criterion for separability for general density operators. We also prove that all density operators that remain invariant after partial transposition with respect to the first system are separable. This last result displays the difference between the $2 \times N$ case (systems composed of a 2–level and a N–level subsystem) and the general $M \times N$ one ($N, M > 2$), where it has been found that there are operators satisfying this condition which are not separable [11, 29, 140, 9].

The structure of this section is the following: First of all we give the definitions that we use throughout this section. Then we derive a series of lemmas concerning product vectors. First, we recover the results given in Ref. [108, 125, 146] concerning the conditions under which one can subtract product vectors from a density operator. We then give a separability criterion for the case in which there is a finite set of product vectors that can be subtracted. Next we show that if there are product vectors in the kernel of ρ, then the problem of separability can be highly simplified. Finally, we analyze under which conditions there exist product vectors in subspaces (e.g. the kernel and the range of ρ), and show that the problem reduces to finding the roots of complex polynomials. The section "Results" contains most of the results of this work concerning separability. We first show that one just has to consider the cases in which the rank of ρ is larger or equal than N. When the rank of ρ is equal to N (and ρ is not trivially supported on a smaller subsystem of B) then it is separable. From this result follows that bound entangled states have a rank larger than N. We continue by analyzing the case in which the sum of the ranks of ρ and its partial transpose is smaller

than $3N$, giving a necessary and sufficient separability criterion for generic density operators and for $N \leq 10$. After that, we show how in the general case one can reduce the problem to that situation. Then, we prove that if ρ is equal to its partial transpose with respect to the first subsystem, then it is separable. The same statement holds when ρ is "sufficiently close" to its partial transpose (in the sense of operator norm, for instance). Finally, we illustrate our results by analyzing the case 2×4.

Definitions and notation

We consider a density operator $\rho \geq 0$ acting on $\mathbb{C}^2 \otimes \mathbb{C}^N$. We wish to find out conditions such that we can state whether ρ is separable or not, that is (Sec. 1.2.1), whether it can be written as

$$\rho = \sum_i |e_i, f_i\rangle\langle e_i, f_i|, \tag{7.1}$$

where $|e_i, f_i\rangle \equiv |e_i\rangle_A \otimes |f_i\rangle_B$ are unnormalized product states. Throughout this section we will make use of the fact that a necessary condition for separability is that the partial transposition of ρ is a positive operator [118]. $K(X), R(X), k(X)$, and $r(X)$ denote the kernel, range, dimension of the kernel, and rank of the operator X, respectively. By $|e^*\rangle$ we will denote the complex conjugated vector of $|e\rangle$ in the basis $|0\rangle_A, |1\rangle_A$ in which we perform the partial transposition; that is, if $|e\rangle = \alpha|0\rangle + \beta|1\rangle$ then $|e^*\rangle = \alpha^*|0\rangle + \beta^*|1\rangle$. The subscript "$r$" will be used to denote real vectors; that is $|e_r\rangle = |e_r^*\rangle$. We will denote by $|\hat{e}\rangle$ the vector which is orthogonal to $|e\rangle$. On the other hand, we will make use of property (1.15),

$${}_A\langle e_i|\rho|e_j\rangle_A = {}_A\langle e_j^*|\rho^{T_A}|e_i^*\rangle_A \tag{7.2}$$

for any pair $|e_i\rangle, |e_j\rangle \in \mathbb{C}^2$. Note that if ρ is separable [cf (7.1)], then

$$\rho^{T_A} = \sum_i |e_i^*, f_i\rangle\langle e_i^*, f_i|, \tag{7.3}$$

is also separable; the opposite is clearly also true.

We say that ρ acting on $\mathbb{C}^2 \otimes \mathbb{C}^N$ is supported in $\mathbb{C}^2 \otimes \mathbb{C}^M$ if the minimal subspace $H \subseteq \mathbb{C}^N$ such that $R(\rho) \subseteq \mathbb{C}^2 \otimes H$ has dimension M. This means that there exist $N - M$ (and not more) linearly independent vectors $\{|f_i\rangle, i = 1, 2, \ldots, N - M\} \in \mathbb{C}^N$ such that $|e, f_i\rangle \in K(\rho)$ for all $|e\rangle \in \mathbb{C}^2$. The utility of this definition can be seen in the following example. Let us consider an operator ρ acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$. We can always trivially regard this operator as acting on a higher dimensional space (e.g., $\mathbb{C}^2 \otimes \mathbb{C}^4$) but giving zero

whenever it acts outside the original space. If we are studying the separability properties of ρ it is useful to get rid of the spurious dimensions and really consider ρ as acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$. Thus, we will concentrate on operators not only acting, but also supported on $\mathbb{C}^2 \otimes \mathbb{C}^N$.

The method we use to find separability conditions is based on subtracting product vectors from ρ in such a way that both ρ and ρ^{T_A} remain positive. If we are able to subtract several of those product vectors until we achieve that the result vanishes, then we will have obtained that ρ is separable. Thus, a crucial point is to find the conditions under which we can find such product vectors. In the next few sections we will determine those conditions.

Product vectors

As mentioned above, our procedure to study separability is based on subtracting product vectors $|e, f\rangle$ from the density operator ρ in such a way that the resulting operator and its partial transpose remain positive. Thus, we have to determine under which conditions this is possible. This section deals with that problem. We have divided it in three parts:

(i) Properties related to the existence of product vectors in the range of ρ or ρ^{T_A};

(ii) Properties related to the existence of product vectors in the kernel of ρ or ρ^{T_A};

(iii) Existence of product vectors in subspaces. In the first subsection we derive some useful properties of a density operator whenever there are product vectors in its range.

In particular, we will recover the results of Ref. [108, 125, 146] which state that we can only subtract product vectors of ρ that belong to its range, and that by subtracting the right amount we can always decrease its rank. Then we will show that if we have a set of product vectors in the range of ρ and another related set in the range of ρ^{T_A}, then ρ is separable iff it can be written as a mixture of those vectors. This means that if we can find all the product vectors satisfying these conditions, then we can check whether ρ is separable or not by using only those vectors. In the second subsection we will derive some other properties of ρ whenever there are product vectors in its kernel. In particular we will show that in that case one can subtract one product vector and not only reduce the rank of ρ, but also reduce the problem to finding whether a related density operator supported on $\mathbb{C}^2 \otimes \mathbb{C}^{N-1}$ is separable. This means that the product vectors in the kernel play a very important role

since they allow to simplify the problem of separability. Finally, in the last subsection we will derive the conditions needed to have product vectors in subspaces; in particular in the kernel and the range of ρ and ρ^{T_A}. We will see that in order to find them, one has to solve some complex polynomial equations. The solutions to those equations determine which are the product vectors that can be subtracted from ρ, which, together with the results of the first subsection, allow us to analyze the separability of certain density operators, as it will be shown in the next section.

Range of ρ

We have divided this subsection in two: In the first one we introduce a lemma which gives the conditions under which the difference of two positive operators is a positive operator itself. This allows us to recover in a simple way the results given in Ref. [108, 125, 146] regarding subtracting product vectors from ρ. In the second one we show that the set of (common) product vectors in the ranges of ρ and ρ^{T_A} suffices to study the separability properties of ρ.

Subtracting product vectors

We use the operator norm, namely $\|A\| = \max_{\||\phi\rangle\|=1} \|A|\phi\rangle\|$. For a given hermitian operator X we will denote by X^{-1} its pseudoinverse; that is, if the spectral decomposition of $X = \sum_k X_k |x_k\rangle\langle x_k|$ with $X_k \neq 0$, then $X^{-1} = \sum_k X_k^{-1} |x_k\rangle\langle x_k|$.

Lemma 7.1 *Given two hermitian operators $X, Y \geq 0$ then $X - Y \geq 0$ iff $K(X) \subseteq K(Y)$ and $\|Y^{\frac{1}{2}} X^{-\frac{1}{2}}\|^2 \leq 1$.*

Proof: (if) We can write an arbitrary vector $|\Psi\rangle = |\Psi^r\rangle + |\Psi^k\rangle$, where $|\Psi^r\rangle \in R(X)$ and $|\Psi^k\rangle \in K(X) \subseteq K(Y)$. Therefore $\langle\Psi|X - Y|\Psi\rangle = \langle\Psi^r|X - Y|\Psi^r\rangle$. Since $|\Psi^r\rangle \in R(X) = R(X^{1/2})$ we have that there exists some $|\Phi\rangle \in R(X^{1/2})$ such that $|\Psi^r\rangle = X^{-1/2}|\Phi\rangle$. Using that

$$\langle\Phi|X^{-1/2} Y X^{-1/2}|\Phi\rangle \leq \langle\Phi|\Phi\rangle, \tag{7.4}$$

we obtain that $\langle\Psi^r|X - Y|\Psi^r\rangle \geq 0$, and thus $X - Y \geq 0$. (only if) First, $K(X) \subseteq K(Y)$ since otherwise there would be a vector $|\Psi\rangle \in K(X)$ for which $\langle\Psi|Y|\Psi\rangle > 0$, and therefore $\langle\Psi|X - Y|\Psi\rangle < 0$. Moreover, $\forall |\Psi^r\rangle \in R(X)$ we can find $|\Phi\rangle \in R(X^{1/2})$ such that $|\Psi^r\rangle = X^{1/2}|\Phi\rangle$. Using that $\langle\Phi|X|\Phi\rangle \geq \langle\Phi|Y|\Phi\rangle$ we obtain that

$$1 \geq \langle\Psi^r|X^{-1/2} Y X^{-1/2}|\Psi^r\rangle / \langle\Psi^r|\Psi^r\rangle, \tag{7.5}$$

which immediately gives $\|Y^{\frac{1}{2}} X^{-\frac{1}{2}}\|^2 \leq 1$.

We can use this lemma to recover the results of Ref. [108, 125, 146]. Given an operator ρ, a product vector $|e, f\rangle$ and $\lambda > 0$, we define

$$\tilde{\rho} \equiv \rho - \lambda |e, f\rangle\langle e, f|, \tag{7.6a}$$

$$\lambda_0 = \frac{1}{\langle e, f|\rho^{-1}|e, f\rangle}, \tag{7.6b}$$

$$\bar{\lambda}_0 = \frac{1}{\langle e^*, f|(\rho^{T_A})^{-1}|e^*, f\rangle}. \tag{7.6c}$$

We then have

Corollary 7.1 *$\tilde{\rho}, \tilde{\rho}^{T_A} \geq 0$ iff $|e, f\rangle \in R(\rho)$, $|e^*, f\rangle \in R(\rho^{T_A})$ and $\lambda \leq min(\lambda_0, \bar{\lambda}_0)$.*

Proof: We can simply use Lemma 7.1 with $X = \rho$ and $Y = \lambda |e, f\rangle\langle e, f|$, and with $X = \rho^{T_A}$ and $Y = \lambda |e^*, f\rangle\langle e^*, f|$.■

The most interesting situation occurs when we choose $\lambda = \min(\lambda_0, \bar{\lambda}_0)$, since in that case we can reduce the ranks of ρ and/or ρ^{T_A}, as states the following

Lemma 7.2 *Let $|e, f\rangle \in R(\rho)$, $|e^*, f\rangle \in R(\rho^{T_A})$. Then*

(i) *If $\lambda = \lambda_0 < \bar{\lambda}_0$ then $r(\tilde{\rho}) = r(\rho) - 1$ and $r(\tilde{\rho}^{T_A}) = r(\rho^{T_A})$.*

(ii) *If $\lambda = \bar{\lambda}_0 < \lambda_0$ then $r(\tilde{\rho}) = r(\rho)$ and $r(\tilde{\rho}^{T_A}) = r(\rho^{T_A}) - 1$.*

(iii) *If $\lambda = \bar{\lambda}_0 = \lambda_0$ then $r(\tilde{\rho}) = r(\rho) - 1$ and $r(\tilde{\rho}^{T_A}) = r(\rho^{T_A}) - 1$.*

Proof: Here, we just prove (i), since for the other two cases one can follow the same arguments. First, note that $r(\tilde{\rho}) \geq r(\rho) - 1$ since they differ only by one one–dimensional projector. On the other hand, $K(\rho) \subseteq K(\tilde{\rho})$ since if $|\Psi\rangle \in K(\rho)$ then $\tilde{\rho}|\Psi\rangle = -\lambda_0 \langle e, f|\Psi\rangle = 0$ since $|e, f\rangle \in R(\rho) \perp K(\rho)$. Besides, the vector $\rho^{-1}|e, f\rangle$ is not in $K(\rho)$ but it is indeed in $K(\tilde{\rho})$, which can be checked by substitution in Eq. (7.6a).■

This lemma allows us to decrease either the rank of ρ, of its partial transpose, or of both of them by subtracting a product vector $|e, f\rangle$ which belongs to $R(\rho)$ and such that $|e^*, f\rangle$ is in $R(\rho^{T_A})$.

Let us denote by $\{|e_i, f_i\rangle, i = 1, 2, \ldots, L\}$ the product vectors such that $|e_i, f_i\rangle \in R(\rho)$ and $|e_i^*, f_i\rangle \in R(\rho^{T_A})$. Note that we assume here that the total number of such vectors L is finite. We also denote by $P_i \equiv |e_i, f_i\rangle\langle e_i, f_i|$. We have

Lemma 7.3 *ρ is separable iff it can be written as a convex combination of P_i.*

Proof: (if) Use the definition of separable state; (only if) We just have to notice that if a positive operator ρ can be written as a convex combination of certain projectors on the vectors $|\Psi_i\rangle$, then these vectors must belong to its range. Otherwise, there would exist a certain vector $|\Psi_{i_0}\rangle = |\Psi_{i_0}^r\rangle + |\Psi_{i_0}^k\rangle$, where $|\Psi_{i_0}^r\rangle \in R(\rho)$ and $0 \neq |\Psi_{i_0}^k\rangle \in K(\rho)$, so that $\langle\Psi_{i_0}^k|\rho|\Psi_{i_0}^k\rangle > 0$, which contradicts the fact that $|\Psi_{i_0}^k\rangle \in K(\rho)$. Thus, if ρ is separable then it can be written as a convex combination of projectors on product vectors $|e_i, f_i\rangle \in R(\rho)$. Also ρ^{T_A} can be written as the same convex combination, but with $|e_i^*, f_i\rangle \in R(\rho^{T_A})$.■

Let the projectors P_i be linearly independent. These projectors belong to the space $\mathcal{L}[R(\rho)]$ of linear operators acting on $R(\rho)$, which has dimension $r(\rho)^2$. On the other hand, the projectors $P_i^{T_A}$ will be linearly independent as well, since partial transposition is a linear invertible map. These projectors belong to the space $\mathcal{L}[R(\rho^{T_A})]$, which has dimension $r(\rho^{T_A})^2$. Therefore, if the P_i are linearly independent we must have $L \leq \min[r(\rho)^2, r(\rho^{T_A})^2]$. We can always complete the set P_i with other operators P_i $(i = L+1, \ldots, r(\rho)^2)$ to form a basis in $\mathcal{L}[R(\rho)]$. That is a Hilbert space with the scalar product $(A, B) = \mathrm{tr}(A^\dagger B)$. Thus, we can construct the biorthogonal basis to $\{P_i\}$ in $\mathcal{L}[R(\rho)]$; that is, we can find a set of operators $Q_i \in \mathcal{L}[R(\rho)]$ such that $\mathrm{tr}(Q_i^\dagger P_j) = \delta_{ij}$. Then we have the following necessary and sufficient separability condition

Lemma 7.4 *If P_i are linearly independent, then ρ is separable iff $tr(Q_i^\dagger \rho) \geq 0$ $\forall i \leq L$ and $tr(Q_i^\dagger \rho) = 0$ $\forall i > L$.*

Proof: Since the P_i form a basis, ρ can be expanded in a unique way as

$$\rho = \sum_{i=1}^{r(\rho)^2} c_i P_i, \tag{7.7}$$

with $c_i = \mathrm{tr}(Q_i \rho)$. (if) since $c_i \geq 0$ we have that ρ can be written as a convex combination of projectors on $|e_i, f_i\rangle$, i.e. it is separable; (only if) If ρ is separable, according to Lemma 7.3 it can be written as (7.7) with $c_i = 0$ if $i > L$ and $c_i \geq 0$ if $i \leq L$.■

This lemma is important since in general, if $L \leq \min[r(\rho)^2, r(\rho^{T_A})]$, the projectors will be linearly independent. The reason is that given a set of $L \leq D^2$ random product vectors which span a Hilbert space of dimension D, then the corresponding projectors are linearly independent.

Kernel of ρ

We will show that if there is a product vector in the kernel of ρ, then one can find a positive operator acting on $\mathbb{C}^2 \otimes \mathbb{C}^{N-1}$ which has the same separability properties as ρ. This means that one can reduce the dimensionality of the Hilbert space of the second subsystem, which simplifies the problem. We will use later on these results to prove facts regarding low rank density operators. We start proving a simple

Lemma 7.5 *$|e^*, f\rangle \in K(\rho^{T_A})$ iff $|e, f\rangle \in K(\rho)$.*

Proof: (if) We have $0 = \langle e, f|\rho|e, f\rangle$. Using (7.2), we have $0 = \langle e^*, f|\rho^{T_A}|e^*, f\rangle$ and since $\rho^{T_A} \geq 0$ then $\rho^{T_A}|e^*, f\rangle = 0$; (only if) One can prove it in the same way.■

Lemma 7.6 *If $|e, f\rangle \in K(\rho)$ then either:*

(i) $|\hat{e}, f\rangle \in K(\rho)$, or

(ii) there exists a non-zero $|g\rangle \in \mathbb{C}^N$ such that $\rho|\hat{e}, f\rangle = |\hat{e}, g\rangle$ and $\rho^{T_A}|\hat{e}^*, f\rangle = |\hat{e}^*, g\rangle$.

Proof: According to Lemma 7.5, if $|e, f\rangle \in K(\rho)$ then $|e^*, f\rangle \in K(\rho^{T_A})$. Therefore

$$0 = \langle\hat{e}^*, h|\rho^{T_A}|e^*, f\rangle = \langle e, h|\rho|\hat{e}, f\rangle, \tag{7.8}$$

$\forall |h\rangle \in \mathbb{C}^N$. Thus we know that either $\rho|\hat{e}, f\rangle = 0$ or $\rho|\hat{e}, f\rangle = |\hat{e}, g_1\rangle$ for some $|g_1\rangle \in \mathbb{C}^N$. Analogously, since $|e, f\rangle \in K(\rho)$ we have that either $\rho^{T_A}|\hat{e}^*, f\rangle = 0$ or $\rho^{T_A}|\hat{e}^*, f\rangle = |\hat{e}^*, g_2\rangle$ for some $|g_2\rangle \in \mathbb{C}^N$. In the first case, using Lemma 7.5 we have (i). For (ii), it remains to be proven that $|g_1\rangle = |g_2\rangle$. Using the orthogonality of $|e\rangle$ and $|\hat{e}\rangle$ we have

$$\||\hat{e}\rangle\|^2|g_1\rangle = \langle\hat{e}|\rho|\hat{e}, f\rangle = \langle\hat{e}^*|\rho^{T_A}|\hat{e}^*, f\rangle = \||\hat{e}\rangle\|^2|g_2\rangle.\blacksquare \tag{7.9}$$

The first part of this lemma simply states that ρ is supported on a smaller space $\mathbb{C}^2 \otimes \mathbb{C}^M$ with $M < N$, since $|e, f\rangle \in K(\rho)$ for all $|e\rangle \in \mathbb{C}^2$. In other words, that we have spurious dimensions in the second subsystem. In the following, we will not consider that trivial case, and therefore we will assume that ρ is supported on the whole space $\mathbb{C}^2 \otimes \mathbb{C}^N$. In that case, Lemma 7.6 together with Lemma 7.2 tell us that there is a vector that can be subtracted from ρ. In fact, this gives rise to one of the most important results of this section:

Lemma 7.7 *If ρ is supported in $\mathbb{C}^2 \otimes \mathbb{C}^N$ and there exists a product vector in $K(\rho)$ then $\rho = \tilde{\rho} + \rho_s$, where ρ_s is a projector on a product vector and*

(i) *$r(\tilde{\rho}) = r(\rho) - 1$ and $r(\tilde{\rho}^{T_A}) = r(\rho^{T_A}) - 1$.*

(ii) *$\tilde{\rho}$ is supported on $\mathbb{C}^2 \otimes \mathbb{C}^{N-1}$.*

(iii) *$\tilde{\rho}$ is separable iff ρ is separable.*

Proof: We have that $|e, f\rangle \in K(\rho)$. Using the previous Lemma (ii) (since ρ is supported in $\mathbb{C}^2 \otimes \mathbb{C}^N$) we have that $\rho|\hat{e}, f\rangle = |\hat{e}, g\rangle$ and $\rho^{T_A}|\hat{e}^*, f\rangle = |\hat{e}^*, g\rangle$. According to Corollary 7.1 we can subtract the product vector $|\hat{e}, g\rangle$, obtaining $\tilde{\rho} = \rho - \rho_s$ where $\rho_s = \lambda|\hat{e}, g\rangle\langle\hat{e}, g|$ and

$$\begin{aligned} \lambda &= \lambda_0 = \frac{1}{\langle\hat{e}, g|\rho^{-1}|\hat{e}, g\rangle} = \frac{1}{\||\hat{e}\rangle\|^2\langle g|f\rangle} \\ &= \frac{1}{\langle\hat{e}^*, g|(\rho^{T_A})^{-1}|\hat{e}^*, g\rangle} = \bar{\lambda}_0. \end{aligned} \tag{7.10}$$

According to Lemma 7.2 (iii) we have decreased the ranks of both ρ and ρ^{T_A} by one, which proves (i). We also have that $|\hat{e}, f\rangle, |e, f\rangle \in K(\tilde{\rho})$ and therefore $\tilde{\rho}$ is supported in $\mathbb{C}^2 \otimes \mathbb{C}^M$ with $M < N$. Now we show that $M = N - 1$. If it was smaller, then there would exist $|h\rangle$ orthogonal to $|f\rangle$ such that $|e, h\rangle, |\hat{e}, h\rangle \in K(\tilde{\rho})$. In that case we would have $\rho|e, h\rangle = 0$ and $\rho|\hat{e}, h\rangle = c|\hat{e}, g\rangle$ where c is a constant. If we define $|f'\rangle = c|f\rangle - |h\rangle \neq 0$ we would have that $|e, f'\rangle, |\hat{e}, f'\rangle \in K(\rho)$, contrary to our assumption that ρ is supported on $\mathbb{C}^2 \otimes \mathbb{C}^N$, which proves (ii). It remains to be shown (iii) that ρ is separable iff $\tilde{\rho}$ is too: (if) trivial; (only if) If ρ is separable, and since $\rho|e, f\rangle = 0$ we can always write

$$\rho = \sum |e_i, \hat{f}_i\rangle\langle e_i, \hat{f}_i| + |\hat{e}\rangle\langle\hat{e}| \otimes \eta, \tag{7.11}$$

where $\langle f|\hat{f}_i\rangle = 0$ and η is a positive operator acting on $\mathbb{C}^N$. If we impose $|\hat{e}, g\rangle = \rho|\hat{e}, f\rangle$ we obtain $|g\rangle = \||\hat{e}\rangle\|^2\eta|f\rangle$, and therefore $|g\rangle \in R(\eta)$. We can write

$$\tilde{\rho} = \sum |e_i, \hat{f}_i\rangle\langle e_i, \hat{f}_i| + |\hat{e}\rangle\langle\hat{e}| \otimes (\eta - \lambda_0|g\rangle\langle g|), \tag{7.12}$$

so that if we show that the operator $(\eta - \lambda_0|g\rangle\langle g|) \geq 0$ then we have that $\tilde{\rho}$ is separable. Using (7.10) we have that such operator is

$$\eta - \frac{1}{\||\hat{e}\rangle\|^2\langle g|f\rangle}|g\rangle\langle g| = \eta - \frac{1}{\langle g|\eta^{-1}|g\rangle}|g\rangle\langle g|, \tag{7.13}$$

which is positive according to Lemma 7.1.■

This lemma simply says that when there is a product vector in the kernel or ρ, then we can reduce the problem without changing the separability properties of ρ. Later on we will consider states which are invariant under partial transposition. In that case, we can particularize this result and obtain:

Lemma 7.8 *If in addition to the premises of Lemma 7.7 $\rho = \rho^{T_A}$ then we can always obtain the results of that lemma with $\tilde{\rho} = \tilde{\rho}^{T_A}$.*

Proof: We know from Lemma 7.5 that if there is a product vector $|e, f\rangle \in K(\rho)$ then $|e^*, f\rangle \in K(\rho^{T_A}) = K(\rho)$. With these two vectors we can always construct $|e_r, f\rangle \in K(\rho)$ where $|e_r\rangle$ is real (in the basis in which we take the partial transposition). If we proceed with this vector as in the previous lemma then we obtain the desired result.■

Finally, we will show a property of the vectors contained in $K(\rho)$ for the case when there is no product vector in $K(\rho)$. We will use this property later on to simplify the search of product vectors in $R(\rho)$. Let us denote by $\{|\Psi_i^1\rangle, i = 1 \ldots k(\rho)\}$ and $\{|\Psi_i^2\rangle, i = 1 \ldots k(\rho^{T_A})\}$ a basis in $K(\rho)$ and $K(\rho^{T_A})$, respectively. Then we have the following:

Lemma 7.9 *If there exists no product vector in $K(\rho)$ then both $\{\langle e|\Psi_i^1\rangle\}$ and $\{\langle e^*|\Psi_i^2\rangle\}$ are sets of linearly independent vectors in $\mathbb{C}^N$ for any $|e\rangle \in \mathbb{C}^2$.*

Proof: We start proving that for any $|e\rangle \in \mathbb{C}^2$, the operator $\langle e|\rho|e\rangle$ is invertible. Otherwise there would exist $|h\rangle \in \mathbb{C}^N$ such that $0 = \langle h|\langle e|\rho|e\rangle|h\rangle$ and since $\rho \geq 0$ then $\rho|\hat{e}, h\rangle = 0$, which contradicts our assumptions. On the other hand, since $\{|e\rangle, |\hat{e}\rangle\}$ is a basis in $\mathbb{C}^2$ we can write the vectors in the kernel of ρ as

$$|\Psi_i^1\rangle = |e, \Psi_i^e\rangle + |\hat{e}, \Psi_i^{\hat{e}}\rangle. \tag{7.14}$$

Using that they are in the kernel of ρ we find that

$$|\Psi_i^{\hat{e}}\rangle = -\frac{1}{\langle\hat{e}|\rho|\hat{e}\rangle}\langle\hat{e}|\rho|e\rangle|\Psi_i^e\rangle, \tag{7.15}$$

where we made use of the fact that the operator $\langle\hat{e}|\rho|\hat{e}\rangle$ is invertible. Substituting this expression in (7.14), we have

$$|\Psi_i^1\rangle = (\mathbb{1} + |\hat{e}\rangle\frac{1}{\langle\hat{e}|\rho|\hat{e}\rangle}\langle\hat{e}|\rho)|e, \Psi_i^e\rangle. \tag{7.16}$$

Since the $|\Psi_{i_1}^1\rangle$'s are linearly independent, so must be the $|\Psi_{i_1}^e\rangle$'s. The same argumentation holds for the vectors in the kernel of ρ^{T_A}.■

In subspaces

As we have shown above, it is important to know when one can be sure that there exists a product vector in either the range or the kernel of a density operator. In this section we will prove that for sufficiently large subspaces there always exist product vectors. We will denote by $\{|0\rangle, |1\rangle\}$, and $\{|1\rangle, \ldots, |N\rangle\}$ orthonormal basis in $\mathbb{C}^2$ and $\mathbb{C}^N$, respectively.

Lemma 7.10 *Any subspace $H \subseteq \mathbb{C}^2 \otimes \mathbb{C}^N$ with $dim(H) = M > N$ contains an infinite number of product vectors. If $M = N$ it contains at least one product vector.*

Proof: We denote by $\{|\Psi_i\rangle, i = 1, \ldots 2N - M\}$ a basis in the orthogonal complement of H. We have

$$|\Psi_i\rangle = \sum_{k=1}^{N} \left[A_{i,k}|0,k\rangle + B_{i,k}|1,k\rangle\right], \tag{7.17}$$

where A and B are $(2N - M) \times N$- matrices. We write the product vector $|e, f\rangle$ as

$$|e, f\rangle = (\alpha|0\rangle_A + |1\rangle_A) \otimes \sum_k f_k|k\rangle_B. \tag{7.18}$$

Imposing that $|e, f\rangle$ is orthogonal to the $|\Psi_i\rangle$ for all i gives $(\alpha A^* + B^*)\vec{f} = 0$. This can be regarded as an equation for $\vec{f}$. When $M > N$ there exist non trivial solutions for each α, i.e. for each $|e\rangle$. For $M = N$ we have non trivial results provided $\det(\alpha A^* + B^*) = 0$; the determinant is a polynomial of N–th degree in α, which always has roots.■

Corollary 7.2 *Any subspace $H \subseteq \mathbb{C}^2 \otimes \mathbb{C}^N$ with $dim(H) = M > N$ contains an infinite number of product vectors of the form $|e_r, f\rangle$, where $|e_r\rangle = |e_r^*\rangle$.*

As we have seen in previous subsections, we can subtract vectors from ρ while keeping the positivity of both ρ and ρ^{T_A} provided we can find a product vector $|e, f\rangle \in R(\rho)$ and such that $|e^*, f\rangle \in R(\rho^{T_A})$. We can use the idea given in the proof of the previous lemma to find out under which conditions this is possible. Given any two subspaces $H_1, H_2 \in \mathbb{C}^2 \otimes \mathbb{C}^N$ with $\dim(H_{1,2}) = M_{1,2}$ we denote by $\{|\Psi_{i_{1,2}}^{1,2}\rangle, i_{1,2} = 1, \ldots 2N - M_{1,2}\}$ a basis in the orthogonal complement of $H_{1,2}$, respectively. Then we have

Lemma 7.11 *(i) If $M_1 + M_2 > 3N$ then there exists an infinite number of product vectors $|e, f\rangle \in H_1$ such that $|e^*, f\rangle \in H_2$; (ii) If $M_1 + M_2 \leq 3N$ then there exists a product vector $|e, f\rangle \in H_1$ such that $|e^*, f\rangle \in H_2$ iff we can find an α such that there are at most $N - 1$ linearly independent vectors among the following vectors: $\{\alpha\langle\Psi_{i_1}^1|0\rangle + \langle\Psi_{i_1}^1|1\rangle, \alpha^*\langle\Psi_{i_2}^2|0\rangle + \langle\Psi_{i_2}^2|1\rangle\}$.*

Proof: We have

$$|\Psi_{i_{1,2}}^{1,2}\rangle = \sum_{k=1}^{N} \left[A_{i,k}^{1,2}|0,k\rangle + B_{i,k}^{1,2}|1,k\rangle\right], \tag{7.19}$$

where $A^{1,2}$ and $B^{1,2}$ are $(2N - M_{1,2}) \times N$- matrices. Writing a product vector $|e, f\rangle$ as in (7.18) and imposing that it is orthogonal to $|\Psi_i^1\rangle$ and $|e^*, f\rangle$ is orthogonal to $|\Psi_i^2\rangle$ for all i, we arrive at the following equations:

$$\left[\alpha(A^1)^* + (B^1)^*\right]\vec{f} = 0, \tag{7.20a}$$

$$\left[\alpha^*(A^2)^* + (B^2)^*\right]\vec{f} = 0, \tag{7.20b}$$

which can be regarded as $4N - M_1 - M_2$ equations for $\vec{f}$. For $M_1 + M_2 > 3N$, there are less equations than variables, and thus there always exists a solution for each α, i.e. for each $|e\rangle$, which proves (i). For $M_1 + M_2 \leq 3N$ there exists a nontrivial solution iff the matrix $M(\alpha, \alpha^*)$ composed of $\alpha(A^1)^* + (B^1)^*$ and $\alpha(A^2)^* + (B^2)^*$ has rank smaller than N, which is equivalent to the statement of the lemma.■

Let us now analyze the case in which $M_1 + M_2 = 3N$. Here, we have that the conditions of Lemma 7.11 are fulfilled iff $\det[M(\alpha, \alpha^*)] = 0$ for some α. This determinant will be a polynomial $P_{2N-M_1,2N-M_2}(\alpha, \alpha^*)$ of degree $2N - M_1$ in α and of degree $2N - M_2$ in α^*. Thus, the existence of product vectors $|e, f\rangle \in H_1$ such that $|e^*, f\rangle \in H_2$ is directly related to the existence of roots of that polynomial. For $M_1 + M_2 < 3N$ we have to impose that

several determinants containing N rows of $M(\alpha,\alpha^*)$ vanish; again, those conditions are equivalent to imposing that several polynomials in α and α^* have common roots.

Note that for complex polynomials there is no theorem which allows to know how many (if any) roots exist. For example, the equation $\alpha^*\alpha+1$ has no roots, whereas $\alpha^2-(\alpha^*)^2=0$ has infinitely many. However, in a generic case, given a polynomial $P(\alpha,\alpha^*)$ one can find a polynomial $Q(\alpha)$ of higher degree in α (say K) such that the roots of P are also roots of Q. Since we know that Q has at most K solutions, it means that P can have at most K solutions as well. For example, if we have $P(\alpha,\alpha^*)=\alpha^2-\alpha^*=0$, we can complex conjugate this equation and obtain $P(\alpha,\alpha^*)^*=(\alpha^*)^2-\alpha=0$, which, upon substituting $\alpha^*=\alpha^2$ we obtain $Q(\alpha)=\alpha^4-\alpha=0$. This equation has four solutions $(0,1,e^{i2\pi/3},e^{i2\pi/3})$ which are exactly the roots of P. Note that we have been able to reduce the original equation to one containing α only given the fact that the $P^*\neq P$. It is clear that the polynomials fulfilling this condition are dense in the ring of all polynomials, and this is the reason why we say that in the generic case one can find $Q(\alpha)$.

In summary, in this section we have shown that if there is a product vector in $K(\rho)$ then we can find another operator ρ_s supported on $\mathbb{C}^2\otimes\mathbb{C}^{N-1}$ with the same separability properties as ρ. In order to check whether we can have such product vectors, we have shown that if the dimension of a subspace [e.g., $K(\rho)$] is greater or equal to N, then we can always find product vectors in it. On the other hand, if there is a product vector $|e,f\rangle\in R(\rho)$ with $|e^*,f\rangle\in R(\rho^{T_A})$, then one can decrease the rank of ρ, ρ^{T_A} or both. This is always possible if the ranks of ρ and ρ^{T_A} are sufficiently large. Otherwise, one has to find roots of polynomials. We have also shown that if there is a finite, sufficiently small number of product vectors fulfilling this condition, then we automatically have a necessary and sufficient condition for separability.

Results

The following subsection contains the main results of this section concerning separability of a density operator supported on $\mathbb{C}^2\otimes\mathbb{C}^N$. We have divided it into four parts. The first three deal with different situations depending on the rank of ρ. Actually, we just have to consider the cases in which $r(\rho)\geq N$ as the following lemma states:

Lemma 7.12 *If ρ is supported on $\mathbb{C}^2\otimes\mathbb{C}^N$ then $r(\rho)\geq N$.*

Proof: Let us assume that $r(\rho)<N$. Then $K(\rho)$ has dimension larger than N, and according to Lemma 7.10 it contains a product vector. Using

Lemma 7.7 we can find an operator $\tilde{\rho}_1$ supported on $\mathbb{C}^2\otimes\mathbb{C}^{N-1}$ and with $r(\tilde{\rho}_1)<N-1$. Again, $K(\tilde{\rho}_1)$ has dimension larger than $N-1$, contains a product vector, and we can find an operator $\tilde{\rho}_2$ supported on $\mathbb{C}^2\otimes\mathbb{C}^{N-2}$ and with $r(\tilde{\rho}_2)<N-2$. We can proceed in the same way until we have an operator $\tilde{\rho}_{N-1}$ supported on $\mathbb{C}^2\otimes\mathbb{C}^1$ and with $r(\tilde{\rho}_{N-1})<1$, which is impossible.■

The first subsection shows that if $r(\rho)=N$ then ρ is separable. From that follows that bound entangled states have rank larger than N. The second subsection deals with operators ρ such that $r(\rho)+r(\rho^{T_A})\leq 3N$. It is shown that in the generic case and for $N\leq 10$ one can perform a constructive separability check. The third subsection shows that given a density operator, one can always subtract vectors until the condition $r(\rho)+r(\rho^{T_A})\leq 3N$ is obtained. In the fourth one, we show that if $\rho=\rho^{T_A}$ then ρ is separable. We also show that if ρ and ρ^{T_A} are "sufficiently close" then ρ is also separable.

$$rank(\rho)=N$$

Theorem 7.1 *If ρ is supported on $\mathbb{C}^2\otimes\mathbb{C}^N$ and $r(\rho)=N$ then ρ is separable.*

Proof: We use induction. For $N=1$ the statement is true. Let us assume that it is true for $N-1$. We take now ρ supported on $\mathbb{C}^2\otimes\mathbb{C}^N$, with $r(\rho)=N$. Then $K(\rho)$ has dimension N, and according to Lemma 7.10 it contains a product vector $|e,f\rangle$. Using Lemma 7.7 we have that ρ is separable iff $\tilde{\rho}$ is separable. But $\tilde{\rho}$ is supported on $\mathbb{C}^2\otimes\mathbb{C}^{N-1}$ and has rank $N-1$, and therefore it is separable by assumption.■

Corollary 7.3 *If ρ is supported on $\mathbb{C}^2\otimes\mathbb{C}^N$ and $r(\rho)=N$, then ρ can be written as a convex sum of projectors on N product vectors.*

Proof: Just given by the construction of the proof of Theorem 7.1.

Corollary 7.4 *If ρ is supported on $\mathbb{C}^2\otimes\mathbb{C}^N$ and $r(\rho)=N$ then $r(\rho^{T_A})=N$.*

Proof: This is a direct application of the previous corollary and Lemma 7.12.

Corollary 7.5 *If ρ is supported on $\mathbb{C}^2\otimes\mathbb{C}^N$ and is not separable, then $r(\rho)>N$.*

Proof: Direct application of Lemma 7.12 and Theorem 7.1.

$$rank(\rho)+rank(\rho^{T_A}) \leq 3N$$

We assume that $r(\rho), r(\rho^{T_A}) > N$. We can use Lemma 7.11 with $H_1 = R(\rho)$ and $H_2 = R(\rho^{T_A})$ to determine the conditions under which there exist product vectors that can be subtracted from ρ. The problem reduces to finding the roots of a polynomial in α and α^*. As explained in the previous section ("In Subspaces"), in the generic case these roots are also roots of another polynomial in α. If the corresponding projectors P_i are linearly independent [which imposes that the number of such product vectors be smaller than the minimum of $r(\rho)^2$ and $r(\rho^{T_A})^2$], then Lemma 7.11 provides us with a necessary and sufficient condition for separability. We will illustrate this with the case $\mathbb{C}^2 \otimes \mathbb{C}^4$ in the following section.

Let us now show that if $N \leq 10$ then for a generic ρ we can always find less than the minimum of $r(\rho)^2$ and $r(\rho^{T_A})^2$ product vectors $|e, f\rangle \in R(\rho)$ with $|e^*, f\rangle \in R(\rho)$. Without loss of generality we can take $k(\rho) = X \geq k(\rho^{T_A}) = Y$ (otherwise we can substitute $\alpha \to \alpha^*$ in what follows). We also assume that there are no product vectors in $K(\rho)$ since otherwise we can trivially reduce the problem to $\mathbb{C}^2 \otimes \mathbb{C}^{N-1}$ decreasing the ranks of ρ and ρ^{T_A} via Lemma 7.7. We therefore have $N > Y \geq X > 0$ and $X + Y \geq N$. Let us analyze separately the cases: (i) $X + Y = N$ and; (ii) $X + Y > N$. If $X + Y = N$ we have $0 < X \leq [N/2]$, where $[W]$ denotes the integer part of W. According of Lemma 7.11, the problem reduces to finding roots of a polynomial of degree X in α and Y in α^*. In Appendix D.1 we give a procedure to find those roots, which states that the number of roots (for a generic case) will not exceed $2^{X-1}[N^2 + (N-X)^2 - X(N-X)]$. This number should be smaller or equal to $(N+X)^2$. One can check that for $N \leq 10$ this condition is always fulfilled. (ii) If $X + Y > N$ then we have $[(N+1)/2] \leq Y < N$. According to Lemma 7.11 there will be two (or more) polynomial equations of degree $N - Y$ in α and Y in α^*. In Appendix D.2 we show that in that case the number of roots cannot exceed $2^{N-Y}Y$. This number should be smaller or equal to $(2N - Y)^2$, which is always the case for $N \leq 10$.

Finally, using the results of the previous subsection we can ensure that if $r(\rho) = r(\rho^{T_A}) = N + 1$ then either the polynomials of Lemma 7.11 have exactly $N+1$ solutions, in which case ρ is separable and expressible in terms of $N+1$ product vectors, or it has none and then ρ is bound entangled. This is so because if one can subtract one product vector, then one recovers the situation of Corollary 7.3.

$$rank(\rho)+rank(\rho^{T_A}) > 3N$$

We can use Lemma 7.11 with $H_1 = R(\rho)$ and $H_2 = R(\rho^{T_A})$ to show that there always exist product vectors that can be subtracted from ρ. We can do that until we reach $r(\rho) + r(\rho^{T_A}) \leq 3N$. In that case, we can use the criterion given in the previous subsection to find out if the remaining operator is separable. Thus, this procedure gives us a constructive sufficient criterion for separability.

Invariance under partial transposition: $\rho = \rho^T$

Theorem 7.2 *If $\rho = \rho^{T_A}$ then ρ is separable.*

Proof: According to Lemma 7.12, we just have to consider two cases: (i) $r(\rho) = N$: Using Theorem 7.1 we have that ρ is separable. (ii) $r(\rho) > N$: according to Corollary 7.2 there is a product vector $|e_r, g\rangle$ with $|e_r\rangle = |e_r^*\rangle$. Using Corollary 7.1 we can use this product vector to reduce the rank of ρ. But since $|e_r, g\rangle = |e_r^*, g\rangle$ we have that the resulting operator is also equal to its partial transpose. We can proceed in this way until $r(\rho) = N$, in which case we use Theorem 7.1 to show that ρ is separable.■

Note that we could have chosen a different basis for the partial transposition. Moreover, since the property of separability is independent of invertible local transformations A acting on $\mathbb{C}^2$, we have the following

Corollary 7.6 *If $[(A \otimes \mathbb{1})\rho(A \otimes \mathbb{1})^\dagger]^{T_A} = (A \otimes \mathbb{1})\rho(A \otimes \mathbb{1})^\dagger$, for some non singular operator A, then ρ is separable.*

Theorem 7.2 suggests that if ρ is not very different from ρ^{T_A}, then it should also be separable. Indeed, one can construct a powerful sufficient separability condition based on that theorem. For that we have to introduce some definitions. In $\mathbb{C}^2 \otimes \mathbb{C}^N$ we can always write ρ as

$$\rho = \frac{\rho + \rho^{T_A}}{2} + \frac{\rho - \rho^{T_A}}{2} \equiv \rho_s + \sigma_y^A \otimes B, \tag{7.21}$$

Here $2\rho_s = \rho + \rho^{T_A}$, $\sigma_y^A = i(|0\rangle_A\langle 1| - |1\rangle_A\langle 0|)$, and $4B = 4B^\dagger = \mathrm{tr_A}[\sigma_y^A(\rho - \rho^{T_A})]$. This operator B can be decomposed as

$$B = \sum_{i=1}^{K} \lambda_i |v_i\rangle\langle v_i|. \tag{7.22}$$

In particular, one of such is the spectral decomposition. Given one of such decomposition $\{\lambda_i, |v_i\rangle\}_{i=1}^K$ and a set of real numbers $\{a_i\}_{i=1}^K$ we define the operator

$$C(a,\lambda,v) \equiv \sum_{i=1}^{K} |\lambda_i|(a_i^2|0\rangle\langle 0| + a_i^{-2}|1\rangle\langle 1|) \otimes |v_i\rangle\langle v_i|, \tag{7.23}$$

which is obviously positive. We have:

Theorem 7.3 *Given a decomposition of B $\{\lambda_i, |v_i\rangle\}_{i=1}^K$ and a set of real numbers $\{a_i\}_{i=1}^K$, if $\|C^{1/2}(a,\lambda,v)\rho_s^{-1/2}\|^2 \leq 1$, then ρ is separable.*

Proof: We define $\tilde{\rho}_s = \rho_s - C(a,\lambda,v) = \tilde{\rho}_s^{T_A} \geq 0$ according to Lemma 7.1. Using Theorem 7.2 we have that $\tilde{\rho}_s$ is separable. Let $|w_i\rangle = a_i|0\rangle - ia_i^{-1}\text{sign}(\lambda_i)|1\rangle$. Then, it is easy to check that

$$\rho = \tilde{\rho}_s + \sum_{i=1}^{K} |\lambda_i||w_i, v_i\rangle\langle w_i, v_i|. \tag{7.24}$$

which shows that ρ is separable.■

Thus, we can show that a density operator is separable if we can find a decomposition of B and a set of real numbers that fulfill certain conditions. In particular we can take the spectral decomposition of B and $a_i = 1$. Using the fact that $\|AB\| \leq \|A\|\|B\|$ one can easily prove the following:

Corollary 7.7 *If $\rho + \rho^{T_A}$ is of full range and $\|(\rho + \rho^{T_A})^{-1}\|\|\rho - \rho^{T_A}\| \leq 1$, then ρ is separable.*

This corollary implies that if ρ is full range and is very close to ρ^{T_A} then it is separable.

Finally, let us mention that we have taken here all partial transposes with respect to the first system. One may wonder whether if ρ is invariant under partial transposition with respect to the second system, then Theorem 7.2 still holds. Actually, this is not the case. A counterexample can be found in Ref. [75, 70] (see subsection "Illustration" in the next section), by simply noting that the bound entangled state given there is equal to its partial transpose if we take that in a different basis.

Example: $\mathbb{C}^2 \otimes \mathbb{C}^4$

We illustrate the methods developed in the previous section in the case of $\mathbb{C}^2 \otimes \mathbb{C}^4$. We will assume that: (i) ρ has no product vector in its kernel since otherwise using Lemma 7.7 we can reduce the problem to $\mathbb{C}^2 \otimes \mathbb{C}^3$ and there we know that ρ is separable; (ii) $r(\rho), r(\rho^{T_A}) > 4$ since otherwise using Theorem 7.1 we know that ρ is separable; (iii) $r(\rho) + r(\rho^{T_A}) \leq 12$ since in that case we can use our separability criterion. This section is divided into 3 parts:

- $r(\rho) = r(\rho^{T_A}) = 5$
- $r(\rho) + r(\rho^{T_A}) \leq 12$ and $r(\rho) \neq r(\rho^{T_A})$.
- $r(\rho) = r(\rho^{T_A}) = 6$

As before, we will denote by $\{|\Psi_i^1\rangle, i = 1 \ldots k(\rho)\}$ and $\{|\Psi_i^2\rangle, i = 1 \ldots k(\rho^{T_A})\}$ a basis in $K(\rho)$ and $K(\rho^{T_A})$, respectively. We will use the fact that, according to Lemma 7.11, there exists a product vector $|e, f\rangle \in R(\rho)$ and $|e^*, f\rangle \in R(\rho^{T_A})$ iff we can find an α such that there are at most 3 linearly independent vectors among $\{\alpha\langle\Psi_{i_1}^1|0\rangle + \langle\Psi_{i_1}^1|1\rangle, \alpha^*\langle\Psi_{i_2}^2|0\rangle + \langle\Psi_{i_2}^2|1\rangle\}$.

$$rank(\rho) = rank(\rho^{T_A}) = 5$$

Each of the two kernels has dimension 3 and therefore, according to Lemma 7.11, in order to find subtractable product vectors we have to solve $M(\alpha, \alpha^*)\vec{f} = 0$, where

$$M(\alpha,\alpha^*) = \begin{pmatrix} \alpha\langle\Psi_1^1|0\rangle + \langle\Psi_1^1|1\rangle \\ \alpha\langle\Psi_2^1|0\rangle + \langle\Psi_2^1|1\rangle \\ \alpha\langle\Psi_3^1|0\rangle + \langle\Psi_3^1|1\rangle \\ \alpha^*\langle\Psi_1^2|0\rangle + \langle\Psi_1^2|1\rangle \\ \alpha^*\langle\Psi_2^2|0\rangle + \langle\Psi_2^2|1\rangle \\ \alpha^*\langle\Psi_3^2|0\rangle + \langle\Psi_3^2|1\rangle \end{pmatrix}, \tag{7.25}$$

is a 6×4 matrix. Using Lemma 7.9 we know that the last three rows in M are linearly independent. Thus, this equation has non trivial solutions iff

$$\det_1(\alpha,\alpha^*) = \det[M_1(\alpha,\alpha^*)] = 0 \tag{7.26a}$$
$$\det_2(\alpha,\alpha^*) = \det[M_2(\alpha,\alpha^*)] = 0 \tag{7.26b}$$
$$\det_3(\alpha,\alpha^*) = \det[M_3(\alpha,\alpha^*)] = 0, \tag{7.26c}$$

where $M_{1,2,3}$ are 4×4 matrices formed by the last three rows of M and the 1–st, 2–nd, and 3–rd rows, respectively. Note that $\det_1$, $\det_2$ and $\det_3$ are polynomials linear in α and cubic in α^*. Thus, we can write them as

$$\begin{aligned} \det_1 &= \alpha P_3^1(\alpha^*) + P_3^0(\alpha^*) = 0 && (7.27a) \\ \det_2 &= \alpha \tilde{P}_3^1(\alpha^*) + \tilde{P}_3^0(\alpha^*) = 0 && (7.27b) \\ \det_3 &= \alpha \hat{P}_3^1(\alpha^*) + \hat{P}_3^0(\alpha^*) = 0, && (7.27c) \end{aligned}$$

where the subscripts denote the degree of the polynomials. In order to solve this equation we treat α and α^* as two independent variables. Multiplying Eq. (7.27a) by $\tilde{P}_3^1(\alpha^*)$, Eq. (7.27b) by $P_3^1(\alpha^*)$ and subtracting them we find an polynomial equation for α^* of degree 6. Doing the same thing but with Eq. (7.27c) instead of Eq. (7.27b) gives another polynomial equation for α^* of 6th degree. Subtracting these two polynomials we obtain a polynomial of degree 5. Thus, there are at most 5 solutions (i.e. 5 product vectors, as stated above). Note that the solutions have still to fulfill all Eq. (7.27). Note also that if we know α we can calculate the kernel of the matrix A for this particular value and find so the corresponding $|f\rangle$.

$$r(\rho)+r(\rho^{T_A}) \leq 12 \text{ where } r(\rho) \neq r(\rho^{T_A})$$

We are going to divide this part itself into:

- r(ρ)= 6 and r(ρ^{T_A})= 5 or r(ρ)= 5 and r(ρ^{T_A})= 6,
- r(ρ)= 7 and r(ρ^{T_A})= 5 or r(ρ)= 5 and r(ρ^{T_A})= 7.

Let us begin with the case where r(ρ)= 6 and r(ρ^{T_A})= 5. Then the dimension of the kernel of ρ is 2 and the one of the kernel of ρ^{T_A} is 3. Thus we can write the equations in the same way as in the previous case, but there are only two of them. We have

$$\begin{aligned} \det_1 = \det[M_1(\alpha, \alpha^*)] &= 0 && (7.28a) \\ \det_2 = \det[M_2(\alpha, \alpha^*)] &= 0, && (7.28b) \end{aligned}$$

where M_1 and M_2 are the same matrices as above. Thus the way of calculating the α's is exactly the same as before, obtaining at most 6 solutions for α^*. On the other hand, it is clear that the same can be done in the case where r(ρ)=5 and r(ρ^{T_A})= 6.

Now we consider the case r(ρ)= 7 and r(ρ^{T_A})= 5. Here we have only one equation that has to be fulfilled. We find

$$\det_1 = \det[M_1(\alpha, \alpha^*)] = 0, \qquad (7.29)$$

which leads to

$$\begin{aligned} 0 &= \alpha P_3^1(\alpha^*) + P_3^0(\alpha^*) && (7.30a) \\ &= (\alpha^*)^3 Q_1^3(\alpha) + (\alpha^*)^2 Q_1^2(\alpha) + \alpha^* Q_1^1(\alpha) + Q_1^0(\alpha) && (7.30b) \end{aligned}$$

Taking the complex conjugate of Eq. (7.30a) we have:

$$\alpha^* \bar{P}_3^1(\alpha) + \bar{P}_3^0(\alpha) = 0, \qquad (7.31)$$

where $\bar{P}$ is the same polynomial as P but with the coefficients complex conjugated. As explained in the Appendix we are using now Eq. (7.31) to transform the polynomial in Eq. (7.30a) in one depending only on α. That is, we multiply Eq. (7.30b) by $\bar{P}_3^1(\alpha)$ and Eq. (7.31) by $(\alpha^*)^2 Q_1^3(\alpha)$ and subtract them. We do the same two more times and end up with a polynomial of 10–th degree in α. For the different values of α we can now calculate the kernel of the matrix M and obtain $|f\rangle$. Thus we have all the product vectors $|e, f\rangle$ fulfilling $|e, f\rangle \in R(\rho)$ and $|e^*, f\rangle \in R(\rho^{T_A})$.

$$rank(\rho) = rank(\rho^{T_A}) = 6$$

Here we have two vectors in both, the kernel of ρ and the one of ρ^{T_A}. Thus the equation that has to be fulfilled is

$$\begin{aligned} 0 = \det(M(\alpha, \alpha^*)) &= \alpha^2 P_2^2(\alpha^*) + \alpha P_2^1(\alpha^*) + P_2^0(\alpha^*) && (7.32a) \\ &= (\alpha^*)^2 Q_2^2(\alpha) + \alpha^* Q_2^1(\alpha) + Q_2^0(\alpha). && (7.32b) \end{aligned}$$

Again, we take the complex conjugate of Eq. (7.32a) and deal with the following two equations:

$$\begin{aligned} (\alpha^*)^2 Q_2^2(\alpha) + \alpha^* Q_2^1(\alpha) + Q_2^0(\alpha) &= 0 && (7.33a) \\ (\alpha^*)^2 \bar{Q}_2^2(\alpha) + \alpha^* \bar{Q}_2^1(\alpha) + \bar{Q}_2^0(\alpha) &= 0. && (7.33b) \end{aligned}$$

First, we multiply Eq. (7.33a) by $\bar{Q}_2^2(\alpha)$, Eq. (7.33b) by $Q_2^2(\alpha)$ and subtract them. Then we multiply Eq. (7.33a) by $\bar{Q}_2^0(\alpha)$, Eq. (7.33b) by $Q_2^0(\alpha)$ and subtract them and divide the resulting polynomial by α^*. Thus we find

$$\begin{aligned} \alpha^* \; & [Q_2^1(\alpha)\bar{Q}_2^2(\alpha) - Q_2^2(\alpha)\bar{Q}_2^1(\alpha)] + \\ & Q_2^0(\alpha)\bar{Q}_2^2(\alpha) - \bar{Q}_2^0(\alpha)Q_2^2(\alpha) = 0 && (7.34a) \\ \alpha^* \; & [Q_2^2(\alpha)\bar{Q}_2^0(\alpha) - \bar{Q}_2^2(\alpha)Q_2^0(\alpha)] + \\ & Q_2^1(\alpha)\bar{Q}_2^0(\alpha) - Q_2^0(\alpha)\bar{Q}_2^1(\alpha) = 0. && (7.34b) \end{aligned}$$

Now we multiply Eq. (7.34a) by $[Q_2^2(\alpha)\bar{Q}_2^0(\alpha) - \bar{Q}_2^2(\alpha)Q_2^0(\alpha)]$, Eq. (7.34b) by $[Q_2^1(\alpha)\bar{Q}_2^2(\alpha) - Q_2^2(\alpha)\bar{Q}_2^1(\alpha)]$ and subtract them again and end up with a polynomial of degree 8 in α. Note that this means that it may not be possible to write the density operator as a convex sum of 6 product vectors. In fact, we have confirmed that and found examples in which one needs 8 product vectors.

Conclusions

We have studied the separability properties of density operators acting on $\mathbb{C}^2 \otimes \mathbb{C}^N$ and with positive partial transpose. In particular, we have found a necessary and sufficient criterion for separability of generic low rank density operators ρ. This criterion requires finding roots of complex polynomials, which give rise to all the product vectors in the ranges of ρ and ρ^{T_A}.

From our analysis it follows that for density operators with positive partial transpose and which are supported on $\mathbb{C}^2 \otimes \mathbb{C}^N$: (i) if $r(\rho) = N$ then ρ is separable and can be written as a convex sum of N product vectors; (ii) if ρ is a bound entangled state, then $r(\rho) > N$; (iii) if $r(\rho) = r(\rho^{T_A}) = N + 1$, then ρ is separable iff there exists a product vector $|e, f\rangle \in R(\rho)$ such that $|e^*, f\rangle \in R(\rho^{T_A})$; (iv) for generic ρ with $r(\rho) + r(\rho^{T_A}) \leq 3N$ we have given a necessary and sufficient criterion for separability; (v) we have shown how one can decrease the rank of an arbitrary state and its partial transpose to end up in the region $r(\rho) + r(\rho^{T_A}) \leq 3N$; (vi) any state which is invariant under partial transposition, that is $\rho = \rho^{T_A}$, is separable; (vii) density operators which are close (where close is defined in terms of the operator norm) to their partial transposes are also separable.

In Ref. [79] the methods derived in this section have been generalized to the $\mathbb{C}^M \otimes \mathbb{C}^N$, $M \leq N$ case. The authors derived necessary and sufficient conditions for separability for generic density operators, fulfilling $r(\rho) + r(\rho^{T_A}) \leq 2MN - M - N + 2$. The methods have also been applied to the multipartite case, in particular to the case of two qubits and a multilevel system, i.e. for density operators corresponding to the Hilbert space $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^N$ [88]. In that paper it has been proven that a PPT state, ρ, with $r(\rho) \leq N$ is fully separable. Computable necessary and sufficient conditions for separability are presented there for states fulfilling $r(\rho) + r(\rho^{T_A}) + r(\rho^{T_B}) + r(\rho^{T_C}) \leq 15N - 1$.

7.1.2 Entanglement witnesses and bound entangled states

From a different point of view, a very general approach to analyze the separability problem is based on the entanglement witnesses (EW) and positive maps (PM) [71] (Sec. 1.2.1). Recall, that EWs [140, 139] are operators that detect the presence of entanglement. Starting from these operators one can define PM's (see [84] and Sec. 1.2.1) that also detect entanglement. As already mentioned, an example of a PM is precisely partial transposition [118, 138, 157]. The importance of EW stems from the fact that a given operator is entangled iff there exists an EW that detects it [71](Theorem 1.1).

Thus, if one was able to construct all possible EW (or PM) one would have solve the problem of separability. Unfortunately, it is not known how to construct EW that detect PPTES in general. The only result in this direction so far has been given in Ref. [140, 139], although some preliminary results exist in the mathematical literature [156, 99, 22]. Starting from a PPTES fulfilling certain properties (related to the existence of unextendible basis of product vectors [11, 29, 9, 77]), it has been shown how to construct an EW (and the corresponding PM) that detects it. Perhaps, one of the most interesting goals regarding the separability problem is to develop a constructive and operational approach using EW and PM that allows us to detect mixed entanglement.

In this section we realize this goal partially: we introduce a powerful technique to construct EW and PM that, among other things, allows us to study the separability of certain density operators . In particular, we show how to construct optimal EW; that is, operators that detect the presence of entanglement in an optimal way. We specifically concentrate on non–decomposable EW, which are those that detect the presence of PPTES. Furthermore, we present a way of constructing optimal EW for edge PPTES. Our method generalizes the one introduced by Terhal [140, 139] to the case in which there are no unextendible basis of product vectors. When combined with our previous results (Sec. 7.1.1 see also [95, 79]) regarding subtracting product vectors from PPTES, the construction of non–decomposable optimal EW starting from edge PPTES (Sec. 1.2.1) gives rise to a novel sufficient criterion for non–separability of general density operators with positive partial transposition. We illustrate our method by constructing optimal EW that detect some known examples of PPTES [75] in $H = \mathbb{C}^2 \otimes \mathbb{C}^4$. The corresponding PM constitute the first examples of PM with minimal "qubit" domain, or – equivalently – minimal hermitian conjugate codomain.

This section is organized as follows. First of all we review the definition of EW and fix some notation. Then we study general EW. We define optimal witnesses and find a criterion to decide whether an EW is optimal or not. In the following section ("Non–decomposable Entanglement Witness") we restrict the results to non–decomposable EW. In particular, we show how to optimize them by subtracting decomposable operators. We give an explicit method to optimize both, general and non–decomposable EW. We also show how to construct non–decomposable EW, and that this leads to a sufficient criterion of non–separability. The construction and optimization is based on the use of "edge" PPTES. After that we extend our results to positive maps. We illustrate our methods and results starting from the examples of PPTES given in Ref. [75]. Then we present a necessary condition for separability. Finally, we derive a canonical form of non–decomposable EWs

and the corresponding PMs. This part of the Thesis also contains three appendices. In Appendix E.1 we describe in detail a method to check whether an EW is optimal or not. As an example we present in Appendix E.2 an optimal EW in $\mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. In Appendix E.3 we discuss separately some important properties of the edge PPTES, and show that they provide a canonical decomposition of mixed states with positive partial transpose.

Definitions and notation

Let us recall here some definitions which we are using throughout the present section.

We say that an operator $W = W^\dagger$ acting on $H = H_A \otimes H_B$ is an EW if [71, 140, 139] (see also Sec. 1.2.1):

(I) $\langle e, f|W|e, f\rangle \geq 0$ for all product vectors $|e, f\rangle$;

(II) has at least one negative eigenvalue (i.e. is not positive);

(III) $\mathrm{tr}(W) = 1$.

As explained already in Sec. 1.2.1 property (I) implies that $\langle\rho\rangle_W \equiv \mathrm{tr}(W\rho) \geq 0$ for all ρ separable. Thus, if $\langle\rho\rangle_W < 0$ for some $\rho \geq 0$, then ρ is entangled. Property (II) implies that every EW detects something, since in particular it detects the projector on the subspace corresponding to the negative eigenvalues of W. The third property (III) is just normalization condition that we need in order to compare the action of different EW [1].

Analogously to the previous section we will denote by $K(\rho)$ and $R(\rho)$ the kernel and range of ρ, respectively. Whenever it does not matter whether we take the partial transpose of an operator X with respect to the first or second system we will simply write X^T.

On the other hand, we will encounter several kinds of operators (EW, positive operators, decomposable operators, etc) and vectors. In order to help to identify the kind of operators and vectors we use, and not to overwhelm the reader by specifying at each point their properties, we will use the following notation throughout this section:

- W will denote an EW.
- P, Q will denote positive operators. Unless specified they will have unit trace [$\mathrm{tr}(P) = \mathrm{tr}(Q) = 1$].

[1] As shown in Sec. 1.2.1, (see footnote [8] on p. 22), if W fulfills (I–II), and λ is a positive number, then λW also fulfills (I–II), so that we can always normalize W to have (III).

- D will denote a decomposable operator. That is, $D = aP + bQ^T$, where $a, b \geq 0$. Unless stated, all decomposable operators that we use will have unit trace (i.e., $b = 1 - a$).
- ρ will denote a positive operator (not necessarily of trace 1).
- $|e, f\rangle$ will denote product vectors with $|e\rangle \in H_A$ and $|f\rangle \in H_B$. Unless specified, they will be normalized.

General entanglement witnesses

In this section we first give some definitions directly related to EW. Then we introduce the concept of optimal EW. We derive a criterion to determine when an EW is optimal. This criterion will serve us to find an optimization procedure for these operators.

Definitions

Given an EW, W, we define:

- $D_W = \{\rho \geq 0$, such that $\langle\rho\rangle_W < 0\}$; that is, the set of operators detected by W.
- Finer: Given two EW, W_1 and W_2, we say that W_2 is *finer* than W_1, if $D_{W_1} \subseteq D_{W_2}$; that is, if all the operators detected by W_1 are also detected by W_2.
- Optimal entanglement witness (OEW): We say that W is an OEW if there exist no other EW which is finer.
- $P_W = \{|e, f\rangle \in H$, such that $\langle e, f|W|e, f\rangle = 0\}$; that is, the set of product vectors on which W vanishes. As we will show, these vectors are closely related to the optimality property.

Note the important role that the vectors in P_W play regarding entanglement (for a method to determine P_W in practice, see Appendix E.1). If we have an EW, W, which detects a given operator ρ, then the operator $\rho' = \rho + \rho_w$ where

$$\rho_w = \sum_k p_k |e_k, f_k\rangle\langle e_k, f_k| \tag{7.35}$$

with $p_k \geq 0$, and $|e_k, f_k\rangle \in P_W$ is also detected by W. In fact, this means that any operator of the form (7.35) is in the border between separable states and non–separable states, in the sense that if we add an arbitrarily small amount

of ρ to it we obtain a non–separable state. Thus, the structure of the sets P_W characterizes the border between separable and non–separable states. In fact, from the results of this section it will become clear that we can restrict ourselves to the structure of the sets of P_W corresponding to OEW's.

Optimal entanglement witnesses

According to [71] (see also Theorem 1.1 in Sec. 1.2.1) ρ is nonseparable iff there exists an EW which detects it. Obviously, we can restrict ourselves to the study of OEW. For that, we need criteria to determine when an EW is optimal. In this subsection we will derive a necessary and sufficient condition for this to happen (Theorem 7.4 below). In order to do that, we first have to introduce some results that tell us under which conditions an EW is finer than another one.

Lemma 7.13 *Let W_2 be finer than W_1 and*

$$\lambda \equiv \inf_{\rho_1 \in D_{W_1}} \left| \frac{\langle \rho_1 \rangle_{W_2}}{\langle \rho_1 \rangle_{W_1}} \right|. \tag{7.36}$$

Then we have:

(i) *If $\langle \rho \rangle_{W_1} = 0$ then $\langle \rho \rangle_{W_2} \leq 0$.*

(ii) *If $\langle \rho \rangle_{W_1} < 0$, then $\langle \rho \rangle_{W_2} \leq \langle \rho \rangle_{W_1}$.*

(iii) *If $\langle \rho \rangle_{W_1} > 0$ then $\lambda \langle \rho \rangle_{W_1} \geq \langle \rho \rangle_{W_2}$.*

(iv) *$\lambda \geq 1$. In particular, $\lambda = 1$ iff $W_1 = W_2$.*

Proof: Since W_2 is finer than W_1 we will use the fact that for all $\rho \geq 0$ such that $\langle \rho \rangle_{W_1} < 0$ then $\langle \rho \rangle_{W_2} < 0$.

(i) Let us assume that $\langle \rho \rangle_{W_2} > 0$. Then we take any $\rho_1 \in \mathcal{D}_{W_1}$ so that for all $x \geq 0$, $0 \leq \tilde{\rho}(x) \equiv \rho_1 + x\rho \in \mathcal{D}_{W_1}$. But for sufficiently large x we have that $\langle \tilde{\rho}(x) \rangle_{W_2}$ is positive, which cannot be since then $\rho(x) \notin \mathcal{D}_{W_2}$.

(ii) We define $\tilde{\rho} = \rho + |\langle \rho \rangle_{W_1}| \mathbb{1} \geq 0$. We have that $\langle \tilde{\rho} \rangle_{W_1} = 0$. Using (i) we have that $0 \geq \langle \rho \rangle_{W_2} + |\langle \rho \rangle_{W_1}|$.

(iii) We take $\rho_1 \in D_{W_1}$ and define $\tilde{\rho} = \langle \rho \rangle_{W_1} \rho_1 + |\langle \rho_1 \rangle_{W_1}| \rho \geq 0$, so that $\langle \tilde{\rho} \rangle_{W_1} = 0$. Using (i) we have $|\langle \rho_1 \rangle_{W_1}| \langle \rho \rangle_{W_2} \leq |\langle \rho_1 \rangle_{W_2}| \langle \rho \rangle_{W_1}$. Dividing both sides by $|\langle \rho_1 \rangle_{W_1}| > 0$ and $\langle \rho \rangle_{W_1} > 0$ we obtain

$$\frac{\langle \rho \rangle_{W_2}}{\langle \rho \rangle_{W_1}} \leq \left| \frac{\langle \rho_1 \rangle_{W_2}}{\langle \rho_1 \rangle_{W_1}} \right|. \tag{7.37}$$

Taking the infimum with respect to $\rho_1 \in D_{W_1}$ in the rhs of this equation we obtain the desired result.

(iv) From (ii) immediately follows that $\lambda \geq 1$. On the other hand, we just have to prove that if $\lambda = 1$ then $W_1 = W_2$ (the only if part is trivial). If $\lambda = 1$, using (i) and (iii) we have that $\langle \rho_v \rangle_{W_1} \geq \langle \rho_v \rangle_{W_2}$ for all $\rho_v = |e, f\rangle\langle e, f|$ projector on a product vector. Since $\mathrm{tr}(W_1) = \mathrm{tr}(W_2)$ we must have $\mathrm{tr}[(W_1 - W_2)\rho_v] = 0$ for all ρ_v, since we can always find a product basis in which we can take the trace. But now, for any given $\rho \geq 0$ we can define $\tilde{\rho}(x) = \rho + x\mathbb{1}$ such that for large enough x, $\tilde{\rho}(x)$ is separable [158]. In that case we have $\langle \tilde{\rho}(x) \rangle_{W_1} = \langle \tilde{\rho}(x) \rangle_{W_2}$ which implies that $\langle \rho \rangle_{W_1} = \langle \rho \rangle_{W_2}$, i.e. $W_1 = W_2$.■

Corollary 7.8 *$D_{W_1} = D_{W_2}$ iff $W_1 = W_2$.*

Proof: We just have to prove the only if part. For that, we define λ as in (7.36). On the other hand, defining

$$\tilde{\lambda} \equiv \inf_{\rho_2 \in D_{W_2}} \left| \frac{\langle \rho_2 \rangle_{W_1}}{\langle \rho_2 \rangle_{W_2}} \right| \tag{7.38}$$

we have that $\tilde{\lambda} \geq 1$ since W_1 is finer than W_2 (Lemma 7.13(iv)). Equivalently,

$$1 \geq \sup_{\rho_1 \in D_{W_1}} \left| \frac{\langle \rho_1 \rangle_{W_2}}{\langle \rho_1 \rangle_{W_1}} \right| \geq \lambda \geq 1, \tag{7.39}$$

where for the last inequality we have used that W_2 is finer than W_1. Now, since $\lambda = 1$ we have that $W_1 = W_2$ according to Lemma 7.13(iv).■

Next, we introduce one of the basic results of this section. It basically tells us that an EW is finer than another one if they differ by a positive operator. That is, if we have an EW and we want to find another one which is finer, we have to subtract a positive operator.

Lemma 7.14 *W_2 is finer than W_1 iff there exists a P and $1 > \epsilon \geq 0$ such that $W_1 = (1 - \epsilon)W_2 + \epsilon P$.*

Proof: (If) For all $\rho \in D_{W_1}$ we have that $0 > \langle \rho \rangle_{W_1} = (1-\epsilon)\langle \rho \rangle_{W_2} + \epsilon \langle \rho \rangle_P$ which implies $\langle \rho \rangle_{W_2} < 0$ and therefore $\rho \in D_{W_2}$. (Only if) We define λ as in (7.36). Using Lemma 7.13(iv) we have $\lambda \geq 1$. First, if $\lambda = 1$ then according to Lemma 7.13(iv) we have $W_1 = W_2$ (i.e., $\epsilon = 0$). For $\lambda > 1$, we define $P = (\lambda - 1)^{-1}(\lambda W_1 - W_2)$ and $\epsilon = 1 - 1/\lambda > 0$. We have that $W_1 = (1-\epsilon)W_2 + \epsilon P$,

so that it only remains to be shown that $P \geq 0$. But this follows from Lemma 7.13(i–iii) and the definition of λ, $\lambda = \inf_{\rho_1 \in D_{W_1}} \left| \frac{\langle \rho_1 \rangle_{W_2}}{\langle \rho_1 \rangle_{W_1}} \right|$.■

The previous lemma provides us with a way of determining when an EW is finer than another one. With this result, we are now at the position of fully characterizing OEW.

Theorem 7.4 *(Optimal entanglement witness) W is optimal iff for all P and $\epsilon > 0$, $W' = (1+\epsilon)W - \epsilon P$ is not an EW [does not fulfill (I)].*

Proof: (If) According to Lemma 7.14, there is no EW which is finer than W, and therefore W is optimal. (Only if) If W' is an EW, then according to Lemma 7.14 W is not optimal.■

The previous theorem tells us that W is optimal iff when we subtract any positive operator from it, the resulting operator is not positive on product vectors. This result is not very practical because of two reasons: (1) for a given P it is typically very hard to check whether there exists some $\epsilon > 0$ such that $W - \epsilon P$ is positive on all product vectors; (2) it may be difficult to find a particular P that can be subtracted from W among all possible positive operators. In Appendix E.1 we show how to circumvent these two drawbacks in practice: we give a simple criterion to determine when a given P can be subtracted from W. This allows us to determine which are the positive operators which can be subtracted from a given EW.

In the rest of this subsection we will present some simple results related to these two questions. First, it is clear that not every positive operator P can be subtracted from an EW, W. In particular, the following lemma tells us that it must vanish on P_W.

Lemma 7.15 *If $PP_W \neq 0$ then P cannot be subtracted from W.*

Proof: There exists some $|e_0, f_0\rangle \in P_W$ such that $\langle e_0, f_0|P|e_0, f_0\rangle > 0$. Substituting this product vector in the condition I for any $W - \epsilon P$ we see that the inequality is not fulfilled for any $\epsilon > 0$, i.e. P cannot be subtracted.■

Corollary 7.9 *If P_W spans H then W is optimal.*

Note that, as announced at the beginning of this section, the set P_W plays an important role in determining the properties of the separable states which lie on the border with the entangled states. We see here, that this set also plays an important role in determining whether an EW is optimal or not.

On the other hand, in order to check whether a given operator P can be subtracted or not from W, one has to check whether there exists some

$\epsilon > 0$ such that $\langle e, f|W - \epsilon P|e, f\rangle > 0$ for all $|e, f\rangle$. The following lemma gives an alternative way to do this. In fact, it gives a necessary and sufficient criterion for an EW to be optimal. For a given $|e\rangle \in H_A$, we will denote by $W_e \equiv \langle e|W|e\rangle$.

Lemma 7.16 *W is optimal iff for all $|\Psi\rangle$ orthogonal to P_W*

$$\epsilon \equiv \inf_{|e\rangle \in H_A} \left[\langle \Psi|e\rangle W_e^{-1} \langle e|\Psi\rangle\right]^{-1} = 0. \tag{7.40}$$

Proof: (If) Let us assume that W is not optimal; that is, there exists $W' \neq W$, finer than W. Then, according to Lemma 7.14 we have that there exists $\epsilon_0 > 0$ and $P \geq 0$ such that $W' = (W - \epsilon_0 P)/(1 - \epsilon_0)$. Imposing that W' is positive on product vectors (i.e. $W'_e \geq 0$ for all $|e\rangle \in H_A$) we obtain $0 \leq \langle e|W - \epsilon_0 P|e\rangle \leq W_e - \epsilon_0 \lambda_\Psi \langle e|\Psi\rangle\langle\Psi|e\rangle$, where $|\Psi\rangle$ is any eigenstate of P with nonzero eigenvalue λ_Ψ. According to Lemma 7.1, this last operator is positive iff both: (i) $\langle e|\Psi\rangle$ is in the range of $\langle e|W|e\rangle$, which imposes that $|\Psi\rangle$ is orthogonal to P_W; (ii) $\lambda_\Psi \epsilon_0 \leq [\langle \Psi|e\rangle W_e^{-1} \langle e|\Psi\rangle]^{-1}$, which imposes that $\epsilon \geq \lambda_\Psi \epsilon_0 > 0$ for that given $|\Psi\rangle$. (Only if) Let us assume that there exists some $|\Psi\rangle$ orthogonal to P_W such that $\epsilon > 0$. Then, using the same arguments one can show that $W' \equiv (W - \epsilon|\Psi\rangle\langle\Psi|)/(1-\epsilon) \neq W$ is an EW. According to Lemma 7.14, W' is finer than W, so that W is not optimal.■

Decomposable entanglement witnesses

As already mentioned in Sec. 1.2.1, the class of decomposable entanglement witnesses (d–EW) is very simple to characterize [157]. Recall that those are EW that can be written in the form

$$W = aP + (1-a)Q^T, \tag{7.41}$$

where $a \in [0, 1]$. As it is well known (see next section), these EW cannot detect PPTES. In any case, for the sake of completeness, we will give some simple properties of optimal d–EW.

Theorem 7.5 *Given a d–EW, W, if it is optimal then it can be written as $W = Q^T$, where $Q \geq 0$ contains no product vector in its range.*

Proof: Since W is decomposable, it can be written as $W = aP + (1-a)Q^T$. $W' \propto W - aP$ is also a witness, which according to Lemma 7.14 is finer than W, and therefore W is not optimal. On the other hand, if $|e, f\rangle \in R(Q)$ then for some $\lambda > 0$ we have that $W \propto (Q - \lambda|e, f\rangle\langle e, f|)^T$ is finer than W, and therefore this last is not optimal.■

This previous result can be slightly generalized as follows:

Theorem 7.6 *Given a d–EW, W, if it is optimal then it can be written as $W = Q^T$, where $Q \geq 0$ and there is no operator $P \in R(Q)$ such that $P^T \geq 0$.*

Proof: Is the same as in previous theorem.■

Corollary 7.10 *Given a d–EW, W, if it is optimal then W^T is not an EW [does not fulfill (II)].*

Proof: Using Theorem 7.5 we have that $W = Q^T$ with $Q \geq 0$. Then $W^T = Q \geq 0$, which does not satisfy property (II). ■

Non–decomposable entanglement witnesses

In the previous section we have been concerned with EW in general. As mentioned above, when studying separability we just have to consider those EW that can detect PPTES. In order to characterize them, one defines non–decomposable witnesses (nd–EW) as those EW which cannot be written in the form (7.41) [157]. This section is devoted to this kind of witnesses. The importance of nd–EW in order to detect PPTES is reflected in the following

Theorem 7.7 *An EW is non–decomposable iff it detects PPTES.*

Proof: (If) Let us assume that the EW is decomposable. Then it cannot detect PPT, since if $\rho, \rho^T \geq 0$ we have $\mathrm{tr}[(aP + (1-a)Q^T)\rho] = a\mathrm{tr}(P\rho) + (1-a)\mathrm{tr}(Q\rho^T) \geq 0$. (Only if) The set of decomposable witnesses is convex and closed, and W, as a set containing one point, is a closed convex set itself. Thus, from Hahn–Banach theorem [121] it follows that there exists an operator ρ such that: (i) $\mathrm{tr}[\rho(aP + (1-a)Q^T)] \geq 0$ for all $P, Q \geq 0$, $a \in [0,1]$; (ii) $\mathrm{tr}(\rho W) < 0$. From (i), taking $a = 1$ we infer that $\rho \geq 0$; on the other hand, taking $a = 0$ we obtain that $\mathrm{tr}[\rho^T Q] \geq 0$ for all $Q \geq 0$, and therefore $\rho^T \geq 0$. Thus, W detects ρ which is a PPTES.■

Corollary 7.11 *Given an operator D, it is decomposable iff $\mathrm{tr}(D\rho) \geq 0$ for all $\rho, \rho^T \geq 0$.*

Definitions

In this subsection we introduce some definitions which are parallel to those given in the previous section. Given a nd–EW, W, we define:

- $d_W = \{\rho \geq 0$, such that $\rho^T \geq 0$ and $\langle\rho\rangle_W < 0\}$; that is, the set of PPT operators detected by W.

- Non–decomposable-finer (nd–finer): Given two nd–EW, W_1 and W_2, we say that W_2 is *nd–finer* than W_1, if $d_{W_1} \subseteq d_{W_2}$; that is, if all the operators detected by W_1 are also detected by W_2.

- Non–decomposable optimal entanglement witness (nd–OEW): We say that W is an nd–OEW if there exist no other nd–EW which is nd–finer.

- $p_W = \{|e,f\rangle \in H$, such that $\langle e,f|W|e,f\rangle = 0\}$; that is, the product vectors on which W vanishes.

Note again the important role that the vectors in p_W play regarding PPTES. If we have a nd–EW, W, which detects a given PPTES ρ, then the operator $\rho' = \rho + \rho_w$ where ρ_w has the form (7.35) with $p_k \geq 0$, and $|e_k, f_k\rangle \in p_W$ also describes a PPTES. Thus, any operator of the form (7.35) lies in the border between separable states and PPTES.

Optimal non–decomposable entanglement witness

The goal of this section is to find a necessary and sufficient condition for a nd–EW to be optimal. We start by proving a similar result to the one given in Lemma 7.13, but for nd–EW:

Lemma 7.17 *Let W_2 be nd–finer than W_1,*

$$\lambda \equiv \inf_{\rho_1 \in d_{W_1}} \left| \frac{\mathrm{tr}(W_2\rho_1)}{\mathrm{tr}(W_1\rho_1)} \right|, \tag{7.42}$$

and now both, $\rho, \rho^T \geq 0$. Then we have (i–iv) as in Lemma 7.13.

Proof: The proof is basically the same as in Lemma 7.13 and will be omitted here.

Corollary 7.12 *Given two nd–EW, $W_{1,2}$, then $d_{W_1} = d_{W_2}$ iff $W_1 = W_2$.*

Proof: The proof is basically the same as Corollary 7.8 and will be omitted here.

Lemma 7.18 *Given two nd–EW, $W_{1,2}$, W_2 is nd–finer than W_1 iff there exists a decomposable operator D and $1 > \epsilon \geq 0$ such that $W_1 = (1-\epsilon)W_2 + \epsilon D$.*

Proof: (If) Given any $\rho, \rho^T \geq 0$, we have that if $\rho \in d_{W_1}$ then $0 > \langle\rho\rangle_{W_1} = (1-\epsilon)\langle\rho\rangle_{W_2} + \epsilon\langle\rho\rangle_D \geq \langle\rho\rangle_{W_2}$, where in the last inequality we have used that $\langle\rho\rangle_D \geq 0$ since D is decomposable (see Corollary 7.11). Therefore $\rho \in d_{W_2}$. (Only if) We define λ as in (7.42), so that $\lambda \geq 1$ according to Lemma 7.17(iv). If $\lambda = 1$ we have $W_1 = W_2$. If $\lambda > 1$ we define $D = (\lambda-1)^{-1}(\lambda W_1 - W_2)$ and $\epsilon = 1 - 1/\lambda$. We have that $W_1 = (1-\epsilon)W_2 + \epsilon D$, so that it only remains to be shown that D is decomposable. But from Lemma 7.17(i–iii) and the definition of λ it follows that $\langle\rho\rangle_D \geq 0$ for all $\rho, \rho^T \geq 0$. Using Corollary 7.11 we then have that D is decomposable.■

Now we are able to fully characterize nd–OEW.

Theorem 7.8 *Given an nd–EW, W, it is nd–optimal iff for all decomposable operators D and $\epsilon > 0$, $W' = (1+\epsilon)W - \epsilon D$ is not an EW [does not fulfill (I)].*

Proof: Is the same as for Theorem 7.4.■

Theorems 7.4 and 7.8 allow us to relate OEW and nd–OEW. In this way we can directly translate the results for general OEW to nd–OEW. We have

Theorem 7.9 *Given a nd–EW, W, W is a nd–OEW iff both W and W^T are OEW.*

Proof: (If) Let us assume that W is not a nd–OEW. Then, according to Theorem 7.8 there exists $\epsilon > 0$ and a decomposable operator D such that $W' = (1+\epsilon)W - \epsilon D$ is a nd–EW. We can write $D = aP + (1-a)Q^T$, with $a \in [0,1]$. If $a \neq 0$, then $W_1 = (1+a\epsilon)W - a\epsilon P$ fulfills $\langle e,f|W_1|e,f\rangle \geq \langle e,f|W'|e,f\rangle \geq 0$, and therefore, according to Lemma 7.14, W is not optimal. If $a \neq 1$ then $W_2 = [1+(1-a)\epsilon]W^T - (1-a)\epsilon Q$ fulfills $\langle e,f|W_2|e,f\rangle \geq \langle e,f|(W')^T|e,f\rangle \geq 0$, i.e. is an EW and therefore W^T is not optimal. (Only if) According to Theorem 7.8, if W is nd–optimal then for all $D = aP + (1-a)Q^T$, with $a \in [0,1]$, and all $\epsilon > 0$ we have that $W' = (1-\epsilon)W - \epsilon D$ does not satisfy (I). Taking $a = 1$ we have for all P and $\epsilon > 0$, $W_1 = (1-\epsilon)W - \epsilon P$ does not fulfill (I), and therefore (Theorem 7.4) W is optimal; analogously, taking $a = 0$ we have that W^T is optimal also.■

Corollary 7.13 *W is a nd–OEW iff W^T is an nd–OEW.*

Optimization

In this section we give a procedure to optimize EW which is based on the results of the previous sections.

Optimization of general entanglement witnesses

Our method is based on the following lemma. It tells us how much we can subtract from an EW. Here we will denote by $W_e = \langle e|W|e\rangle$ and $P_e = \langle e|P|e\rangle$ where $|e\rangle \in H_A$, by $[\ldots]_{\min}$ the minimum eigenvalue, and by $[\ldots]_{\max}$ the maximum eigenvalue. On the other hand, $X^{-1/2}$ will denote the square root of the pseudoinverse of X[2].

Lemma 7.19 *If there exists some P such that $PP_W = 0$ and*

$$\begin{aligned} \lambda_0 &\equiv \inf_{|e\rangle\in H_A} \left[P_e^{-1/2} W_e P_e^{-1/2}\right]_{\min} \\ &= \left(\sup_{|e\rangle\in H_A} \left[W_e^{-1/2} P_e W_e^{-1/2}\right]_{\max}\right)^{-1} > 0. \end{aligned} \tag{7.43}$$

then

$$W'(\lambda) \equiv (W - \lambda P)/(1-\lambda) \tag{7.44}$$

with $\lambda > 0$ is an EW iff $\lambda \leq \lambda_0$.

Proof: Let us find out for which values of $\lambda \geq 0$, $W'(\lambda)$ is an EW. We have to impose condition (I), which can be written as $\langle e|W'(\lambda)|e\rangle \geq 0$, i.e.

$$W_e - \lambda P_e \geq 0. \tag{7.45}$$

Multiplying by $P_e^{-1/2}$ on the right and left of this equation we obtain $P_e^{-1/2} W_e P_e^{-1/2} \geq \lambda$, which immediately gives that $\lambda \leq \lambda_0$ given in the first part of Eq. (7.43). On the other hand, multiplying by $W_e^{-1/2}$ on the right and left of Eq. (7.45) we obtain $W_e^{-1/2} P_e W_e^{-1/2} \leq 1/\lambda$, which immediately gives that $\lambda \leq \lambda_0$ given in the second equality of Eq. (7.43).■

Lemma 7.19 provides us with a direct method to optimize EW by subtracting positive operators for which the elements of P_W are contained in

[2]Given a selfadjoint operator X, its pseudoinverse X^{-1} is defined as the one that vanishes in $K(X)$ and so that $XX^{-1} = X^{-1}X$ is the projector in $R(X)$. If X has no zero eigenvalue, the pseudoinverse coincides with the inverse operator.

their kernels. The method thus consists of: (1) determining P_W; (2) choosing an operator P so that $PP_W = 0$ and determining λ using (7.43); (3) if $\lambda \neq 0$ then we subtract the operator P according to Lemma 7.19. Continuing in the same vein we will reach an OEW. In Appendix E.1 we show how to accomplish steps (1) and (2) in practice.

Optimization of non–decomposable entanglement witnesses

For nd–EW we have the following generalization of Lemma 7.19:

Lemma 7.20 *Given a nd–EW, W, if there exists some decomposable operator D such that $Dp_W = 0$ and*

$$\lambda_0 \equiv \inf_{|e\rangle \in H_A} \left[D_e^{-1/2} W_e D_e^{-1/2}\right]_{\min} = \left(\sup_{|e\rangle \in H_A} \left[W_e^{-1/2} D_e W_e^{-1/2}\right]_{\max}\right)^{-1} > 0. \tag{7.46}$$

then

$$W'(\lambda) \equiv (W - \lambda D)/(1 - \lambda) \tag{7.47}$$

with $\lambda > 0$ is a nd–EW iff $\lambda \leq \lambda_0$.

Proof: Is the same as for Lemma 7.19.

With the help of Lemma 7.20 we can optimize nd–EW by subtracting decomposable operators as follows: (1) determining p_W and p_{W^T}; (2) choosing P, Q so that $Pp_W = 0$ and $Qp_{W^T} = 0$, building $D = aP + (1-a)Q^T$ with $a \in [0,1]$, and determining λ_0 using (7.46); (3) if $\lambda_0 \neq 0$ then we subtract the operator D according to Lemma 7.20.

Detectors of "edge" PPTES

In the previous subsections we have given two optimization procedures. In both of them, starting from a general EW one can obtain one which is optimal (or nd–optimal). It may well happen that the EW found in this way is non–decomposable even though the original one was decomposable. To check that one simply has to use Corollary 7.10; that is, check whether W^T is an EW or not. In case it is, then the OEW W is non–decomposable. However, nothing guarantees that the final EW is non–decomposable if the original one is not. In this subsection we describe a general method to construct nd–EW using

the optimization procedures introduced earlier. This method generalizes the one presented in Ref. [140, 139].

We are going to use the results presented in Sec. 7.1.1 (see also [95, 79]). There, we have already used and discussed the "edge" PPTES, without naming them, however. Let us now recall the following definition (Sec. 1.2.1, Sec. 7.1.1):

Definition 7.1 *[see Sec. 7.1.1 and Ref. [95]] A PPTES δ is an "edge" PPTES if for all product vector $|e,f\rangle$ and $\epsilon > 0$, $\delta - \epsilon|e,f\rangle\langle e,f|$ is not a PPTES.*

This definition implies that the "edge" states lie on the boundary between the PPTES and entangled states with non–positive partial transpose. In this subsection we will show how, out of an "edge" PPTES, we can construct a nd–OEW that detects it. As we mentioned in the introduction, "edge" PPTES are of special importance. In particular, they allow to provide a canonical form to write PPTES in arbitrary Hilbert spaces. For these reasons, some of the properties of the "edge" PPTES are discussed in Appendix E.3.

In order to check whether a PPTES δ is an "edge" PPTES we can use the range criterion (Lemma 1.1) of Ref. [75] (see also Sec. 7.1.1 and [95]). That is, δ is an "edge" PPTES iff for all $|e,f\rangle \in R(\delta)$, $|e,f^*\rangle \notin R(\delta^{T_B})$.

Let δ be an "edge" PPTES, and let us denote by P_1 the projector onto $K(\delta)$ and by Q_1 the projector onto $K(\delta^T)$. We define

$$W_\delta = a(P_1 + Q_1^T), \tag{7.48}$$

where $a = 1/\mathrm{tr}(P_1 + Q_1)$. Let us also define

$$\epsilon_1 \equiv \inf_{|e,f\rangle} \langle e,f|W_\delta|e,f\rangle. \tag{7.49}$$

Then we have

Lemma 7.21 *Given an "edge" PPTES δ, then $W_1 \propto W_\delta - \epsilon_1 \mathbb{1}$ is a nd–EW, where ϵ_1 and W_δ are defined in (7.49,7.48), respectively.*

Proof: We have that $\langle e,f|W_\delta|e,f\rangle = a(\langle e,f|P_1|e,f\rangle + \langle e,f^*|Q_1|e,f^*\rangle) \geq 0$. This quantity is zero iff $\langle e,f|P_1|e,f\rangle = \langle e,f^*|Q_1|e,f^*\rangle = 0$. But this is not possible since δ is an "edge" PPTES. Thus, $\langle e,f|W_\delta|e,f\rangle > 0$ for all $|e,f\rangle$. Defining ϵ_1 as in (7.49), and taking into account that $\langle e,f|W_\delta|e,f\rangle$ is a continuous function of (the coefficients of) $|e,f\rangle$ and that the set in which we are taken the infimum is compact, we obtain $\epsilon_1 > 0$. Then we

obviously have that W_1 fulfills properties (I) and (III). On the other hand, $\langle\delta\rangle_{W_1} \propto a(\langle\delta\rangle_{P_1} + \langle\delta^T\rangle_{Q_1}) - \epsilon_1 < 0$, since $P_1\delta = Q_1\delta^T = 0$. Thus, W_1 detects a PPTES, and therefore, according to Theorem 7.7 is non–decomposable.■

Note that Lemma 7.21 provides an important generalization of the method of Terhal [140, 139], based on the use of unextendible product bases [11, 29, 9, 77]. Our method works in Hilbert spaces of arbitrary dimensions, and in particular when $\dim(H_A) = 2$ (in $\mathbb{C}^2 \otimes \mathbb{C}^N$ dimensional systems) for which unextendible product basis do not exist. By combining Lemma 7.21 and the optimization procedure introduced earlier, we obtain a way of creating nd–OEW. Once we have W_1 we find p_{W_1} and $p_{W_1^T}$. We denote by P_2 and Q_2 the projector operators orthogonal to these two sets, respectively,

$$\epsilon_2 = \inf_{|e,f\rangle} \frac{\langle e,f|W_1|e,f\rangle}{\langle e,f|P_2 + Q_2^T|e,f\rangle}, \tag{7.50}$$

and $W_2 \propto W_1 - \epsilon_2(P_2 + Q_2^T)$. According to Lemma 7.18 we have that W_2 is nd–finer than W_1. Now we can define $p_{W_2}, p_{W_2^T}, P_3, Q_3$ and W_3 in the same way, and continue in this vein until for some k, $\epsilon_k = 0$. If W_k is not yet optimal, we still have to find other projectors such that we can optimize as explained in the previous subsections.

In a following section (denoted by "Illustration") we illustrate this method with a family of edge PPTES from Ref. [75]. In fact, as we will mention in that section, we have checked that the optimization method typically works as well by starting with three random vectors, and following a similar procedure to the one indicated here. This means that in our construction method we do not need in practice to start from an "edge" PPTES.

Sufficient condition for PPTES

In this subsection we use the results derived in the previous one to construct a sufficient criterion for non–separability of PPTES. Given an operator $\rho \geq 0$, with $\rho^T \geq 0$, we can always decompose it in the form [95, 79])

$$\rho = \rho_s + \delta, \tag{7.51}$$

where ρ_s is separable and δ is an "edge" PPTES. One such decomposition can be obtained by subtracting product vectors from ρ keeping it and its partial transpose positive, as explained in Sec. 7.1.1. More details concerning this decomposition, and in particular its canonical optimal form are presented in Appendix E.3. In this section we use this decomposition together with the following

Lemma 7.22 *Given a non–separable operator $\rho = \rho_s + \delta$, where $\rho_s \geq 0$ is separable then for all EW, W, such that $\langle\rho\rangle_W < 0$ we have that $\langle\delta\rangle_W < 0$.*

Proof: Obvious from the definition of EW.■

Lemma 7.22 tells us that if ρ is non–separable, then there must exist some EW that detect both δ and ρ. Actually, it is clear that there must exist an OEW with that property. In particular, if $\rho^T \geq 0$, it must be a nd–OEW. In the previous subsection we have shown how to build them out of "edge" PPTES. Thus, given ρ we can always decompose it in the form (7.51), construct an OEW that detects δ and check whether it detects ρ. In that case, we will have that ρ is non–separable. Thus, this provides a sufficient criterion for non–separability.

We stress the fact that for PPTES only a special class of states, namely the class of "edge" PPTES, is responsible for the entanglement properties. In fact, one should stress that very many of the examples of PPTES discussed so far in the literature belong to the class of "edge" PPTES: the $2\otimes4$ family from [75], the $n \otimes n$ states obtained via unextendible product basis construction [11, 29, 9, 77], the $3\otimes3$ states obtained via the chess-board method [19], and projections of continuous variable PPTES onto finite dimensional subspaces [78].

Positive maps

As shown in Sec. 1.2.1, the isomorphism [84] between a linear map, $\mathcal{E}_X : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_C)$ and an operator, X is given by

$$\mathcal{E}_X(Y) = \mathrm{tr}_A(X^{T_A}Y), \tag{7.52}$$

for all $Y \in \mathcal{B}(\mathcal{H}_A)$, where tr_A denotes the trace in H_A and the partial transpose is taken in the basis O_A and $X \propto \mathcal{E}_X(|\Psi\rangle\langle\Psi|)$, where

$$|\Psi\rangle = \sum_{k=1}^{d_A} |k\rangle_A \otimes |k\rangle_C. \tag{7.53}$$

Transposition (in a given basis O_A); that is, the map $\mathcal{E}_T$ such that $\mathcal{E}_T(Y) = Y^T$ is an example of positive (but not completely positive) map[3].The corresponding extension is the partial transposition.

We call a map $\mathcal{E}$ which can be written as $\mathcal{E} = \mathcal{E}_1 + \mathcal{E}_2 \cdot \mathcal{E}_T$, where $\mathcal{E}_{1,2}$ are completely positive[4] decomposable. Otherwise it is non–decomposable. Let us recall here the following equivalences (Sec. 1.2.1)

[3]Note that the corresponding operator is $T = (|\Psi\rangle\langle\Psi|)^{T_A}$, where $|\Psi\rangle$ is given in (7.53)

[4]Recall that a linear map is called completely positive if all the extensions of this map are positive, see Sec. 1.2.1 and Sec. 2.1.

(a) $\mathcal{E}_X$ is completely positive iff $X \geq 0$;

(b) $\mathcal{E}_X$ is positive but not completely positive iff X is an EW [except for the normalization condition (III)];

(c) $\mathcal{E}_X$ is decomposable iff X is decomposable.

As shown in Sec. 1.2.1, a state, $\rho \geq 0$ is entangled iff there exists a PM such that acting on ρ gives a non–positive operator, i.e. iff there exists a PM which "detects" ρ. This is simply due to the fact that

$$\langle \rho \rangle_X = \langle \Psi | \bar{\mathcal{E}}_X(\rho) | \Psi \rangle, \tag{7.54}$$

where $|\Psi\rangle = \sum_{k=1}^{d_B} |k\rangle_C \otimes |k\rangle_B$ and $\bar{\mathcal{E}}_X \equiv \mathcal{E}_X \otimes 1 : \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B) \rightarrow \mathcal{B}(\mathcal{H}_C) \otimes \mathcal{B}(\mathcal{H}_B)$ with $d_B \equiv \dim(H_B) = \dim(H_C)$ is an extension of the map $\mathcal{E}$. And, on the other hand, $\bar{\mathcal{E}}_X(\rho) \geq 0$ for any ρ separable (see Sec. 1.2.1). Note that PMs are "more efficient" in detecting entanglement than EW. The reason for this is that it may happen that $\bar{\mathcal{E}}_X(\rho)$ is non–positive but still $\langle \rho \rangle_X \geq 0$.

It is convenient to define finer and optimal PM as for EW. That is, given two PM, $\mathcal{E}_{1,2}$, we say that $\mathcal{E}_2$ is finer than $\mathcal{E}_1$ if it detects more. We say that a PM, $\mathcal{E}$, is optimal if there exists no one that is finer. In the same way we can define nd–finer and nd–optimal.

The results presented in the previous sections can be directly translated to PM given the following fact.

Lemma 7.23 *If W_2 is finer (nd–finer) than W_1 then $\mathcal{E}_{W_2}$ is finer (nd–finer) than $\mathcal{E}_{W_1}$.*

Proof: Using Lemma 7.14 we can write $W_1 = (1-\epsilon)W_2 + \epsilon P$. According to (7.52) we have that $\mathcal{E}_{W_1} = (1-\epsilon)\mathcal{E}_{W_2} + \epsilon \mathcal{E}_P$. Since $\mathcal{E}_P(\rho) \geq 0$ for all $\rho \geq 0$, we have that $\mathcal{E}_{W_2}$ is finer than $\mathcal{E}_{W_1}$. Using Lemma 7.18 we can also prove that it is nd–finer.■

From this lemma it follows that optimizing EWs implies optimizing PMs. In fact, the constructions that we have given in the previous section can be viewed as ways of constructing non–decomposable PM. In fact, since the method works for $\dim(H_A) = 2$, the resulting PM $\mathcal{E} : \mathcal{B}(\mathcal{H}_A) \rightarrow \mathcal{B}(\mathcal{H}_C)$ has a minimal "qubit" domain, or – equivalently – minimal hermitian conjugate codomain. Up to our knowledge, our method is the first one that permits to construct non–decomposable PM with these characteristics.

Illustration

In this section we explicitly construct a nd–OEW out of edge PPTES. We use, as a starting point, the family of PPTES introduced in Ref. [75].

Family of "edge" PPTES

We consider $H_A = \mathbb{C}^2$ and $H_B = \mathbb{C}^4$, and denote by $\{|k\rangle\}_{k=0}^{d_\alpha}$ ($\alpha = A, B$) an orthonormal basis in these spaces, respectively. Most of the time we will write the operators in those bases; that is, as matrices. For operators acting in $H_A \otimes H_B$ we will always use the following order $\{|0,0\rangle, |0,1\rangle, \ldots, |1,0\rangle, |1,1\rangle, \ldots\}$. On the other hand, all partial transposes will be taken with respect to H_B.

We consider the following family of positive operators [75]

$$\rho_b = \frac{1}{7b+1} \begin{pmatrix} b & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1+b}{2} & 0 & 0 & \frac{\sqrt{1-b^2}}{2} \\ b & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & b & 0 & \frac{\sqrt{1-b^2}}{2} & 0 & 0 & \frac{1+b}{2} \end{pmatrix}, \tag{7.55}$$

where $b \in [0,1]$. For $b = 0, 1$ those states are separable, whereas for $0 < b < 1$, ρ_b is an "edge" PPTES. This can be shown by checking directly that they violate the range criterion (Lemma 1.1) of Ref. [75].

If we take the partial transpose in the basis $\{|k\rangle\}$, the density operators ρ_b have the property that $\rho_b^T = U_B \rho_b U_B^\dagger$ with $U_B = (\sigma_x)_{03} \oplus (\sigma_x)_{12}$. Here, the subscript ij denotes the subspace, $\mathcal{H}_{Bij} \subset \mathcal{H}_B$ spanned by $\{|i\rangle, |j\rangle\}$ and σ_x is one of the Pauli-operators. Note that U_B is a real unitary operator acting only on H_B. This immediately implies that

$$\tilde{\rho}_b^T = \tilde{\rho}_b, \tag{7.56}$$

where $\tilde{\rho}_b = V_B \rho_b V_B^\dagger$ and $V_B = 1\sqrt{2}[(\mathbb{1} + i\sigma_x)_{03} \oplus (\mathbb{1} + i\sigma_x)_{12}]$. We will use the property (7.56) to simplify the problem of constructing the nd–OEW. Thus, we will concentrate from now on the operators $\tilde{\rho}_b$[5]. Obviously, $\tilde{\rho}_b$ is an "edge" PPTES for $1 > b > 0$.

[5]Note that if we define a basis in H_B as $\{V_B^\dagger |k\rangle\}$ we have that $\rho_b^T = \rho_b$, where the partial transposition is taken in that basis. This is an example, mentioned in Sec. 7.1.1, of a state being invariant under partial transposition (of system B!) but being entangled.

The projector onto the kernel of $\tilde{\rho}_b$, P_1, is invariant under the transformation $T_{AB} = T_A \otimes T_B$, where

$$T_A = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/3} \end{pmatrix}, \qquad (7.57)$$

$$T_B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(2\pi/3) & -\sin(2\pi/3) & 0 \\ 0 & \sin(2\pi/3) & \cos(2\pi/3) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that T_B is a real matrix. Later on we will need its eigenstates with real coefficients; they are $|0\rangle \pm |3\rangle$. Note also that $T_{AB}^3 = \mathbb{1}$.

Construction of nd–EW's

We use now the methods developed before to obtain a nd–OEW starting from $\tilde{\rho}_b$. That is, we define $W_b = P_1 + P_1^T$, where P_1 is the projector onto $K(\tilde{\rho}_b) = K(\tilde{\rho}_b^T)$. Our procedure consists of first subtracting the identity to obtain $W_1 = W_b - \epsilon_1 \mathbb{1}$. Then, we subtract $P_2 + Q_2^T$, $P_3 + Q_3^T$, etc. In the n–th step we will have

$$W_n = W_{n-1} - \epsilon_n (P_n + Q_n^T), \qquad (7.58)$$

where P_n (Q_n) is the projector orthogonal to the space spanned by $P_{W_{n-1}}$ ($P_{W_{n-1}^T}$). We will use the symmetries of $\tilde{\rho}_b$ to better understand the structure of W_n.

(a) $W_n = W_n^T$. We can prove this by induction. First, it is clear that $W_1 = W_1^T$. Let us now assume that $W_{n-1} = W_{n-1}^T$. Then we show that $W_n = W_n^T$. For that, we just have to show that the subspace spanned by $P_{W_{n-1}}$ is the same that the one spanned by $P_{W_{n-1}^T}$, so that $Q_n = P_n$. But this is clear since $W_{n-1} = W_{n-1}^T$.■

(b) $T_{AB} W_n T_{AB}^\dagger = W_n$. We prove this by induction. First, for $W_1 = P_1 + P_1^T - \epsilon_1 \mathbb{1}$ we have that $T_{AB} W_1 T_{AB}^\dagger = T_{AB} P_1 T_{AB}^\dagger + T_{AB} P_1^T T_{AB}^\dagger - \epsilon_1 \mathbb{1} = W_1$, since $T_{AB} P_1^T T_{AB}^\dagger = (T_{AB} P_1 T_{AB}^\dagger)^T$ (given the fact that T_B is real) and P_1 is invariant under T_{AB}. Then, let us assume that $T_{AB} W_{n-1} T_{AB}^\dagger = W_{n-1}$. In order to show that $T_{AB} W_n T_{AB}^\dagger = W_n$ we just have to show that P_n is invariant under T_{AB}, or, equivalently, that the subspace spanned by $P_{W_{n-1}}$ is invariant under T_{AB}. But this follows immediately from the fact that $T_{AB} W_{n-1} T_{AB}^\dagger = W_{n-1}$.■

From property (a) it follows that the vectors $|e, f\rangle \in P_{W_n}$ will have $|f\rangle$ real (unless we have degeneracies). This can be seen by noticing that those vectors minimize $\langle e, f|W_n|e, f\rangle$; defining $W_e \equiv \langle e|W_n|e\rangle$, we have that $W_e^T = W_e = W_e^\dagger$ is symmetric, and therefore the eigenstate corresponding to its minimum eigenvalue can be chosen to be real. On the other hand, starting from the property (b) it follows that if $|e, f\rangle \in P_{W_n}$ then $T_{AB}^\dagger |e, f\rangle, T_{AB}^{\dagger 2} |e, f\rangle \in P_{W_n}$. According to that, we will typically have two kinds of product vectors in P_{W_n}:

(1) $|e, f\rangle$ is an eigenstate of $T_{AB}^\dagger$ with $|f\rangle$ real: There are only 4 possible product vectors which fulfill these conditions: $\{|0\rangle, |1\rangle\} \otimes \{|0\rangle + |3\rangle, |0\rangle - |3\rangle\}$.

(2) $|e, f\rangle$ is not an eigenstate of $T_{AB}^\dagger$: Then, we will also have: $T_{AB}^\dagger |e, f\rangle$ and $(T_{AB}^\dagger)^2 |e, f\rangle \in P_W$.

We have carried out this procedure for $\tilde{\rho}_b$ and found nd–OEW for each b. We find that for the optimal EW we have two vectors of the kind (1) and six of the kind (2). In total we find eight product vectors in P_W, which span the whole Hilbert space and therefore the corresponding EW are optimal (see Corollary 7.9). This means that any operator of the form (7.35) with $|e_k, f_k\rangle \in P_W$ the product vectors we have found, and $p_k > 0$ will be a full range separable density operator that lies on the boundary between separable and PPTES. Up to our knowledge, this constitutes the first example of those operators[6].We have also created the PM corresponding to the nd–OEW, which are the first examples of non–decomposable PM with minimal "qubit" domain, or – equivalently – minimal hermitian conjugate codomain.

In Fig. 7.1 we show for which b' $\tilde{\rho}_{b'}$ is still detected by the nd–OEW created out of $\tilde{\rho}_b$. We find that for a given b, the optimal witness that we create detects all $\tilde{\rho}_{\tilde{b}}$ for $\tilde{b} \leq b'$. Thus, in the figure we plot b' as a function of b. As explained above, the corresponding positive map detects more than the witness itself. In the figure one can also see how much is detected by the positive map.

Obviously, the witnesses that we create do not only detect the density operators $\tilde{\rho}_b$. For instance one can check how much one can add the identity to certain $\tilde{\rho}_b$ keeping the state entangled. That is for which λ, $\tilde{\rho}_b + \lambda \mathbb{1}$ is still detected by the entanglement witness. This is shown in Fig. 7.2.

Finally, let us note that we have observed using numerical calculations that if one starts with a random projector, P of rank 3, and optimizes the

[6]These states can be prepared locally and, can be used to construct the PPTES by mixing them "weakly" with entangled states. This provides an interesting possibility of experimental realization of PPTES. This suggestion has been formulated by H. Weinfurter.

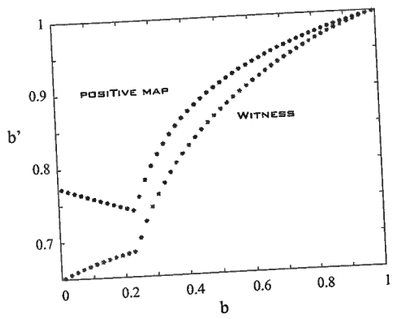

Figure 7.1: Values of b' for which if $\tilde{b} \leq b'$ $\tilde{\rho}_{\tilde{b}}$ is detected by the witness and the positive map created starting from $\tilde{\rho}_b$.

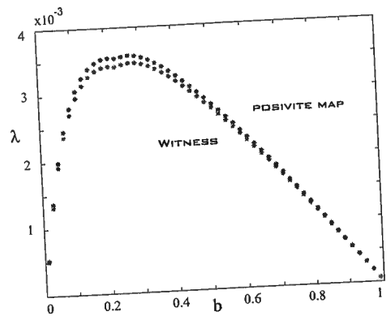

Figure 7.2: Maximum λ such that $\tilde{\rho}_b + \lambda \mathbb{1}$ is still detected by the witness and the positive map created starting from $\tilde{\rho}_b$.

decomposable operator $W \equiv P + P^{T_B}$ in the same way as the one described here, then one will end up with a nd–OEW $\tilde{W}$, where $p_{\tilde{W}}$ is complete. This means that in order to create nd–OEW one does not need to know in practice an edge PPTES. In another words, optimization itself is a way to reach nondecomposableness.

Analytical procedure

In this subsection we will present an analytical way to create nd–EW's. Furthermore we will given an example of such a witness, which detects ρ_b for all $b \in (0, 1)$. From Fig. 7.1 we see that the witness which detects most is the one we created out of $\tilde{\rho}_b$, where b is very close to 1. We will work with the original ρ_b (7.55).

We consider two hermitian operators A and B, with A positive on product vectors, i.e., $\langle e, f|A|e, f\rangle \geq 0$, whereas B does not have to. As before we denote by P_A (P_B) the (not necessarily complete) set of product vectors on which A (B) vanishes. We require that for all $|e, f\rangle \in P_A$, $\langle e, f|B|e, f\rangle \geq 0$. Then we define $W(x) \equiv \frac{1}{x}(A + xB)$ for any real x. So we have the following

Lemma 7.24 *If* $lim_{x\to 0}\langle\rho\rangle_{W(x)} < 0$ *then* ρ *is entangled.*

Proof: We prove that $\lim_{x\to 0}\langle e, f|W(x)|e, f\rangle \geq 0$. This implies that if ρ is separable, then $\lim_{x\to 0}\langle\rho\rangle_{W(x)} \geq 0$. Let us therefore distinguish two cases: (i) if $|e, f\rangle \in P_A$ then we have that $\lim_{x\to 0}\langle e, f|W(x)|e, f\rangle = \langle e, f|B|e, f\rangle$, which is, per assumption, positive. (ii) $|e, f\rangle \notin P_A$ then we have $\lim_{x\to 0}\langle e, f|W(x)|e, f\rangle = \lim_{x\to 0}\frac{a}{x} + b$, where $a = \langle e, f|A|e, f\rangle > 0$ and $b = \langle e, f|B|e, f\rangle$. Thus this limit tends to infinity, which proves the statement.■

Note that $W(x)$ is not an EW since it is not necessarily positive on product vectors. However, one can make it positive by adding the identity operator to convert it into an EW.

Corollary 7.14 *Given any* $x_0 > 0$, *then* $W(x_0) \equiv \frac{1}{x_0}(A + x_0B) + \lambda_{x_0}\mathbb{1}$, *with* $\lambda_{x_0} = -\ min_{|e,f\rangle}\langle e, f|\frac{1}{x_0}(A + x_0B)|e, f\rangle$ *is an EW.*

Let us now illustrate how we can use Lemma 7.24 to detect all the states ρ_b. We define

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{7.59}$$

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -2 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ -2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & 0 & -1 & 0 & 0 & 1 \end{pmatrix}. \tag{7.60}$$

One can easily show that $A = |\psi\rangle\langle\psi| + (|\phi\rangle\langle\phi|)^{T_B}$, where $|\psi\rangle = |01\rangle - |12\rangle$ and $|\phi\rangle = |02\rangle - |11\rangle$. Thus this operator is positive on product vectors, since it is decomposable. Let us now use unnormalized states in order to present the set of product vectors on which A vanishes, i.e. P_A. $P_A = P_{A_1} \cup P_{A_2}$, where $P_{A_1} = \{(|0\rangle + \alpha|1\rangle) \otimes (x|0\rangle + y|3\rangle) \forall \alpha, x, y\}$ and $P_{A_2} = \{(|0\rangle + e^{i\Phi}|1\rangle) \otimes [x|0\rangle + y|3\rangle + z(|1\rangle + e^{-i\Phi}|2\rangle)] \forall \Phi, x, y, z\}$. The operator B has to be positive on those product vectors, i.e., $\forall |e, f\rangle \in P_A$, $\langle e, f|B|e, f\rangle \geq 0$. In order to show that this is indeed like that let us distinguish the two cases: $|e, f\rangle \in P_{A_1}$ and $|e, f\rangle \in P_{A_2}$. In the first case we have that

$$\langle e|B|e\rangle = \begin{pmatrix} 1 + |\alpha|^2 & -2\alpha & 0 & 1 - |\alpha|^2 \\ -2\alpha^* & 1 + |\alpha|^2 & 0 & 0 \\ 0 & 0 & 1 + |\alpha|^2 & -2\alpha \\ 1 - |\alpha|^2 & 0 & -2\alpha^* & 1 + |\alpha|^2 \end{pmatrix} \tag{7.61}$$

and so $\langle e, f|B|e, f\rangle = |x + y|^2 + |\alpha|^2 |x - y|^2 \geq 0$. If $|e, f\rangle \in P_{A_2}$ then

$$\langle e|B|e\rangle = \begin{pmatrix} 2 & -2e^{i\Phi} & 0 & 0 \\ -2e^{-i\Phi} & 2 & 0 & 0 \\ 0 & 0 & 2 & -2e^{i\Phi} \\ 0 & 0 & -2e^{-i\Phi} & 2 \end{pmatrix} \tag{7.62}$$

which is a positive operator and so $\langle e, f|B|e, f\rangle \geq 0$. So those two operators A and B fulfill all the required properties. Furthermore one can show that $\langle \rho_b \rangle_A = 0$ and $\langle \rho_b \rangle_B < 0$ for all $0 < b < 1$. Thus we have that $\lim_{x \to 0} \langle W(x) \rho_b \rangle < 0$ for all $0 < b < 1$, where we defined $W(x) = \frac{1}{x}(A + xB)$.

As mentioned above we can use now $W(x)$ in order to create other PPTES just by adding product vectors on which $W(x)$ vanishes. To find the product vectors we can add, all we need to do is to determine the intersection between P_A and P_B. Since $P_B = \{(|0\rangle + e^{i\phi}|1\rangle) \otimes [a(|0\rangle + e^{-i\phi}|1\rangle + b(|2\rangle + e^{-i\phi}|3\rangle)] \forall \phi, a, b\}$ we have that $S \equiv P_A \cap P_B = P_{A_2} \cap P_B = \{(|0\rangle + e^{i\phi}|1\rangle) \otimes (|0\rangle + e^{-i\phi}|1\rangle + e^{-i2\phi}|2\rangle + e^{-i3\phi}|3\rangle) \forall \phi\}$. Note that S spans a 5 dimensional subspace and that the orthogonal subspace is spanned by the vectors $\{-|02\rangle + |13\rangle, -|01\rangle + |12\rangle, -|00\rangle + |11\rangle\}$.

Sufficient condition for inseparability

We present here another sufficient condition of inseparability (i.e. a necessary condition for separability), which is based on EWs. Let us assume the product vectors $|e, f\rangle$ to be normalized.

Lemma 7.25 *If* $max\{\mathrm{tr}(\rho^2), \mathrm{tr}[(\rho^{T_B})^2], \mathrm{tr}(\rho\rho^{T_B})\} > max_{|e,f\rangle} \langle e, f|\rho|e, f\rangle$, *then* ρ *is inseparable.*

Proof: Let us prove that this statement is true in the case where $\mathrm{tr}(\rho^2) = \max\{\mathrm{tr}(\rho^2), \mathrm{tr}[(\rho^{T_B})^2], \mathrm{tr}(\rho\rho^{T_B})\}$. All the other cases can be proven in the same way which implies that we can take the maximum of those three values. We define $r = \max_{|e,f\rangle} \langle e, f|\rho|e, f\rangle$ and the entanglement witness, $X = 1 - \frac{1}{r}\rho$. Assuming that $\mathrm{tr}(\rho) = 1$ we have that $\mathrm{tr}(X\rho) < 0$. It remains to prove that $\mathrm{tr}(X\tilde{\rho}) > 0$ for all $\tilde{\rho}$ separable. We write $\tilde{\rho} = \sum_i \lambda_i |e_i, f_i\rangle\langle e_i, f_i|$, and observe that: $r\mathrm{tr}(X\tilde{\rho}) = \mathrm{tr}[(\max_{|e,f\rangle} \langle e, f|\rho|e, f\rangle \mathbb{1} - \rho)\tilde{\rho}] = \sum_i \lambda_i (\max_{|e,f\rangle} \langle e, f|\rho|e, f\rangle - \langle e_i, f_i|\rho|e_i, f_i\rangle) \geq 0$. ∎

Unfortunately this criterion does not work for the family of states $\rho_b \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^4)$ [75] presented in Eq. (7.55). It does, however, detect the entanglement of the PPT states constructed from unextendible product bases (UPB's) [11]. In such case $\rho = P/K$, where P is a projector onto a space that does not contain any product vectors, $K = r(P)$, and $P = P^{T_B}$. Our criterion gives $\mathrm{tr}(\rho^2) = \mathrm{tr}[(\rho^{T_B})^2] = \mathrm{tr}(\rho\rho^{T_B}) = 1/K$, while $\langle e, f|\rho|e, f\rangle = \langle e, f|P|e, f\rangle/K < 1/K$.

Characterization of entanglement witnesses and positive maps

In this section we introduce a canonical form of nondecomposable entanglement witnesses and the corresponding positive maps. We also present a

nontrivial necessary condition for entanglement witnesses and positive maps to be extremal.

Let us recall here that every PPTES ρ is a convex combination of some separable state, ρ_{sep}, and an edge state, δ (1.16), i.e [7],

$$\rho = (1-p)\rho_{sep} + p\delta, \tag{7.63}$$

Let $\mathcal{S} \subset \mathcal{P}$ denote the convex set (cone) of separable (resp. PPT) states. Let $\mathcal{P}^\perp \subset \mathcal{S}^\perp$ be the convex sets (dual cones) of nd-EW's (resp. EW's). All those sets are closed.

Definition 7.2 *An EW (resp. decomposable EW), W is tangent to $\mathcal{S}$ (resp. tangent to $\mathcal{P}$) if there exists a state $\rho \in \mathcal{S}$ ($\rho \in \mathcal{P}$) such that* $\mathrm{tr}(W\rho) = 0$. *Furthermore, we say that W is tangent to $\mathcal{S}$ ($\mathcal{P}$) at $\rho \in \mathcal{S}$ ($\mathcal{P}$) if* $\mathrm{tr}(W\rho) = 0$.

Observation 1 *The state ρ is separable iff for all EW's tangent to $\mathcal{S}$,* $\mathrm{tr}(W\rho) \geq 0$.

Proof: (only if) is trivial; (if) Let ρ be an entangled state, and let W be an EW that detects ρ, i.e., $\mathrm{tr}(W\rho) < 0$. We define $0 < \epsilon = \inf_{|e,f\rangle} \langle e,f|W|e,f\rangle$. If $\epsilon = 0$ then W is tangent to $\mathcal{S}$. If $\epsilon > 0$ then $W' = W - \epsilon\mathbb{1}$ is still an EW which detects the entanglement of ρ and it is tangent to $\mathcal{S}$.

Observation 2 *If a decomposable EW, W, is tangent to $\mathcal{P}$ at ρ, then for any decomposition (7.63) W must also be tangent to $\mathcal{P}$ at the edge state δ.*

We can prove now

Proposition 7.1 *If an EW, W, which does not detect any PPTES, is tangent to $\mathcal{P}$ at some edge state δ then it is of the form*

$$W = P + Q^{T_B} \tag{7.64}$$

where $P, Q \geq 0$ such that $R(P) \subseteq K(\delta)$, $R(Q) \subseteq K(\delta^{T_B})$.

Proof: As mentioned before, an EW, W, which does not detect any PPTES must be decomposable; that is, $W = P + Q^{T_B}$. From the PPT property of δ and the positivity of P, Q we have that the ranges $R(\delta)$ and $R(P)$ [resp. $R(\delta^{T_B})$ and $R(Q)$] must be orthogonal.

We are now in the position to introduce a canonical form of nd–EW's:

[7] Note that the weight of the edge state, $p\mathrm{tr}(\delta)$, can be chosen minimal (see Appendix E.3).

Proposition 7.2 *Any nd–EW, W, has the form*

$$W = P + Q^{T_B} - \epsilon\mathbb{1}, \quad 0 < \epsilon \leq \inf_{|e,f\rangle} \langle e,f|P + Q^{T_B}|e,f\rangle. \tag{7.65}$$

where P and Q fulfill the conditions of Prop. 7.1 for some edge state δ [8].

Proof: Consider $W(\lambda) = W + \lambda\mathbb{1}$. Obviously for some $\lambda > 0$, say λ_0, $W(\lambda_0)$ becomes decomposable (or positive). Note that for any $\lambda < \lambda_0$, $W(\lambda)$ is nondecomposable and therefore it detects some PPTES ρ. Using continuity we conclude that $W(\lambda_0)$ is tangent to $\mathcal{P}$. From Obs. 2 there exists an edge state δ to which $W(\lambda_0)$ is tangent. From Prop. 7.1 we obtain that $W(\lambda_0) = P + Q^{T_B}$, where P and Q satisfy the needed conditions, and consequently $W = P + Q^{T_B} - \epsilon\mathbb{1}$ with $\epsilon = \lambda_0$. Since W is EW, ϵ must not be greater than $\inf_{|e,f\rangle} \langle e,f|P + Q^{T_B}|e,f\rangle$.

Proposition 7.3 *If the assumptions of Prop. 7.2 hold then W is of the form (7.65) with $R(P)$, $R(Q)$ orthogonal to some Hilbert subspaces $\mathcal{H}^a$ and $\mathcal{H}^b$, respectively, where: (i) there exists no $|e,f\rangle \in \mathcal{H}^a$ s.t. $|e,f^*\rangle \in \mathcal{H}^b$; (ii) $R[\mathrm{tr}_B(P_{\mathcal{H}^a})] = R[\mathrm{tr}_B(P_{\mathcal{H}^b})]$, $R[\mathrm{tr}_A(P_{\mathcal{H}^a})] = R[\mathrm{tr}_A(P_{\mathcal{H}^b})^*]$, where P_X stands for the projector onto the subspace X; (iii)* $\dim\mathcal{H}^x > \max[r(\mathrm{tr}_A(P_{\mathcal{H}^x})), r(\mathrm{tr}_B(P_{\mathcal{H}^x}))]$, $x = a, b$.

Proof: The point (i) is clear; (ii) and (iii) follow from simple analysis of the ranges of the partial reductions of δ as well as the properties of the range of PPT states (see Sec. 7.1.1 and [95, 80]).

Remark 7.1 *The presented formulation permits to release ourselves from dealing with edge states in the canonical decomposition (7.65). Instead, we may consider only the pairs of "strange" subspaces $H^{a,b}$ of the Hilbert space.*

Remark 7.2 *Recall that all EW's are in one to one correspondence to PM's [84]. In particular, any nd-EW leads to a nondecomposable positive map (nd-PM), i.e., a map which cannot be written as a convex sum of a completely positive map and some other completely positive map followed by transposition. As mentioned already, the characterization of nd-PM's is one of the most challenging open problems in mathematical physics. Prop. 7.2 (7.3) thus provides us with a canonical form for nd–PM.*

[8] Note that we could replace the identity operator in (7.65) by some other decomposable operator.

As we remember, the key problem is to find the minimal set of EW's detecting PPTES. Obviously, this minimal set will consist of nd-OEW's. A related problem is to find a set of extremal points of $\mathcal{P}^\perp$. Note that a nonoptimal nd-EW is a convex sum of an optimal one and a decomposable operator (Theorem 7.8), so it cannot be an extremal point. Note that Prop. 7.2 (7.3) combined with the optimality property provides *the necessary form of extremal points* of both EW's, as well as PM's, which has not been known so far. We have thus the following

Proposition 7.4 *The set of extremal points of the set of EW's, $\mathcal{S}^\perp$, is contained in the set $\mathcal{A}$ of all optimal EW's of the form (7.65) plus projectors and transposed projectors.*

Proposition 7.5 *The set of extremal points of the cone of nd-EW's, $\mathcal{P}^\perp$, is contained in the set $\mathcal{B}$ of all optimal nd-EW's of the form (7.65).*

Remark 7.3 *Moreover, applying the isomorphism [84] to the members of $\mathcal{A}$ ($\mathcal{B}$) we obtain the set $\mathcal{A}'$ ($\mathcal{B}'$) of PM's (nd-PM's) containing the set of all extreme PM's. The above theorems thus provide the first nontrivial necessary condition for EW's and PM's to be extremal. In particular, following Prop. 7.3 we can obtain a weaker condition by considering optimal EW's of the form (7.65) without involving the notion of the edge states, but only pairs of "strange" subspaces $\mathcal{H}^a$ and $\mathcal{H}^b$.*

Entanglement witnesses and edge states for N–partite systems

In this section we generalize the notion of EW (see also Sec. 1.2.1) as well as the one of PPTES to multiparite systems. Let us therefore consider a system composed of N subsystems. The corresponding Hilbert space is $\mathcal{H}_A \otimes \ldots \otimes \mathcal{H}_Z$. We use the notation $|x\rangle \in \mathcal{H}_X$, for any system X.

Recall that an operator, $W = W^\dagger$ acting on $\mathcal{H}_A \otimes \ldots \otimes \mathcal{H}_Z$ is called an N–partite EW (EW between the N parties) if

(i) $\langle a, \ldots, z| W |a, \ldots, z\rangle \geq 0 \quad \forall |a\rangle \in \mathcal{H}_A, \ldots, |z\rangle \in \mathcal{H}_Z$

(ii) W is not positive

(iii) $\mathrm{tr}(W) = 1$ [9] .

[9] As we have seen in Sec. 1.2.1 this conditions is just a normalization. Whenever the aim is not to compare two EWs, we will ignore it.

We defined the decomposable (non–decomposable) EWs to be the ones which can (cannot) be written as $W = O_0 + O_1^{T_A} + \ldots O_N^{T_Z}$, where the operators O_i are positive semidefinite. Generalizing now the results derived for bipartite EWs we have [10]:

Lemma 7.26 *A N–partite EW, W, is a NDEW iff it detects a PPTES.*

As we have seen in the previous section, an EW, W, is optimal iff $\forall R \geq 0, \epsilon > 0$ $W' = W - \epsilon R$ is not an EW, in the sense that it does not fulfill (i). This method of optimization can be easily generalized to the case of more parties. We define, analogously to the bipartite case, for an EW, W, the set $P_W = \{|a, \ldots z\rangle \in \mathcal{H}$ such that $\langle a, \ldots z| W |a, \ldots z\rangle = 0\}$. Then we have

Lemma 7.27 *If P_W spans $\mathcal{H}$ then W is optimal.*

Note that multipartite EWs can be used in order to characterize the different entanglement classes for multipartite systems (Sec. 1.2.1, [39]). They allow us to distinguish the class of fully separable states from the others. Let us now also generalize the notion of the range criterion (Lemma 1.1) as well as the one of edge states to the multipartite case. We have

Lemma 7.28 *(Generalized Range Criterion) If a N–partite state, ρ is fully separable then there exists a set $\{|a_i, b_i, \ldots, z_i\rangle\}$ such that span $\{|a_i, b_i, \ldots, z_i\rangle\} = R(\rho)$ and span $\{|a_i, \ldots, x_i^*, \ldots, z_i\rangle\} = R(\rho^{T_X})$, for any system $X = A, \ldots, Z$.*

It is straight forward to define then multi–partite edge PPTES[11].

Definition 7.3 *A N–partite PPTES δ is a N–partite edge PPTES if for all product vectors $|a, b, \ldots, z\rangle$ and $\epsilon > 0$, $\delta - \epsilon |a, b, \ldots z\rangle \langle a, b, \ldots z|$ is not a PPTES.*

Note that we have, analogously to the bipartite case the following characterization of edge states: A N–partite state, δ is an "edge" PPTES iff for all $|a, b, \ldots, z\rangle \in R(\delta)$, one of the states $|a, \ldots, x^*, \ldots z\rangle \notin R(\delta^{T_X})$, for some system $X = A, \ldots, Z$.

[10] Note that the proofs are basically the same as in the bipartite case and will be omitted here.

[11] Note that in Sec. 7.2.2 we will generalize the notion of edge states even to Gaussian states.

Conclusions

Entanglement witnesses allow us to study the separability properties of density operators. We have defined optimal entanglement witnesses, which are those that detect entanglement in an optimal way. We have given necessary and sufficient conditions for an EW to be optimal, and we have shown a way to construct them. We have also concentrated on nd–EW, which are those that detect PPTES. We have extended the definitions of optimality and the optimization procedure to those EW. It turns out that one can optimize nd–EW by subtracting decomposable operators. We also introduced the "edge" PPTES, which violate the range criterion of separability in an extreme manner. As shown in Appendix E.3, the "edge" PPTES allow us to construct a canonical form of PPTES, in terms of a convex combination of a separable and an edge state, in Hilbert spaces of arbitrary dimensions. We have also given an explicit method to construct nd–EW starting from "edge" PPTES. We have mentioned that this method works by starting out from random operators. We have extended our techniques to PM, and therefore given a method to systematically construct non–decomposable positive maps. We have illustrated our methods with a family of "edge" PPTES acting on $\mathbb{C}^2 \otimes \mathbb{C}^4$. The corresponding PM constitute the first examples of PM with minimal "qubit" domain, or – equivalently – minimal hermitian conjugate codomain. We have also constructed the first examples of separable states of full range that lie on the boundary between separable and PPTES. These states can be used for experimental realization of PPTES [12]. We also derived a canonical form for NDEW and presented a necessary condition for EWs and PMs to be extremal. Furthermore we have shown that the results obtained for bipartite EWs can be easily generalized to EWs which distinguish between fully separable and entangled multipartite states.

Note that the edge PPTES also allow us to give a novel sufficient condition for non–separability which applies to operators with positive partial transpose. It is based on the fact that among all PM (or EW) only the subset $\{\Lambda_{edge}\}$ of those PM that detect edge PPTES are needed to study the separability of PPTES. This opens many interesting questions. Is it possible that in the set $\{\Lambda_{edge}\}$ there is some map that is globally finer than the transposition? In another words, is there a map detecting the entanglement of *all* the states with non–positive partial transpose? What is the minimal subset of $\{\Lambda_{edge}\}$ providing such condition? Is it finite?

Finally, let us consider the implications of the our results for the very interesting problem of locality of PPTES. There is a conjecture [117] that those states can be local in the sense that they admit a local hidden variable

[12] (see footnote [6] on p. 131).

(LHV) model for any set of possible local measurements. The problem is not trivial given the fact that it may be important to take into account the role of sequential measurements and the possible existence of many copies. Quite recently it has been shown that PPTES satisfy Bell-type inequalities introduced by Mermin [152]. It is not difficult to convince oneself that the set of states admitting LHV model for *any* fixed type of measurements is a convex set. Furthermore, extending the reasoning from [151] it is easy to see that the set of separable states admits LHV models for any possible set of measurements. Hence, taking into account the results of this section it follows that in order to prove, or to disprove locality of PPTES it is enough to study only "edge" PPTES.

Note that the "edge" states have typically very small rank (the minimal rank is four in $3 \otimes 3$ systems, see Ref. [79]). There have been no examples of LHV models for states of low rank, so far. Thus, perhaps completely new techniques will be needed to study this problem. In this case the most symmetric PPTES provided recently [78] seem to be the best suitable for the first test.

Recently, it was shown how to use EWs and PMs to detect entanglement experimentally [51, 76, 65, 64]. Since an EW is an observable one simply has to measure the expectation value of the EWs to check if the experimentally created state is entangled. In Ref. [65] it was shown how to do so in an efficient way without consuming entanglement for the measurement. The authors assumed to have some a priori knowledge about the, experimentally created state. On the other hand, in Ref. [76] it was shown how to implement an operation corresponding to partial transposition and to detect in this way the two–qubit entangled states. Note, as mentioned in Sec. 2.1 only completely positive maps can be implemented physically and since partial transposition is positive, but not completely positive (otherwise it would not be possible to detect entanglement with it) it is not possible to transform a state, ρ into ρ^{T_A} experimentally. However, if one mixes the positive map with the depolarizing map, i.e. the map which transforms any density operator into a maximally mixed state, then the resulting map can be made completely positive. It was proposed in Ref. [76] to implement this map and then measure whether the resulting density operator is larger than $k\mathbb{1}$, where the number k depends on the implemented CPM [13].

Note that the formalism of EWs and PMs can be used for many other instances. Whenever the goal is to distinguish between two convex, closed

[13] Theoretically we simply check whether the operator ρ^{T_A} is positive, it was shown that this is equivalent to check whether $\tilde{\rho} \geq k\mathbb{1}$, where $\tilde{\rho}$ is the state one obtains after transforming ρ according to the CPM corresponding to partial transposition.

sets, where one of them is compact one can apply the formalism of EWs and PMs, see for instance [124, 44, 1]. The reason for this is that in this case the Hahn–Banach Theorem [121] holds. In order to obtain then the corresponding maps (similar to the PMs), one uses the isomorphism presented in Ref. [84] (see also Sec. 1.2.1). On the other hand, we will use in Chapter 8 the notion of EW to characterize distillable and activatable states.

7.1.3 Symmetric states

Let us now use the methods introduced in the preceding sections to address the problem of separability for *symmetric states* composed of N d–level systems. By symmetric we mean that the N–partite state is supported on the subspace which is invariant under exchanging the particles. These states are particulary interesting from the experimental point of view. As mentioned in Chapter 5, several experiments deal with an ensemble of atoms, which can be addressed and manipulated globally. Since the particles are in addition indistinguishable, the states produced in those experiments are symmetric.

Whenever the system is composed of more than two particles there are many ways in which the particles can be entangled to each other, as already mentioned in Sec. 1.2. We consider the N–partite state as a bipartite state, with m systems on one and $N-m$ systems on the other side and investigate the entanglement properties of all these bipartite splittings of the system.

In the first part of this section we present some results concerning separability of symmetric states. We show that such a state is fully separable iff it is biseparable, i.e. iff there exists a bipartite splitting in which the state is separable. The second part of this section deals with the contrary problem. There we characterize and study states, describing a system composed of N qubits, which are maximally entangled. We will call a state maximally entangled if it is maximally entangled with respect to any bipartite splitting (see also [137]). Then we show that those state exist for $N = 2, 3, 4, 6$, but it seems that they do not exist for any other number of particles, as stated in Ref. [60]. For the case $N = 5$ the non–existence of maximally entangled states can be proven analytically [96].

Let us, first of all, introduce the notation that we use throughout this section. We denote by $M_N = \{f : \{1, \dots N\} \to \{1, \dots N\} \mid \text{ f bijectiv}\}$, for $N > 1$ the set of permutations. M_N forms with the composition the permutation group. The cardinality of M_N can be shown to be $N!$. Furthermore it can be shown that any permutation can be written as a product of transpositions, which are permutations that change only two numbers and leave the rest invariant. We denote by Π_f the operator corresponding to the linear map $f \in M_N$.

Let us now consider a system composed of N d–level subsystems. The operator corresponding to the transposition, changing the particles i and j can be written as

$$P_{i,j} = \otimes_{k\neq i,j}^{N} \mathbb{1}_k \otimes U_{i,j}^{swap}, \tag{7.66}$$

where

$$U_{i,j}^{swap} = \sum_{k,l=0}^{d-1} |k\rangle_i \langle l| \otimes |l\rangle_j \langle k|, \tag{7.67}$$

with $\{|k\rangle\}_{k=0}^{d-1}$ an orthonormal basis of $\mathbb{C}^d$. U_{ij}^{swap} is the swap operator between the particles i and j. The projector

$$P_N^S = \frac{1}{N!}\Big(\sum_{f\in M_N} \Pi_f\Big) \tag{7.68}$$

defines the space which is invariant under all the permutations, i.e. the symmetric subspace. It is the set of states, $|\Psi\rangle$ for which $P_{i,j}|\Psi\rangle = |\Psi\rangle$, for any pair of particles i, j. We call such a state symmetric. The symmetric subspace can be shown to be

$$S_N = \text{span}\,\{|a\rangle^{\otimes N}, \forall |a\rangle \in \mathbb{C}^d\} \tag{7.69}$$

A density operator, ρ describing the state of N d–level systems is called symmetric if $P_N^S \rho P_N^S = \rho$.

Let us, as an example, consider the case of N qubits. We have that

$$U_{i,j}^{swap} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{7.70}$$

The symmetric space can be written as

$$S_N = \text{span}\,\{|a\rangle^{\otimes N}, \forall |a\rangle \in \mathbb{C}^2\} = \text{span}\,\{|\Phi_{k,N-k}\rangle\}_{k=0}^{N}, \tag{7.71}$$

where the state $|\Phi_{k,N-k}\rangle$ denotes the unnormalized N–partite symmetric state containing k zeros and $N-k$ ones, e.g $|\Phi_{2,3}\rangle = |001\rangle + |010\rangle + |100\rangle$, which is the well–known W–state introduced in Ref. [41]. From the second equality of Eq. (7.71) it can be easily seen that the dimension of the space S_N is $N+1$. The projector onto the symmetric subspace can be written as

$$P_N^S = \frac{1}{N+1} \sum_{k=0}^{N} |\Phi_{k,N-k}\rangle \langle \Phi_{k,N-k}|. \tag{7.72}$$

Mixed states

We consider a system composed of N d–level systems. As mentioned already, a multi–partite mixed state might be separable in some bipartite splitting, but non–separable with respect to some other. Thus, the problem of separability gets very complicated in this case. However, we will show now, using the methods developed in the previous sections, that for symmetric states the situation can be simplified a lot (see Lemma 7.29 below). Using those methods it is also possible to show that there exist all kind of PPTES in this restricted set of states that we consider here.

Lemma 7.29 *A N–partite symmetric state, ρ, is fully separable iff it can be written as*

$$\rho = \sum_i |a_i\rangle \langle a_i|^{\otimes N} . \tag{7.73}$$

Proof: Due to the fact that any state, $|\phi_i\rangle$ occurring in a decomposition $\rho = \sum_i \lambda_i |\phi_i\rangle \langle \phi_i|$ must belong to the range of ρ (see proof of Lemma 7.3) it is clear that a decomposition into product vectors exists iff all of them are symmetric, i.e. of the form $|a\rangle^{\otimes N}$. ■

Note that this lemma implies the following important

Corollary 7.15 *A N–partite symmetric state, ρ, is fully separable iff it is biseparable with respect to any bipartite splitting.*

Proof: Let ρ be biseparable, say in the splitting $m/(N-m)$. Then it can be written as $\rho = \sum_i |\xi_i\rangle_{1,\ldots,m} \langle \xi_i| \otimes |\chi_i\rangle_{m+1,\ldots,N} \langle \chi_i|$, where $|\xi_i\rangle_{1,\ldots,m}$ ($|\chi_i\rangle_{m+1,\ldots,N}$) belongs to S_m (the first m systems) [S_{N-m} (system $m+1,\ldots N$)], respectively. As before, the states $|\xi_i\rangle_{1,\ldots,m} |\chi_i\rangle_{m+1,\ldots,N}$ belong to the range of ρ and must therefore be symmetric. We prove now that any of those states must be of the form $|a\rangle^{\otimes N}$. First of all, as seen in Lemma 7.29, for $m = 1$ it is clear that a state $|a\rangle_1 |\chi\rangle_{m+1,\ldots,N}$ is invariant under any exchange of particle 1 with some other only if $|\chi\rangle_{2,\ldots,N} = |a\rangle^{\otimes(N-1)}$. Now, if $m > 1$, we have that $\langle \phi_{2,\ldots m}| (|\xi\rangle_{1,\ldots,m} |\chi\rangle_{m+1,\ldots,N}) = |a\rangle_1 |\chi\rangle_{m+1,\ldots,N}$, for some $|a\rangle_1 \in \mathbb{C}^d$, has to be invariant under $P_{1,k}$ for any state $|\phi_{2,\ldots m}\rangle$. Thus, $|\chi\rangle_{m+1,\ldots,N}$ must be $|a\rangle^{\otimes(N-m)}$ which proves the statement. ■

Because of Corollary 7.15 we call in this section a state simply separable if it is fully separable. The next lemma shows that it is very easy to determine entanglement witnesses (see Sec. 1.2.1 and Sec. 7.1.2) in the case of symmetric states.

Lemma 7.30 *Let A be a hermitian, non–positive semidefinite operator, which has at least one strictly positive eigenvalue. Then the operator $P_N^S(A^{\otimes 2n} \otimes \mathbb{1}_{N-2n})P_N^S$ is an N–partite EW for symmetric states, for any $N \geq 2n$.*

Proof: The proof is very simple. Since $A^{\otimes 2n} \otimes \mathbb{1}_{N-2n}$ is hermitian and non–positive we just have to show that it is positive on all symmetric separable states[14]. Using that any separable state, ρ_{sep} can be written as $\rho_{sep} = \sum_i |a_i\rangle \langle a_i|^{\otimes N}$ (Lemma 7.29), it is easy to see that $\mathrm{tr}(A^{\otimes 2n} \otimes \mathbb{1}_{N-2n}\rho_{sep}) = \sum_i \||a_i\rangle\|^{N-2n} (\langle a_i| A |a_i\rangle)^{2n}$ is positive for any separable state, since A is hermitian. ■

On the other hand, we have

Lemma 7.31 *For any NPPT state, $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, there exists an operator A such that*

$$W = (P_{AB} A \otimes A^\dagger)^{T_B} \tag{7.74}$$

detects ρ.

Proof: Let ρ be NPPT, then there exists a state $|\Psi\rangle = \sum_{i,j} c_{i,j} |i\rangle_A |j\rangle_B$ such that $\langle \Psi| \rho^{T_B} |\Psi\rangle < 0$. Defining $A = \sum_{i,j} c_{i,j} |i\rangle \langle j|$ it is easy to prove that $|\Psi\rangle \langle \Psi| = P_{AB} A \otimes A^\dagger$, which proves the statement. ■

Let us now, as an example, consider a system composed of N qubits. We can write the most general hermitian operator in $\mathcal{B}(\mathbb{C}^2)$ in the form $A = \mathbb{1} + \alpha \vec{n}^T \vec{\sigma}$, where $\vec{n}$ is a real normalized three–dimensional vector, α is a real number, and $\vec{\sigma}$ is the vector containing the Pauli operators (1). As we have already seen before, the operator $P_N^S(A^{\otimes 2n} \otimes \mathbb{1}_{N-2n})P_N^S$ is an EW for symmetric states, as long as it is not positive semindefinite. Similarly to Sec. 7.1.2 one can "optimize" this EW and finds, for instance in the case of two qubits, the operator $P_2^S(\sigma_z \otimes \sigma_z)P_2^S = P_2^S - 2|\Psi^+\rangle \langle \Psi^+|$, where $|\Psi^+\rangle$ is one of the Bell states (1.3). This EW is optimal, since it detects, up to local operations, all symmetric NPPT–states. This is due to the fact that it equals the operator $P_2^S W_{opt} P_2^S$, with $W_{opt} = (|\Phi^-\rangle \langle \Phi^-|)^{T_A}$ which is optimal as shown in Appendix E.2.

One may wonder whether there exist all kinds of entanglement in this restricted set of states. One might think for instance that, due to the symmetry, there exists no state with the property that $\rho^{T_{XY}} \geq 0$, but ρ^{T_X} not positive semidefinite, for some subsystems X, Y. Even more important, the

[14] As mentioned, property (iii) in Sec. 7.1.2 is just a normalization

symmetry might prevent the particles from being bound entangled, in the sense that the state is PPTE.

Using the methods of Section 7.1 it will be easy to solve these problems. In particular, one can construct and detect all kinds of entangled states using the developed methods. The idea is to start with some separable state, $\rho = \sum_i |a_i\rangle \langle a_i|^{\otimes N}$. Then one subtracts product vectors of the form $|a\rangle^{\otimes N}$ according to the desired conditions. For instance, we can easily construct a PPTES[15]. One only has to make sure at each step of the procedure that the state ρ and all its partial transposes remain positive. As we have seen (Sec. 7.1.1 and Sec. 7.1.2) this is ensured if the subtracted state, $|a\rangle^{\otimes N}$ is orthogonal to the kernel of ρ and $|a_X^*\rangle |a\rangle^{\otimes N-1}$ is orthogonal to the kernel of ρ^{T_X}, for all subsystems X. One can also easily construct, for instance 4 qubit states with the properties $\rho^{T_{AB}} \geq 0$, and ρ^{T_A} is not positive semidefinite. Analogously one can also study symmetric $\mathbb{C}^M \otimes \mathbb{C}^M$ systems. For instance, one can show, using the same methods as above, that there exist PPTES in $\mathbb{C}^3 \otimes \mathbb{C}^3$.

Pure states

We consider a system composed of N qubits. The goal of this section is then to identify the maximally entangled states. As mentioned already, we call a state maximally entangled if it is maximally entangled in any bipartite splitting. Using the fact that any measure of entanglement is convex (1.12), we can restrict ourselves to pure states when determining those states. On the other hand, the symmetric states seem to best suitable for being maximally entangled. However, it turns out that symmetric maximally entangled states do not exist for an arbitrary number of qubits. In particular, one can prove that in the case $N = 5$, there exists no such state [96]. Moreover, for all $N > 6$ it also seems to be impossible to construct such a state, as stated in Ref. [60]. For the other cases we present here the states being maximally entangled.

Let us consider the bipartite splitting $m/(N-m)$ qubits, where we choose without loos of generality $m \leq [N/2]$, with $[N/2] = N/2$ for N even and $(N-1)/2$ otherwise. Since the states we consider are symmetric, the state describing the system composed of m qubits belongs to a $m+1$ dimensional space[16]. This implies that the Schmidt number of the state is at most $m+1$. Thus, the maximum amount of entanglement [measured in terms of the Entropy of Entanglement (1.7)] that can be included in this bipartite splitting

[15] This is possible for $N > 3$. Otherwise they do not exist, as was shown in Ref. [44]

[16] Since the state is also symmetric in the m qubits on the one side.

is bounded by

$$E_m(|\Psi\rangle) = S(\rho_m) \leq \log_2(m+1), \tag{7.75}$$

where $\rho_m = \mathrm{tr}_{1,\ldots,N-m}(|\Psi\rangle \langle\Psi|)$ is the reduced state of m qubits, and S denotes the Von Neumann entropy (1.7). Note that the maximum can be reached only if the reduced density operator ρ_m is the projector into the symmetric subspace. Mathematically stated, $E_m(|\Psi\rangle) = \log_2(m+1)$ iff $\rho_m = P_m^S$. Note that, if a state is maximally entangled with respect to some measure of entanglement, then it is so with respect to any other. The reason for this is that (Sec. 1.1.2), a bipartite state is maximally entangled iff the Schmidt number equals the minimum of the dimension of the Hilbert spaces corresponding to the two subsystems and all the Schmidt coefficients are equal. Note further that the condition implies that $\rho_{m-k} = P_{m-k}^S$, for any k, $k < m$, which means that if a state is maximally entangled with respect to the bipartite splitting $m/(N-m)$, then it is also with respect to $k/(N-k)$, for any $k < m$. This implies the following criterion.

A symmetric state $|\Psi\rangle$ is maximally entangled with respect to all the bipartite splittings $m/(N-m)$ iff $\rho_{[N/2]} = P_{[N/2]}^S$, i.e. iff it is maximally entangled with respect to the splitting $[N/2]/(N-[N/2])$.

We present now examples of maximally entangled states for the cases $N = 2, 3, 4, 6$. They are all of the form

$$|\Psi_N(a,c)\rangle = \frac{1}{k}[a(|\Phi_{N,0}\rangle - |\Phi_{0,N}\rangle) + c\,|\Phi_{N/2,N/2}\rangle], \tag{7.76}$$

where k is a normalization factor. For $N = 2$ the state $|\Psi_2(a=0,c)\rangle = 1/\sqrt{2}(|1,0\rangle + |0,1\rangle) \equiv |\Phi_{1,1}\rangle$ represents a symmetric maximally entangled state. The state $|\Psi_3(a,c=0)\rangle = 1/\sqrt{2}(|\Phi_{3,0}\rangle - |\Phi_{0,3}\rangle)$, i.e. the GHZ–state for three qubits fulfills that $E_1(|\Psi_N(a,c=0)\rangle) = 1$ and is therefore maximally entangled. Note that the entanglement included in the GHZ–state for 4 qubits, i.e $|\Psi_4(a,c=0)\rangle$ is not maximal, since $E_2(|\Psi_4(a,c=0)\rangle) = 1 < \log_2(3)$ (7.75). However, the state $|\Psi_4(a=1,c=1/\sqrt{3})\rangle$ reaches the maximum $\log_2(3)$ for E_2. For the $N = 6$ case we find that $|\Psi_6(a=1,c=1/\sqrt{8})\rangle$ fulfills the desired property, $E_3(|\Psi_6(a=1,c=1/\sqrt{8})\rangle) = 2$. Note that for the case $N = 5$ it can be shown analytically that there exists no maximally entangled state according to our definition [96]. For $N > 6$ it is also not possible to find those states numerically. In Fig. 7.3 the maximal entanglement included in the states of the form (7.76) for $N = 2n$ is shown. Note further that the "scaled" entanglement does not vanish in the asymptotic limit, in particular [96]

$$\lim_{n\to\infty} \frac{\max_{a,c} E_n(\Psi_{2n}(a,c))}{\log_2(n+1)} = \frac{1}{2}. \tag{7.77}$$

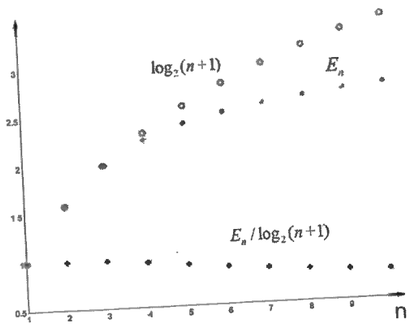

Figure 7.3: dots: The maximal entanglement of the state $|\Psi_{2n}(a,c)\rangle$; circles: The upper bound of entanglement of a $2n$–partite symmetric state; crosses: The ratio between those two quantities.

7.1.4 Three qubit states

As another application of the methods developed in the previous sections we study here mixed states describing a system composed of three qubits. We consider the state

$$\rho_\alpha = \mathbb{1}_8 + \alpha |W\rangle\langle W|, \tag{7.78}$$

where [41]

$$|W\rangle = |001\rangle + |010\rangle + |100\rangle. \tag{7.79}$$

We will use the notation

$$U = \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}. \tag{7.80}$$

Again, we denote by $|x\rangle$ a state belonging to the Hilbert space $\mathcal{H}_X$, for $x = a, b, c$. As in the previous section P_{ij} denotes the permutation operator of particle i and$j$. Note that ρ_α commutes with $P_{12}, P_{23}, P_{13}, \sigma_z^1 \otimes \sigma_z^2 \otimes \sigma_z^3 \equiv S_z^3$ and with $U \otimes U \otimes U \equiv U_3$.

First of all we are going to use these symmetries to derive the most general EW which is capable to detect an entangled state of the form (7.78). Then we present an example of an edge PPTES[17]. We prove that it is an edge PPTES by showing that it violates the range criterion (Lemma 7.28) in an extreme manner. Note that it is easy to construct the corresponding

[17] A multipartite edge PPTES is analogously definite as the bipartite edge PPTES (Def. 7.1), see Def. 7.3

3–partite NDEW (analog to Lemma 7.21). After that we present some full rank PPTES [i,e. $r(\rho) = 8$] which is of the form (7.78). This state is no egde state. We prove that it is entangled by showing that there are only 6 product states, $|a,b,c\rangle \in R(\rho)$[18] such that $|a^*,b,c\rangle \in R(\rho^{T_A})$, $|a,b^*,c\rangle \in R(\rho^{T_B})$, and $|a,b,c^*\rangle \in R(\rho^{T_C})$.

Let us derive the most general operator, W, which can detect an entangled state of the form (7.78). Using the symmetries of ρ_α, we have, for any $O \in \{S_z^3, U_3, P_{12}, P_{13}, P_{23}\}$

$$\mathrm{tr}(W\rho_\alpha) = \mathrm{tr}(WO\rho_\alpha O^\dagger) = \frac{1}{2}\mathrm{tr}[(W + O^\dagger W O)\rho_\alpha]. \tag{7.81}$$

From this equation we see that if the entanglement witness W detects ρ_α then $W + O^\dagger W O$ detects it as well, for any $O \in \{S_z^3, U_3, P_{12}, P_{13}, P_{23}\}$. Thus, we can choose the operator W to be symmetric with respect to the operators $S_z^3, U_3, P_{12}, P_{13}, P_{23}$. We determine the most general operator obeying those symmetries by imposing that the sets, $\{P_{12}, S_z^3, U_3, W\}, \{P_{13}, S_z^3, U_3, W\}, \{P_{23}, S_z^3, U_3, W\}$ form complete sets of commuting operators. Then we find that the most general operator, which is capable of detecting ρ_α can be written as:

$$W = \begin{pmatrix} a_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_2 & a_3 & 0 & a_3 & 0 & 0 & 0 \\ 0 & a_3 & a_2 & 0 & a_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_4 & 0 & a_5 & a_5 & 0 \\ 0 & a_3 & a_3 & 0 & a_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_5 & 0 & a_4 & a_5 & 0 \\ 0 & 0 & 0 & a_5 & 0 & a_5 & a_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_7 \end{pmatrix} \tag{7.82}$$

Note that, analog to this example, one can always use the symmetries of a state in order to determine the EWs which could detect it. Note further that for an operator W, as in (7.82), it is not very complicated to find a range for the parameters a_i, for which W is an EW (either bipartite, to distinguish the classes of biseparable states (including the fully separable states), or three–partite to distinguish the class of fully inseparable states from the others).

Examples of PPTES

We present here two examples of three–partite PPTES. The first one is an egde PPTES (Sec. 7.1.2), whereas the second example is full rank PPTES of

[18] Analogously to the before we denote by $R(X)$, $K(X)$, and $r(X)$, the range, kernel, and rank of an hermitian operator X.

the form (7.78). To prove that the states are entangled we use the methods developed in Sec. 7.1.1.

Example 1

The state

$$\rho = \rho_{1/\sqrt{2}} - P, \tag{7.83}$$

where

$$P = |001\rangle\langle 001| + |010\rangle\langle 010| + |100\rangle\langle 100| + |111\rangle\langle 111| \tag{7.84}$$

is a three–qubit edge PPTES (Def. 7.3), i.e. there exists no product state, $|abc\rangle$ which can be subtracted form ρ keeping it and all the partial transposes, $\rho^{T_A}, \rho^{T_B}, \rho^{T_C}$ positive semidefinite (see Sec. 7.1.2).

Let us prove this statement. Recall that any state, which can be subtracted from an operator such that the resulting operator is positive must belong to its range, i.e. it must be orthogonal to its kernel. Thus the product vector, which can be subtracted from ρ, keeping it and its partial transposes positive must fulfill the following conditions:

$$\begin{aligned} &|abc\rangle \quad \perp K(\rho) = \\ \text{span}\{ &|111\rangle \quad , -|001\rangle + |010\rangle , -|001\rangle + |100\rangle\} \end{aligned} \tag{7.85}$$

$$\begin{aligned} &|a^*bc\rangle \quad \perp K(\rho^{T_A}) = \\ \text{span}\{ &|111\rangle \quad , -|001\rangle + |010\rangle , -\sqrt{2}|000\rangle + |101\rangle + |110\rangle\} \end{aligned} \tag{7.86}$$

$$\begin{aligned} &|ab^*c\rangle \quad \perp K(\rho^{T_B}) = \\ \text{span}\{ &|111\rangle \quad , -|001\rangle + |100\rangle , -\sqrt{2}|000\rangle + |011\rangle + |110\rangle\} \end{aligned} \tag{7.87}$$

$$\begin{aligned} &|abc^*\rangle \quad \perp K(\rho^{T_C}) = \\ \text{span}\{ &|111\rangle \quad , -|100\rangle + |010\rangle , -\sqrt{2}|000\rangle + |101\rangle + |011\rangle\} \end{aligned} \tag{7.88}$$

First of all, we have that $\langle 111|\, abc\rangle = 0$ this implies that either $|a\rangle = |0\rangle$, $|b\rangle = |0\rangle$ or $|c\rangle = |0\rangle$ Using the symmetry of the problem we only have to show that there exists no state fulfilling Eq:(7.85–7.88) in the case where $|a\rangle = |0\rangle$. Here Eq (7.85) implies that $\langle 01|\, bc\rangle = \langle 10|\, bc\rangle = 0$. Thus the only solution is that $|bc\rangle = |11\rangle$. It is easy to see that the state $|011\rangle$ does not fulfill Eq.(7.87), i.e. is not orthogonal to the kernel of ρ^{T_B}. Thus, there exists

no product vector which can be subtracted from ρ keeping it a PPT state, which shows the statement.

The decomposable witness "corresponding" to this edge state is

$$W = P_{K(\rho)} + P^{T_A}_{K(\rho^{T_A})} + P^{T_B}_{K(\rho^{T_B})} + P^{T_C}_{K(\rho^{T_C})} \tag{7.89}$$

After determining the minimal overlap, ϵ with a product state it is easy to create the non–decomposable witness (analog to Lemma 7.21), $W - \epsilon\mathbb{1}$ which detects ρ. Defining $x = 5/6 + 1/\sqrt{2}$, we have

$$W = \begin{pmatrix} \frac{3}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{5}{3} & -x & 0 & -x & 0 & 0 & 0 \\ 0 & -x & \frac{5}{3} & 0 & -x & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} & 0 \\ 0 & -x & -x & 0 & \frac{5}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{2} & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}. \tag{7.90}$$

Example 2

Another example of a three–partite PPTES is the state

$$\rho = \rho_{1/\sqrt{2}}. \tag{7.91}$$

Here, in contrast to the previous example there exist states which can be subtracted form ρ, keeping it and its partial transposes positive[19] . However, if ρ was separable, then there must be at least $r(\rho) = 8$ linearly independent product vectors which can be subtracted from ρ keeping it a PPT state. We will show now that there are at most 6 such product vectors, which implies that ρ is a PPTES.

Similarly to the previous section, it is straight forward to determine the product states, $|a, b, c\rangle$ which can be subtracted from ρ, keeping it a PPT state. We find that those states belong to the set:

$$S = \{|111\rangle , |001\rangle , |010\rangle , |100\rangle , |a_\Phi a_\Phi a_\Phi\rangle , 0 \leq \Phi < 2\Pi\}, \tag{7.92}$$

where $|a_\Phi\rangle = |0\rangle + 1/\sqrt[4]{2}e^{i\Phi}|1\rangle$. It can be seen as follows that this set has at most dimension 6. Let us denote by S_3 the 4–dimensional symmetric

[19] In particular the states belonging to the range of the projector P [Eq. (7.84)] can be subtracted. Note, that this subtraction leads to the edge entangled state of the previous example.

subspace of three qubits (7.71), that is $S_3 = \text{span}\{|000\rangle, |111\rangle, |W\rangle, |\bar{W}\rangle\}$, where $|W\rangle = |100\rangle + |010\rangle + |001\rangle$ and $|\bar{W}\rangle = |110\rangle + |101\rangle + |011\rangle$. The states $|111\rangle$ and $|a_\Phi a_\Phi a_\Phi\rangle$, for any Φ belong to the symmetric subspace. The remaining states, $|001\rangle, |010\rangle, |100\rangle$ form a 3–dimensional subspace, containing the state $|W\rangle$. Thus, there are at most two linearly independent states in S, which do not belong to S_3, and so the dimension of the set S is at most 6. Note that here we did not restrict ourselves to product states, which might span a even less dimensional space.

7.2 Infinite dimensional Hilbert space (continuous variable systems)

We consider a continuous variable system (CV) in a Gaussian state. A practical advantage of CV systems is the relative ease with which entangled states can be generated in the lab [54, 132]. First results on separability and distillability of Gaussian states were reported in Ref. [34, 133, 55, 153, 150]. One finds striking similarities between the situations of two qubits and two one–mode CV systems in a Gaussian state: PPT is necessary and sufficient for separability [34, 133], and all inseparable states are distillable [55]. Generalizing the methods presented in Sec. 7.1 it was shown that for more than two modes at either side PPT entangled states exist [153]. In Ref. [150] a computable measure of entanglement, the negativity (Sec. 1.3.1), for bipartite Gaussian states was derived.

The study of CV multipartite entanglement was initiated in Ref. [144, 145], where a scheme was suggested to create pure CV N-party entanglement using squeezed light and $N-1$ beamsplitters. In fact, this discussion indicates that tripartite entanglement has already been created (though not investigated or detected) in the CV quantum teleportation experiment [54].

This section is divided into two main parts. In 7.2.1 we present a necessary and sufficient condition for separability for an arbitrary bipartite Gaussian state. Since the criterion is computable the problem of separability is solved for this case. In Sec. 7.2.2 we investigate the entanglement properties of three–mode Gaussian states. We classify them, analogously to the three qubit case (see Sec. 1.2.1, [39, 40]), according to their separability properties. Then we derive conditions which have to be fulfilled for a state to be in a particular class. Again those conditions can be easily computed and so the problem of three–modes Gaussian states is also solved.

Due to the fact that all the information concerning non–locality of a state is included in its CM, we will occasionally say, e.g., that "a CM is separable"

when the Gaussian state with this CM is separable. Furthermore, in this section "state" will always mean "Gaussian state" (unless stated otherwise).

Let us now present two lemmas which will be very useful throughout the following sections.

Positivity of symmetric matrices

Let us consider three real matrices $0 \leq A = A^T \in M_{n,n}$, $0 \leq B = B^T \in M_{m,m}$, and $C \in M_{n,m}$, and

$$M = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} = M^T \in M_{n+m,n+m}. \tag{7.93}$$

Lemma 7.32 *The following statements are equivalent:*

(i) $M \geq 0$.

(ii) $\ker(B) \subseteq \ker(C)$ *and* $A - CB^{-1}C^T \geq 0$.

(iii) $\ker(A) \subseteq \ker(C^T)$ *and* $B - C^T A^{-1} C \geq 0$[20].

Proof: We will just prove the first equivalence since the other one is analogous. We use that $M \geq 0$ iff for any two real vectors $a \in \mathbb{R}^n$ and $b \in \mathbb{R}^m$

$$a^T A a + b^T B b + a^T C b + b^T C^T a \geq 0. \tag{7.94}$$

On the other hand, $A - CB^{-1}C^T \geq 0$ iff for any $a \in \mathbb{R}^n$ we have

$$a^T A a - a^T C B^{-1} C^T a \geq 0. \tag{7.95}$$

(i)⇒(ii): We assume (7.94). First, $\ker(B) \subseteq \ker(C)$ since otherwise we could always choose a $b \in \ker(B)$ so that $-2a^T C b > a^T A a$. Second, if we choose $b = -B^{-1}C^T a$ then we obtain (7.95). (ii)⇒(i): We now assume (7.95). Then, $A = CB^{-1}C^T + P$, where $P \geq 0$. Defining $\tilde{a} \equiv B^{-1}C^T a$, we have that $C^T a = B\tilde{a}$ (since $\ker(B) \subseteq \ker(C)$), and thus the lhs of (7.94) can be expressed as $a^T P a + (\tilde{a} + b)^T B (\tilde{a} + b)$, which is positive.■

Let us consider two real matrices $A = A^T \in M_{n,n}$ and $C = -C^T \in M_{n,n}$, and

$$M = \begin{pmatrix} A & C \\ C^T & A \end{pmatrix} = M^T \in M_{2n,2n}. \tag{7.96}$$

[20] Analog to preceding sections, we denote by X^{-1} the pseudoinverse of an operator X (see footnote [2] on p. 123).

Lemma 7.33 *$M \geq 0$ iff $A + iC \geq 0$.*

Proof: This follows from the observation that M is real, and that for any pair of real vectors $a, b \in \mathbb{R}^N$ we have $(a - ib)^\dagger (A + iC)(a - ib) = (a \oplus b)^T M (a \oplus b)$.■

Let us recall the definition $R_{2k-1} = X_k, R_{2k} = P_k$, for $k = 1, 2 \ldots, n$. Then we have $[R_k, R_l] = -iJ_{kl}$ with [21]

$$J_n \equiv \oplus_{k=1}^n J_1, \quad J_1 \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{7.97}$$

7.2.1 Separability Criterion for bipartite Gaussian states

In this section we solve the problem of separability for bipartite Gaussian states of an arbitrary number of modes per side. Our method does not rely in any sense on the concept of partial transposition, and therefore is diametrically different from the ones that have been introduced so far to study the separability problem (see Sec. 7.1.1, Sec. 7.1.2 and references therein). It is based on a *nonlinear* map $f : \gamma_N \to \gamma_{N+1}$ between matrices γ_N which reveals whether a state ρ is entangled state or not. The condition provides an operational criterion since it can be checked by simple computation. Furthermore, once ρ is shown to be separable, our method allows to find an explicit decomposition of ρ as a convex combination of product states.

We consider two systems A and B, composed of n and m modes, respectively, in a Gaussian state. The corresponding CM will be written as (1.35)

$$\gamma_0 = \begin{pmatrix} A_0 & C_0 \\ C_0^T & B_0 \end{pmatrix} \geq iJ_{n,m} \tag{7.98}$$

where $A_0 \in M_{2n,2n}$ and $B_0 \in M_{2m,2m}$ are CM themselves, $C_0 \in M_{2n,2m}$ and $J_{n,m} \equiv J_n \oplus J_m$, with J_k, the direct sum of k J's, defined in (7.97). In order to simplify the notation, when it is clear from the context we will not write the subscripts to the matrices J and we will not specify the dimensions of the matrices involved in our derivations. As mentioned in Sec. 1.3.2, it was shown [153] that a CM of the form (7.98) is separable (i.e., it corresponds to a separable state) iff there exist two CMs, $\gamma_{A,B}$, such that

$$\gamma_0 \geq \gamma_A \oplus \gamma_B. \tag{7.99}$$

[21] We use, as mentioned in Sec. 1.3 the direct sum notation for matrices and vectors.

Recall that this condition, even though it can be very useful to show that some particular states are entangled [153, 58], cannot be directly used in practice to determine whether an arbitrary state is entangled or not, since there is no way of determining $\gamma_{A,B}$ in general.

Below we will present a criterion which allows us to determine whether a given CM, γ_0, is separable or not, and which allows us to determine a product–state decomposition if this is the case. To this aim, we define a sequence of matrices $\{\gamma_N\}_{N=0}^\infty$ of the form (7.98). The matrix γ_{N+1} can be determined through the discrete map defined as follows: (i) if γ_N is not a CM then $\gamma_{N+1} = 0$; (ii) if γ_N is a CM then

$$A_{N+1} \equiv B_{N+1} \equiv A_N - \mathrm{Re}(X_N), \tag{7.100a}$$
$$C_{N+1} \equiv -\mathrm{Im}(X_N), \tag{7.100b}$$

where $X_N \equiv C_N (B_N - iJ)^{-1} C_N^T$ (see footnote [20] on p. 153). Note that for $N \geq 1$ we have that $A_N = A_N^T = B_N$ and $C_N = -C_N^T$ are real matrices. The importance of this sequence is that, as we will show below, γ_0 is separable iff γ_N is a valid separable CM. In particular, for some finite number of iterations γ_N will acquire a form in which it is simple to check that it is separable. Furthermore, starting from that CM we will be able to construct the CMs $\gamma_{A,B}$ of Eq. (7.99) for the original γ_0. We will present several propositions from which the above results will follow.

First we show that if γ_N is separable, so is γ_{N+1}. Moreover, the CMs $\gamma_{A,B}$ associated to γ_N [cf. Eq. (7.99)] allow us to construct the corresponding CMs for γ_{N+1}.

Proposition 7.6 *If for some CMs, $\gamma_{A,B}$, we have $\gamma_N \geq \gamma_A \oplus \gamma_B$ then $\gamma_{N+1} \geq \gamma_A \oplus \gamma_A$.*

Proof: We use the equivalence (i)–(iii) of Lemma 7.32 to obtain that $B_N - C_N^T (A_N - \gamma_A)^{-1} C_N \geq \gamma_B \geq iJ$, where the last inequality follows from the fact that γ_B is a CM. Using the equivalence (ii)–(iii) of Lemma 7.32 we obtain $\gamma_A \leq A_N - C_N (B_N - iJ)^{-1} C_N^T = A_{N+1} + iC_{N+1}$, where we have also used the map (7.100)[22]. According to Lemma 7.33, this immediately proves the proposition.■

Now, we show that the converse of Prop. 7.6 is true. That is, if γ_{N+1} is separable, so is γ_N. Apart from that, the following proposition exhibits how

[22] We have not included explicitly the conditions imposed by Lemma 7.32 on the kernels of B and C. However, one can easily verify that all the problems that may arise from these kernels are eliminated by using pseudoinverses instead of inverses of matrices (see footnote [20] on p. 153)

to construct the matrices $\gamma_{A,B}$ [cf. Eq. (7.99)] related to γ_N starting from the ones corresponding to γ_{N+1}.

Proposition 7.7 *If for some CM, γ_A, we have that $\gamma_{N+1} \geq \gamma_A \oplus \gamma_A$ then $\gamma_N \geq \gamma_A \oplus \gamma_B$, where*

$$\gamma_B \equiv B_N - C_N(A_N - \gamma_A)^{-1}C_N^T, \tag{7.101}$$

is a CM.

Proof: We use Lemma 7.33 and the map (7.100) to transform the inequality $\gamma_{N+1} \geq \gamma_A \oplus \gamma_A$ into $A_N - C_N^T(B_N - iJ)^{-1}C_N \geq \gamma_A$. According to the equivalence (ii)–(iii) of Lemma 7.32 this implies that $\gamma_B \geq iJ$. Since it is clear from its definition (7.101), γ_B is also real and symmetric, it is a CM. On the other hand, using the equivalence (i)–(iii) of Lemma 7.32 we immediately obtain that $\gamma_N \geq \gamma_A \oplus \gamma_B$.■

Using the fact that for $N \geq 1$, $A_N = B_N$ and the symmetry of the corresponding matrix γ_N we have

Corollary 7.16 *Under the conditions of Prop. 7.7, if $N \geq 1$ we have that $\gamma_N \geq \tilde{\gamma}_A \oplus \tilde{\gamma}_A$, where $\tilde{\gamma}_A \equiv (\gamma_A + \gamma_B)/2 \geq iJ$ is a CM.*

The above propositions imply that γ_0 is separable iff γ_N is separable for all $N > 0$. Thus, if we find some γ_N fulfilling (7.99) then γ_0 is separable. Thus, we can establish now the main result of this section.

Theorem 7.10 *(Separability criterion)*

(1) *If for some $N \geq 1$ we have $A_N \not\geq iJ$ then γ_0 is not separable.*

(2) *If for some $N \geq 1$ we have*

$$L_N \equiv A_N - ||C_N||_{\rm op}\mathbb{1} \geq iJ \tag{7.102}$$

then γ_0 is separable [23]

Proof: (1) It follows directly from Prop. 7.6; (2) We will show that $\gamma_N \geq L_N \oplus L_N$, so that according to Prop. 7.7 γ_0 is separable. We have

$$\gamma_N = L_N \oplus L_N + \begin{pmatrix} ||C_N||_{\rm op}\mathbb{1} & C_N \\ C_N^T & ||C_N||_{\rm op}\mathbb{1} \end{pmatrix}, \tag{7.103}$$

[23] $||A||_{\rm tr} \equiv {\rm tr}(A^\dagger A)^{1/2}$ denotes the trace norm of A. The operator norm of A, $||A||_{\rm op}$ is the maximum eigenvalue of $(A^\dagger A)^{1/2}$.

so that we just have to prove that the last matrix is positive. But using Lemma 7.32 this is equivalent to $||C_N||_{\rm op}^2\mathbb{1} \geq C_N^T C_N$, which is always the case.■

This theorem tells us how to proceed in order to determine if a CM is separable or not. We just have to iterate the map (7.100) until we find that either A_N is no longer a CM or L_N is a CM. In the first case, we have that γ_0 is not separable, whereas in the second one it is separable. If we wish to find a decomposition of the corresponding density operator as a convex set of product vectors we simply use the construction given in Corollary 7.16 until $N = 1$ and then the one of Prop. 7.7. This will give us the CMs, $\gamma_{A,B}$, such that $\gamma_0 \geq \gamma_A \oplus \gamma_B$, from which the decomposition can be easily found [153].

In order to check how fast our method converges we have taken families of CMs and applied to them our criterion. We find that typically with less than 5 iterations we are able to decide whether a given CM is entangled or not. The most demanding states for the criterion are those which lie very close to the border of the set of separable states (see Corollary 7.17 below). We challenged the criterion by applying it to states close to the border of the set of separable states and still the convergence was very fast (always below 30 steps). Figure 7.4 illustrates this behavior. We have taken $n = m = 2$ modes, an entangled CM γ_a of the GHZ form [145] (Fig. 7.4a) and an entangled CM γ_b with positive partial transposition [153] (Fig. 7.4b). We produced two families of CMs as $\gamma_{a,b}(\epsilon) = \gamma_{a,b} + \epsilon\mathbb{1}$. We have determined $\epsilon_{a,b}$ such that the CMs become separable. In the figure we see that in both cases, as we approach exponentially fast $\epsilon_{a,b}$, the number of steps only increases linearly. We have also added, instead of $\mathbb{1}$ other positive projectors with all possible ranks and found the same behavior. By taking other initial CMs we also find the same results.

Even though we have tested numerically the rapid convergence of our method, we still have to prove that, except for a zero measure set, it can decide whether a CM is entangled or not after a finite number of steps[24].We start out by considering the set of separable states. Since for them $\gamma_0 \geq \gamma_A \oplus \gamma_B$ with $\gamma_{A,B} \geq iJ$, if we just consider those with $\gamma_A > iJ$, we will leave out a zero measure set. In this case we can show that after a finite number of steps these separable states will be detected by using our procedure.

[24] Note that the fact that there exists a zero measure set which is not possible to characterize in a finite number of steps is not particular for our method, but a simple consequence of finite precision. For example, if we have a density operator ρ for two qubits such that the partial transpose has one negative eigenvalue $-\epsilon$, it will be increasingly difficult to check whether $\rho^T \geq 0$ as $\epsilon \to 0$.

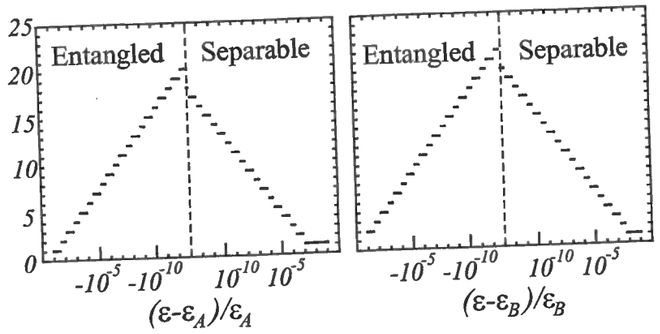

Figure 7.4: Number of steps as a function of ϵ for CMs of the form $\gamma_{a,b}(\epsilon) = \gamma_{a,b} + \epsilon\mathbb{1}$ where: (a) γ_a taken from Eq. (1) in Ref. [145] with $r = 1/4$, and $\epsilon_a = 0.305774915510(1)$; (b) γ_b taken from Eq. (9) in Ref. [153] and $\epsilon_b = 0.0978667902228(4)$.

Proposition 7.8 *If $\gamma_0 \geq \gamma_A \oplus \gamma_B$ with $\gamma_A \geq iJ + \epsilon\mathbb{1}$, then there exists some*

$$N < N_0 \equiv \frac{1}{\epsilon}(||A_0||_{\text{tr}} - 2n) + 1, \tag{7.104}$$

for which condition (7.102) is fulfilled.

Proof: Using Prop. 7.6 we have that for all N,

$$A_N - iJ \geq \epsilon\mathbb{1}. \tag{7.105}$$

Thus, $0 \leq \text{Re}(X_N) = A_N - A_{N+1}$. Since all the matrices in this expression are positive, taking the trace norm we have $||A_N||_{\text{tr}} - ||A_{N+1}||_{\text{tr}} = ||\text{Re}(X_N)||_{\text{tr}}$. Adding both sides of this equation from $N = 0$ to N_0, taking into account that $||\ldots||_{\text{tr}} \geq ||\ldots||_{\text{op}}$, and $||\text{Re}(X_N)||_{\text{op}} \geq ||C_{N+1}||_{\text{op}}$ [since $\text{Re}(X_N) \geq \pm i\text{Im}(X_N)$], we have

$$\sum_{N=0}^{N_0-1} ||C_{N+1}||_{\text{op}} \leq ||A_0||_{\text{tr}} - ||A_{N_0}||_{\text{tr}} \leq ||A_0||_{\text{tr}} - 2n, \tag{7.106}$$

where the last inequality is a consequence of the fact that $A_N \geq iJ$ for all N. Thus, among $\{C_N\}_{N=1}^{N_0}$ there must be at least one for which $||C_N||_{\text{op}} \leq \epsilon$. Thus, $A_N - ||C_N||_{\text{op}}\mathbb{1} \geq A_N - \epsilon\mathbb{1} \geq 0$ where for the last inequality we have used Eq. (7.105), and therefore, for that particular value of N, condition (7.102) must be fulfilled.■

It is worth stressing that from the proof of Prop. 7.8 it follows directly that if γ_0 is separable, then the sequence γ_N converges to a fixed point $\gamma_\infty = A_\infty \oplus B_\infty$, where $A_\infty = B_\infty \geq iJ$ are CMs. On the other hand, for the sake of completeness, we will now show that if γ_0 is not separable, then we can always detect it in a finite number of steps. We will use the fact that the CMs of inseparable Gaussian states form an open set, a fact that can be directly inferred from condition (7.99). This means that if γ_0 is inseparable, there always exist some $\epsilon_0 > 0$ such that if $\epsilon < \epsilon_0$ then $\gamma_0 + \epsilon\mathbb{1}$ is still inseparable and therefore condition (7.102) is never fulfilled. However, if γ_0 was separable, then, according to Prop. 7.8, $\gamma_0 + \epsilon\mathbb{1}$ should fulfill that condition before reaching $N = N_0$. This can be summarized as follows.

Corollary 7.17 *If γ is inseparable then there exists some $\epsilon > 0$ such that starting out from $\gamma_0 = \gamma + \epsilon\mathbb{1}$, condition (7.102) is not fulfilled for any $N \leq N_0 \equiv (||A_0||_{\text{tr}} - 2n)/\epsilon$.*

Together, Prop. 7.8 and Corollary 7.17 indicate that whether γ_0 is separable or not, and except for a set of zero measure, we will be able to detect it in a finite number of steps. However, as mentioned above, according to our numerical calculations we see that the process always converges very fast and in practice one can directly use the method sketched after Theorem 7.10.

Physical interpretation

The main tool to derive the necessary and sufficient condition of separability in the previous section is the map

$$M : \gamma_N \to \gamma_{N+1}, \tag{7.107}$$

where γ_0 is the initial CM and

$$\gamma_{N+1} = \begin{pmatrix} A_{N+1} & C_{N+1} \\ C_{N+1}^T & B_{N+1} \end{pmatrix}, \tag{7.108}$$

with

$$A_{N+1} = A_N - Re(X_N) \tag{7.109}$$

$$C_{N+1} = -Im(X_N), \tag{7.110}$$

where $X_N = C_N(B_N - iJ)^{-1}C_N^T$.

We are going to show now that this map has a nice physical interpretation. The transformation $\gamma_N \to \gamma_{N+1}$ corresponds to the following procedure. Take two copies of a state corresponding to the CM γ_N. Then apply some

operator, Z to both subsystems on one side, say, B and B' and then trace over those subsystems. It remains an operator in systems A and A'. This is the operator corresponding to the "CM" γ_{N+1}. The operator Z allows to detect entanglement [compare to EW (Sec. 7.1.2)]; the original state is entangled iff the outcoming state, after a finite number of iterations of the procedure explained above, is no longer a Gaussian state, that is the CM is no longer physical (Lemma 1.3).

Mathematically stated: We denote the Gaussian state, corresponding to the CM γ_N by ρ_N. Then we show that there exists an operator, $Z_{BB'}$ such that the correlation matrix of the operator $\rho_{AA'} = \mathrm{tr}_{BB'}(\rho_N^{AB} \otimes \rho_N^{A'B'} Z_{BB'})$ is the correlation matrix which we obtain after applying the map (7.107) to γ_N, i.e. γ_{N+1}.

We define $x_Y = (q_Y, p_Y) \in \mathbb{R}^2$, for all the 1–mode subsystem that we consider here, i.e. for $Y = A, A', B, B'$. Let Z be the operator

$$Z = \int dx_B dx_{B'} D(x_B, x_{B'}) e^{\frac{1}{4}(x_{B'}^T J x_B - x_B^T J x_{B'})}, \tag{7.111}$$

where $D(x_Y, x_Z) = e^{-i(q_Y X_Y + p_Y P_Y + q_Z X_Z + p_Z P_Z)}$, is the displacement operator (1.30) for $Y, Z \in \{A, A', B, B'\}$ and $J = J_1$ as defined in Eq. (7.97). Then we have

Lemma 7.34 *Given the operator Z as defined in (7.111). Then $\tilde{\rho}_{AA'} = \mathrm{tr}_{BB'}[\rho_N^{AB} \otimes \rho_N^{A'B'} Z_{BB'}]$ is a "Gaussian operator" (not necessarily physical) whose corresponding correlation matrix is γ_{N+1}.*

This lemma will be proven in Appendix F.

Note that translating this idea to the case of density operators acting on finite dimensional Hilbert spaces does not lead to a new insight in the separability problem of this case. The reason for this is the following lemma:

Lemma 7.35 *If $Z = Z^\dagger$ such that $\rho_{AA'} = \mathrm{tr}_{BB'}(\rho_{AB} \otimes \rho_{A'B'} Z_{BB'}) \geq 0$ for all ρ_{AB} separable, then $Z_{BB'}$ is an entanglement witness (between B and B') or positive.*

Proof: We choose $\rho = |a_1 b_1\rangle\langle a_1 b_1| + |a_2 b_2\rangle\langle a_2 b_2|$ where $|a_1\rangle \perp |a_2\rangle$. Then

$$\begin{aligned} & \rho_{AA'} \qquad\qquad (7.112) \\ = \; & |a_1 a_2\rangle\langle a_1 a_2| \langle b_1 b_2| Z |b_1 b_2\rangle + |a_1 a_1\rangle\langle a_1 a_1| \langle b_1 b_1| Z |b_1 b_1\rangle \\ + \; & |a_2 a_1\rangle\langle a_2 a_1| \langle b_2 b_1| Z |b_2 b_1\rangle + |a_2 a_2\rangle\langle a_2 a_2| \langle b_2 b_2| Z |b_2 b_2\rangle \end{aligned}$$

Since $|a_1\rangle$ and $|a_2\rangle$ are orthogonal, this operator is positive semidefinite iff all the terms in Eq. (7.112) are positive. Since this must hold for all $|b_i\rangle$, Z must be positive on product vectors.■

In conclusion, we have obtained a necessary and sufficient condition for bipartite Gaussian states to be separable. The condition provides an operational criterion in that it can be easily checked by direct computation. It is also worth mentioning that our criterion can be used to study the separability properties with respect to bipartite splitting of multipartite systems in Gaussian states [39, 40], (see also Sec. 7.2.2). Our criterion is based on a non–linear map, and is more powerful than partial transposition. This fact indicates that in other situations, like the one in which the systems A and B are n and m–level systems with $n \times m > 6$, there might exist a more powerful criterion than partial transposition to determine whether states are separable or not. This problem still remains open. However, the results presented here represent a significant step in understanding one of the most challenging problems in the field of Quantum Information, the separability problem.

7.2.2 Three-mode Gaussian states

When systems that are composed of $N > 2$ parties are considered, there are many "types" of entanglement due to the many ways in which the different subsystems may be entangled with each other. We will use the scheme introduced in Ref. [39, 40], see Sec. 1.2.1, to classify three-mode tripartite Gaussian states. The important point is that from the extension of Theorem 1.3 (Sec. 1.3.2) (γ is separable iff there exist CMs γ_A and γ_B such that $\gamma \geq \gamma_A \oplus \gamma_B$) we can derive a simple criterion that allows to determine which class a given state belongs to. This is in contrast to the situation for three qubits, where up until now no such criterion is known. In particular, we show that none of these classes are empty and we provide an example of a genuine tripartite bound entangled state, i.e. a state of three modes A, B, and C that is separable whenever two parties are grouped together but cannot be written as a mixture of tripartite product states and therefore cannot be prepared by local operations and classical communication of three separate parties.

Classification

As explained in Sec. 1.2.1, the scheme of [39, 40] considers all possible ways to group the N parties into $m \leq N$ subsets, which are then themselves considered each as a single party. Now, it has to be determined whether the resulting m-party state can be written as a mixture of m-party product

states. The complete record of the m-separability of all these states then characterizes the entanglement of the N-party state.

For tripartite systems, we need to consider four cases, namely the three bipartite cases in which AB, AC, or BC are grouped together, respectively, and the tripartite case in which all A, B, and C are separate. We formulate a simple extension to Theorem 1.3 to characterize mixtures of tripartite product states

Theorem 7.11 *(Three-party Separability)*
A Gaussian three-party state with CM γ can be written as a mixture of tripartite product states iff there exist one-mode correlation matrices $\gamma_A, \gamma_B, \gamma_C$ such that

$$\gamma - \gamma_A \oplus \gamma_B \oplus \gamma_C \geq 0. \tag{7.113}$$

Proof: The proof is in complete analogy with that of Theorem 1.45 in Ref. [153] and is therefore omitted here.

A state fulfilling condition (7.113) will be called *fully separable*. A state for which there are a one-mode CM γ_A and a two-mode CM γ_{BC} such that $\gamma - \gamma_A \oplus \gamma_{BC} \geq 0$ is called $A - BC$ *biseparable* (and similarly for the two other bipartite groupings). In total, we have the following five different entanglement classes:

Class 1 *Fully inseparable states* are those which are not separable for any grouping of the parties.

Class 2 *1-mode biseparable states* are those which are separable if two of the parties are grouped together, but inseparable with respect to the other groupings.

Class 3 *2-mode biseparable states* are separable with respect to two of the three bipartite splits but inseparable with respect to the third.

Class 4 *3-mode biseparable states* separable with respect to all three bipartite splits but cannot be written as a mixture of tripartite product states.

Class 5 The *fully separable* states can be written as a mixture of tripartite product states.

Examples for Class 1 (the GHZ-like states of [145]), Class 2 (two-mode squeezed vacuum in the first two and the vacuum in the third mode), and

Class 5 (vacuum state in all three modes) are readily given; we will provide examples for Classes 3 and 4 in this section.

How can we determine to which Class a given state with CM γ belongs? States belonging to Classes 1, 2, or 3 can be readily identified using the NPPT-criterion (Theorem 1.2). Denoting the partially transposed CM by $\tilde{\gamma}_x = \Lambda_x \gamma \Lambda_x, x = A, B, C$, with Λ_x defined in (1.41) we have the following equivalences:

Lemma 7.36 *(Classification)*

$$\tilde{\gamma}_A \not\geq iJ, \tilde{\gamma}_B \not\geq iJ, \tilde{\gamma}_C \not\geq iJ \quad \Leftrightarrow \quad \textit{Class 1} \tag{7.114}$$
$$(*)\tilde{\gamma}_A \not\geq iJ, \tilde{\gamma}_B \not\geq iJ, \tilde{\gamma}_C \geq iJ \quad \Leftrightarrow \quad \textit{Class 2} \tag{7.115}$$
$$(*)\tilde{\gamma}_A \not\geq iJ, \tilde{\gamma}_B \geq iJ, \tilde{\gamma}_C \geq iJ \quad \Leftrightarrow \quad \textit{Class 3} \tag{7.116}$$
$$\tilde{\gamma}_A \geq iJ, \tilde{\gamma}_B \geq iJ, \tilde{\gamma}_C \geq iJ \quad \Leftrightarrow \quad \textit{Class 4 or 5}, \tag{7.117}$$

where the $(*)$ reminds us to consider all permutations of the indices A, B, and C.

The proof follows directly from the definitions of the different classes and Theorem 1.2.

What is still missing is an easy way to distinguish between Class 4 and Class 5. Thus to complete the classification we now provide a criterion to determine whether a CM γ satisfying Ineqs. (7.117) is fully separable or 3-mode biseparable, that is we have to decide whether there exist one-mode CMs $\gamma_A, \gamma_B, \gamma_C$ such that (7.113) holds, in which case γ is fully separable. In the next subsection we will describe a small set consisting of no more than nine CMs among which γ_A is necessarily found if the state is separable.

Criterion for full separability

This subsection contains the main result of this section: a separability criterion for PPT $1 \times 1 \times 1$ Gaussian states, i.e. states whose CM fulfills Ineqs. (7.117). We start from Theorem 7.11 and obtain in several steps a simple, directly computable necessary and sufficient condition. The reader mainly interested in this result may go directly to Theorem 7.12, from where she will be guided to the necessary definitions and Lemmas.

Since the separability condition in Theorem 7.11 is formulated in terms of the positivity of certain matrices Lemma 7.32 will be very useful throughout the section. As mentioned above, in this section we exclusively consider three-mode CMs γ that satisfy Ineqs. (7.117). We write γ in its block form (1.35) as

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{7.118}$$

where A is a 2×2 matrix, whereas B is a 4×4 matrix. We observe that Ineqs. (7.117) impose some conditions on γ that will be useful later on:

Observation 3 *Let γ satisfy Ineqs. (7.117), then*

$$\gamma \geq \begin{pmatrix} \sigma_A iJ & 0 & 0 \\ 0 & \sigma_B iJ & 0 \\ 0 & 0 & \sigma_C iJ \end{pmatrix}, \tag{7.119}$$

where $\sigma_x \in \{0, \pm 1\}, \forall x = A, B, C$.

Proof: Ineqs. (7.117) say that $\gamma \pm iJ \geq 0$ and $\gamma \pm i\tilde{J}_x \geq 0 \; \forall x$. By adding these positive matrices all combinations of σ_x can be obtained. ∎

From this it follows that

Observation 4 *For a PPT CM γ as in Eq. (7.118)*

$$\ker(B + iJ), \ker(B + i\tilde{J}) \subseteq \ker C, \tag{7.120}$$

where $\tilde{J} = J \oplus (-J)$ is the partially transposed J for two modes.

Proof: Cond. (7.120) on the kernels is an immediate consequence of the equivalence of (i)–(ii) in Lemma 7.32 applied to the matrices $\gamma - 0 \oplus iJ \oplus (\pm iJ)$, which are positive by Obs. 3. ∎

Then the matrices

$$\tilde{N} \equiv A - C\frac{1}{B - i\tilde{J}}C^T, \tag{7.121a}$$

$$N \equiv A - C\frac{1}{B - iJ}C^T \tag{7.121b}$$

are well-defined and

Observation 5 *It holds that both*

$$\mathrm{tr}N, \mathrm{tr}\tilde{N} > 0, \tag{7.122}$$

Proof: Cond. (7.122) is true since, again by the equivalence of (i)–(ii) in Lemma 7.32 and Obs. 3, both N and $\tilde{N}$ are positive and $N \pm iJ, \tilde{N} \pm iJ \geq 0$. This implies that $N, \tilde{N}$ cannot be zero, which is the only positive matrix with vanishing trace. Therefore $\mathrm{tr}N, \mathrm{tr}\tilde{N}$ are strictly positive. ∎

The remainder of this section leads in several steps to the separability criterion. First, we simplify the condition (7.113) by reducing it to a condition which involves only one one-mode CM γ_A.

Lemma 7.37 *A PPT 3-mode CM γ is fully separable if and only if there exists a one-mode CM γ_A such that*

$$\tilde{N} \geq \gamma_A, \tag{7.123a}$$

$$N \geq \gamma_A, \tag{7.123b}$$

where $N, \tilde{N}$ were defined in Eqs. (7.121b). Without loss of generality we require γ_A to be a pure state CM, i.e. $\det \gamma_A = 1$.

Proof: By Theorem 7.11 full separability of γ is equivalent to the existence of one-mode CMs $\gamma_A, \gamma_B, \gamma_C \geq iJ$ such that $\gamma - \gamma_A \oplus \gamma_B \oplus \gamma_C \geq 0$. Let γ_x stand for $\gamma_{A,B,C}$.

By Lemma 7.32 [(i)–(ii)] this is equivalent to $\exists \gamma_x$ such that $M' \equiv B - C^T \frac{1}{A - \gamma_A} C \geq \gamma_B \oplus \gamma_C$ and the kernels fulfill the condition in Lemma 7.32 (ii). This is true iff the matrix M' is a CM belonging to a separable state, i.e. (Theorem 1.2) iff $M' \geq i\tilde{J}, iJ$. Using $B \geq i\tilde{J}, iJ$ [which holds since γ fulfills Ineqs. (7.117)] we obtain that γ is separable iff there exists $\gamma_A \geq iJ$ such that

$$\begin{pmatrix} A - \gamma_A & C \\ C^T & B'_k \end{pmatrix} \geq 0, \; k = 1, 2, \tag{7.124}$$

where $B'_1 = B - iJ$ and $B'_2 = B - i\tilde{J}$. Since the condition in Lemma 7.32 (ii) holds, this is [Lemma 7.32 (i)–(ii)] equivalent to Ineqs. (7.123). That we can always choose $\det \gamma_A = 1$ follows directly from Eq. (1.34d), since it shows that for any CM γ there exists a pure CM γ_0 such that $\gamma_0 \leq \gamma$. ∎

While we can always find a γ_A fulfilling Ineq. (7.123b), since γ belongs to a PPT state [and there exists a two-mode CM $\gamma_{BC} \geq iJ$ such that $\gamma_A \oplus \gamma_{BC}$ is smaller than γ], it may well happen that Ineq. (7.123a) cannot be satisfied at all, or that it is impossible to have both Ineqs. (7.123) fulfilled for one γ_A simultaneously. Note that due to Ineqs. (7.117), N and $\tilde{N}$ as above are always positive. From Ineqs. (7.123) we observe that

Observation 6 *for the CM γ of a separable state it is necessary to have*

$$\mathrm{tr}N, \mathrm{tr}\tilde{N} \geq 2, \tag{7.125a}$$

$$\det N, \det \tilde{N} > 0, \tag{7.125b}$$

where γ as in Eq. (7.118) and $N, \tilde{N}$ as in Eq. (7.121b).

Proof: A selfadjoint 2×2 matrix is positive iff its trace and determinant are positive. Since the trace of the RHS of both Ineqs. (7.123) is ≥ 2 (see Sec. 1.3.1) the same is necessary for the LHS. Also, since $\det \gamma_A = 1$, i.e. γ_A

has full rank, any matrix $\geq \gamma_A$ must also have full rank (see Sec. 7.1.1) and thus a strictly positive determinant. ∎

For a selfadjoint positive 2×2 matrix

$$R = \begin{pmatrix} a & b \\ b^* & c \end{pmatrix}, \tag{7.126}$$

we show

Lemma 7.38 *There exists a CM $\gamma_A \leq R$ if and only if there exist $(y, z) \in \mathbb{R}^2$ such that*

$$\begin{aligned} \mathrm{tr}R &\geq 2\sqrt{1+y^2+z^2}, & \text{(7.127a)} \\ \det R + 1 + L^T \begin{pmatrix} y \\ z \end{pmatrix} &\geq \mathrm{tr}R\sqrt{1+y^2+z^2}, & \text{(7.127b)} \end{aligned}$$

where

$$L = (a - c, 2\mathrm{Re}b). \tag{7.128}$$

Proof: As noted in Lemma 7.37 we need only look for γ_A with $\det \gamma_A = 1$. We parameterize

$$\gamma_A = \begin{pmatrix} x+y & z \\ z & x-y \end{pmatrix}, \tag{7.129}$$

with real parameters x, y, z and $x^2 = 1 + y^2 + z^2$ for purity. This is a CM iff $\gamma_A - iJ \geq 0$ (Lemma 1.3), that is iff $\mathrm{tr}\gamma_A = 2x \geq 0$ (where we use that positivity of the a 2×2 matrix is equivalent to the positivity of its trace and determinant and $\det(\gamma_A - iJ) = 0$ by construction). By the same argument, $R - \gamma_A \geq 0$ leads to the two conditions (7.127). ∎

The inequalities (7.127) have a simple geometrical interpretation that will be useful for the proof of the promised criterion: Ineq. (7.127a) restricts (y, z) to a circular disk $\mathcal{C}'$ of radius $\sqrt{(\mathrm{tr}R)^2/4 - 1}$ around the origin, while Ineq. (7.127b) describes a (potentially degenerate) ellipse $\mathcal{E}$ (see Fig. 7.6), whose elements are calculated below, and the existence of a joint solution to Ineqs. (7.127) is therefore equivalent to a nonempty intersection of $\mathcal{C}'$ and $\mathcal{E}$.

Applying this now to the matrices (7.126) we find that in order to simultaneously satisfy both conditions in Lemma 7.37, the intersection between the two ellipses $\mathcal{E}, \tilde{\mathcal{E}}$ and the smaller of the two concentric circles $\mathcal{C}', \tilde{\mathcal{C}}'$ (which we denote in the following by $\mathcal{C}$) must be nonempty. This condition leads to three inequalities in the coefficients of the matrices $\tilde{N}, N$ which can be satisfied simultaneously if and only if the PPT trimode state is separable. Thus we can reformulate the condition for separability (Lemma 7.37) as follows

Lemma 7.39 *(Reformulated Separability Condition)*
A three-mode state with CM γ satisfying Ineqs. (7.117) is fully separable if and only if there exists a point $(y, z) \in \mathbb{R}^2$ fulfilling the following inequalities:

$$\begin{aligned} \min\{\mathrm{tr}N, \mathrm{tr}\tilde{N}\} &\geq 2\sqrt{1+y^2+z^2}, & \text{(7.130a)} \\ \det N + 1 + L^T \begin{pmatrix} y \\ z \end{pmatrix} &\geq \mathrm{tr}N\sqrt{1+y^2+z^2}, & \text{(7.130b)} \\ \det \tilde{N} + 1 + \tilde{L}^T \begin{pmatrix} y \\ z \end{pmatrix} &\geq \mathrm{tr}\tilde{N}\sqrt{1+y^2+z^2}. & \text{(7.130c)} \end{aligned}$$

Proof: According to Lemma 7.37 γ belongs to a separable state iff we can find γ_A smaller than $\tilde{N}$ and smaller than N. According to Lemma 7.38 we can find such a γ_A iff we can find (y, z) such that Ineqs. (7.127) are satisfied for both N and $\tilde{N}$. ∎

In the following paragraphs we have a closer look at the sets $\mathcal{E}, \tilde{\mathcal{E}}$, and $\mathcal{C}$. The goal of this discussion is to identify a few special points – directly computable from γ – among which a solution to Ineqs. (7.130) will be found iff the state under consideration is separable. This will then lead to the final practical form of the separability criterion which is stated at the end of this section.

By squaring Ineq. (7.130b) we obtain

$$\left[\begin{pmatrix} y \\ z \end{pmatrix} - \mu L\right]^T K \left[\begin{pmatrix} y \\ z \end{pmatrix} - \mu L\right] \leq m, \tag{7.131}$$

where $\mu = (\det N + 1)/k_1$, $m = \frac{k_2}{k_1}\left[(\det N + 1)^2 - k_1\right]$, and the matrix K is[25]

$$K = k_1 P_L + k_2 P_{L^\perp},$$

with the orthogonal projectors $P_L, P_{L^\perp}$ on $L, L^\perp$ and

$$\begin{aligned} k_1 &= 4\left[\det N + (\mathrm{Im}b)^2\right], \\ k_2 &= (\mathrm{tr}N)^2. \end{aligned}$$

Due to Ineqs. (7.125) k_1 and k_2 are strictly positive, μ, m are well-defined and K is a positive matrix of rank 2. Let us now distinguish the cases $m < 0$

[25] The following definitions assume that $L, \tilde{L} \neq 0$. (If one of them is 0, the corresponding ellipse degenerates into a circle around $(0, 0)$ and we can take an arbitrary $L \neq 0$ to make sense of P_L. The criterion is not affected by this assumption, since it relies on Ineqs. (7.130).

and $m \geq 0$. For $m < 0$ Ineq. (7.131) can never be fulfilled since K is a positive matrix. In the case $m \geq 0$, Ineq. (7.131) describes an ellipse $\mathcal{E}$ which is centered at $m_e = \mu L$ with major axis L and minor axis $L^\perp$ of lengths $\sqrt{m/k_1} \geq \sqrt{m/k_2}$, respectively. From Ineq. (7.130c) we obtain the same equations for the tilded quantities derived from $\tilde{N}$.

The final argument for the derivation of the separability criterion is as follows. By Lemma 7.39 the state is separable if and only if the three sets described by Ineqs. (7.130) have a common intersection, i.e. iff $I \equiv \mathcal{E} \cap \tilde{\mathcal{E}} \cap \mathcal{C} \neq \emptyset$. The border of I is contained in the union of the borders of the ellipses and circle: $\partial I \subseteq \partial\mathcal{E} \cup \partial\tilde{\mathcal{E}} \cup \partial\mathcal{C}$. Now we can distinguish two cases, both of which allow to calculate a definite solution to the Ineqs. (7.130) if the state is separable: Either ∂I has nonempty intersections with the borders of two of the sets $\mathcal{E}, \tilde{\mathcal{E}}, \mathcal{C}$ or ∂I coincides with the border of one of the three. In the latter case this whole set is contained in I. In the former case, at least one of the points at which the borders intersect must be in I and thus a solution. If no solution is found this way the state is inseparable. This argument is made more precise in the final theorem. Formulas for the nine candidate solutions – the centers $m_c, m_e, m_{\tilde{e}}$ and the intersections points $i^{\pm}_{e\tilde{e}}, i^{\pm}_{ce}, i^{\pm}_{c\tilde{e}}$ – are given in Appendix G.1.

Theorem 7.12 *(Criterion for full separability)*
A three-mode state corresponding to the CM γ satisfying Ineq. (7.117) is fully separable if and only if Ineqs. (7.125b) holds and there exists a point ξ_{sol}

$$\xi_{sol} \in \{m_c, m_e, m_{\tilde{e}}, i^{\pm}_{e\tilde{e}}, i^{\pm}_{ce}, i^{\pm}_{c\tilde{e}}\} \tag{7.132}$$

fulfilling the Ineqs. (7.130).

Proof: We already saw (Obs. 6) that $\det N, \det \tilde{N} > 0$ are necessary for separability. If this holds, the quantities used in (7.130, 7.132) and in their derivation are all well-defined.

According to Lemma 7.39 γ is fully separable iff there exists a point $(y, z)^T$ such that the Ineqs. (7.130) are fulfilled. Therefore, if one of the points (7.132) satisfies Ineqs. (7.130) then it determines a γ_A fulfilling Ineqs. (7.123) thus proving that the state is separable. To complete the proof, we show that if the state is separable, then we find a solution to Ineqs. (7.130) among the points (7.132).

As pointed out before, the condition that Ineqs. (7.130) can simultaneously be satisfied has the geometrical interpretation that the circle $\mathcal{C}$ and the two ellipses $\mathcal{E}, \tilde{\mathcal{E}}$ have a nonempty intersection, i.e. $I \equiv \mathcal{E} \cap \tilde{\mathcal{E}} \cap \mathcal{C} \neq \emptyset$.

Thus it remains to prove that if I is nonempty then one of the nine points in (7.132) lies in I. But if $I \neq \emptyset$ there are only the following two possibilities: since all the sets considered are convex and closed, either the border of I coincides with that of one of the sets $\mathcal{C}, \mathcal{E}, \tilde{\mathcal{E}}$ (which means that one of these sets, call it $\mathcal{S}$, is contained in *both* others) or at least two of the borders $\partial\mathcal{C}, \partial\mathcal{E}, \partial\tilde{\mathcal{E}}$ contribute to ∂I, in which case the points at which these two intersect belong to ∂I and thus to I.

In the former case, the center of $\mathcal{S}$ is a solution and given by one of the Eqs. (G.1); in the latter, one can find a solution among the intersections of the borders of the sets $\mathcal{E}, \tilde{\mathcal{E}}, \mathcal{C}$. That these are given by the $i^{\pm}_x$ is shown in Appendix G.1. ∎

If a CM γ belongs to a separable state according to the above theorem then the point ξ_{sol} provides us with a pure one-mode CM γ_A such that $N, \tilde{N} \geq \gamma_A$. By construction $\gamma' = B - C(A - \gamma_A)^{-1}C^T$ is a separable 2×2 CM and by repeating a similar procedure as above with γ' we can calculate a pure product-state decomposition of the original state with CM γ.

Examples of bound entangled states

In this section we construct states belonging to Classes 3 and 4. Our construction makes use of ideas that were first applied in finite dimensional quantum systems to find PPT entangled states [75] and that we then generalized in Sec. 7.1 [106] to construct the so-called *edge states*. Recall that these states lie on the border of the convex set of states with positive partial transpose. Similarly, one can define "edge CMs" as those that lie on the border of the convex set of PPT CMs (they are called "minimal PPT CMs" in Ref. [153]).

This section is divided into three subsections. In the first one we define "edge CMs" and characterize them. In the second and third subsections we present two different families of CMs which contain edge CMs. We also show that within those families we have CMs belonging to all classes.

Edge correlation matrices

In the following we will consider CMs γ corresponding to PPT states, i.e. fulfilling

$$\gamma - i\tilde{J}_x \geq 0, \quad \text{for all } x = 0, A, B, C, \tag{7.133}$$

where $\tilde{J}_0 \equiv J$.

Definition 7.4 *(Edge Correlation Matrices)*
A CM γ is an edge CM if it corresponds to a non–separable state, fulfills

(7.133), and $\gamma' \equiv \gamma - P$ does not fulfill (7.133) for all real operators P with $0 \neq P \geq 0$. [26]

Note that a state with an edge CM automatically belongs to class 4 (i.e. edge CMs correspond to 3-mode biseparable states). In order to fully characterize them, we will need the following definition. Let us consider the complex vector space $V \subseteq \mathbb{C}^6$ of dimension d spanned by the vectors belonging to the kernels of all $\gamma - i\tilde{J}_x$ $(x = 0, A, B, C)$. We will define $K(\gamma)$ as a real vector space which is spanned by the real parts and imaginary parts of all the vectors belonging to V. More specifically, let us denote by $B = \{f_R^k + i f_I^k\}_{k=1}^d$ a basis of V, such that f_R^k and f_I^k are real. We define

$$K(\gamma) = \left\{ \sum_k \lambda_k f_R^k + \mu_k f_I^k, \lambda_k, \mu_k \in \mathbb{R} \right\} \subseteq \mathbb{R}^6; \tag{7.134}$$

that is, the real span of the vectors f_R^k and f_I^k. Note that this definition does not depend on the chosen basis B [As it is pointed out in Appendix G.2, $K(\gamma)$ coincides with the real vector space spanned by all the vectors in the kernels of $\gamma + \tilde{J}_x \gamma^{-1} \tilde{J}_x$.]. We then have the following

Theorem 7.13 *(Characterization of $1 \times 1 \times 1$ edge CMs) A CM γ fulfilling (7.133) is an edge CM if and only if there exist no CMs $\gamma_A, \gamma_B, \gamma_C$ such that $\gamma = \gamma_A \oplus \gamma_B \oplus \gamma_C$ and $K = \mathbb{R}^6$.*

Proof: We will use the fact, see Lemma 7.1, that, given two positive matrices $A, B \neq 0$, there exists some $\epsilon > 0$ such that $A - \epsilon B \geq 0$ iff $R(B) \subseteq R(A)$. According to the Def. 7.4 we cannot subtract any real positive matrix from γ without violating the conditions (7.133). This is equivalent to imposing that there is no real vector in the intersection of the ranges of the matrices $\gamma - i\tilde{J}_x$. This is again equivalent to saying that there is no real vector orthogonal to all the vectors in $K(\gamma - i\tilde{J}_x)$, which in turn is equivalent to $K = \mathbb{R}^6$, since that vector should be orthogonal to all the real and imaginary parts of the vectors spanned by those kernels. Now, if γ corresponds to an entangled state it is clear that $\gamma \neq \gamma_A \oplus \gamma_B \oplus \gamma_C$. Conversely, if $\gamma \neq \gamma_A \oplus \gamma_B \oplus \gamma_C$ was separable, then there must exist some real positive P such that $\gamma - P = \gamma_A \oplus \gamma_B \oplus \gamma_C$ is separable, and therefore fulfills (7.133), which is not possible. ∎

In the construction of the following two examples of tripartite bound entangled states we are going to use this theorem. The idea is to take a CM

[26] Note that this definition can be easily adapted to CMs corresponding to a density operator (Gaussian state) describing the state of any system

γ_0 of a pure entangled state [which, of course, does not fulfill (7.133)] and add real positive matrices until the conditions (7.133) as well as $K = \mathbb{R}^6$ are fulfilled. If the resulting CM is not of the form $\gamma_A \oplus \gamma_B \oplus \gamma_C$ then Theorem 7.13 implies that it is an edge CM. In fact, we can add more real positive matrices keeping the state entangled [and fulfilling (7.133)]. In order to see how much we can add, we can use the criterion derived in the previous section.

This method of constructing CMs belonging to Class 4 also indicates how the corresponding states may be prepared experimentally. Adding a positive matrix P to the CM γ_0 corresponds to the following preparation process: start with an ensemble of states with CM γ_0, displace them randomly by d according to the Gaussian probability distribution with covariance matrix given by the inverse of P. This is a *local* operation (that potentially needs to be supplemented by classical communication) on each individual mode. The state produced by this randomization has CM $\gamma + P$ [153].

Example 1

In the first example we start out with an entangled state between the two parties Alice and Bob and the vacuum state in Charlie and add two projectors to the corresponding CM. More specifically, we consider the CMs of the form $\gamma_{a_1,a_2} = \gamma + a_1 P_1 + a_2 P_2$, where

$$\gamma = \gamma_{AB} \oplus \mathbb{1}_C, \tag{7.135}$$

and

$$\gamma_{AB} = \begin{pmatrix} a & 0 & c & 0 \\ 0 & a & 0 & -c \\ c & 0 & a & 0 \\ 0 & -c & 0 & a \end{pmatrix}, \tag{7.136}$$

with $a = \sqrt{1 + c^2}$ and c can take any value different from zero. Here, $P_1 = \tilde{p}_1 \tilde{p}_1^T$ and $P_2 = \tilde{p}_1 \tilde{p}_1^T$, where $\tilde{p}_1 = (0, 1, 0, 1, 1, 2)^T$ and $\tilde{p}_2 = (1, 0, -1, 0, 0, 1)^T$.

In order to explain why the CM γ_{a_1,a_2} achieves our purposes, let us first consider the two–mode case in which the correlation matrix is γ_{AB}. We denote now by $p = p_1 + i p_2$ [where $p_1 = (0, 1, 0, 1)^T$ and $p_2 = (1, 0, -1, 0)^T$] the eigenvector corresponding to the negative eigenvalue of $\gamma_{AB} - i\tilde{J}_A$. Since $(-i\tilde{J}_A)^* = -i\tilde{J}_B$ we have that the eigenvector corresponding to the negative eigenvalue of $\gamma_{AB} - i\tilde{J}_B$ is $p^* = p_1 - i p_2$. By adding a sufficiently large multiple of the projectors onto those vectors, we obtain a CM whose partial transposes are positive. Note that in this case (just two modes) this would already make the state separable.

In the case of three modes with a correlation matrix γ the same argumentation applies, namely that by adding some projectors we can make the

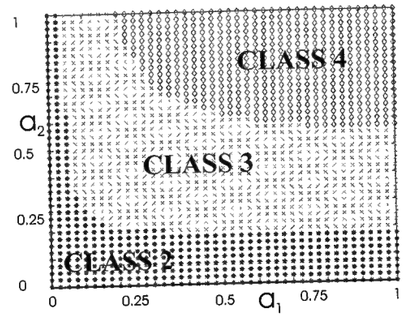

Figure 7.5: The Entanglement Classes of γ_{a_1,a_2}

partial transposes with respect to A and B positive. However, we have to involve C and thereby smear out the initial entanglement between A and B among all three parties. This is exactly what is achieved by adding the projectors P_1 and P_2. If we choose now, for instance, $c = 0.3$, $a_1 = 1$, and $a_2 \approx 0.5531095$, then one can show that the set $K(\gamma_{a_1,a_2})$ defined as in Eq. (7.134) spans $\mathbb{R}^6$. As mentioned at the end of the previous subsection, since the resulting CM is not of the form $\gamma_A \oplus \gamma_B \oplus \gamma_C$ it corresponds to an edge CM.

In Fig. 7.5 we illustrate to which class γ_{a_1,a_2} belongs as a function of the parameters $a_{1,2}$. In order to determine this, we have used the criterion derived in the previous section. It is worth noting that γ_{a_1,a_2} never becomes separable. This follows from Theorem 7.12 and the fact that both $m = \tilde{m} = 0$ for all values of $a_{1,2}$, as can be easily verified. This implies that the two ellipses [c.f. Ineq. (7.131)] are just two points [which coincide with the centers given in Eq. (G.1)]. Thus, the only possibility that the circle and the two ellipses intersect is that the centers of the ellipses are the same and lie inside the circle. It is easy to show that for all values of a_1 and a_2 the centers of the two ellipses are never the same. Thus the state corresponding to the CM γ_{a_1,a_2} is never separable and is a PPTES for all values of a_1, a_2 for which the partial transposes are positive.

Example 2

Here we present a family of states which belong either to Class 1, 4, or 5. The states of this family are obtained from a pure GHZ-like state [145] by adding a multiple of the identity, i.e.,

$$\gamma_\alpha = \gamma + \alpha \mathbb{1}, \tag{7.137}$$

where

$$\gamma = \begin{pmatrix} a & 0 & c & 0 & c & 0 \\ 0 & b & 0 & -c & 0 & -c \\ c & 0 & a & 0 & c & 0 \\ 0 & -c & 0 & b & 0 & -c \\ c & 0 & c & 0 & a & 0 \\ 0 & -c & 0 & -c & 0 & b \end{pmatrix}, \tag{7.138}$$

with $a > 1$ and

$$b = \frac{1}{4}(5a - \sqrt{9a^2 - 8}), \tag{7.139}$$

$$c = \frac{1}{4}(a - \sqrt{9a^2 - 8}). \tag{7.140}$$

For the following discussion, we pick $a = 1.2$. It is clear that for $\alpha = 0$ the state is fully inseparable, i.e., it belongs to Class 1, whereas for $\alpha \geq 1$ the state will be fully separable (Class 5). We will show now that for $\alpha_0 \leq \alpha \leq \alpha_1$, where $\alpha_0 \approx 0.29756$ and $\alpha_1 \approx 0.31355$ the state is biseparable and belongs therefore to Class 4.

The CM γ_α is symmetric with respect to permutations between the parties, and therefore the negative eigenvalues of the matrices $\gamma - i\tilde{J}_x, x = A, B, C$ are the same. We denote its absolute value by $\alpha_0 \approx 0.29756$. It is easy to determine the real and imaginary part of the corresponding eigenvectors. One finds that all those vectors are linearly independent. If we add now $\alpha_0 \mathbb{1}$ to γ then all those vectors belong to $K(\gamma_{\alpha_0})$ which immediately implies that $K(\gamma_{\alpha_0}) = \mathbb{R}^6$. Since $\gamma_{\alpha_0} \neq \gamma_A \oplus \gamma_B \oplus \gamma_C$ we have that it is an edge CM.

Let us now use Theorem 7.12 in order to determine α_1. First of all, we show, independently of the discussion above that γ_{α_0} belongs to class 4. In particular, we find that $m = \tilde{m} = 0$ [cf. Eq. (7.131)], which implies that there exists a solution to the Ineqs. (7.130) only if the centers of the two ellipses are the same and lie within the circle. Here one can also show that the two centers are not the same and so the state corresponding to the CM γ_{α_0} is a PPTES. Let us determine the values of α for which it is still the case that there exists no intersection of the two ellipses and the circle given by the Ineqs. (7.130). It is easy to show that if $\alpha > \alpha_0$ then $\mathrm{tr}N \leq \mathrm{tr}\tilde{N}$, which implies that the circle that has to be considered has radius $r_c = \sqrt{(\mathrm{tr}N)^2/4 - 1}$. One can also easily verify that the two ellipses never intersect the border of the circle, which simplifies the problem. The ellipses must always lie inside the circle (since if they where outside it would never be possible to obtain a separable state even for $\alpha > 1$). Thus, the problem reduces to check at which point the ellipses intersect each other. This occurs when $\alpha = \alpha_1 \approx 0.31355$. Thus the CM γ_α, where $\alpha_0 \leq \alpha < \alpha_1$ corresponds to a PPTES, whereas for $\alpha \geq \alpha_1$,

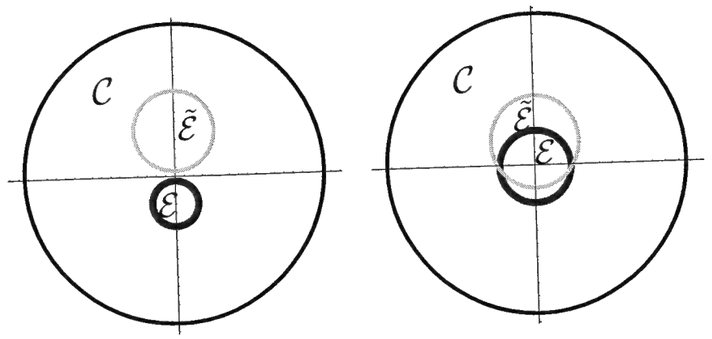

Figure 7.6: (a) The circle and the two ellipses do not have a joint intersection, therefore the state corresponding to γ_α is a PPTES, (b) the circle and the two ellipses have a joint intersection, therefore the state corresponding to γ_α is separable.

the corresponding state is fully separable. In the following Fig. 7.6 we have plotted the circle and the two ellipses, which are almost circles in this case, for (a) $\alpha < \alpha_1$ and (b) $\alpha > \alpha_1$.

Note that, using the separability criterion for multi-mode bipartite Gaussian states, Sec. 7.2.1 the results presented above can be extended to cover the case of n modes at location C. Nothing changes in the argumentation to distinguish 3-party biseparable from fully separable states. However, the separability criterion presented in Sec. 7.2.1 is now necessary to determine the properties under bipartite splitting, since for AB-C we deal with a $2 \times n$ state and PPT is then no longer sufficient for biseparability [153].

Conclusions

We have discussed nonlocal properties of Gaussian states of three tripartite modes. We have distinguished five classes with different separability properties and given a simple necessary and sufficient criterion that allows to determine which of these classes a given Gaussian state belongs to. The first three classes contain only NPPT states and positivity of a state under the three partial transpositions suffices to determine to which of those it belongs. The separability criterion, which allows to distinguish PPT entangled states from separable states is the main result of this section. For the case of three qubits such a criterion is still missing. Lastly, we have constructed examples for all the classes and in particular for tripartite entangled state with positive partial transpose. Not that the results derived in Sec. 7.2.1 allow to

generalize the results presented here to the $1 \times 1 \times N$ case.

It is worth pointing out that the separability criterion can be checked experimentally. The CM γ can be measured, and thus the criterion is entirely formulated in terms of quantities that are measurable with current technology.

Gaussian CV states promise to be a fruitful testing ground for quantum nonlocality: Pure entanglement is comparatively easy to create in quantum optical experiments, as described in Ref. [145]. Likewise, tripartite bound entangled states are experimentally accessible: the states discussed in the examples of Subsec. 7.2.2 can be obtained by mixing differently displaced pure Gaussian states.

The study of entanglement of multiparty Gaussian states is still in a very early stage. The interesting cases of more parties or more modes are very challenging. But even for the simple three-mode case there are important open question. In particular nothing is known about the distillability of tripartite states. As in Ref. [39, 40] for qubits, it is easy to see that Gaussian states in Classes 3 and 4 cannot be distilled at all and are therefore bound entangled. For this, we consider N copies of a Class 3 state ρ, and apply an arbitrary local quantum operation $\mathcal{P}_{locc}$ consisting of a classically correlated sequence of operations of the form $\mathcal{P} = \mathcal{P}_A \otimes \mathcal{P}_B \otimes \mathcal{P}_C$. Since ρ is in Class 3 we can write $\rho^{\otimes N}$ as a mixture of $AB - C$ product states $\sum_k p_k \rho^{(N)}_{AB,k} \otimes \rho^{(N)}_{C,k}$ and as a mixture of $AC - B$ product states $\sum_k p'_k \rho^{(N)}_{AC,k} \otimes \rho^{(N)}_{B,k}$. After applying an operation such as $\mathcal{P}$ the resulting state $\tilde{\rho} = \mathcal{P}(\rho^{\otimes N})$ will still be separable along these cuts, and no sequence of operations $\mathcal{P}$ can change this. Thus ρ is bound entangled.

Whether all states in Class 2 may be distilled to maximally entangled states between the two non-separable parties is an open question. If this were shown, it would follow that all states in Class 1 could be distilled into arbitrary tripartite entangled states.

Chapter 8

The distillation and activation problems

It was shown by Bennett et al. [7], Deutsch et al. [27], and by Gisin [61], how to obtain, out of some copies of an entangled mixed state, pure maximally entangled states, using only local operations and classical communication [109, 90]. As mentioned before, this process is called distillation and a state is said to be distillable if one can produce using LOCC, out of N copies (where N tends to infinity) of the state a maximally entangled state. It was shown that any NPPT state, describing the state of one qubit and a M–level system can be distilled to a maximally entangled state [72, 38]. The Horodecki family showed that a general necessary condition for distillability is that the partial transpose of the density operator must be non–positive semidefinite [70]. However, it is likely that the opposite is not true [38, 30]. At least, when considering a finite number of copies, there exist states, fulfilling this necessary condition for distillation, but it is not possible to transform some copies of this state into a maximally entangled state. Then there is still the possibility to distill some entanglement, if one allows Alice and Bob to share, in addition to there states a PPT entangled state [77]. This process is called activation, since the entanglement contained in the copies of the original state is activated by a PPTES.

Recently, it has been shown [45] that one copy of any bipartite state can always be either distilled or activated by a PPTES. In the following chapter we show that this is not the case if we consider systems composed of more than two subsystems [97]. That is we give an example of a three–partite state, where one (even two) copy of it can neither be distilled, nor activated. We introduce a formalism, which allows to connect the problem of entanglement witnesses (EW) to the problem of distillation and activation, for arbitrary

states[1] [97].

This chapter is divided into 4 sections. In Sec. 8.1 we introduce our notation and summarize some known results concerning distillation and activation of entanglement [72], see also Sec. 1.2.2. We reformulate the problem of distillation and activation of entanglement in terms of CPM's (see Sec. 2.1 and Sec. 4.1) in Appendix H. The reason for this is that the main results of this chapter can be understood without those technical details, but we need them to prove our statements. Sec. 8.2 is divided into two parts. In the first part we consider a density operator, ρ which describes the state of a system composed of two subsystems. For an arbitrary number, say N, of copies of this state we define an operator $W_{\rho^{\otimes N}}$. Then we show that those N copies of the state can be distilled iff $W_{\rho^{\otimes N}}$ is no EW (Sec. 7.1.2); the entanglement of those N copies can be activated via a PPTES iff $W_{\rho^{\otimes N}}$ is a special EW, namely a non–decomposable EW (NDEW). Furthermore, if the entanglement of a state can be distilled, then the introduced formalism gives us a distillation protocol. If the entanglement can be activated, then we know which PPTES activates it. In the second part of Sec. 8.2 we generalize those results to density operators describing more than two parties, by concentrating on three systems. Sec. 8.3 contains two applications of the formalism developed. First we rederive the above explained result presented in Ref. [45] in a simple manner. Second, we present an example of a three–partite state, whose partial transpose is not positive semidefinite, but, nevertheless one copy of the state can neither be distilled, nor activated. We then show that even if we consider two copies of some of those states the entanglement can neither be distilled, nor activated. Sec. 8.4 contains a summary of the results.

8.1 Notation and review

Throughout this section we consider a density operator, ρ, describing the state of several, say N, spatially separated systems. The Hilbert space on which ρ acts is $\mathcal{H} = \mathcal{H}_A \otimes \ldots \otimes \mathcal{H}_Z$, with $\dim(\mathcal{H}_X) = d_X$. We will only consider the nontrivial situations when $d_X \geq 2$. Whenever we consider the situation where Alice, Bob, Charly, ... have more than one particle we will denote them by $A_1, A_2, \ldots A_n$, $B_1, B_2, \ldots B_n$, $C_1, C_2, \ldots C_n$, ... respectively. The corresponding total Hilbert space of each party is then $\mathcal{H}_X = \mathcal{H}_{X_1} \otimes \ldots \mathcal{H}_{X_n}$, for $X \in \{A, B, C, \ldots\}$. We will also use the notation $\mathcal{H}_i = \mathcal{H}_{A_i} \otimes \ldots \otimes \mathcal{H}_{X_i}$, for $i \in \{1, \ldots, n\}$. Furthermore we denote by $\mathbb{1}_n$ the identity matrix acting

[1] in Ref. [30] the problem of distillability is connected to the problem of 2–positivity of linear maps, in contrast to the results presented here.

on a n–dimensional Hilbert space. For simplicity we will not normalize the states which we consider. We write the (unnormalized) maximally entangled state in $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ as,

$$|\Phi_d\rangle = \sum_{k=1}^{d} |k,k\rangle\,, \tag{8.1}$$

where $d = \min\{d_1, d_2\}$.

In the following we will call a density operators, ρ separable if is fully separable, i.e. $\rho = \sum_i |a_i\rangle_A \langle a_i| \otimes \ldots \otimes |z_i\rangle_Z \langle z_i|$,, where the states $|x_i\rangle$ belong to the Hilbert space of particle X (Sec. 1.2.1). Analogously we call a fully separable CPM simply separable. As mentioned in Sec. 1.2.1 ρ, is called Y–PPT (Y–NPPT) if its partial transpose with respect to system Y is (is not) a positive semidefinite operator. If a state has a positive (non–positive) semidefinite partial transpose with respect to all systems then we call it simply PPT (NPPT). We will see later on that partial transposition plays also an important role in establishing the distillation and activation properties of a state.

Here, an operator, $W = W^\dagger$ acting on $\mathcal{H}_A \otimes \ldots \otimes \mathcal{H}_Z$ is called an N–partite EW if (Sec. 1.2.1)

(I) $\langle a, \ldots, z|\, W\, |a, \ldots, z\rangle \geq 0 \quad \forall\, |a\rangle \in \mathcal{H}_A, \ldots, |z\rangle \in \mathcal{H}_Z$

(II) W is not positive.

Note that we do not assume here that the EW is normalized [condition (III) in Sec. 1.2.1]. An EW is called decomposable (non–decomposable) EW (DEW) [NDEW] if it can (cannot) be written as $W = O_0 + O_1^{T_A} + \ldots O_N^{T_Z}$, where the operators O_i are positive semidefinite. Recall that a N–partite EW, W, is a NDEW iff it detects a PPTES (Lemma 7.26 in Sec. 7.1.2). Let us now review some facts concerning distillation and activation properties.

Distillation and activation of entanglement

We consider the situation where an arbitrary number of parties share an arbitrary number of copies of the state ρ. Then, we call ρ fully distillable if the parties can, using LOCC, produce a maximally entangled state, shared among all the parties. Note that a PPT state can never be distilled, which can be easily seen as follows. If ρ is PPT then $\rho^{\otimes N}$ is PPT for all N, and so is, $\mathcal{E}[(\rho^{\otimes N})^{T_A}]$ for all N and $\mathcal{E}$ separable, as shown in Sec. 4.1.5. Thus, by LOCC one can never produce, out of a PPT state a maximally entangled state, which is NPPT. Note that, in the bipartite case with $d_A = 2$ and

d_B arbitrary, it has been shown [38] that all NPPT states are distillable. However, for higher dimensions, there is a strong conjecture [38, 30] that this is no longer true, i.e. that there exist undistillable NPPT states. In the case of more than two parties, the argumentation above implies that a state can only be distillable if all the partial transposes are non–positive semidefinite, i.e. if the state is NPPT.

If a state is not distillable, then it might be possible to activate its entanglement using a PPTES. That is, if the parties share, in addition to N copies of a state, ρ, a PPTES, then they might be able to produce a maximally entangled state, using LOCC. As mentioned, this process is called activation. Using the argumentation above, one immediately sees that only NPPT states are activatable.

Let us now, in order to be more specific, treat the case of two parties and the one of three independently. The next part of this section deals with the bipartite case. There we review the conditions which must be fulfilled for a state to be distillable or activatable. In the second part of this section we show how to generalize the results of two parties to three.

Two Parties

In this scenario a state, $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, is called distillable if Alice and Bob can produce by LOCC a maximally entangled state (8.1), with $d = \min(d_A, d_B)$. Recall that the problem of distillation of a state, ρ, can be formulated in the following way (Lemma 1.2):

A state, ρ, is distillable iff there exists a positive integer N and a state of the form

$$|\Psi\rangle = |e_1, f_1\rangle + |e_2, f_2\rangle\,, \tag{8.2}$$

such that

$$\langle\Psi|\,(\rho^{\otimes N})^{T_A}\,|\Psi\rangle < 0, \tag{8.3}$$

where $\{e_1, e_2\}$ ($\{f_1, f_2\}$) are two unnormalized orthogonal vectors in $(\mathbb{C}^{d_A})^{\otimes N}$ [$(\mathbb{C}^{d_B})^{\otimes N}$].

We call a state N–distillable if for this integer N condition (8.3) is fulfilled. Otherwise we call it N–undistillable.

We call a m–undistillable state, ρ, activatable if there exists a positive integer $N \leq m$ and a PPTES, σ, such that $\rho^{\otimes N} \otimes \sigma$ is 1–distillable.

Given a N–undistillable state, ρ, we call it N–activatable if there exists a PPTES, σ, such that $\rho^{\otimes N} \otimes \sigma$ is 1–distillable.

Three Parties

A three–partite state, $\rho \in \mathcal{B}(\mathcal{H}) = \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ is fully–distillable if Alice, Bob and Charly can produce, using LOCC, out of an arbitrary number of copies of ρ a GHZ–state [63]. Note, that this is possible iff (up to permutations) Alice and Bob can produce a state of the form (8.1) with $d = d_{AB} = \min(d_A, d_B)$ and Bob and Charly can distill a state of the form (8.1) with $d = d_{BC} = \min(d_B, d_C)$. This can be easily understood using that 2 maximally entangled state, one in A and B and the other in B and C can always, by LOCC be combined to a GHZ-state, $\sum_{i=1}^{\min(d_{AB},d_{BC})} |iii\rangle$. The other direction is also true, since, given two GHZ states one can, using LOCC, transform them into a maximally entangled state in A and B and one in B and C. Using this fact we only have to answer the question: 'Can Alice, Bob, and Charly distill a maximally entangled state in A, B and one in B, C?'. Therefore, from now on we will only deal with the problem of bipartite entanglement distillation. We call a state, ρ, BC–distillable if Alice, Bob and Charly can produce, using LOCC, out of an arbitrary number of copies of ρ in BC a maximally entangled state, i.e a state of the form (8.1) with $d = \min(d_B, d_C)$. Note that the best strategy for them to distill a maximally entangled state in B and C is that Alice measure a projector. The reason for this is that if they apply any other measurement, then they always reduce the entanglement of the outcoming state. We define AB, and AC–distillability analogously for the other cases.

If a state is undistillable we have, analogously to the bipartite case, the possibility to activate its entanglement using a PPTES. That is the parties share, in addition to some copies of their state a PPTES. Then they distill out of those states a maximally entangled state. If this is possible then we call the state activatable. Again, we have that it is activatable iff it is (up to permutations) AB–activatable and BC–activatable; that is the entanglement among all parties can be activated iff the entanglement between A and B and the one between B and C can be activated.

Let us now show under which conditions a state is XY–distillable, where $X, Y \in \{A, B, C\}$, on the example of BC–distillation.

Lemma 8.1 *A state, ρ, is BC–distillable iff there exists a positive integer N and a state of the form*

$$|\Psi\rangle = |e_1, f_1\rangle + |e_2, f_2\rangle\,, \tag{8.4}$$

where $\{e_1, e_2\}$ ($\{f_1, f_2\}$) are two unnormalized orthogonal vectors in $(\mathcal{H}_B)^{\otimes N}$ [$(\mathcal{H}_C)^{\otimes N}$], and a state $|h\rangle \in (\mathcal{H}_A)^{\otimes N}$ such that

$$\langle\Psi| \langle h| (\rho^{\otimes N})^{T_C} |h\rangle |\Psi\rangle < 0. \tag{8.5}$$

Note that condition (8.5) can only be fulfilled if ρ is B–NPPT as well as C–NPPT.

Analogously to the bipartite case, we call a state, ρ, N–BC–distillable if for the integer N condition (8.5) is fulfilled. We call ρ N–fully distillable if it is (up to permutations) N–AB–distillable and N–BC–distillable.

If a state is not distillable then we still have the possibility to activate its entanglement using a PPTES. Let us now characterize those states which are XY–activatable on the example $X = B$, $Y = C$.

We call a state, ρ, which is not m–BC–distillable, BC–activatable if there exists an integer $N \leq m$ and a PPTES σ such that $\rho^{\otimes N} \otimes \sigma$ is 1–BC–distillable.

Given a N–BC–undistillable state, ρ, we call it N–BC–activatable if there exists a PPTES, σ, such that $\rho^{\otimes N} \otimes \sigma$ is 1–BC–distillable. We call ρ N–fully activatable if it is (up to permutations) N–AB–activatable and N–BC–activatable.

8.2 Characterization using entanglement witnesses

In this section we show that there exists a connection between EW's and the distillation and activation properties of states [97]. We will define an operator which allows to answer the questions, if N copies of a state are distillable, or if not, if their entanglement can be activated using a PPTES. Using this formalism it is easy to rederive the result [45] that any bipartite NPPT is either 1–distillable, or 1–activatable. One the other hand, it allows us to prove that there exist three–partite NPPT state which are neither 2–distillable, nor 2–activatable.

This section is divided into two parts. In the first part we show this connection for the bipartite case, whereas in the second part we extend those results to three parties. Both parts have the same structure; first we define the operator which allows us to draw the connection between EW's and the distillation and activation properties of a state. Then we state the main results of this chapter. In the last part of each section we prove those results. The reader, who is not interested in the proofs can skip the last part of Sec. 8.2.1 and Sec. 8.2.2 respectively.

8.2.1 Two parties

Let us denote by X is an arbitrary positive operator acting on $\mathcal{H}_2 = \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2}$. We define

$$W_X = P_{A_1,B_1} \otimes X^{T_{A_2}}_{A_2,B_2}, \tag{8.6}$$

where P_{A_1,B_1}, acting on $\mathcal{H}_1 = \mathbb{C}^2 \otimes \mathbb{C}^2$ is the projector onto the maximally entangled state (8.1), with $d = 2$. Now, we will show that W_ρ allows us to answer the questions, if the entanglement of this state can be distilled, or, if not, if it can be activated using a PPTES. In particular, we show that, depending on, whether $W_{\rho^{\otimes N}}$ is no EW, a NDEW, or a DEW, the corresponding state ρ is N–distillable, N–activatable, or neither N–distillable nor N–activatable, respectively. This is stated by the following Theorems and Corollaries, which will be proven below.

Main results

Theorem 8.1 *(Characterization of N–distillable states) A state, ρ, is N–distillable iff $W_{\rho^{\otimes N}}$ is no EW [it does not fulfill (I)].*

Theorem 8.2 *(Characterization of N–activatable states) A state, ρ, which is N–undistillable, is N–activatable iff $W_{\rho^{\otimes N}}$ is a NDEW.*

Those theorems state that EW's do not only allow us to determine whether a state is entangled or not, but also characterize the distillability properties of a state. We have that W_ρ is no EW iff ρ is 1–distillable (Theorem 8.1). Now, if ρ is 1–undistillable it can be either 1–activatable or not. In this case W_ρ is an EW (Theorem 8.1), which can be either decomposable or non–decomposable. Then the entanglement of ρ can be activated via a PPTES iff W_ρ is a NDEW (Theorem 8.2). It is worth to mention that using these results it is not only possible to know if the entanglement of a state is distillable, or if it can be activated. It can be seen by the proofs that these results provide us with a distillation protocol. That is, given a state, which can be distilled, then the separable state, which is 'detected' by the witness, W_ρ corresponds to a LOCC, which distills a maximally entangled state (see Appendix H) On the other hand, the PPTES, which activates the entanglement is easily determined by the state, which is detected by the NDEW, W_ρ. Those Theorems also imply the following

Corollary 8.1 *A state, ρ, is neither N–distillable nor N–activatable iff $W_{\rho^{\otimes N}}$ is decomposable*[2].

[2]Note that a hermitian operator is either no EW, a DEW or a NDEW

Note that the results above are not only a way of rewriting the problems, but they really allow for a new insight in the problem of distillation and activation. For instance in Sec. 8.3, we review in a simple manner the fact that every bipartite NPPT state is either 1–distillable or 1–activatable [45].

Proofs

The reader who is not interested in the proofs can continue reading in the next section. For simplicity we prove the statements for $N = 1$, since the argumentation holds for arbitrary N. The technical details and the definitions, which are needed to follow the proofs can be found in the appendix. Let us start out by determine the properties of the operator W_X:

(a) W_X is not positive semidefinite iff $X^{T_{A_2}}$ is not positive semidefinite, i.e iff X is NPPT.

(b) If W_X fulfills condition (I) then both, $W_X^{T_A}$ and $W_X^{T_B}$ are optimal EW's.

(c) W_X is decomposable iff $W_X = R \geq 0$.

Proof: Property (a): is clear since P_{A_1,B_1} is positive. Property (b): If W_X fulfills condition (I) then so do $W_X^{T_A}$ and $W_X^{T_B}$. On the other hand, P is NPPT, implying that both $W_X^{T_A}$ and $W_X^{T_B}$ are not positive semidefinite and therefore they are both EW's. It remains to show that they are optimal. Using that $P_{P^{T_A}} = \{|e\rangle |e^\perp\rangle \forall |e\rangle \in \mathbb{C}^2\}$ (see Sec. 7.1.2 and proof of Lemma E.9) we find that $W_X^{T_A}$ vanishes on the set $\{|e\rangle_{A_1} |e^\perp\rangle_{B_1} |\psi\rangle, \forall |e\rangle \in \mathbb{C}^2, |\psi\rangle \in \mathcal{H}_2\}$ (note that these are not only product states). This contains the set $P_{W_X^{T_A}} = \{|e,g\rangle_A |e^\perp, f\rangle_B \quad \forall |e\rangle \in \mathbb{C}^2, \forall |g\rangle \in \mathcal{H}_{A_2} \forall |f\rangle \in \mathcal{H}_{B_2}\}$. Using the fact that $\{|e\rangle |e^\perp\rangle \forall |e\rangle \in \mathbb{C}^2\}$ spans $\mathbb{C}^2 \otimes \mathbb{C}^2$, we have that $P_{W_X^{T_A}}$ spans the whole Hilbert space, $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathcal{H}_2$. Thus, $W_X^{T_A}$ is optimal. Now, using the fact that W is an optimal EW iff W^T is an optimal EW, we also have that $W_X^{T_B}$ is optimal. Property (c): We only have to prove the only if part. Let us assume that W_X is decomposable. Then we can write it as $W_X = R + Q^{T_A}$ (1.19) and therefore $W_X^{T_A} = R^{T_A} + Q$. Using property (b) and the discussion concerning optimality in Sec. 7.1.2 we find that $Q = 0$, which proves the statement.■

Note, that Property (a) tells us that, since we only have to consider NPPT states, W_ρ is no EW iff it does not fulfill (I). With that we are now in the position to prove the results of the previous section.

Proof of Theorem 8.1: Using Corollary H.1 (Appendix H) we have that ρ is 1–distillable iff there exists a separable CPM (Sec. 4.1.5) $\mathcal{E} : \mathcal{B}(\mathcal{H}_2) \to$

$\mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ such that $0 > \mathrm{tr}_1(P_1^{T_B}\mathcal{E}(\rho))$. Using Eq. (4.15) we can write this inequality as $0 > \mathrm{tr}_1[P_1^{T_B}\mathrm{tr}_2(\rho_2^T E_{1,2})] = \mathrm{tr}_{1,2}[P_1^{T_B} \otimes \rho_2^T E_{1,2}]$. Taking now the partial transpose with respect to B_1, B_2 within the trace we have $0 > \mathrm{tr}_{1,2}[P_1 \otimes \rho_2^{T_A} E_{1,2}^{T_B}] = \mathrm{tr}(W_\rho E_{1,2}^{T_B})$. Thus, we have that ρ is 1–distillable iff W_ρ 'detects' the state E^{T_B}. Now, since $\mathcal{E}$ is separable iff E is separable [Sec. 4.1.5 (p1)], we have that the inequality above is true iff W_ρ is no EW (since it detects E^{T_B} which is separable).■

Note that this proof implies the following fact. Given a distillable state, ρ, we determine the separable state, E^{T_B}, which is 'detected' by W_ρ. Then the state E corresponds to the CPM, $\mathcal{E}$, (Sec. 4.1.5) which fulfills the property that $\mathcal{E}(\rho)$ is a two qubit entangled state. Thus, we found the LOCC, which distills the state, ρ.

Proof of Theorem 8.2 The proof is basically the same as the one of Theorem 8.1, but now with $\mathcal{E}$ a PPT-preserving CPM, which implies that E is PPT. Then W, which must be an EW (Theorem 8.1), detects a PPTES and is therefore (Lemma 7.26) a NDEW.■

Using the same arguments as before, if we determine the PPTES, E^{T_B}, which is detected by the NDEW, W_ρ, then we know which PPTES activates the entanglement of ρ, namely E.

Proof of Corollary 8.1 W_ρ must be either no EW, a NDEW or a DEW. It is no EW iff ρ is 1–distillable. It is a NDEW iff ρ is 1–activatable. Therefore ρ is neither 1–distillable nor 1–activatable iff W_ρ is a DEW.

8.2.2 Three parties

Let us now generalize the results obtain in the previous section for the bipartite case to the case where we consider more parties. Here we will show how to do it for three, but one can generalize the methods introduced in the previous section to any number of particles.

Let us now denote by X an arbitrary positive semidefinite operator acting on $\mathcal{H}_2 = \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2} \otimes \mathcal{H}_{C_2}$. We define

$$W_X^a = P_{B_1,C_1} \otimes X_{A_2,B_2,C_2}^{T_{C_2}} \tag{8.7}$$

$$W_X^b = P_{A_1,C_1} \otimes X_{A_2,B_2,C_2}^{T_{A_2}} \tag{8.8}$$

$$W_X^c = P_{A_1,B_1} \otimes X_{A_2,B_2,C_2}^{T_{B_2}}$$

where $P_{Y,Z} \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is the projector onto the maximally entangled state (8.1), with $d = 2$ for $\{Y, Z\} \in \{A_1, B_1, C_1\}$.

Main results

We will now, analogously to Sec. 8.2.1, characterize the distillation and activation properties of a state, by the operators W_ρ^a, W_ρ^b, and W_ρ^c. For the seek of clarity we state our results only for the BC–distillation and BC–activation. That is we assume that ρ is B–NPPT and C–NPPT (recall that otherwise it is neither possible to distill, nor to activate the entanglement shared between Bob and Charly). All the results presented here can be formulated for the other partitions, AB, AC too, using then the operators W_X^c and W_ρ^b, respectively.

Theorem 8.3 *(Characterization of N–BC–distillable states) A state, ρ, is N–BC–distillable iff $W_{\rho^{\otimes N}}^a$ is no EW [does not fulfill (I)].*

Theorem 8.4 *(Characterization of N–BC–activatable states) A state, ρ, which is N–BC–undistillable, is N–BC–activatable iff $W_{\rho^{\otimes N}}^a$ is a NDEW.*

Those Theorems state that a state is, for instance, 1–fully distillable iff at least two of the operators W_ρ^a, W_ρ^b or W_ρ^c are no EW's. If it is not fully distillable then at least two of the operators W_ρ^a, W_ρ^b or W_ρ^c must be EW's (Theorem 8.3). Then its entanglement can be fully activated via a PPTES iff at least two of the operators W_ρ^a, W_ρ^b or W_ρ^c (the one which are EW's) are NDEW's. Note that, the states which are 'detected' by W_ρ^a are the ones which allow us to derive a distillation protocol. That is, given a 1–BC–distillable state, ρ, the separable state which is 'detected' by W_ρ^a corresponds to a LOCC (Sec. 4.1.5), that distills ρ. If the state is 1–BC–undistillable, but it is 1–BC–activatable, then the PPTES, which activates its entanglement is easily determined by the one which is detected by the NDEW W_ρ^a. On the other hand, we have that a state, ρ, is neither 1–fully distillable nor 1–fully activatable iff at least two of the operators W_ρ^a, W_ρ^b and W_ρ^c are decomposable. This can be, concerning the bipartite entanglement, stated as:

Corollary 8.2 *A state, ρ, is neither N–BC–distillable nor N–BC–activatable iff there exist positive semidefinite operators R, Q such that $\rho^{\otimes N} = R^{T_C} + Q^{T_B}$.*

Note that, as mentioned before a three–partite state is fully distillable (activatable) iff it is (up to permutations) AB–distillable (activatable) and BC–distillable (activatable). Thus, Corollary 8.2 provides a necessary and sufficient condition for a state to be neither N–fully distillable nor N–fully activatable.

In the next section we show that using these theorems we are able to prove in a simple way that there exist three–partite NPPT states which are neither 1–distillable nor 1–activatable. This is in contrast to the bipartite case, where all NPPT states are either 1–distillable or 1–activatable. The methods even allow us to prove that some of those states are not even 2–distillable nor 2–activatable. We show that by proving that all the operators W^a_ρ, W^b_ρ and W^c_ρ are decomposable.

Proofs

We prove the statements above for the case $N = 1$ since all the arguments remain the same for arbitrary N. Again, if a reader is not that interested in the proofs he can skip this part of this chapter and continues reading in the next section.

We start by showing the properties of the operators W^a_X:

(A) W^a_X is not positive semidefinite iff X^{T_C} is not positive semidefinite, i.e. X is C–NPPT.

(B) If W^a_X fulfills condition (I) then $(W^a_X)^{T_B}$ and $(W^a_X)^{T_C}$ are optimal EW's.

(C) W^a_X is decomposable iff there exists $R, Q \geq 0$ such that $X = R^{T_C} + Q^{T_B}$.

Proof: The proofs of property (A) and property (B) are similar to the ones of property (a) property (b) in Sec Sec. 8.2.1 and will be omitted here. Property (C): We denote by $\tilde{Y}$ the total transpose of an operator Y. (if): If $X = R^{T_C} + Q^{T_B}$ then $W^a_X = P_{B_1,C_1} \otimes X^{T_C} = P_{B_1,C_1} \otimes (R + \tilde{Q}^{T_A}) = O + S^{T_A}$, with $O = P_{B_1,C_1} \otimes R \geq 0$ and $S = P_{B_1,C_1} \otimes \tilde{Q} \geq 0$ and so it is decomposable. (only if) If W^a_X is decomposable then there exist operators (1.20) $Q_0, Q_1, Q_2, Q_3 \geq 0$ such that $W^a_X = Q_0 + Q_1^{T_A} + Q_2^{T_B} + Q_3^{T_C}$ and so $(W^a_X)^{T_B} = Q_0^{T_B} + \tilde{Q}_1^{T_C} + Q_2 + \tilde{Q}_3^{T_A}$ and $(W^a_X)^{T_C} = Q_0^{T_C} + \tilde{Q}_1^{T_B} + \tilde{Q}_2^{T_A} + Q_3$. Since $(W^a_X)^{T_B}$ and $(W^a_X)^{T_C}$ are both optimal EW's, because of property (B), we have that $Q_2 = Q_3 = 0$ and so $W^a_X = Q_0 + Q_1^{T_A}$. Let us now use that $P^{T_C}_{BC}$ and $P^{T_B}_{BC}$ are optimal decomposable EW's (see Sec. 7.1.2 and proof of Lemma E.9) and that the sets $P_{P^{T_C}_{BC}} = P_{P^{T_B}_{BC}} = \{|e\rangle \left|e^\perp\right\rangle \forall |e\rangle \in \mathbb{C}^2\}$ span $\mathbb{C}^2 \otimes \mathbb{C}^2$. This implies that $(W^a_X)^{T_C} = Q_0^{T_C} + \tilde{Q}_1^{T_B}$ vanishes on $\{|e\rangle_{B_1} \left|e^\perp\right\rangle_{C_1} |\phi\rangle_{A_2} |\psi\rangle_{B_2} |\chi\rangle_{C_2}, \forall e, \phi, \psi, \chi\}$. Thus, $Q_0^{T_C}$ and $\tilde{Q}_1^{T_B}$ must vanish on those states. This implies that $Q_0^{T_C} = P^{T_C}_{B_1,C_1} \otimes R^{T_C}$, $\tilde{Q}_1^{T_B} = P^{T_C}_{B_1,C_1} \otimes Q^{T_B}$ and so $Q_0 = P_{B_1,C_1} \otimes R$, and $Q_1 = P_{B_1,C_1} \otimes \tilde{Q}$ where $R, Q \geq 0$. Thus, we have that $W^a_X = P_{B_1,C_1} \otimes X^{T_C} = P_{B_1,C_1} \otimes (R + (\tilde{Q})^{T_A})$ and so $X = R^{T_C} + Q^{T_B}$.■

Property (A) implies that, since we only have to consider C–NPPT states, the operator W^a_ρ is not positive semidefinite. Thus, W^a_ρ is no EW iff it does not fulfill (I) [3].

The proofs of the theorems are basically the same as the one in the previous section, but now with $\mathcal{E} \equiv \mathcal{E}_a : \mathcal{B}(\mathcal{H}_2^{\otimes N}) \to \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, where $\mathcal{H}_2 = \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2} \otimes \mathcal{H}_{C_2}$ and the corresponding operator $E_{1,2} \equiv E_{A_2,B_1,B_2,C_1,C_2} \in \mathcal{B}(\mathcal{H}_2^{\otimes N} \otimes \mathbb{C}^2 \otimes \mathbb{C}^2)$.

Proof of Theorem 8.3 Using the same arguments as in the proof of Theorem 8.1 we find $\mathrm{tr}[P^{T_B}_{B_1,C_1} \mathcal{E}_a(\rho)] = \mathrm{tr}[W^a_\rho (E^T_{1,2})^{T_C}]$, where $E_{1,2}$ is the operator corresponding to the CPM $\mathcal{E}_a$. Recall that $\mathcal{E}_a$ is separable iff $(E^T_{1,2})^{T_C}$ is separable. Now, the left hand side of the last equation is negative, for $\mathcal{E}_a$ separable, iff ρ is BC–distillable. And on the other hand, (looking at the right had side of this equation) this is true iff W^a_ρ is no EW, since it 'detects' the separable state $(E^T_{1,2})^{T_C}$.■

Proof of Theorem 8.4 Same Proof as for Theorem 8.3, but now with E a PPTE and $\mathcal{E}$ a PPT–preserving CPM. Using that the operator W^a_ρ must be an EW (8.3), we have that the PPTES, $(E^T)^{T_C}$ is detected by the EW, W^a_ρ, implying that it is a NDEW.■

Proof of Corollary 8.2 Same Proof as for Corollary 8.1, but now W^a_ρ is a DEW iff there exist operators $R, Q \geq 0$ such that $\rho = R^{T_C} + Q^{T_B}$ [property (C)].■

8.3 Applications

In this section we use the formalism introduced in the previous section to show the following facts. On the one hand, the entanglement of one copy of any bipartite NPPT can either be distilled or activated [45]. On the other hand, this formalism allows us to show that this is not the case for multipartite states. That is that there exist states describing a system composed of more than two subsystems which are neither 1–distillable nor 1–activatable. Indeed, in the following subsections we will show that, using the connection between EW's and the distillation and activation properties of a state, there are NPPT states which are not even 2–distillable nor 2–activatable.

[3] Note that W^a_ρ does not fulfill (I) iff $(W^a_\rho)^{T_A} = P_{B_1,C_1} \otimes (\rho^T_{A_2,B_2,C_2})^{T_{B_2}}$ does not fulfill (I). Thus, if W^a_ρ does not fulfill (I) then $(W^a_\rho)^{T_A}$ must be in particular non–positive semidefinite. But this is the case iff ρ^{T_B} is non–positive semidefinite. And so we have, if W^a_ρ does not fulfill (I) then ρ is B–NPPT.

8.3.1 Two parties

Observation 7 *[45] Any bipartite NPPT state, ρ is either 1–distillable or 1–activatable.*

This can be easily seen using Corollary 8.1, which states that ρ is neither 1–distillable nor 1–activatable iff W_ρ is a DEW. Using then property (c) we have that W_ρ is a DEW iff it is a positive semidefinite operator, which is true iff ρ is PPT [property (a)].

8.3.2 Example of a 1–unactivatable three–partite state

In this section we present a family of density operators, $\{\rho_\alpha\}$, which describe the state of a system composed of three qubits. We show, using the formalism of the previous section, that for $\alpha \leq 1$ one copy of these states can neither be distilled nor activated. Then we prove that for $\alpha \leq \alpha_0$, with $\alpha_0 \approx 0.8507$ even two copies of the states can neither be distilled, nor activated. Recall that in the bipartite case there exists no such state. The states of interest are (see also Sec. 7.1.4)

$$\rho_\alpha = \mathbb{1}_8 + \alpha \left|W\right\rangle \left\langle W\right|, \tag{8.9}$$

where $\left|W\right\rangle = \left|001\right\rangle + \left|010\right\rangle + \left|100\right\rangle$. Note first, that ρ_α is NPPT iff $\alpha > \frac{1}{\sqrt{2}}$, which implies that only in this region the state might be distillable or activatable. Note further that ρ_α is symmetric under all the permutations of the three parties, A, B, C. This symmetry implies that this state is N–AB–distillable iff it is N–AC–distillable iff it is N–BC–distillable. Let us therefore, without loos of generality, consider the situation where Alice performs a measurement and Bob and Charly distill out of the remaining density operator a maximally entangled state. That is we are interested in the N–BC–distillation of the state and therefore in the properties of the operator $W^a_{\rho^{\otimes N}}$ Eq.(8.7). Note that, according to our definitions the state is (because of the symmetry) N–BC–distillable iff it is N–distillable. Then the theorems and the corollary of the previous section simplify to

Remark 8.1 *ρ_α is N–distillable iff $W^a_{\rho_\alpha^{\otimes N}}$ is no EW.*

Remark 8.2 *If ρ_α is N–undistillable it is N–activatable iff $W^a_{\rho_\alpha^{\otimes N}}$ is a NDEW.*

Remark 8.3 *ρ_α is neither N–distillable nor N–activatable iff there exist positive semidefinite operators R_α, Q_α such that $(\rho_\alpha^{\otimes N})^{T_C} = R_\alpha + Q_\alpha^{T_A}$.*

One copy

We show that one copy of the state, ρ_α cannot be distilled for $\alpha \leq 1$, i.e (Remark 8.1) $W^a_{\rho_\alpha}$ is an EW for $\frac{1}{\sqrt{2}} < \alpha \leq 1$. Note that the remaining state, after Alice performs a measurement is a state of two qubits, which is distillable iff it is NPPT (Sec. 8.1). And so we only have to find the measurement in A, $\left|\psi\right\rangle \left\langle\psi\right|$, which maximizes the region of α, for which the state $\left\langle\psi\right| \rho_\alpha \left|\psi\right\rangle$ is NPPT. It can be easily shown that the best measurement Alice can do is to measure $\left|0\right\rangle \left\langle 0\right|$. Then the remaining state, $\left\langle 0\right| \rho_\alpha \left|0\right\rangle$, is NPPT iff $\alpha > 1$, which implies that the state, ρ_α can be distilled, $\forall \alpha > 1$. On the other hand, using Remark 8.1 we have that $W^a_{\rho_\alpha}$ is an EW for $\frac{1}{\sqrt{2}} < \alpha \leq 1$. Now we show that $W^a_{\rho_\alpha}$ is for $\frac{1}{\sqrt{2}} < \alpha \leq 1$ a DEW and therefore ρ cannot be activated for $\alpha \leq 1$ (Remark 8.2). Using Remark 8.3 we have to find $R_\alpha, Q_\alpha \geq$ such that $\rho_\alpha^{T_C} = R_\alpha + Q_\alpha^{T_A}$. It can be easily verified that the operators $R_\alpha = \alpha \left|\Psi^+\right\rangle \left\langle\Psi^+\right|_{A,B} \otimes \left|0\right\rangle \left\langle 0\right|_C$, where $\left|\Psi^+\right\rangle = \left|01\right\rangle + \left|10\right\rangle$, and $Q_\alpha = \rho_\alpha^{T_B} - (R_\alpha)^{T_A}$ are both positive semidefinite and lead to the desired decomposition. Thus, we have shown that the NPPT state, ρ_α, is neither 1–distillable nor 1–activatable $\forall \alpha \in]\frac{1}{\sqrt{2}}, 1]$. Note that the given decomposition of ρ_α proves this statement already.

Two copies

Using the same method as above one can also show that two copies of ρ_α can neither be distilled, nor activated if $\alpha \in]\frac{1}{\sqrt{2}}, \alpha_0]$, with $\alpha_0 \approx 0.8507$. In this case $R_\alpha = y(\rho^{T_C}_{1/\sqrt{2}} \otimes R_1 + R_1 \otimes \rho^{T_C}_{1/\sqrt{2}})$, with $R_1 = \left|\Psi^+\right\rangle \left\langle\Psi^+\right|_{A,B} \otimes \left|0\right\rangle \left\langle 0\right|_C$, where $\left|\Psi^+\right\rangle = \left|01\right\rangle + \left|10\right\rangle$, and $Q_\alpha = (\rho_\alpha^{\otimes 2})^{T_B} - R_\alpha^{T_A}$ are both positive semidefinite for $y \approx 0.4953$ and fulfill $(\rho_\alpha^{\otimes 2})^{T_C} = R_\alpha + Q_\alpha^{T_A}$.

8.4 Conclusions

We have shown that one can connect the problem of entanglement witnesses to the one of distillation and activation of entanglement. We defined, depending on the state, ρ, and on the number of copies, N, of it an operator which has the following properties: It is an entanglement witness iff ρ is N–undistillable, i.e. those N copies cannot be distilled via LOCC; It is a decomposable entanglement witness iff the state is N–unactivatable; i.e. those N copies cannot be distilled via LOCC, even if we allow for a PPTES in addition. Using those methods we have shown that there exist three–partite NPPT states, which are neither 2–distillable, nor 2–activatable. We showed it by proving that the corresponding operator is a decomposable entanglement witness.

Chapter 9

Conclusions

In this part of the Thesis we have addressed two central questions of Quantum Information Theory – the separability problem and the distillability problem. For density operators acting on a finite dimensional Hilbert space we derived the following results:

We presented necessary and sufficient conditions for separability for low and medium rank density operators describing the state of a system composed of one qubit and a N–level system. We showed that the rank of any PPTES is larger then N. On the other hand, we proved that if a state is invariant under partial transposition with respect to the 2–level system, then it is separable. Furthermore, we analyzed a different method of detecting entanglement, based on entanglement witnesses and positive maps. We showed how one can create out of a given EW an optimal one, where optimal means that there exists no EW which detects more states than the new EW, including all the states which were detected by it. Furthermore we introduced the notion of egde states, which are PPTES lying on the boundary between PPT and NPPT states. We showed that any PPTES can be written as a convex combination of a separable state and an edge state, where the wight of the edge state can always be chosen to be minimal. We also showed that there exists a canonical form of the EWs which are capable of detecting PPTES, i.e. the non–decomposable EWs and proved that any such EW detects a PPTES.

We applied the developed formalisms to the case of symmetric states. There we showed that a state is separable iff it is separable with respect to any bipartite splitting. We showed, using the derived results, that, even in this restricted set of states, PPTES exist. Furthermore we studied N qubit maximally entangled states. We presented those states for $2, 3, 4, 6$ qubits. There is a strong evidence that in all the other cases those states do not exist. As another application of the methods developed, we considered three qubit

systems. We presented an example of an egde PPTES and a full rank PPTES and showed how one can analytically prove that they are indeed entangled.

On the other hand, we showed that the problem of distillation and activation can be related to EWs. For the bipartite case we constructed an operator $W_{\rho^{\otimes N}}$, which depends on the state ρ and the number of copies of it, N. We showed that this operator is an EW iff ρ is N–undistillable; it is a decomposable entanglement witness iff the state is N–unactivatable. Using the properties of this operator, in particular the fact that if it is positive on all product vectors [see condition (I) in Sec. 8.1, for any EW] then its partial transposes are optimal, it is easy to derive the following results: (a) Any NPPT bipartite state is either 1–distillable or 1–activatable [45] (b) Generalizing the formalism to the multipartite case, one can show that there exist three–partite NPPT states, which are neither 2–distillable, nor 2–activatable. We showed it by proving that the corresponding operator is a decomposable entanglement witness.

In the case of continuous variable systems we presented complete solutions to the separability problem of bipartite Gaussian states. We obtained a necessary and sufficient condition for Gaussian states to be separable, that provides an operational criterion in that it can be easily checked by direct computation. Our criterion is based on a non–linear map and is independent of and more powerful than partial transposition. This represents a significant step in understanding the separability problem and may be helpful for other situations. Note that the problem of distillation has also been solved for this case [55]. In particular, it has been shown that a $n \times m$ Gaussian state is distillable if and only if it has non-positive partial transpose. Thus for Gaussian states we can draw a simple, complete sketch of the convex set of CMs, cf. Fig. 9.1 (c): The distillable states are distinguished from the undistillable ones by the NPPT property and the PPT entangled states can be distinguished from the separable states by the criterion Theorem 7.10.

On the other hand, we investigated the nonlocal properties of Gaussian states of three tripartite modes. We distinguished five classes with different separability properties and gave a simple necessary and sufficient criterion that allows to determine to which of these classes a given Gaussian state belongs to. Using the bipartite separability criterion, which allows to distinguish PPT entangled states from separable states is the main result concerning the tripartite case. Using the bipartite separability criterion (Theorem 7.10) those results can be generalized to the $1 \times 1 \times N$ case.

It is worth pointing out that the separability criteria as well as the distillation criterion can be checked experimentally. The CM γ can be measured, and thus the criteria presented here are entirely formulated in terms of quantities that are measurable with current technology.

Figure 9.1: Bipartite system: (a) Separable and entangled states; (b) Distillable and undistillable states; (c) Gaussian States. The dashed lines represent the open questions to be answered by separability/distillability criteria. NPPT undistillable states were conjectured in Ref. [38, 30].

Chapter 10

Notation and abbreviations

$\oplus$	direct sum (of vector spaces, matrices, vectors, ...)
$\otimes$	tensor product (of Hilbert spaces, operators, vectors, ...)
$\mathcal{H}_X$	Hilbert space of system X
$\mathcal{B}(\mathcal{H})$	Hilbert space of linear operators acting on the finite dimensional Hilbert space $\mathcal{H}$
$\|j\rangle, j = 0, 1, 2, \ldots$	computational basis
$M_{n,m}(K)$	$n \times m$ matrices with elements in K
ρ	density operator of a state
$\rho_X = \mathrm{tr}_Y(\rho_{XY})$	reduced density operator
X^T	transposition of the operator X in the computational basis
X^{T_Y}	partial transposition with respect to system Y, of the operator X in the computational basis
$\left\|\Psi^{\perp}\right\rangle$, or $\left\|\hat{\Psi}\right\rangle$	state which is orthogonal to $\|\Psi\rangle$
$\|\Psi^*\rangle$	the complex conjugate of $\|\Psi\rangle$ in the computational basis
$\sigma_x, \sigma_y, \sigma_z$	the Pauli operators
$\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$	

CPM	completely positive map
EW	entanglement witness
DEW	decomposable entanglement witness
NDEW	non–decomposable entanglement witness
LOCC	local operations and classical communication
PM	positive map
PPT	positive partial transposed state, i.e. a positive semidefinite state whose partial transpose is positive semidefinite
PPTES	positive partial transposed entangled state
NPPT	non–positive semidefinite partial transposed state, i.e. a states whose partial transpose is not positive semidefinite

Danksagung

Es ist mir eine grosse Freude, mich an dieser Stelle bei den Menschen zu bedanken, die während der letzten drei Jahre so hilfreich an meiner Seite gestanden sind.

Herrn Univ. Prof. Dr. Juan Ignacio Cirac danke ich für die interessante Themenstellung und die Betreuung während meiner Dissertation. Die langen, lehrreichen Diskussionen, seine Unterstützung und seine Geduld trugen sehr dazu bei, dass ich meine Begeisterung und Freude an der Physik auch in schwierigen Situationen nie verlor.

Ich möchte mich auch bei Herrn Univ. Prof. Dr. Maciej Lewenstein, Herrn Dr. Géza Giedke und Herrn Dr. Wolfgang Dür bedanken. Die Zusammenarbeit mit ihnen hat mir sehr geholfen und mich vieles gelehrt.

Besonders möchte ich mich bei meinen Eltern bedanken. Ihre moralische und finanzielle Unterstützung ermöglichte es mir, mein Studium durchzuführen. Meiner Mutter möchte ich ganz besonders für ihren liebevollen und unermüdlichen Beistand, den ich während meiner ganzen Ausbildung genoss, danken. Bei meinen Geschwistern möchte ich mich für ihre Hilfe und die vielen netten und unterhaltsamen Stunden bedanken. Ganz besonders möchte ich meinem Freund für seine Unterstützung und Geduld danken. Er hat es immer wieder geschafft mich auch in schwierigen Zeiten zum Lachen zu bringen und hat mir zu verstehen gegeben, dass manche Dinge gar nicht so wichtig sind, wie sie oft zu sein scheinen.

Meinen Freunden und Studienkollengen, Karl Schulze, Gernot Hanel, Armin Würtenberger, Barbara Schallhart, Géza Giedke und Tamara Hösel, möchte ich für die Abwechslung neben dem Studium danken. Ich möchte auch meinen Freunden und Kollegen am Max–Planck–Institut für Quanten Optik, Christian Schön, Klemens Hammerer, Juan José García Ripoll und Belén Paredes, für die vielen lustigen Stunden, die netten Unterhaltungen, ihre Hilfe und Unterstützung danken.

Curriculum Vitae

name:	Barbara Kraus
born:	26. 12. 1975 in Innsbruck, Austria
1994–1998	studied physics at the University of Innbruck
1998–1999	Master thesis "Separability and Entanglement" at the Institute of Theoretical Physics, University of Innbruck
1999	began PhD. studies in physics at the Institute of Theoretical Physics, University of Innbruck
Dec. 2001	PhD-student at the Max–Planck–Institute for Quantum Optics, Garching, Germany

Chapter 11

List of publications

Refereed paper

1. B. Kraus, M. Lewenstein, and J. I. Cirac, *Characterization of Distillable and Activatable States using Entanglement Witnesses*, Phys. Rev. A, **65**, p. 042327, 2002. (quant-ph/0110174)

2. G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, *Entanglement Criteria for All Bipartite Gaussian States*, Phys. Rev. Lett. **87**, p. 167904, 2001 (quant-ph/0104050).

3. G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, *Separability Properties of Three-mode Gaussian States*, Phys. Rev. A, **64**, p. 052303, 2001 (quant-ph/0103137).

4. B. Kraus and J. I. Cirac, *Optimal Creation of Entanglement Using a Two-qubit Gate*, Phys. Rev. A, **63**, p. 062309, 2001 (quant-ph/0011050).

5. J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, *Entangling Operations and Their Implementation Using a Small Amount of Entanglement*, Phys. Rev. Lett, **86**, p 544, 2001 (quant-ph/0007057).

6. M. Lewenstein, D. Bruss, J. I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, and R. Tarrach, *Separability and Distillability in Composite Quantum Systems -a Primer-*, J. Mod. Opt. **47**, p. 2481, 2000 (quant-ph/0006064).

7. M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac, *Characterization of Separable States and Entanglement Witnesses*, Phys. Rev. A, **63**, p. 044304, 2001 (quant-ph/0005112).

8. M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, *Optimization of Entanglement Witnesses*, Phys. Rev. A, **62**, p. 052310, 2000 (quant-ph/0005014).

9. B. Kraus, J.I. Cirac, S. Karnas, and M. Lewenstein, *Separability in $2 \times N$ Composite Quantum Systems*, Phys. Rev. A, **61**, p. 062302, 2000 (quant-ph/9912010) .

Preprints

- B. Kraus, K. Hammerer, G. Giedke, and J. I. Cirac, *Entanglement Generation and Hamiltonian Simulation in Continuous-Variable Systems*, quant-ph/0210136

Proceedings

1. D. Bruss, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera, *Reflections upon Separability and Distillability*, J. Mod. Opt. **49**, p. 1399, 2002 (quant-ph/0110081).

2. B. Kraus, G. Giedke, M. Lewenstein, and J. I. Cirac, *Entanglement Properties of Gaussian States* to appear in Fort. Phys.

3. B. Kraus, W. Dür, G. Vidal, J. I. Cirac, M. Lewenstein, N. Linden, and S. Popescu, *Entanglement Capability of Two–qubit Operations*, Z. Naturforsch. **56a**, p. 91, 2001.

4. G. Giedke, B. Kraus, L.-M. Duan, P. Zoller, M. Lewenstein, and J. I. Cirac, *Separability and Distillability of Gaussian states – the Complete Story*, Fort. Phys. **49**, p. 973, 2001

Master Thesis

B. Kraus, *Separability and Entanglement*, Master Thesis, University of Innsbruck, Austria, 1999

Research visits, conference contributions and invited talks

- B. Kraus, S. Karnas, M. Lewenstein, J. I. Cirac, *Separability in $2 \times N$ composite quantum systems* (poster), conference "Complexity, Computation and the Physics of Information", Cambridge, U.K, July 1999
- B. Kraus, *Separability of Composite $\mathbb{C}^2 \otimes \mathbb{C}^N$ Systems* talk at SFB meeting, Vienna, Austria, December 1999
- invited research visit at University of Hannover, Germany, February 2000
- B. Kraus, *Entangling operations and their implementation using a small amount of entanglement* talk at Workshop on Quantum Information, Benasque Center for Science, Spain, July 2000
- B. Kraus, *Optimal creation of entanglement using a two–qubit gate*, talk at the conference: "Quantum Measurement and Information", Vienna, Austria, December 2000
- B. Kraus, *Entanglement Capability of Two–Qubit Operations* talk at A3 meeting, Hannover, Germany, February 2001
- invited research visit at the University of Hannover, Germany, February 2001
- B. Kraus, G. Giedke, M. Lewenstein, J. I. Cirac, *Separability Properties of Three-mode Gaussian States* (poster), ESF QIT Programme Conference - "Quantum Information: Theory, Experiments and Perspectives", Gdansk, Poland, July 2001
- B. Kraus, G. Giedke, M. Lewenstein, J. I. Cirac, *Separability Properties of Three-mode Gaussian States* (poster), Euresco conference: "Quantum Optics", San Feliu de Guixols, Spain, October 2001
- invited research visit at the California Institute of Technology, talk: *Separable, Distillable, and Activatable States*, March 2002
- B. Kraus, M. Lewenstein, J. I. Cirac, *Separable, Distillable, and Activatable States* (poster), Euresco conference: "Quantum Information", San Feliu de Guixols, Spain, March 2002

- B. Kraus, *Separable, Distillable, and Activatable States*, talk at Ludwig-Maximilians-University Munich, Institute of Theoretical Physics, May 2002

- B. Kraus, *Entanglement Properties of Multi–partite States*, invited talk at the conference "Quantum Information: Conceptual Foundations, Developments and Perspectives", Oviedo, Spain, July 2002

Appendix A

Properties of matrices

Positive semi-definite operators

A matrix A is positive semi-definite iff $\langle \Psi \mid A \mid \Psi \rangle \geq 0 \; \forall \mid \Psi \rangle$, which implies that all eigenvalues of A are nonnegative. Note that in general it is not true that an operator which has positive eigenvalues is positive, as long as it is not hermitian.

Range, kernel, rank

- The *range* of a matrix A is defined as $R(A) = \{|\psi\rangle \in \mathcal{H} : \exists \mid \phi\rangle \in \mathcal{H} \text{ such that } \mid \psi\rangle = A \mid \phi\rangle\}$
- The *kernel* of a matrix A is defined as $K(A) = \{|\phi\rangle \in \mathcal{H} \text{ such that } A|\phi\rangle = 0\}$.
- The *rank* of a matrix A is the number of eigenvalues which are different than zero.

Note that the direct sum of the range and the kernel of an operator span the whole Hilbert space, that is $R(A) \oplus K(A) = \mathcal{H}$. And so $r(A) + \dim(K(A)) = \dim(\mathcal{H})$.

Symplectic matrices

The real symplectic group of $2n$ dimensions is defined as

$$Sp(2n, \mathbb{R}) = \{S \text{real } 2n \times 2n \text{ matrix such that } SJS^T = J\}, \qquad \text{(A.1)}$$

where J is given in (1.27). The physical importance of this group is due to the fact that it contains all linear transformations of the operators R_k,

with $R = (X_1, P_1 \ldots X_n, P_n)$. In other words, whenever the observables R_k are linearly transformed into new operators, R'_k, i.e. $R'_k = S_{kl}R_l$, then, since the new observables also have to obey the commutation relations ($[R'_k, R'_l] = iJ_{kl}$), the matrix S must be symplectic. Due to the fact that this linear transformation $R'_k = S_{kl}R_l$ can always be written as $R'_k = U(S)^\dagger R_k U(S)$ (Stone–von Neumann theorem [85]), where $U(S)$ is a unitary operator acting on $L^2(\mathbb{R}^n)$, any such transformation can be implemented unitarily. On the other hand, the symplectic transformations contain those physical operations on CV states that can currently be routinely realized in the lab. They comprise all unitary operations generated by a Hamiltonian which is quadratic in the canonical operators X_k, P_k, i.e., in quantum optical terms, beam splitter, phase shifter, and squeezer.

Symplectic diagonalization

Any symmetric $n \times n$ matrix $M > 0$ with n even can be symplectically diagonalized. This means that there exist symplectic matrix S and a positive diagonal matrix D such that $M = S^T D S$. The diagonal elements of D are called the symplectic eigenvalues . They occur in pairs of the form (λ, λ^{-1}) [3].

Appendix B

Two–qubit gates

B.1 Periodicity and symmetry

In this section we investigate the periodicity and symmetry of the maximal amount of entanglement created by a two–qubit gate. Let us start out by proving the periodicity of the entanglement created by U_d [Eq. (4.17)]. We define d,(d') as a matrix whose diagonal elements are $\alpha_x, \alpha_y, \alpha_z$ ($\alpha_x + \pi/2, \alpha_y, \alpha_z$) respectively. It is simple to verify that $U_d = -iS_x U_{d'}$, where $S_x = \sigma_x \otimes \sigma_x$. Since S_x is a tensor product of two local unitary operators the entanglement created by U_d is the same as the one created by $U_{d'}$. The same argumentation holds for α_y and α_z and therefore the amount of entanglement created by U_d is $\pi/2$ periodic in α_x, α_y and α_z.

To prove the symmetry around $\pi/4$ in $\alpha_x, \alpha_y, \alpha_z$ of the maximal amount of entanglement we use the following definition; d, (d') is a matrix whose diagonal elements are $\pi/4 + \alpha_x, \alpha_y, \alpha_z$ ($\pi/4 - \alpha_x, \alpha_y, \alpha_z$). It is straightforward to show that $U_d = -i\sigma_x^A U^*_{d'} \sigma_x^B$, where $U^*_{d'}$ denotes the complex conjugate of $U_{d'}$ in the standard basis. And so we have that $E(U_d|\Psi\rangle) = E(U^*_{d'}\sigma_x^B|\Psi\rangle)$, where we used that local unitary operators do not change the entanglement. Now, we use that for any measure of entanglement, E, $E(|\Psi\rangle) = E(|\Psi^*\rangle)$. This is obvious, since all the measures are determined by the Schmidt coefficients and they are real. Thus, we have that $E(U_d|\Psi\rangle) = E[U_{d'}(\sigma_x^B|\Psi\rangle)^*]$. It is clear that the maximal amount of entanglement created by U_d is the same as the one created by $U_{d'}$. Again the same argumentation holds for the other angles, which proves the statement.

B.2 Creation of maximally entangled states

We are going to prove here that there exists a normalized product state $|\phi\rangle|\psi\rangle$ such that $|\Phi\rangle = U_d|\phi\rangle|\psi\rangle$ is a maximally entangled state iff $\alpha_x + \alpha_y \geq \pi/4$ and $\alpha_y + \alpha_z \leq \pi/4$.

According to our discussions in Sec. 1.1.2 [(i),(ii)] and Sec. 4.2.2, this is equivalent to fulfilling the conditions (c1) and (c2), where $\mu_k^2 = |\mu_k|^2 e^{-i\gamma}$. Multiplying condition (c2) by $e^{-i(\gamma+2\lambda_3)}$, we obtain

$$|\mu_3|^2 + |\mu_1|^2 e^{i\alpha_2} + |\mu_2|^2 e^{i\alpha_3} + |\mu_4|^2 e^{i\alpha_1} = 0, \tag{B.1}$$

where we have defined $\alpha_1 = 4(\alpha_x + \alpha_y)$, $\alpha_2 = 4(\alpha_x + \alpha_z)$ and $\alpha_3 = 4(\alpha_y + \alpha_z)$. Note that since $\pi/4 \geq \alpha_x \geq \alpha_y \geq \alpha_z \geq 0$, we have that $2\pi \geq \alpha_1 \geq \alpha_2 \geq \alpha_3 \geq 0$.

Let us distinguish the following two cases now:

- $\alpha_1 < \pi$ (or $\alpha_3 > \pi$). In this case all the imaginary parts appearing in Eq. (B.1) are positive (negative) and therefore the sum can never vanish.

- $\alpha_1 \geq \pi$ and $\alpha_3 \leq \pi$. Here the imaginary part of $|\mu_4|^2 e^{i\alpha_1}$ is negative, whereas the one of $|\mu_2|^2 e^{i\alpha_3}$ is positive and therefore it is always possible to find a solution to Eq. (B.1). In particular we can choose $\mu_1 = 0$. Then writing the real and imaginary part of Eq. (B.1) and the normalization condition (c1) we simply have to solve:

$$\sin(\alpha_3)|\mu_2|^2 + \sin(\alpha_1)|\mu_4|^2 = 0 \tag{B.2}$$
$$|\mu_3|^2 + \cos(\alpha_3)|\mu_2|^2 + \cos(\alpha_1)|\mu_4|^2 = 0 \tag{B.3}$$
$$|\mu_2|^2 + |\mu_3|^2 + |\mu_4|^2 = 1. \tag{B.4}$$

Note that since we have found the solution for the μ_k's, it is easy to determine the input state by using the formula $w_k = \mu_k e^{i\lambda_k}$.

B.3 Best input state for Example 2 of Sec. 4.2.3

Here we prove that the input state which leads to the most entangled output state can be written as

$$|\phi\rangle = c_a|00\rangle + s_a|11\rangle \tag{B.5a}$$
$$|\psi\rangle = s_b|00\rangle + c_b|11\rangle, \tag{B.5b}$$

where $s_a^2 + c_a^2 = s_b^2 + c_b^2 = 1$. We will use that $[\sigma_{\vec{n}}^A \otimes \sigma_{\vec{n}}^B, U_d] = 0$, where $\sigma_{\vec{n}} = \vec{\sigma}\cdot\vec{n}$. This can be easily verified using the commutation relations of the Pauli operators.

Let us now recall that the input state in system AA' can be written as $|\phi\rangle = c_a|\phi_0\rangle_A|0\rangle_{A'} + s_a|\phi_0^\perp\rangle_A|1\rangle_{A'}$, where $c_a^2 + s_a^2 = 1$. It is clear that there exists a vector $\vec{n}$ such that $\sigma_{\vec{n}}|\phi_0\rangle = |\phi_0\rangle$ and $\sigma_{\vec{n}}|\phi_0^\perp\rangle = -|\phi_0^\perp\rangle$. Note that $|\phi\rangle$ is invariant under $\sigma_{\vec{n}}^A \otimes \sigma_z^{A'}$, i.e.

$$\sigma_{\vec{n}}^A \otimes \sigma_z^{A'}|\phi\rangle = |\phi\rangle. \tag{B.6}$$

Using the fact that U_d commutes with $\sigma_{\vec{n}}^A \otimes \sigma_{\vec{n}}^B$ and with local operators acting on the auxiliary systems together with Eq.(B.6) we have that, $\sigma_{\vec{n}}^A \otimes \sigma_z^{A'} \otimes \sigma_{\vec{n}}^B \otimes V_{B'}U_d|\phi\rangle|\psi\rangle = U_d|\phi\rangle\sigma_{\vec{n}}^B \otimes V_{B'}|\psi\rangle$, for any unitary operator $V_{B'}$.

Let us now introduce a new auxiliary system which we denote by C. Then, using property (1.12) of any measure of entanglement, E, we have that

$$E(U_{AB}|\phi\rangle_{AA'}\left|\tilde{\psi}\right\rangle_{BB'C}) \geq E(U_{AB}|\phi\rangle_{AA'}|\psi\rangle_{BB'}), \tag{B.7}$$

where

$$\left|\tilde{\psi}\right\rangle_{BB'C} = 1/\sqrt{2}(|\psi\rangle_{BB'}|0\rangle_C + \sigma_{\vec{n}}^B \otimes V_{B'}|\psi\rangle_{BB'}|1\rangle_C). \tag{B.8}$$

Now choosing $V_{B'} = \sigma_z^{B'}$ and requiring that $\sigma_{\vec{n}}^B \otimes V_{B'}|\psi\rangle_{BB'} = |\psi\rangle_{BB'}$, which implies that $|\psi\rangle = s_b|\phi_0 0\rangle + c_b|\phi_0^\perp 1\rangle$, we get that $E(U_{AB}|\phi\rangle_{AA'}|\psi\rangle_{BB'}) \geq E(U_{AB}\left|\tilde{\phi}\right\rangle_{AA'}\left|\tilde{\psi}\right\rangle_{BB'})$, $\forall\left|\tilde{\phi}\right\rangle, \left|\tilde{\psi}\right\rangle$, where both, $|\phi\rangle$and $|\psi\rangle$ are invariant under the operation $\sigma_{\vec{n}} \otimes \sigma_z$. Using the same argumentation as before, we can apply the local operator $\sigma_{\vec{n'}} \otimes \sigma_{\vec{n'}}$, where $\vec{n'}$ is defined as $\sigma_{\vec{n'}}|\phi_0\rangle = |0\rangle$ and $\sigma_{\vec{n'}}|\phi_0^\perp\rangle = -|1\rangle$. Combining all that we have that

$$E(U_{AB}|\phi\rangle|\psi\rangle) \leq E\{U_{AB}[(c_a|00\rangle + s_a|11\rangle)(s_b|00\rangle + c_b|11\rangle)]\}, \tag{B.9}$$

$\forall\,|\phi\rangle, |\psi\rangle$.

Appendix C

Interaction simulation (infinite dimensional Hilbert space)

C.1 Hamiltonian simulation

In this section we derive the necessary and sufficient condition for Hamiltonian simulation. First we prove necessity. If H can simulate H' efficiently (5.6) has to hold for $\kappa = 1$ and $H_{\text{eff}} = H'$. Therefore and because of (5.7) and (5.9) there must exist a probability distribution $\{p_i\}_{i=1}^n$ and special orthogonal matrices $\{R_i, S_i\}_{i=1}^n$ such that

$$\begin{pmatrix} s_1' & 0 \\ 0 & s_2' \end{pmatrix} = \sum_{i=1}^n p_i R_i \begin{pmatrix} s_1 & 0 \\ 0 & s_2 \end{pmatrix} S_i. \tag{C.1}$$

Rotation matrices which should in principle appear on the left hand side can be removed by left and right multiplication with corresponding transposed matrices. In (C.1) we assume these ones to be already included in the R_i, S_i on the right hand side.

By using the fact that the vector of the diagonal elements of a product R $\text{diag}(s_1, s_2)$ S can be written as $(R \circ S^T)(s_1, s_2)^T$ where $R \circ S^T$ denotes the component-wise (so-called Hadamard) product of matrices we can express the last equation in compact form as

$$\begin{pmatrix} s_1' \\ s_2' \end{pmatrix} = \sum_{i=1}^n p_i \left(R_i \circ S_i^T\right) \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} =: N \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}. \tag{C.2}$$

The definition of the matrix N in (C.2) is obvious. Using that all matrices

R_i, S_i are elements of $SO(2, \mathbb{R})$ it can be seen easily that

$$N_{11} = N_{22}, \quad N_{12} = N_{21} \quad \text{and}$$
$$|N_{11} \pm N_{21}| \leq 1.$$

Conditions (5.12) follow now directly from (C.2) and these properties of N:

$$s_1' + s_2' = (N_{11} + N_{21})(s_1 + s_2) \leq s_1 + s_2$$

The same holds identically for all plus signs replaced by minus signs proving necessity.

To demonstrate sufficiency we show that conditions (5.12) guarantee the existence of a matrix N as in (C.2) which in turn admits to connect the primed and unprimed restricted singular values as in (C.1). This provides an efficient simulation protocol of the form (5.5).

Given s_1, s_2 and s_1', s_2' fulfilling (5.12) we can for the time being assume that $s_1 \neq |s_2|$ and define

$$N := \begin{pmatrix} e & f \\ f & e \end{pmatrix}, \text{ where}$$
$$e = \frac{s_1 s_1' - s_2 s_2'}{s_1^2 - s_2^2}, \quad f = \frac{s_1 s_2' - s_2 s_1'}{s_1^2 - s_2^2}.$$

With this definition we have $(s_1', s_2')^T = N(s_1, s_2)^T$. Next we have to show that N can be written as a convex sum of Hadamard products of rotation matrices which is in fact exactly what inequalities (5.12) ensure.

It is again easy to check that if $|e| + |f| \leq 1$ we can find probabilities $\{p_i : p_i \geq 0, \sum_{i=1}^4 p_i\}_{i=1}^4$ such that $e = p_1 - p_2$ and $f = p_3 - p_4$ and therefore

$$\begin{aligned} N = p_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p_2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \circ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ + p_3 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + p_4 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \end{aligned} \tag{C.3}$$

This decomposition of N allows to pass from (C.2) to (C.1) conserving the diagonal structure as can be checked easily. Thus it suffices to show how (5.12) implies $|e| + |f| \leq 1$. Multiplying the first [second] line of (5.12) by $(s_1 - s_2)$ $[(s_1 + s_2)]$ yields respectively

$$s_1^2 - s_2^2 \geq (s_1 s_1' - s_2 s_2') + (s_1 s_2' - s_2 s_1'),$$
$$s_1^2 - s_2^2 \geq (s_1 s_1' - s_2 s_2') - (s_1 s_2' - s_2 s_1').$$

The first term on the right hand sides is nonnegative due to premise (5.11) such that these inequalities are equivalent to

$$s_1^2 - s_2^2 \geq |s_1 s_1' - s_2 s_2'| + |s_1 s_2' - s_2 s_1'|$$

which is, regarding the definition of e and f, exactly what we had to show and proves sufficiency for the case $s_1 \neq |s_2|$.

The complementary cases $s_1 = |s_2|$ turn out to be trivial, since conditions (5.12) then require $s_1' = s_2' = s_1$ or $s_1' = -s_2' = s_1$ respectively and this means that we can exclusively simulate Hamiltonians where $H' =.(U \otimes V)\, H\, \left(U^\dagger \otimes V^\dagger\right)$ for some local rotations $U \otimes V$, i.e. H' has to be - in this sense - locally equivalent to H. Hence, nothing has to be shown in this case. □

We point out that this proof provides the possibility to construct simulation protocols explicitly. Given H and H' one has to calculate the decomposition in C.3. Then the probabilities and rotations appearing there will fix the time steps t_i and control operations $U_i \otimes V_i$ in (5.5). As can be seen such a protocol will contain at most three intervals of interaction and control operations being rotations about $\pm\pi/2$ and π.

C.2 Gate simulation

To show that any unitary $U = \exp(-iG)$ where G is a quadratic expression in the operators X_k, P_k can be decomposed as given in (5.19) we will proceed in three steps:

(i) As shown in Ref. [134, 16] any such U can be decomposed into a sequence of one passive transformation, single mode squeezing and another passive transformation. That is to say the symplectic matrix S corresponding to the unitary transformation U can be decomposed as $S = O\tilde{D}\tilde{O}$ where $O, \tilde{O}$ are orthogonal, symplectic and, therefore, passive transformations and the diagonal matrix $D = \mathrm{diag}(e^{\alpha+\beta}, e^{-(\alpha+\beta)}, e^{\alpha-\beta}, e^{-(\alpha-\beta)})$ amounts to local squeezing. Note that this is basically a singular value decomposition of S.

(ii) Passive transformations contain essentially beam-splitter transformations and local rotations and it is well known from quantum optics that any such transformation on two modes can be decomposed into a sequence of a pair of local rotations, one beam-splitter operation and another pair of local rotations. Thus, a unitary U_O corresponding to a orthogonal symplectic transformation O can be decomposed as $U_O = (V \otimes W) U_{\mathrm{bs}}(t_0) (\tilde{V} \otimes \tilde{W})$ where $U_{\mathrm{bs}}(t)$ is defined in (5.16).

(iii) What is left to show is how to attain single mode squeezing. For this we split the matrix D into two components, $D =$

$\mathrm{diag}(e^{\alpha}, e^{-\alpha}, e^{\alpha}, e^{-\alpha})\mathrm{diag}(e^{\beta}, e^{-\beta}, e^{-\beta}, e^{\beta})$ and show how each of them can be attained by means of beam-splitters and two-mode squeezing. Let us denote by $\overline{U}_{\mathrm{bs}}(t)$ and $\overline{U}_{\mathrm{tms}}(t)$ the variants of beam splitter and two-mode squeezing operators which are attained from (5.16) and (5.17) respectively by locally rotating $X_2 \to P_2, P_2 \to -X_2$. Then it can be easily shown that the sequence $\overline{U}_{\mathrm{bs}}(-\pi/4) U_{\mathrm{tms}}(\alpha) \overline{U}_{\mathrm{bs}}(\pi/4)$ generates a symplectic transformation $\mathrm{diag}(e^{\alpha}, e^{-\alpha}, e^{\alpha}, e^{-\alpha})$ and $U_{\mathrm{bs}}(-\pi/4) \overline{U}_{\mathrm{tms}}(\beta) U_{\mathrm{bs}}(\pi/4)$ correspondingly $\mathrm{diag}(e^{\beta}, e^{-\beta}, e^{-\beta}, e^{\beta})$.

Collecting things together and ordering all passive components as in (ii), i.e. such that it contains only one application of a beam-splitter operation, decomposition (5.19) follows immediately.

Appendix D

Solving polynomial equations

D.1 Reduction of one polynomial

In this appendix we show that given a generic polynomial $P_{X,Y}(\alpha, \alpha^*)$ of degree X and Y in α and α^* respectively, there are at most $2^{X-1}[X+Y(Y-X+1)]$ roots, where without loss of generality we have assumed $Y \geq X$. The idea is to find another polynomial $Q(\alpha)$ of degree $2^{X-1}[X+Y(Y-X+1)]$ such that all the roots of P are also roots of Q. Since Q has at most $2^{X-1}[X+Y(Y-X+1)]$ roots, this will prove our statement.

We start by writing the equation $P=0$ as

$$0 = P_{X,Y}(\alpha, \alpha^*) = \sum_{k=0}^{X} \alpha^k P_Y^k(\alpha^*) \quad \text{(D.1a)}$$

$$= \sum_{k=0}^{Y} (\alpha^*)^k Q_X^k(\alpha), \quad \text{(D.1b)}$$

where P_Y^k and Q_X^k denote polynomials of degree Y and X, respectively. We complex conjugate the last line in this equation and obtain

$$0 = \sum_{k=0}^{Y} \alpha^k \bar{Q}_X^k(\alpha^*), \quad \text{(D.2)}$$

where $\bar{Q}$ is the same polynomial as Q but with the coefficients complex conjugated. From now on we treat α and $\beta \equiv \alpha^*$ as two independent variables.

Thus, we can write Eqs. (D.1a) and (D.2) as

$$\sum_{k=0}^{X} \alpha^k P_Y^k(\beta) = 0 \quad \text{(D.3a)}$$

$$\sum_{k=0}^{Y} \alpha^k \bar{Q}_X^k(\beta) = 0. \quad \text{(D.3b)}$$

We proceed now in two steps:

(1) If $Y \neq X$ we use Eq. (D.3a) to transform Eq. (D.3b) to one of the form

$$\sum_{k=0}^{X} \alpha^k R_Z^k(\beta) = 0, \quad \text{(D.4)}$$

where $Z = X + Y(Y-X)$. This can be done in the following way. First we multiply Eq. (D.3a) by $\alpha^{Y-X}\bar{Q}_X^Y(\beta)$, Eq. (D.3b) by $P_Y^X(\beta)$, and subtract them. In this way we obtain a polynomial equation of degree $Y-1$ in α and $Y+X$ in β. We use again Eq. (D.3a) to transform this one to a polynomial equation of degree $Y-2$ in α. We proceed in the same way until we reach Eq. (D.4). Note that if $Y=X$ then we have automatically Eq. (D.4) with $Z=X$.

(2) First, we multiply Eq. (D.3a) by $R_Z^X(\beta)$, Eq. (D.4) by $P_Y^X(\beta)$ and subtract them. In parallel, we multiply Eq. (D.3a) by $R_Z^0(\beta)$, Eq. (D.4) by $P_Y^0(\beta)$, subtract them, and divide by α the result. In this way, we obtain two polynomial equations of degree $X-1$ in α and $Y+Z$ in β. We can do the same thing with these two, and proceed in the same vein until we reach a polynomial equation of the form $\bar{Q}(\beta)=0$ (i.e. $Q(\alpha)=0$) of degree $2^{(X-1)}(Z+Y)$. All the roots of the original polynomial must be roots of Q.

D.2 Reduction of two polynomials

Following a similar procedure as in the previous appendix, we show here that given two generic polynomials $P_{X,Y}$ and $\tilde{P}_{X,Y}$ of degree X and Y in α and α^* respectively, there are at most $2^X Y$ common roots, where without loss of generality we have assumed $Y \geq X$. Treating α and $\beta \equiv \alpha^*$ as independent

variables, if we write

$$0 = P_{X,Y}(\alpha, \alpha^*) = \sum_{k=0}^{X} \alpha^k P_Y^k(\beta), \tag{D.5a}$$

$$0 = \tilde{P}_{X,Y}(\alpha, \alpha^*) = \sum_{k=0}^{X} \alpha^k \tilde{P}_Y^k(\beta), \tag{D.5b}$$

$$\tag{D.5c}$$

we can use the same procedure presented in step (2) in the previous appendix to obtain a polynomial equation $Q(\alpha)$ of degree $2^X Y$.

We emphasize that if one has more polynomials, one can further decrease the degree of $Q(\alpha)$. An example is shown in Sec. 7.1.1, for the $\mathbb{C}^2 \otimes \mathbb{C}^4$ case, when the ranks of ρ and ρ^{T_A} equal 5.

Appendix E

Optimization of entanglement witnesses and PPTES

E.1 Optimality of entanglement witnesses

In this appendix we study necessary and sufficient conditions for an EW to be optimal. According to Theorem 7.4 of Sec. 7.1.2 we have that an EW, W, is optimal iff no positive operator can be subtracted from W while keeping property (i): $\langle e, f | W | e, f \rangle \geq 0 \forall |e\rangle \in \mathcal{H}_A, |f\rangle \in \mathcal{H}_B$. This condition can be reexpressed in terms of the infimum of some scalar products in Lemma 7.16. This infimum is, in general, difficult to calculate (at least analytically). In this section we will give a different method to determine whether an EW is optimal or not. This method will turn out to be very simple for the case in which $\dim(\mathcal{H}_A) = 2$. The idea is to find the conditions such that a given operator $P \geq 0$ can/cannot be subtracted from an EW. This will give us automatically a criterion to determine when W is optimal.

In all this appendix we will use that given an EW, W, and an operator $P \geq 0$ we say that P cannot be subtracted from W if for all $\lambda > 0$, $W - \lambda P$ does not fulfill (i). In other words, there exist $|e(\lambda)\rangle \in H_A$ and $|f(\lambda)\rangle \in H_B$ such that

$$\langle e(\lambda), f(\lambda) | (W - \lambda P) | e(\lambda), f(\lambda) \rangle < 0. \tag{E.1}$$

Note that $\langle e(\lambda), f(\lambda) | P | e(\lambda), f(\lambda) \rangle$ must be strictly positive, so that (E.1) can be expressed as

$$\lim_{\lambda \to 0} \frac{\langle e(\lambda), f(\lambda) | W | e(\lambda), f(\lambda) \rangle}{\langle e(\lambda), f(\lambda) | P | e(\lambda), f(\lambda) \rangle} = 0. \tag{E.2}$$

In the first subsection we will introduce some definitions and notation. In the second one we give a method to determine the set of product vectors

P_W, on which W vanishes. In the third subsection we find a necessary and sufficient condition under which an operator cannot be subtracted from an EW. We will see that there must exist a vector $|e_0, f_0\rangle \in P_W$, some other vectors $|e_1\rangle$ and $|f_1\rangle$, and certain phases $\phi_{e,f}$ and θ such that some quantity is zero. In the next subsection we will see that the problem can be reduced to finding only the vectors $|e_{0,1}\rangle$ and $|f_{0,1}\rangle$. Finally, we will show that if $\dim(H_A) = 2$ we just have to find $|e_0\rangle$ and $|f_0\rangle$, which is very simple.

E.1.1 Definitions and notation

In order to prove the results of this appendix in a compact and readable form we have made an extensive numbers of definitions.

We will always denote by $|e_0, f_0\rangle$ a product vector in P_W, and by $|e_1\rangle \in H_A$ and $|f_1\rangle \in H_B$ two vectors orthogonal to $|e_0\rangle$ and $|f_0\rangle$, respectively. We will use the following notation:

$$W_{i,j}^{k,l} = \langle e_i, f_j|W|e_k, f_l\rangle, \quad (i,j,k,l = 0,1). \tag{E.3}$$

and we will write

$$W_{1,0}^{0,1} = |W_{1,0}^{0,1}|e^{i\phi_0} \tag{E.4a}$$
$$W_{0,0}^{1,1} = |W_{0,0}^{1,1}|e^{i\phi_1}. \tag{E.4b}$$

We will also define the following operators:

$$w_{i,j}^{e} \equiv \langle e_i|W|e_j\rangle, \tag{E.5a}$$
$$w_{i,j}^{f} \equiv \langle f_i|W|f_j\rangle. \tag{E.5b}$$

The following vectors will be used in the context of Eq. (E.2):

$$|e(\epsilon)\rangle = \frac{1}{\sqrt{1+|\cos(\theta)\epsilon|^2}}(|e_0\rangle + \epsilon\cos(\theta)e^{i\phi_e}|e_1\rangle), \tag{E.6a}$$
$$|f(\epsilon)\rangle = \frac{1}{\sqrt{1+|\sin(\theta)\epsilon|^2}}(|f_0\rangle + \epsilon\sin(\theta)e^{i\phi_f}|f_1\rangle), \tag{E.6b}$$

where ϵ is a real number, and $\phi_{e,f} \in [0,\pi)$ and $\theta \in [0,\pi/2]$ are certain constants. Given a product vector $|e(\epsilon), f(\epsilon)\rangle$ and an operator, W, we will expand $\langle e(\epsilon), f(\epsilon)|W|e(\epsilon), f(\epsilon)\rangle$ by collecting terms with the same powers in ϵ; that is, except for a normalization constant,

$$\langle e(\epsilon), f(\epsilon)|W|e(\epsilon), f(\epsilon)\rangle \propto \sum_{i=1}^{4}\epsilon^i A_i(W), \tag{E.7}$$

where

$$A_0(W) = W_{0,0}^{0,0}, \tag{E.8a}$$
$$A_1(W) = 2\mathrm{Re}\left[\cos(\theta)e^{i\phi_e}W_{0,0}^{1,0} + \sin(\theta)e^{i\phi_f}W_{0,0}^{0,1}\right], \tag{E.8b}$$
$$A_2(W) = \cos^2(\theta)W_{1,0}^{1,0} + \sin^2(\theta)W_{0,1}^{0,1} + 2\sin(\theta)\cos(\theta) \times\mathrm{Re}\left[e^{-i(\phi_e-\phi_f)}W_{1,0}^{0,1} + e^{i(\phi_e+\phi_f)}W_{0,0}^{1,1}\right], \tag{E.8c}$$
$$A_3(W) = 2\sin(\theta)\cos(\theta) \times\mathrm{Re}\left[\cos(\theta)e^{i\phi_f}W_{1,0}^{1,1} + \sin(\theta)e^{i\phi_e}W_{0,1}^{1,1}\right], \tag{E.8d}$$
$$A_4(W) = \sin^2(\theta)\cos^2(\theta)W_{1,1}^{1,1}. \tag{E.8e}$$

On the other hand, we will define

$$|\Psi_{0,1}\rangle \equiv \sin(\theta)e^{i\phi_f}|e_0, f_1\rangle + \cos(\theta)e^{i\phi_e}|e_1, f_0\rangle. \tag{E.9}$$

Finally, the following quantity will play an important role in determining whether there exist vectors and parameters for which (E.2):

$$X(W) \equiv W_{1,0}^{1,0}W_{0,1}^{0,1} - (|W_{1,0}^{0,1}| + |W_{0,0}^{1,1}|)^2. \tag{E.10}$$

E.1.2 Determining P_W

As stated in Lemma 7.15, not every positive operator P can be subtracted from an EW, W; it must vanish on P_W. Thus, in order to choose P one has to know the set P_W. In this subsection we give a method to determine it.

We start by characterizing the vectors in P_W:

Lemma E.1 *Given an operator W satisfying (i), then $|e_0, f_0\rangle \in P_W$ iff*

$$\langle e_0|W|e_0\rangle|f_0\rangle = 0, \tag{E.11a}$$
$$\langle f_0|W|f_0\rangle|e_0\rangle = 0, \tag{E.11b}$$

Proof: (If) We just apply $\langle f_0|$ to Eq. (E.11a). (Only if) Since W fulfills (i) then $W_{e_0} \equiv \langle e_0|W|e_0\rangle$ must be positive. Thus, $\langle f_0|W_{e_0}|f_0\rangle = 0$ implies Eq. (E.11a). In the same way we obtain Eq. (E.11b).■

In practice, for a given W the set P_W can be found as follows. Due to the fact that W is an EW we have that for any $|e\rangle \in H_A$, $W_e \equiv \langle e|W|e\rangle$ must be a positive operator (i.e. $\langle f|W_e|f\rangle \geq 0$ for all $|f\rangle \in H_B$). Thus, the determinant $\det(W_e) \geq 0$. According to Lemma E.1, this determinant is zero iff there exists some $|f_0\rangle \in H_B$ such that $\langle f_0|W_{e_0}|f_0\rangle = 0$, i.e., if

$|e_0, f_0\rangle \in P_W$. That is, the determinant as a function of $|e\rangle$ has a minimum (which is zero) at $|e_0\rangle$. We can use this fact to find $|e_0\rangle$. Then, we can easily obtain $|f_0\rangle$ via Eq. (E.11a). We can expand an unnormalized state $|e\rangle$ in an orthonormal basis $\{|k\rangle\}$ as

$$|e\rangle = \sum_{k=1}^{\dim(H_A)} c_k |k\rangle, \tag{E.12}$$

and impose that the corresponding determinant is zero. This gives us a polynomial equation for the coefficients c_k, i.e.

$$P(c_k, c_k^*) = 0. \tag{E.13}$$

We also impose that, given the fact that the determinant is a minimum,

$$\frac{\partial}{\partial c_k} P(c_k, c_k^*) = \frac{\partial}{\partial c_k^*} P(c_k, c_k^*) = 0, \tag{E.14}$$

which also give a set of polynomial equations. These equations can be solved using the method explained in Appendix D.

E.1.3 Necessary and sufficient conditions for subtracting an operator

In this subsection we give a necessary and sufficient condition for an operator P to be subtractable from an EW. We start out by giving some properties of the coefficients $A(W)$ defined above (E.8).

Lemma E.2 *Given W satisfying (i) and $|e_0, f_0\rangle \in P_W$, then for all $|e_1\rangle \in H_A$ and $|f_1\rangle \in H_B$ we have*

(i) $A_0(W) = A_1(W) = 0$.

(ii) $A_2(W) \geq 0$.

(iii) *If $A_2(W) = 0$ then $A_3(W) = 0$.*

Proof: (i) It is a direct consequence from Lemma E.1. In order to prove (ii–iii) we use the fact that W satisfies (i). We define $|e(\epsilon)\rangle$ and $|f(\epsilon)\rangle$ as in (E.6). We impose that $\langle e(\epsilon), f(\epsilon)|W|e(\epsilon), f(\epsilon)\rangle \geq 0$. Using the expansion (E.7) and taking into account (i), we have $A(\epsilon) \equiv A_2(W) + \epsilon A_3(W) + \epsilon^2 A_4(W) \geq 0$ for all ϵ. This automatically implies (ii), since otherwise for

sufficiently small ϵ we would have $A(\epsilon) < 0$. It also implies (iii), since if $A_3(W) < 0$ ($A_3(W) > 0$) then for sufficiently small $\epsilon > 0$ ($\epsilon < 0$) we would have $A(\epsilon) < 0$.■

Now, we are in the position of giving a necessary and sufficient condition under which an operator cannot be subtracted from an EW:

Lemma E.3 *Given P fulfilling $PP_W = 0$, it cannot be subtracted from W iff there exists $|e_0, f_0\rangle \in P_W$, $|e_1\rangle \perp |e_0\rangle$, $|f_1\rangle \perp |f_0\rangle$, $\phi_{e,f}$, and θ such that $A_2(W) = 0$ but $A_2(P) \neq 0$.*

Proof: If) We define $|e(\lambda)\rangle$ and $|f(\lambda)\rangle$ as in (E.6). Using Lemma E.2(i) we have $A_0(W) = A_0(P) = A_1(W) = A_1(P) = 0$. Using Lemma E.2(iii) we have that $A_3(W) = 0$. Thus, we can write the limit (E.2) as

$$\lim_{\lambda \to 0} \frac{\lambda^2 A_4(W)}{A_2(P) + \lambda A_3(P) + \lambda^2 A_4(P)} \tag{E.15}$$

which obviously tends to zero given that $A_2(P) \neq 0$. (Only if) There exist two normalized vectors $|\tilde{e}(\lambda)\rangle$ and $|\tilde{f}(\lambda)\rangle$ (continuous functions of λ) fulfilling (E.2). Taking the limit $\lambda \to 0$ in this expression we have that $\langle \tilde{e}(0), \tilde{f}(0)|W|\tilde{e}(0), \tilde{f}(0)\rangle = 0$, and therefore $|e_0, f_0\rangle \equiv |\tilde{e}(0), \tilde{f}(0)\rangle \in P_W$. This means that we can always choose $|\tilde{e}(\lambda)\rangle = |e[\epsilon(\lambda)]\rangle$ and $|\tilde{f}(\lambda)\rangle = |f[\epsilon(\lambda)]\rangle$ given in (E.6), where $|e_1\rangle \perp |e_0\rangle$ and $|f_1\rangle \perp |f_0\rangle$ are two normalized vectors, $\lim_{\lambda \to 0} \epsilon(\lambda) = 0$, and $\langle e(\epsilon), f(\epsilon)|P|e(\epsilon), f(\epsilon)\rangle \neq 0$. We use (E.6) to expand the numerator and denominator of (E.2) as in (E.7). According to Lemma E.2(i) we have that $A_0(W) = A_0(P) = A_1(W) = A_1(P) = 0$. Thus, we must have

$$\lim_{\epsilon \to 0} \frac{A_2(W) + \epsilon A_3(W) + \epsilon^2 A_4(W)}{A_2(P) + \epsilon A_3(P) + \epsilon^2 A_4(P)} = 0. \tag{E.16}$$

This implies $A_2(W) = 0$ and $A_2(P) \neq 0$. Note that if both $A_2(W) = A_2(P) = 0$ then, according to Lemma E.2(iii) we have that $A_3(W) = A_3(P) = 0$, so that (E.15) would require $A_4(W)/A_4(P) = 0$. But this cannot be since $A_4(W) = 0$ would imply that $|e(\epsilon), f(\epsilon)\rangle \in P_W$, and therefore $\langle e(\epsilon), f(\epsilon|P|e(\epsilon), f(\epsilon)\rangle = 0$.■

Finally, we show in the next lemma that condition $A_2(P) = 0$ is equivalent to having certain vector in the kernel of P. We will use the vector $|\Psi_{0,1}\rangle$ defined in (E.9).

Lemma E.4 *Given a positive operator P and a set of vectors $|e_0, f_0\rangle \in K(P)$, $|e_1\rangle \perp |e_0\rangle$ $|f_1\rangle \perp |f_0\rangle$, and parameters $\phi_{e,f}$, and θ then $A_2(P) = 0$ iff $|\Psi_{0,1}\rangle \in K(P)$.*

Proof: Since $P \geq 0$ and $|e_0, f_0\rangle \in K(P)$ we have $P^{0,0}_{1,1} = 0$. Then, we can write $A_2(P) = \langle \Psi_{0,1}|P|\Psi_{0,1}\rangle$, with $|\Psi\rangle$ defined in (E.9), from which it is obvious that $A_2(P) = 0$ iff $|\Psi_{0,1}\rangle \in K(P)$.■

E.1.4 Necessary and sufficient conditions for $A_2(W) = 0$

The previous lemmas tell us that we cannot subtract a given operator P provided we can find some vectors and parameters such that $A_2(W) = 0$. The task of finding these vectors is difficult, in general. Here we will give a way to check whether these vectors exist. As before, we will denote by $|e_0, f_0\rangle$ a vector in P_W, and by $|e_1\rangle$ and $|f_1\rangle$ two vectors orthogonal to the first two. The quantity $X(W)$ defined in (E.10) will play an important role in determining whether there exist vectors and parameters for which $A_2(W) = 0$. In this subsection, we will always have to choose the phases $\phi_{e,f}$ that minimize $A_2(W)$. That is

$$e^{-i(\phi_e - \phi_f - \phi_0)} = -1, \quad e^{i(\phi_e + \phi_f + \phi_1)} = -1. \tag{E.17}$$

We will denote $\tilde{A}_2(W)$ the value of $A_2(W)$ for this particular choice of phases. We have

$$\begin{aligned} \tilde{A}_2(W) &= \cos^2(\theta) W^{1,0}_{1,0} + \sin^2(\theta) W^{0,1}_{0,1} \\ &\quad -2\sin(\theta)\cos(\theta)\sqrt{W^{1,0}_{1,0} W^{0,1}_{0,1} - X(W)}, \end{aligned} \tag{E.18}$$

where we have used (E.10).

Let us start showing that $X(W)$ is positive. We will use this property later on to reexpress the condition $A_2(W) = 0$ in terms of one that is simpler to check.

Lemma E.5 $X(W) \geq 0$.

Proof: This follows from the fact that $A_2(W) \geq 0$ for all values of $\phi_{e,f}$. In particular, $\tilde{A}_2(W) \geq 0$, which according to (E.18) implies $X(W) \geq 0$.■

The next lemma shows that we just have to check whether $X(W) = 0$ if we want to see if there exist parameters $\phi_{e,f}$ and θ such that $A_2(W) = 0$. This first condition is therefore much more useful than the last one.

Lemma E.6 $X(W) = 0$ *iff there exist* $\phi^0_{e,f}$ *and* θ^0 *such that* $A_2(W) = 0$.

Proof: (If) Given the phase $\theta = \theta^0$ we have that $0 = A_2(W) \geq \tilde{A}_2(W)$. Thus, $\tilde{A}_2(W) = 0$. According to (E.18) we can have two cases: (a) $\theta \neq 0, \pi/2$. In that case it is obvious that $X(W) = 0$. (b) $\theta = 0, \pi/2$. In the first (second) case we must have $W^{1,0}_{1,0} = 0$ ($W^{0,1}_{0,1} = 0$). But this implies that $W^{1,1}_{0,0} = W^{1,0}_{0,1} = 0$ since otherwise we could always find some other value of θ such that $\tilde{A}_2(W) < 0$. Then, $X(W) = 0$. (Only if) We choose $\phi_{e,f}$ as in (E.17). For this value, according to (E.18) we have

$$\tilde{A}_2(W) = \left[\cos(\theta)\sqrt{W^{1,0}_{1,0}} - \sin(\theta)\sqrt{W^{0,1}_{0,1}}\right]^2, \tag{E.19}$$

which can always be zero for some particular value of θ.■

Note that according to the proof of Lemma E.6, if $W^{1,0}_{1,0} = 0$ then $A_2(W) = 0$ only for $\theta = 0$. But in that case one can easily check that the vector $|e(\lambda), f(\lambda)\rangle \in P_W$ [see (E.6)] which cannot be. Similarly, we conclude that $W^{1,0}_{1,0} \neq 0$ if we want $A_2(W) = 0$. Thus, from now one we will assume that both $W^{1,0}_{1,0}$ and $W^{1,0}_{1,0}$ are not zero.

E.1.5 Optimality test

Thus, we can now state the steps to check whether an EW, W, can be optimized or not. (1) For each $|e_0, f_0\rangle \in P_W$ we must check whether there exist $|e_1\rangle \perp |e_0\rangle$ and $|f_1\rangle \perp |f_0\rangle$ such that $X(W) = 0$. Let us denote by $|e^{(i)}_{0,1}\rangle$ and $|f^{(i)}_{0,1}\rangle$ the set of vectors fulfilling that. (2) For each of these vectors, we have to find the corresponding values of $\phi^{(i)}_{e,f}$ by using (E.17) and of $\theta^{(i)}$ by imposing that $\tilde{A}_2(W) = 0$ in (E.19). (3) Construct $|\Psi^{(i)}\rangle$ according to (E.9). (4) See whether the space spanned by P_W and $\{|\Psi^{(i)}\rangle\}$ is equal to $H_A \otimes H_B$. If it is, then W is optimal. If it is not, we can always find some $|\psi\rangle$ orthogonal to that subspace that can be subtracted from W.

E.1.6 Necessary and sufficient conditions for $X(W) = 0$

The hard part of the procedure outlined before to see whether and EW is optimal is the step (1), namely to find $|e_1\rangle$ and $|f_1\rangle$ such that $X(W) = 0$. We start out by giving a necessary and sufficient condition for $X(W) = 0$.

Lemma E.7 *Given* $|e_0, f_0\rangle \in P_W$, *and* $|e_1\rangle \perp |e_0\rangle$ *and* $|f_1\rangle \perp |f_0\rangle$, *then* $X(W) = 0$ *iff*

$$w^e_{0,0}|f_1\rangle = -\sqrt{\frac{W^{0,1}_{0,1}}{W^{1,0}_{1,0}}}e^{-i\phi_f}(e^{-i\phi_e}w^e_{1,0} + e^{i\phi_e}w^e_{0,1})|f_0\rangle, \tag{E.20a}$$

$$w^f_{0,0}|e_1\rangle = -\sqrt{\frac{W^{0,1}_{0,1}}{W^{1,0}_{1,0}}}e^{-i\phi_e}(e^{-i\phi_f}w^f_{1,0} + e^{i\phi_f}w^f_{0,1})|e_0\rangle, \tag{E.20b}$$

where $\phi_{e,f}$ *are given in (E.17).*

Proof: (If) We multiply by $\langle f_1|$ Eq. (E.20a) and take the square of the absolute value of the result. We obtain

$$\begin{aligned} W^{1,0}_{1,0}W^{0,1}_{0,1} &= |e^{-i(\phi_e+\phi_f)}W^{0,0}_{1,1} + e^{i(\phi_e-\phi_f)}W^{1,0}_{0,1}|^2 \\ &\leq (|W^{1,1}_{0,0}| + |W^{0,1}_{1,0}|)^2. \end{aligned} \tag{E.21}$$

Using Lemma E.5 we conclude that $X(W) = 0$. (Only if) Since $X(W) = 0$ and according to Lemma E.5 $X(W) \geq 0$, then $X(W)$ must be a minimum with respect to $|e_1\rangle$ and $|f_1\rangle$. Taking the derivatives of $X(W)$ with respect to these two vectors and imposing that they vanish, one obtains (E.20).■

Equations (E.20) are particularly useful if the dimension of one of the Hilbert spaces is 2. Without loss of generality, let us assume that $\dim(H_A) = 2$. In that case we can choose $|e_1\rangle$ as the one that is orthogonal to $|e_0\rangle$ (with an arbitrary choice of the global phase). The determination of ϕ_e can be done as follows. Using (E.20) we write

$$\sqrt{\frac{W^{1,0}_{1,0}}{W^{0,1}_{0,1}}}e^{i\phi_f}|f_1\rangle = -\frac{1}{w^e_{0,0}}(e^{-i\phi_e}w^e_{1,0} + e^{i\phi_e}w^e_{0,1})|f_0\rangle \tag{E.22}$$

where $1/w^e_{0,0}$ denotes the pseudo–inverse (see footnote [2] on p. 123). We can use this expression to impose

$$W^{0,1}_{1,0}e^{-i(\phi_e-\phi_f)}, W^{1,1}_{0,0}e^{i(\phi_e+\phi_f)} < 0, \tag{E.23}$$

i.e. they are negative real numbers. We obtain that

$$e^{-i2\phi_e}\langle f_0|w^e_{1,0}\frac{1}{w^e_{0,0}}w^e_{1,0}|f_0\rangle < 0, \tag{E.24}$$

so that we determine ϕ_e. With these results, we can prove the following necessary and sufficient condition for $X(W) = 0$ when $\dim(H_A) = 2$.

Lemma E.8 *If* $\dim(H_A) = 2$, *given* $|e_0, f_0\rangle \in P_W$, *then there exists* $|e_1, f_1\rangle$ *such that* $X(W) = 0$ *iff*

$$\begin{aligned} &\langle f_0|\left[w^e_{1,1} - w^e_{0,1}\frac{1}{w^e_{0,0}}w^e_{1,0} - w^e_{1,0}\frac{1}{w^e_{0,0}}w^e_{0,1}\right]|f_0\rangle = \\ &2\left|\langle f_0|w^e_{0,1}\frac{1}{w^e_{0,0}}w^e_{0,1}|f_0\rangle\right|. \end{aligned} \tag{E.25}$$

Proof: (If) We define

$$|f_1\rangle = -\frac{1}{w^e_{0,0}}(e^{-i\phi_e}w^e_{1,0} + e^{i\phi_e}w^e_{0,1})|f_0\rangle \tag{E.26}$$

where ϕ_e is determined by the condition (E.24). Using this expression to calculate $X(W)$ one finds that indeed $X(W) = 0$. (Only if) Using Lemma E.7 we can write $|f_1\rangle$ as in (E.22) so that the phases $\phi_{e,f}$ ensure that (E.23) is fulfilled. Substituting $|f_1\rangle$ in the equation $X(W) = 0$ one finds (E.25).■

In summary, for a given $|e_0, f_0\rangle \in P_W$, in order to find whether there exist $|e_1, f_1\rangle$ such that $X(W) = 0$ we just have to check the condition (E.25). If it is fulfilled, we can easily find $|f_1\rangle$ and the phases $\phi_{e,f}$ using (E.23) and (E.22).

E.2 Example of an optimal entanglement witness

We introduce here an example of an optimal decomposable 2–partite EW in $\mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. We denote by $P_{AB} \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ the projector onto the maximally entangled state, that is

$$P_{AB} = |\Phi_2\rangle\langle\Phi_2|, \tag{E.27}$$

with $|\Phi_2\rangle$ given in (8.1). Then we have

Lemma E.9 $P^{T_A}_{AB}$ *is an optimal DEW.*

Proof: Using Corollary 7.9 it is sufficient to show that $P_{P^{T_A}_{AB}}$ spans $\mathbb{C}^2 \otimes \mathbb{C}^2$. It can be easily verified that $P_{P^{T_A}_{AB}} = \{|e, e^\perp\rangle \forall |e\rangle \in \mathbb{C}^2\}$. On the other hand, on can easily check that there exists no state orthogonal to this set, which implies that $P_{P^{T_A}_{AB}}$ spans $\mathbb{C}^2 \otimes \mathbb{C}^2$.■

Note that an EW, W, is optimal iff W^T is optimal, implying that $P_{AB}^{T_B}$ is optimal too. Note further that this EW enables us to draw the connection between EW's and the criterion that a state in $\mathbb{C}^2 \otimes \mathbb{C}^2$ is entangled iff it is NPPT [118, 71]:

Lemma E.10 *[72] A state $\rho_{AB} \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is NPPT iff there exist some local operators A, B such that* $\mathrm{tr}(P_{AB}^{T_B} A \otimes B \rho A^\dagger \otimes B^\dagger) < 0$.

E.3 Canonical form of PPTES

The concept of "edge" PPTES seems to play a very special role in the characterization of PPTES. In particular, in view of the criterion given in Lemma 7.22, which is based on the fact that any density operator ρ can be decomposed into a separable part and an "edge" PPTES (7.51) and the fact that one can easily create a nd–EW out of the edge state (Lemma 7.21), which might detect both, the edge state and ρ. Among all the possible decompositions there might be one for which the trace of the separable part is maximal. When it exists, such a decomposition was termed positive partial transpose best separable approximation (PPT BSA) to ρ [79]. It extended the idea of BSA introduced in Refs. [125, 146, 108] to the case of PPTES, which were based on the method of diminishing the range of ρ by subtracting product vectors from its range, while keeping the remainder and, at the same time, its partial transpose, positive (see Sec. 7.1.1, [125, 146, 108, 95, 79]). In this Appendix we formalize the results regarding the existence and properties of the PPT BSA. In particular, the proofs presented in the quoted papers were restricted to the case in which there exist a finite, or at most, countable number of projectors on product vectors that can be subtracted from ρ. We will extend them below to continuous families of product vectors. The Appendix is written in a self-contained way, and can be read independently of Sec. 7.1.2.

We denote by Γ_ρ the set of projectors on product vectors $\{|e_\alpha, f_\alpha\rangle\langle e_\alpha, f_\alpha|\}$ such that $|e_\alpha, f_\alpha\rangle \in R(\rho)$ and $|e_\alpha, f_\alpha^*\rangle \in R(\rho^{T_B})$. In Ref. [79] it was shown that if Γ_ρ is finite then there exist an optimal decomposition (PPT BSA) $\rho = (1-p)\rho_{sep} + p\delta$ where δ is an "edge" PPTES, and p is minimal. Note that PPT BSA involves the state δ which violates the range criterion in a rather special way. It can happen that there is an uncountable family of product vectors depending on continuous parameter that can be used for subtracting projectors. In the following we will show that in such case the above result is valid.

In order to consider the case of continuous families of product vectors we first prove the following:

Lemma E.11 *Let ρ be a PPTES defined on a Hilbert space $\mathcal{H}$, $\dim\mathcal{H} < \infty$. Then the set of product vectors Γ_ρ is compact.*

Proof: Obviously Γ_ρ is a bounded set in finite-dimensional space, so it is enough to show that it is closed. Consider any sequence $|g_n, h_n\rangle \to |\phi\rangle$, $|g_n, h_n\rangle \in R(\rho)$, $|g_n, h_n^*\rangle \in R(\rho^{T_B})$. The limit vector must: (i) respect the condition of orthogonality to $K(\rho)$ [i.e. it must belong to $R(\rho)$], (ii) belong to the sphere (i.e. to the set of all vectors $|\phi\rangle$ with $||\phi|| = 1$), (iii) finally, it must be a product state, because if it was entangled then its distance from the compact set of product pure states [75] defined as $\min_{|e,f\rangle} |||\phi\rangle - |e, f\rangle||$ would be nonzero, which is obviously impossible. We conclude that $|\phi\rangle = |g, h\rangle \in R(\rho)$ for some $|g\rangle, |h\rangle$, which implies (up to irrelevant phase factors) that $|g_n\rangle \to |g\rangle$ and $|h_n\rangle \to |h\rangle$. We have (again up to irrelevant external phase factor) $|g_n, h_n^*\rangle \to |g, h^*\rangle$. The latter must belong to $R(\rho^{T_B})$ as any element of the corresponding sequence is orthogonal to $K(\rho^{T_B})$.■

Let us now prove the following general lemma, which is a generalization of a theorem in Ref. [108]:

Lemma E.12 *Let the PPTES ρ be defined on a finite dimensional Hilbert space. Consider the set Σ_ρ consisting of the trivial zero operator plus all unnormalized states $\tilde{\rho}$ ($\mathrm{tr}\tilde{\rho} \leq 1$) such that $\tilde{\delta} \equiv \rho - \tilde{\rho}$ is positive and has positive partial transpose. Then, one can find $\hat{\rho} \in \Sigma_\rho$ such that with $\mathrm{tr}(\hat{\rho}) \leq 1$ is optimal in the sense that:*

(i) *The trace of $\hat{\delta} \equiv \rho - \hat{\rho}$ is minimal with respect to all separable $\tilde{\rho}$'s leading to positive partial transpose $\tilde{\delta}$'s.*

(ii) *The state $\delta = \hat{\delta}/\mathrm{tr}(\hat{\delta})$ is an "edge" PPTES.*

Proof: To prove the existence of $\hat{\rho} \in \Sigma_\rho$ we just have to show that Σ_ρ is compact. This can be done by showing that Σ_ρ is a closed subset of another compact set, namely $C = \mathrm{conv}\{\Gamma_\rho \cup \mathbf{0}\}$. The latter set C is compact as it is a convex hull of the compact set $\{\Gamma_\rho \cup \mathbf{0}\}$ in a finite dimensional space.

Note first that $\Sigma_\rho \subset C$. Indeed, by virtue of $\tilde{\delta} \geq 0$ any nonzero $\tilde{\rho}$ cannot have any vector in its range not belonging to $R(\rho)$. Analogously $R(\tilde{\rho}^{T_B}) \subset R(\rho^{T_B})$. Hence, according to the properties of the ranges of density operators in general [75], $\tilde{\rho}$ must be a convex combination of vectors from Γ_ρ, and as such it belongs to C. Let us show that Σ_ρ is closed. This follows immediately form the fact that Σ_ρ is a cross-section (performed over any projections P, Q) of the sets: $\Sigma_{\rho,P}^1 \equiv \{\tilde{\rho} : f_{P,\rho}(\tilde{\rho}) \equiv \mathrm{tr}(P\rho - P\tilde{\rho}) \geq 0\}$ and $\Sigma_{\rho,Q}^2 = \{\tilde{\rho} : g_{Q,\rho}(\tilde{\rho}) \equiv \mathrm{tr}(Q^{T_B}\rho - Q^{T_B}\tilde{\rho}) \geq 0\}$. Since the functions $f_{P,\rho}, g_{Q,\rho}$

are continuous, all the sets participating in the cross section are closed. Now, the cross-section of closed sets is again a closed one.

Consider now the statement (ii). Since $\delta, \delta^{T_B} \geq 0$, we always have $\delta = \beta P_{R(\delta)} + A$ and $\delta^{T_B} = \beta' P_{R(\delta^{T_B})} + A'$ with $\beta, \beta' > 0$, some positive operators A, A' (here, P_X denotes a projector onto the subspace $X \subset \mathcal{H}$). Then if, contrary to (ii), there were any $|e, f\rangle \in R(\delta)$ such that $|e, f^*\rangle \in R(\delta^{T_B})$, then the new operator $\hat{\rho}^* = \hat{\rho} + \gamma |e, f\rangle\langle e, f|$, $\gamma = \min[\beta, \beta']$ would fulfill that $\hat{\delta}^* = \rho - \hat{\rho}^*$ is a PPTES, and would contradict optimality with respect to (i).■

Let us remark that if we give up the condition regarding positivity of $\tilde{\delta}^{T_B}$, then we obtain a modified statement (ii) where the state δ has no product vectors in its range. This is nothing but the best separable approximation (BSA) of Ref. [108], extended here rigorously to the states ρ having uncountable set of product vectors in $R(\rho)$.

From the Lemma E.12 we obtain the following characterization of PPTES, which can be regarded to be among the main results of this appendix, since it provides *a canonical form of PPTES*:

Proposition E.1 *If the state ρ is PPTES, then it is a convex combination*

$$\rho = (1 - p)\rho_{sep} + p\delta \tag{E.28}$$

of some normalized separable ρ_{sep} and a normalized "edge" PPTES δ. In the above decomposition the weight p is minimal [i. e. there does not exist a decomposition of type (E.28) with a smaller p].

Appendix F

Interpretation of separability criterion

In this section we show the correctness of the physical interpretation of the separability criterion for bipartite Gaussian states, given in Lemma 7.34. We need the following two lemmas:

Lemma F.1 *[121] Let A be a symmetric $n \times n$ matrix such that $Re(A) \geq 0$. Then for any $z \in C^n$:*

$$\int e^{-\pi x^T A x - 2\pi i z x} dx = \frac{1}{\sqrt{det(A)}} e^{-\pi z^T A^{-1} z} \tag{F.1}$$

Lemma F.2 *Given a matrix*

$$M_X = \begin{pmatrix} X & J \\ -J & X \end{pmatrix} \tag{F.2}$$

, (F.3)

where J is defined in Eq. (7.97) and X is an arbitrary 2×2 matrix, then

$$M_X^{-1} = \begin{pmatrix} Re(Y) & -Im(Y) \\ Im(Y) & Re(Y) \end{pmatrix}, \tag{F.4}$$

where

$$Y = \frac{1}{X - iJ} \tag{F.5}$$

and $Re(Y)$, $Im(Y)$ denote the real and imaginary part of Y.

Proof:

$$\begin{aligned} Re(Y) &= \frac{1}{2}\left(\frac{1}{X-iJ}+\frac{1}{X+iJ}\right) \\ Im(Y) &= \frac{-i}{2}\left(\frac{1}{X-iJ}-\frac{1}{X+iJ}\right) \end{aligned} \tag{F.6}$$

It is easy to verify that

$$\begin{aligned} (M_X^{-1}M_X)_{1,1} = (M_X M_X^{-1})_{1,1} &= XRe(Y)+JIm(Y) = \mathbb{1} \\ (M_X^{-1}M_X)_{1,2} = (M_X M_X^{-1})_{1,2} &= -XIm(Y)+JRe(Y) = 0, \end{aligned} \tag{F.7}$$

where the indices denote the matrix entry in the blockmatrix $M_X M_X^{-1}$. Using the symmetry we have that the matrix (F.4) is the inverse of M_X.■

We are now going to prove that the characteristic function, [Eq. (1.29)] of the operator $\tilde{\rho}_{AA'} = \mathrm{tr}_{BB'}[\rho_{AB}\otimes\rho_{A'B'}Z_{BB'}]$ is proportional to $e^{-1/4x^T\gamma_1 x}$, where γ_1 is the "CM" that we obtain after applying the map M [Eq. (7.107)] to γ.

Let us therefore consider two copies of a Gaussian state, ρ, which have zero displacement and correspond to the correlation matrix:

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}. \tag{F.8}$$

We use the definition of the operator Z, Eq. (7.111) and the notation $x_a^T = (x_A, x_{A'})$ and $x_b^T = (x_B, x_{B'})$, where $x_Y = (q_Y, p_Y) \in \mathbb{R}^2$, for $Y = A, A', B, B'$. Then we find for the characteristic function of $\tilde{\rho}_{AA'}$

$$\begin{aligned} \chi(x_a) &= \int dx_b \mathrm{tr}[\rho_{AB}\otimes\rho_{A'B'}D(x_a,x_b)]e^{\frac{1}{4}(x_{B'}^T J x_B - x_B^T J x_{B'})} \\ &= \int dx_b \chi(x_A,x_B)\chi(x_{A'},x_{B'})e^{\frac{1}{4}(x_{B'}^T J x_B - x_B^T J x_{B'})} \\ &\equiv \int dx_b e^{-\frac{1}{4}G}, \end{aligned} \tag{F.9}$$

where

$$G = \begin{pmatrix} x_A \\ x_B \end{pmatrix}^T \gamma \begin{pmatrix} x_A \\ x_B \end{pmatrix} + \begin{pmatrix} x_{A'} \\ x_{B'} \end{pmatrix}^T \gamma \begin{pmatrix} x_{A'} \\ x_{B'} \end{pmatrix} - x_{B'}^T J x_B + x_B^T J x_{B'}$$

We can write this matrix also as:

$$G = \begin{pmatrix} x_A \\ x_{A'} \\ x_B \\ x_{B'} \end{pmatrix}^T \begin{pmatrix} A & 0 & C & 0 \\ 0 & A & 0 & C \\ C^T & 0 & B & J \\ 0 & C^T & -J & B \end{pmatrix} \begin{pmatrix} x_A \\ x_{A'} \\ x_B \\ x_{B'} \end{pmatrix} = x_a^T M_A x_a + 2x_a^T M_C x_b + x_b^T M_B x_b,$$

where

$$M_A = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}, M_C = \begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}, M_B = \begin{pmatrix} B & J \\ -J & B \end{pmatrix} \tag{F.11}$$

. (F.12)

Thus we have

$$\chi(x_a) = e^{-\frac{1}{4}x_a^T M_A x_a}\int dx_b e^{-\frac{1}{4}[x_b^T M_B x_b + 2x_a^T M_C x_b]}. \tag{F.13}$$

Let us now use the following definition: $M_{B'} = M_B/(4\pi)$ and $z^T = -\frac{i}{4\pi}x_a^T M_C$. Then we have:

$$\chi(x_a) = e^{-\frac{1}{4}x_a^T M_A x_a}\int dx_b e^{-\pi x_b^T M_{B'} x_b - 2i\pi z^T x_b}. \tag{F.14}$$

Note that $M_B \geq 0$. This can be seen using that $M_B \geq 0$ iff $B + iJ \geq 0$ (Lemma 7.33) which must be always fulfilled since B must be a valid CM (Lemma 1.3). Thus, we can use Lemma F.1 and obtain

$$\begin{aligned} \chi(x_a) &= \frac{1}{\sqrt{\det(M_{B'})}}e^{-\frac{1}{4}x_a^T M_A x_a}e^{-\pi z^T (M_{B'})^{-1} z} \\ &= \frac{1}{\sqrt{\det(M_{B'})}}e^{-\frac{1}{4}x_a^T [M_A - M_C \frac{1}{M_B} M_C^T] x_a}. \end{aligned} \tag{F.15}$$

Since $\chi(x_A, x_{A'})$ is the characteristic function of the state $\rho_{AA'} = \mathrm{tr}_{BB'}[\rho_{AB}\otimes\rho_{A'B'}Z_{BB'}]$, its CM is given by $M_A - M_C\frac{1}{M_B}M_C^T$. Using now Lemma F.2 for M_B we have that

$$\chi(x_A, x_{A'}) = \frac{1}{\sqrt{\det(M_{B'})}}e^{-\frac{1}{4}x_a^T \gamma x_a}, \tag{F.16}$$

where

$$\gamma = \begin{pmatrix} A_1 & C_1 \\ C_1^T & B_1 \end{pmatrix} \tag{F.17}$$

with $A_1 = A - CRe(Y)C^T$, $C_1 = CIm(Y)C^T$, and $Y = (B - iJ)^{-1}$.■

Appendix G

Details for 3–mode Gaussian states

This appendix contains some mathematical details concerning the separability properties of three–mode Gaussian states.

G.1 Points of intersection

As shown in Theorem 7.12 a state is separable iff solutions to Ineqs. (7.130) are found among the points of intersection of the curves described by the *equalities* (7.130), or the centers of the three sets. Here we give the formulas to directly calculate these points from γ.

The centers of circle and the ellipses have already been shown to be

$$\begin{aligned} m_c &= (0,0)^T, \\ m_e &= \frac{\det N + 1}{k_1} L, \\ m_{\tilde{e}} &= \frac{\det \tilde{N} + 1}{\tilde{k}_1} \tilde{L}, \end{aligned} \tag{G.1}$$

where $N, \tilde{N}$ were defined in (7.121b), L in (7.128), and $k_1, \tilde{k}_1$ after (7.131). The intersections of the borders of $\mathcal{C}, \mathcal{E}, \tilde{\mathcal{E}}$ are calculated as follows. Consider first the two ellipses, whose borders are defined by the *equalities* (7.130b, 7.130c). Dividing by $\mathrm{tr}N$, respectively by $\mathrm{tr}\tilde{N}$ and subtracting the two equalities we find that a point on both $\partial\mathcal{E}$ and $\partial\tilde{\mathcal{E}}$ must lie on the straight line $\mathcal{G}_{e\tilde{e}}$ defined by

$$(\det N + 1 + L^T\xi)/\mathrm{tr}N = (\det \tilde{N} + 1 + \tilde{L}^T\xi)/\mathrm{tr}\tilde{N}, \tag{G.2}$$

where $\xi = (y, z)$. $\mathcal{G}_{e\tilde{e}}$ can be parameterized with $s \in \mathbb{R}$ as $g_{e\tilde{e}} + s f_{e\tilde{e}}$, where

$$g_{e\tilde{e}} = \left(\frac{\det N + 1}{\mathrm{tr}N} - \frac{\det \tilde{N} + 1}{\mathrm{tr}\tilde{N}} \right) L'/\|L'\|^2, \tag{G.3}$$

where $L' = \tilde{L}/\mathrm{tr}\tilde{N} - L/\mathrm{tr}N$ [1] and $f_{e\tilde{e}}$ is a vector orthogonal to L'.

Inserting $\mathcal{G}_{e\tilde{e}}$ in the equation (7.130b) for $\partial\mathcal{E}$ we obtain a quadratic polynomial in s, whose roots $s^{\pm}_{e\tilde{e}}$ (if they are real) give the intersection points. For the intersections of $\partial\mathcal{C}$ with the ellipses we proceed similarly. In summary, we get for the intersection points

$$i^{\pm}_{e\tilde{e}} = g_{e\tilde{e}} + s^{\pm}_{e\tilde{e}} f_{e\tilde{e}}, \tag{G.4}$$

$$i^{\pm}_{ce} = g_{ce} + s^{\pm}_{ce} f_{ce}, \tag{G.5}$$

$$i^{\pm}_{c\tilde{e}} = g_{c\tilde{e}} + s^{\pm}_{c\tilde{e}} f_{c\tilde{e}}, \tag{G.6}$$

where the vectors $g_x, x = ce, c\tilde{e}$ are

$$g_{ce} = \left(\mathrm{tr}N\sqrt{r_c^2 + 1} - \det N - 1 \right) L/\|L\|^2, \tag{G.7a}$$

f_{ce} is a vector orthogonal to L, and r_c is the smaller of the two radii

$$r_c = \min\left\{ \sqrt{(\mathrm{tr}N)^2/4 - 1}, \sqrt{(\mathrm{tr}\tilde{N})^2/4 - 1} \right\}. \tag{G.8}$$

$g_{c\tilde{e}}, f_{e\tilde{e}}$ are defined likewise for tilded quantities. And, finally, by $s^{\pm}_{e\tilde{e}}, s^{\pm}_x$ we denote the real roots of the quadratic polynomials

$$\begin{aligned} P_{e\tilde{e}}(s) &= \left(L^T(g_{e\tilde{e}} + s f_{e\tilde{e}}) + \det N + 1 \right)^2 - \\ &\quad (\mathrm{tr}N)^2 \left(1 + \|g_{e\tilde{e}} + s f_{e\tilde{e}}\|^2 \right), \qquad \text{(G.9a)} \\ P_x(s) &= r_c^2 - \|g_x + s f_x\|^2, x = ce, c\tilde{e}. \qquad \text{(G.9b)} \end{aligned}$$

Thus all the nine candidates are given in terms of $N, \tilde{N}$ which can be directly obtained from γ.

G.2 Characterization of K

Here we show that $K(\gamma)$ as defined in Eq. (7.134) coincides with the (real) span of the vectors belonging to the kernels of $\gamma + \tilde{J}_x \gamma^{-1} \tilde{J}_x$. This fact automatically follows from the following

[1] In the case $L' = 0$ the borders of the ellipses do either not intersect at all or coincide. In both cases we have to look for solutions among the remaining seven candidates.

Lemma G.1 *(Characterization of $K(\gamma)$)*
Let $f = f_R + if_I$, where f_R and f_I are real. Then $f \in \ker(\gamma - i\tilde{J}_x)$ iff $f_I = \frac{1}{\gamma} J f_R$ and both f_R and f_I belong to the kernel of $\gamma + \tilde{J}_x \gamma^{-1} \tilde{J}_x$.

Proof: Taking the real and imaginary part of the equation $(\gamma - i\tilde{J}_x)f = 0$ we find $\gamma f_R + \tilde{J}_x f_I = 0$ and $\gamma f_I - \tilde{J}_x f_R = 0$. Since γ must be invertible we obtain from the second equation that $f_I = \gamma^{-1}\tilde{J}_x f_R$. Using now the first equation we find that $(\gamma + \tilde{J}_x\gamma^{-1}\tilde{J}_x)f_R = 0$. Analogously, $(\gamma + \tilde{J}_x\gamma^{-1}\tilde{J}_x)f_I = 0$. The same argumentation holds for the other direction of the proof. ∎

Appendix H

Distillation/activation in terms of completely positive maps

In this appendix we show how the notion of CPM's can be used in order to characterize distillable and activatable states. As mentioned in Sec. 4.1.5 we can generalize the isomorphism between CPMs and positive semidefinite operators to CPM's of the form $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\bar{\mathcal{H}})$. The corresponding operator E is then an element of $\mathcal{B}(\mathcal{H} \otimes \bar{\mathcal{H}})$.

Note that the properties (p1–p3) in Sec. 4.1.5 imply the following facts: First, we can implement a separable (Y–PPT-preserving) CPM, $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\bar{\mathcal{H}})$, on a state, ρ, if we allow the parties to apply LOCC on the state $\rho \otimes E$, where $E \in \mathcal{B}(\mathcal{H} \otimes \bar{\mathcal{H}})$ is separable (Y–PPT). Second, the scenario, where the parties are allowed to apply LOCC on the state $\rho \otimes E$, where E is separable (Y–PPT), is equivalent to the one where the parties are allowed to implement a separable (Y–PPT-preserving) CPM.

H.1 Two parties

We consider a bipartite state, ρ, acting on $\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}$. Using Lemma 1.2 and Lemma E.10 we have the following

Corollary H.1 *A state, ρ, is distillable iff there exists a positive integer N and a separable CPM $\mathcal{E} : \mathcal{B}(\mathcal{H}_1^{\otimes N}) \to \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ such that*

$$\mathrm{tr}[P^{T_B}\mathcal{E}(\rho^{\otimes N})] < 0, \tag{H.1}$$

where $P = P_{AB}$, given in (E.27), is the projector onto the maximally entangled state of two qubits. Note that condition (H.1) is equivalent to $\mathrm{tr}[P^{T_A}\mathcal{E}(\rho^{\otimes N})] < 0$. Note further that the operator E corresponding to

the CPM $\mathcal{E}$ is separable and acts an the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A = \mathcal{H}_{A_1}^{\otimes N} \otimes \mathbb{C}^2$ and $\mathcal{H}_B = \mathcal{H}_{B_1}^{\otimes N} \otimes \mathbb{C}^2$.

As mentioned before, the possibility for Alice and Bob to use a PPTES and then apply LOCC equals the possibility for them to use a PPT-preserving CPM. And so we have

Lemma H.1 *A state, ρ, which is m–undistillable, is activatable iff there exists a positive integer $N \leq m$ and a PPT-preserving CPM $\mathcal{E} : \mathcal{B}(\mathcal{H}_1^{\otimes N}) \to \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ such that $\mathrm{tr}[P^{T_B}\mathcal{E}(\rho^{\otimes N})] < 0$, or, equivalently $\mathrm{tr}[P^{T_A}\mathcal{E}(\rho^{\otimes N})] < 0$.*

Note that the operator E corresponding to the CPM $\mathcal{E}$ is PPT and acts on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A = \mathcal{H}_{A_1}^{\otimes N} \otimes \mathbb{C}^2$ and $\mathcal{H}_B = \mathcal{H}_{B_1}^{\otimes N} \otimes \mathbb{C}^2$.

A N–undistillable state, ρ, is N–activatable if for this integer N, condition (H.1) is fulfilled, for a PPT–preserving CPM, $\mathcal{E}$.

H.2 Three parties

Let us now consider a density operator, ρ, describing the state of a system composed of three subsystems. The Hilbert space ρ is acting on is $\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{C_1}$. Analogously to the previous section we reformulate the problem of distillation and activation in terms of CPM's. In the following we will, without loos of generality concentrate on the distillation and activation of the entanglement between Bob and Charly.

Corollary H.2 *A state, ρ, is BC–distillable iff there exists a positive integer N and a separable CPM $\mathcal{E}_a : \mathcal{B}(\mathcal{H}_1^{\otimes N}) \to \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ such*

$$\mathrm{tr}[P_{B,C}^{T_C}\mathcal{E}_a(\rho^{\otimes N})] < 0, \tag{H.2}$$

where $P_{B,C}$ is defined in (E.27) and the small letter a indicates that $\mathcal{E}_a$ maps a density operator describing the state of the particles A, B, C to a density operator describing the state of two qubits, one held by Bob and the other one by Charly.

Then ρ is N–BC–distillable if for the integer N condition (H.2) is fulfilled, for $\mathcal{E}_a$ separable.

Lemma H.2 *A state, ρ, which is not m–BC–distillable, is BC–activatable iff there exists an integer $N \leq m$ and a PPT-preserving CPM $\mathcal{E}_a : \mathcal{B}(\mathcal{H}_1^{\otimes N}) \to \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ such that condition (H.2) is fulfilled.*

A N–BC–undistillable state, ρ, is N–BC–activatable if for the integer N condition (H.2) is fulfilled, for a PPT–preserving CPM, $\mathcal{E}_a$.

Let us summarize this section: A state is N–(XY) distillable (activatable) iff there exists a separable (PPT–preserving) CPM, which transforms N copies of the state into an entangled state acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$. This automatically implies that all PPTES are bound entangled, in the sense that their entanglement cannot be distilled nor activated.

Bibliography

[1] A. Acin, D. Bruss, M. Lewenstein, and A. Sanpera. Classification of mixed three-qubit states. *Phys. Rev. Lett*, **87**, p. 040401, 2001.

[2] F. T. Arecchi, E. Courtens, R. Gilmore, and H. Thomas. Atomic coherent states in quantum optics. *Phys. Rev. A*, **6**, p. 2211, 1972.

[3] Arvind, B. Dutta, N. Mukunda, and R. Simon. The real symplectic groups in quantum mechanics and optics. `arXiv:quant-ph/9509002`.

[4] A. Barenco. Quantum physics and computers. *Contem. Phys.*, **37**, p. 375, 1996.

[5] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, **53**, p. 2046, 1996.

[6] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, **70**, p. 1895, 1993.

[7] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, **76**, p. 722, 1996.

[8] C. H. Bennett, J. I. Cirac, M. S. Leifer, D. W. Leung, N. Linden, S. Popescu, and G. Vidal. Optimal simulation of two-qubit hamiltonians using general local operations. *Phys. Rev. A*, **66**, p. 012305, 2002.

[9] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A*, **59**, p. 1070, 1999.

[10] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, **69**, p. 2881, 1992.

[11] C. Bennett, D. DiVincenzo, T. Mor, P. Shor, J. Smolin, and B. Terhal. Unextendible product bases and bound entanglement. *Phys. Rev. Lett.*, **82**, p. 5385, 1999.

[12] D. W. Berry and B. C. Sanders. Near optimal two-mode spin squeezing via feedback. *Phys. Rev. A*, **66**, p. 012313, 2002.

[13] D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, **80**, p. 1121, 1998.

[14] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, **390**, p. 575, 1997.

[15] S. L. Braunstein and H. J. Kimble. Teleportation of continuous quantum variables. *Phys. Rev. Lett.*, **80**, p. 869, 1998.

[16] S. L. Braunstein. Squeezing as an irreducible resource. `arXiv:quant-ph/9904002`.

[17] M. J. Bremner, C. M. Dawson, J. L. Dodd, A. Gilchrist, A. W. Harrow, D. Mortimer, M. A. Nielsen, and T. J. Osborne. Practical scheme for quantum computation with any two-qubit entangling gate. *Phys. Rev. Lett*, **89**, p. 247902, 2002.

[18] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, **81**, p. 5932, 1998.

[19] D. Bruß and A. Peres. Construction of quantum states with bound entanglement. *Phys. Rev. A*, **61**, p. 030301, 2000.

[20] A. Chefles, C. R. Gilson, and S. M. Barnett. Entanglement and collective quantum operations. `arXiv:quant-ph/0003062`.

[21] A. Chefles, C. R. Gilson, and S. M. Barnett. Entanglement, information and multiparticle quantum operations. *Phys. Rev. A*, **63**, p. 032314, 2000.

[22] M. D. Choi. Positive linear maps. *Proc. Sympos. Pure Math.*, **38**, p. 583, 1982.

[23] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein. Entangling operations and their implementation using a small amount of entanglement. *Phys. Rev. Lett.*, **86**, p. 544, 2001.

[24] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello. Distributed quantum computation over noisy channels. *Phys. Rev. A*, **59**, p. 4249, 1999.

[25] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani. Bell-type inequalities to detect true n-body non-separability. *Phys. Rev. Lett.*, **88**, p. 170405, 2002.

[26] D. Collins, N. Linden, and S. Popescu. The non-local content of quantum operations. *Phys. Rev. A*, **64**, p. 032302, 2000.

[27] D. Deutsch, A. Ekert, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, **77**, p. 2818, 1996.

[28] D. P. DiVincenzo. Quantum computation. *Science*, **270**, p. 255, 1995.

[29] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases, uncompletable product bases and bound entanglement. `arXiv:quant-ph/9908070`.

[30] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal. Evidence for bound entangled states with negative partial transpose. *Phys. Rev. A*, **61**, p. 062312, 2000.

[31] A. Doherty, P. A. Parrilo, and F. M. Spedalieri. Distinguishing separable and entangled states. *Phys. Rev. Lett.*, **88**, p. 187904, 2002.

[32] L.-M. Duan, J. I. Cirac, and P. Zoller. Three-dimensional theory for interaction between atomic ensembles and free-space light. *Phys. Rev. A*, **66**, p. 023818, 2002.

[33] L.-M. Duan, J. I. Cirac, P. Zoller, and E. S. Polzik. Quantum communication between atomic ensembles using coherent light. *Phys. Rev. Lett.*, **85**, p. 5643, 2000.

[34] L.-M. Duan, G. Giedke, J. Cirac, and P. Zoller. Physical implementation for entanglement purification of Gaussian continuous-variable quantum states. *Phys. Rev. A*, **62**, p. 032304, 2000.

[35] L.-M. Duan, A. Sørensen, J. I. Cirac, and P. Zoller. Squeezing and entanglement of atomic beams. *Phys. Rev. Lett.*, **85**, p. 3991, 2000.

[36] W. Dür and J. I. Cirac. Non-local operations: Purification, storage, compression, tomography, and probabilistic implementation. *Phys. Rev. A*, **64**, p. 012317, 2001.

[37] W. Dür and J. I. Cirac. Equivalence classes of non-local unitary operations. *Quant. Inf. Comp.*, **2**, p. 240, 2002.

[38] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruß. Distillability and partial transposition in bipartite system. *Phys. Rev. A*, **61**, p. 062313, 2000.

[39] W. Dür, J. I. Cirac, and R. Tarrach. Separability and distillability of multiparticle quantum systems. *Phys. Rev. Lett*, **83**, p. 3562, 1999.

[40] W. Dür and J. Cirac. Classification of multiqubit mixed states: Separability and distillability properties. *Phys. Rev. A*, **61**, p. 042314, 2000.

[41] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, **62**, p. 062314, 2000.

[42] W. Dür, G. Vidal, and J. I. Cirac. Optimal conversion of nonlocal unitary operations. *Phys. Rev. Lett.*, **89**, p. 057901, 2002.

[43] W. Dür, G. Vidal, J. I. Cirac, N. Linden, and S. Popescu. Entanglement capabilities of non-local hamiltonians. *Phys. Rev. Lett.*, **87**, p. 137901, 2001.

[44] K. Eckert, J. Schliemann, D. Bruss, and M. Lewenstein. Quantum correlations in systems of indistinguishable particles. *Annals of Physics*, **299**, p. 88, 2002.

[45] T. Eggeling, K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf. Distillability via protocols respecting the positivity of partial transpose. *Phys. Rev. Lett*, **87**, p. 257902, 2001.

[46] T. Eggeling and R. F. Werner. Separability properties of tripartite states with $UxUxU$-symmetry. *Phys. Rev. A*, **63**, p. 042111, 2001.

[47] J. Eisert, K. Jacobs, P. Papadopoulos, and M. Plenio. Optimal local implementation of non-local quantum gates. *Phys. Rev. A*, **62**, p. 052317, 2000.

[48] J. Eisert and M. B. Plenio. Conditions for the local manipulation of Gaussian states. *Phys. Rev. Lett.*, **89**, p. 097901, 2002.

[49] A. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, **67**, p. 661, 1991.

[50] A. Ekert and R. Josza. Quantum computation and shor's factoring algorithm. *Rev. Mod. Phys.*, **68**, p. 733, 1996.

[51] R. Filip. Overlap and entanglement-witness measurements. *Phys. Rev. A*, **65**, p. 062320, 2002.

[52] J. Fiurášek. Gaussian transformations and distillation of entangled Gaussian states. *Phys. Rev. Lett.*, **89**, p. 137904, 2002.

[53] G. Folland, editor. *Harmonic Analysis in Phase Space.* Princeton University Press, Princeton, 1989.

[54] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science*, **282**, p. 706, 1998.

[55] G. Giedke, L.-M. Duan, J. Cirac, and P. Zoller. All inseparable two-mode Gaussian continuous variable states are distillable. `arXiv:quant-ph/0007061`.

[56] G. Giedke, L.-M. Duan, P. Zoller, and J. I. Cirac. Distillability criterion for all bipartite Gaussian states. *Quant. Inf. Comp.*, **1(3)**, p. 79, 2001.

[57] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac. Entanglement criteria for all bipartite Gaussian states. *Phys. Rev. Lett.*, **87**, p. 167904, 2001.

[58] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac. Separability properties of three-mode Gaussian states. *Phys. Rev. A*, **64**, p. 052303, 2001.

[59] G. Giedke and J. I. Cirac. The characterization of Gaussian operations and distillation of Gaussian states. *Phys. Rev. A*, **66**, p. 032316, 2002.

[60] N. Gisin and H. Bechmann-Pasquinucci. Bell inequality, Bell states and maximally entangled states for n qubits. *Phys. Lett. A*, **246**, p. 1, 1998.

[61] N. Gisin. Hidden quantum nonlocality revealed by local filters. *Phys. Lett. A*, **210**, p. 151, 1996.

[62] D. Gottesman. The heisenberg representation of quantum computers. `arXiv:quant-ph/9807006`.

[63] D. M. Greenberger, M. Horne, and A. Zeilinger. *Bell's Theorem, Quantum Theory and Conceptions of the Universe. ed. M. Kafatos*, **64**, p. 042313, 1989.

[64] O. Guehne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. Experimental detection of entanglement via witness operators and local measurements. `arXiv:quant-ph/0210134`.

[65] O. Guehne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. Detection of entanglement with few local measurements. *Phys. Rev. A*, **66**, p. 062305, 2002.

[66] J. Hald, J. L. Sørensen, C. Schori, and E. S. Polzik. Spin squeezed atoms: A macroscopic entangled ensemble created by light. *Phys. Rev. Lett.*, **83**, p. 1319, 1999.

[67] S. Hill and W. K. Wootters. Entanglement of a pair of quantum bits. *Phys. Rev. Lett.*, **78**, p. 5022, 1997.

[68] R. A. Horn and C. R. Johnson. *Matrix Analysis.* Cambridge University Press, 1987.

[69] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis.* Cambridge University Press, 1994.

[70] M. Horodecki, P. Horodecki, , and R. Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Phys. Rev. Lett.*, **80**, p. 5239, 1998.

[71] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, **223**, p. 1, 1996.

[72] M. Horodecki, P. Horodecki, and R. Horodecki. Inseparable two spin-1/2 density matrices can be distilled to a singlet form. *Phys. Rev. Lett.*, **78**, p. 574, 1997.

[73] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for entanglement measures. *Phys.Rev.Lett.*, **84**, p. 2014, 2000.

[74] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed quantum states: linear contractions approach. `arXiv:quant-ph/0206008`.

[75] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transpose. *Phys. Lett. A*, **232**, p. 333, 1997.

[76] P. Horodecki and A. Ekert. Method for direct detection of quantum entanglement. *Phys. Rev. Lett.*, **89**, p. 127902, 2002.

[77] P. Horodecki, M. Horodecki, and R. Horodecki. Bound entanglement can be activated. *Phys.Rev.Lett.*, **82**, p. 1056, 1999.

[78] P. Horodecki and M. Lewenstein. Bound entanglement and continuous variables. *Phys. Rev. Lett.*, **85**, p. 2657, 2000.

[79] P. Horodecki, M. Lewenstein, G. Vidal, and J. I. Cirac. Operational criterion and constructive checks for the separability of low rank density matrices. *Phys. Rev. A*, **62**, p. 032310, 2000.

[80] P. Horodecki, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal. Rank two bipartite bound entangled states do not exist. `arXiv:quant-ph/9910122`.

[81] R. Horodecki and M. Horodecki. Information-theoretic aspects of inseparability of mixed states. *Phys. Rev. A.*, **54**, p. 1838, 1996.

[82] R. Horodecki, M. Horodecki, and P. Horodecki. Einstein-Podolsky-Rosen paradox without entanglement. *Phys. Rev. A*, **60**, p. 4144, 1999.

[83] R. Horodecki, P. Horodecki, and M. Horodecki. Quantum α-entropy inequalities: independent condition for local realism? *Phys. Rev. A*, **210**, p. 377, 1996.

[84] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, **3**, p. 275, 1972.

[85] T. F. Jordan, editor. *Linear operators for quantum mechanics.* John Wiley, New York, 1974.

[86] R. Jozsa. Quantum algorithms and the fourier transform. `arXiv:quant-ph/9707033`.

[87] B. Julsgaard, A. Kozhekin, and E. S. Polzik. Experimental long-lived entanglement of two macroscopic objects. *Nature*, **413**, p. 400, 2000.

[88] S. Karnas and M. Lewenstein. Separability and entanglement in $2 \times 2 \times N$ composite quantum systems. *Phys. Rev. A*, **64**, p. 042313, 2001.

[89] S. Karnas and M. Lewenstein. Separable approximations of density matrices of composite quantum systems. *J Phys. A-Math. Gen.*, **34**, p. 6919, 2001.

[90] A. Kent. Entangled mixed states and local purification. *Phys. Rev. Lett.*, **81**, p. 2839, 1998.

[91] N. Khaneja and S. J. Glaser. Cartan decomposition of $SU(2^n)$, constructive controllability of spin systems and universal quantum computing. `arXiv:quant-ph/0010100`.

[92] M. Kitagawa and M. Ueda. Squeezed spin states. *Phys. Rev. A*, **47**, p. 5138, 1993.

[93] A. E. Kozekhin, K. Mølmer, and E. S. Polzik. Quantum memory for light. *Phys. Rev. A*, **65**, p. 033809, 2000.

[94] B. Kraus and J. I. Cirac. Optimal creation of entanglement using a two-qubit gate. *Phys. Rev. A*, **63**, p. 062309, 2001.

[95] B. Kraus, J. Cirac, S. Karnas, and M. Lewenstein. Separability in $2 \times N$ composite quantum systems. *Phys. Rev. A*, **61**, p. 062302, 2000.

[96] B. Kraus, W. Dür, and J. I. Cirac. private discussion.

[97] B. Kraus, M. Lewenstein, and J. I. Cirac. Characterization of distillable and activatable states using entanglement witnesses. *Phys. Rev. A*, **65**, p. 042327, 2002.

[98] B. Kraus, K. Hammerer, G. Giedke, and J. I. Cirac. Entanglement generation and Hamiltonian simulation in continuous-variable systems. `arXiv:quant-ph/0210136`.

[99] Kryszyński and S. L. Woronowicz. Partial transposition and non–extendible maps. *Lett. Math. Phys.*, **3**, p. 319, 1979.

[100] A. Kuzmich, N. P. Bigelow, and L. Mandel. Atomic quantum nondemolition measurements and squeezing. *Europhys. Lett.*, **42**, p. 481, 1998.

[101] A. Kuzmich, L. Mandel, and N. P. Bigelow. Generation of spin squeezing via continuous quantum nondemolition measurement. *Phys. Rev. Lett.*, **85**, p. 1594, 2000.

[102] A. Kuzmich and E. S. Polzik. Atomic quantum state teleportation and swapping. *Phys. Rev. Lett.*, **85**, p. 5639, 2000.

[103] M. S. Leifer, L. Henderson, and N. Linden. Optimal entanglement generation from quantum operations. `arXiv:quant-ph/0205055`.

[104] M. Lewenstein, D. Bruss, J. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, and R. Tarrach. Separability and distillability in composite quantum systems -a primer-. *J. Mod. Opt.*, **47**, p. 2481, 2000.

[105] M. Lewenstein, J. I. Cirac, and S. Karnas. Separability and entanglement in $2 \times N$ composite quantum systems. `arXiv:quant-ph/9903012`.

[106] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki. Optimization of entanglement witnesses. *Phys. Rev. A*, **62**, p. 052310, 2000.

[107] M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac. Characterization of separable states and entanglement witnesses. *Phys. Rev. A*, **63**, p. 044304, 2001.

[108] M. Lewenstein and A. Sanpera. Separability and entanglement of composite quantum systems. *Phys. Rev. Lett*, **80**, p. 2261, 1998.

[109] N. Linden, S. Massar, and S. Popescu. Purifying noisy entanglement requires collective measurements. *Phys. Rev. Lett.*, **81**, p. 3279, 1998.

[110] S. Lloyd and S. L. Braunstein. Quantum computing over continuous variables. *Phys. Rev. Lett.*, **82**, p. 1784, 1999.

[111] W. Lüst and W. Schleich, editors. *Special Issue Fort. Phys. **46***. VCH, 1998.

[112] J. Manuceau and A. Verbeure. Quasi-free states of the c.c.r.–algebra and bogoliubov transformations. *Comm. Math. Phys.*, **9**, p. 293, 1968.

[113] K. Mølmer. Twin-correlations in atoms. *Eur. Phys. J. D*, **5**, p. 301, 1999.

[114] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett*, **83**, p. 436, 1999.

[115] M. A. Nielsen and J. Kempe. Separable states are more disordered globally than locally. *Phys. Rev. Lett.*, **86**, p. 5184, 2001.

[116] A. Peres, editor. *Quantum Theory: Concepts and Methods.* Kluwer Asademic Publishers, 1993.

[117] A. Peres. All the Bell inequalities. *Found. Phys.*, **29**, p. 589, 1999.

[118] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, **77**, p. 1413, 1996.

[119] E. S. Polzik. Einstein-Podolsky-Rosen–correlated atomic ensembles. *Phys. Rev. A*, **49**, p. 4202, 1999.

[120] E. M. Rains. Entanglement purification via separable superoperators. `arXiv:quant-ph/9707002`.

[121] W. Rudin, editor. *Functional Analysis.* Mc Graw Hill, New York, 1973.

[122] O. Rudolph. Further results on the cross norm criterion for separability. `arXiv:quant-ph/0202121`.

[123] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe. Experimental entanglement of four particles. *Nature*, **404**, p. 256, 2000.

[124] A. Sanpera, D. Bruss, and M. Lewenstein. Schmidt number witnesses and bound entanglement. *Phys. Rev. A*, **63**, p. 050301, 2001.

[125] A. Sanpera, R. Tarrach, and G. Vidal. Quantum inseparability as local pseudomixture. *Phys. Rev. A*, **58**, p. 826, 1998.

[126] V. Scarani, M. Ziman, P. Stelmachovic, N. Gisin, and V. Buzek. Thermalizing quantum machines: Dissipation and entanglement. *Phys. Rev. Lett.*, **88**, p. 097905, 2002.

[127] R. Schnabel, W. P. Bowen, N. Treps, T. C. Ralph, H.-A. Bachor, and P. K. Lam. Stokes operator squeezed continuous variable polarization states. `arXiv:quant-ph/0208103`.

[128] C. Schori, B. Julsgaard, J. L. Sørensen, and E. S. Polzik. Recording quantum properties of light in a long-lived atomic spin state: Towards quantum memory. *Phys. Rev. Lett.*, **89**, p. 057903, 2002.

[129] B. Schumacher and M. Nielsen. Quantum data processing and error correction. *Phys. Rev. A*, **54**, p. 2629, 1996.

[130] H. Scutaru. Transition probabilities for quasifree states. *J. Math. Phys.*, **39**, p. 6403, 1998.

[131] P. W. Shor, J. A. Smolin, and B. M. Terhal. Nonadditivity of bipartite distillable entanglement follows from conjecture on bound entangled Werner states. *Phys. Rev. Lett.*, **86**, p. 2681, 2001.

[132] C. Silberhorn, P. K. Lam, O. Weiss, F. Koenig, N. Korolkova, and G. Leuchs. Generation of continuous variable Einstein-Podolsky-Rosen entanglement via the kerr nonlinearity in an optical fibre. *Phys. Rev. Lett.*, **86**, p. 4267, 2001.

[133] R. Simon. Peres-horodecki separability criterion for continuous variable systems. *Phys. Rev. Lett.*, **84**, p. 2726, 2000.

[134] R. Simon, N. Mukunda, and B. Dutta. Quantum-noise matrix for multimode systems: $\mathbf{U}(n)$ invariance, squeezing, and normal forms. *Phys. Rev. A*, **49**, p. 1567, 1994.

[135] A. Sørensen, L.-M. Duan, J. I. Cirac, and P. Zoller. Many-particle entanglement with Bose-Einstein-Condensates. *Nature*, **409**, p. 63, 2001.

[136] A. Steane. Quantum computing. *Rep. Prog. Phys.*, **61**, p. 117, 1998.

[137] J. K. Stockton, J. Geremia, A. C. Doherty, and H. Mabuchi. Characterizing the entanglement of symmetric many-particle spin-1/2 systems. `arXiv:quant-ph/0210117`.

[138] E. Störmer. Positive linear maps of operator algebras. *Acta Math*, **110**, p. 233, 1963.

[139] B. M. Terhal. Bell inequalities and the separability criterion. *Physics Letters A*, **271**, p. 319, 2000.

[140] B. M. Terhal. A family of indecomposable positive linear maps based on entangled quantum states. *Lin. Alg. Appl.*, **323**, p. 61, 2000.

[141] L. K. Thomsen, S. Mancini, and H. M. Wiseman. Continuous quantum nondemolition feedback and unconditional atomic spin squeezing. `arXiv:quant-ph/0208160`.

[142] L. Vaidman. Teleportation of quantum states. *Phys. Rev. A*, **49**, p. 1473, 1994.

[143] S. J. van Enk. Discrete formulation of teleportation of continuous variables. *Phys. Rev. A*, **60**, p. 5095, 1999.

[144] P. van Loock and S. L. Braunstein. Multipartite entanglement for continuous variables: A quantum teleportation network. *Phys. Rev. Lett.*, **84**, p. 3482, 2000.

[145] P. van Loock and S. L. Braunstein. Greenberger-Horne-Zeilinger nonlocality in phase space. *Phys. Rev. A*, **63**, p. 022106, 2001.

[146] G. Vidal. Phd thesis.

[147] G. Vidal and J. I. Cirac. Catalysis in nonlocal quantum operations. *Phys. Rev. Lett.*, **88**, p. 167903, 2002.

[148] G. Vidal, K. Hammerer, and J. I. Cirac. Interaction cost of non-local gates. *Phys. Rev. Lett.*, **88**, p. 237902, 2002.

[149] G. Vidal. Entanglement monotones. *J. Mod. Opt.*, **47**, p. 355, 2000.

[150] G. Vidal and R. F. Werner. A computable measure of entanglement. *Phys. Rev. A*, **65**, p. 032314, 2001.

[151] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, **40**, p. 4277, 1989.

[152] R. F. Werner and M. M. Wolf. Bell's inequalities for states with positive partial transpose. *Phys. Rev. A*, **61**, p. 062102, 2000.

[153] R. F. Werner and M. M. Wolf. Bound entangled Gaussian states. *Phys. Rev. Lett.*, **86**, p. 3658, 2001.

[154] M. M. Wolf, J. Eisert, and M. B. Plenio. The entangling power of passive optical elements. `arXiv:quant-ph/0206171`.

[155] W. K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, **80**, p. 2245, 1998.

[156] S. L. Woronowicz. Nonextendible positive maps. *Commun. Math. Phys.*, **51**, p. 243, 1976.

[157] S. L. Woronowicz. Positive maps of low dimensional matrix algebras. *Rep. Math. Phys.*, **10**, p. 165, 1976.

[158] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Phys. Rev. A*, **58**, p. 883, 1998.

Index