Characterizing Entanglement in Quantum Information

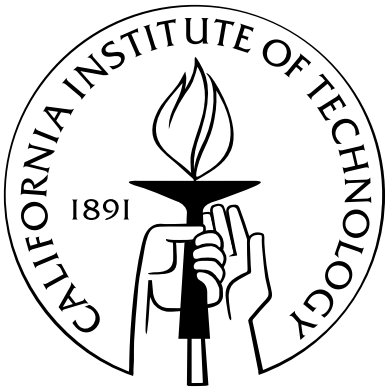
Thesis by

Federico M. Spedalieri

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy



California Institute of Technology

Pasadena, California

2003

(Defended May 19, 2003)

To my parents

Acknowledgements

First of all, I would like to express my sincere gratitude to my advisor, John Preskill, for his support and encouragement during all these years. I really appreciate the freedom he gave me to find the research projects that were more appealing to me, while at the same time being always ready to give me useful suggestions and advice. I feel that this perfect balance of freedom and guidance made my Ph.D. studies at Caltech a challenging, enriching and rewarding experience.

I would also like to thank my collaborators Pablo Parrilo and Andrew Doherty, and all the members of the Institute for Quantum Information (past and present), for their help and for creating a very exciting and fertile research environment. I extend my gratitude to the Physics Department and the California Institute of Technology for their valuable support.

During my time at Caltech, I was very fortunate to be surrounded by a very special group of people. Martín Basch, Diego Dugatkin, Alfredo Martinez and Pablo Parrilo, with their unconditional friendship, their loyal support and their inexhaustible good humor made all these years truly unforgettable. Kathleen Walker, Gabriela Surpi, Monica Giannelli, Sergey and Evgenya Pekarsky, Luz Vela, Athanasios Nenes, Sven Khatri, Andrew Doherty, Mario and Pili Munich, Tania and Anita Dugatkin, have all helped to make my life at Caltech actually quite a lot of fun. Thanks to Martín and Luján Mosconi, Santiago and Karina Serebrinsky, and the rest of the argentinian legion at Caltech for so many good moments. Thanks also to Diego Dalvit, for his good friendship and constant support.

I want to give a very special thanks to my aunt Gilda, my uncle Freddy, and my cousins Germán and Gustavo, for making me feel at home and among family during

all these years.

Finally, my deepest gratitude goes to my family. The support, encouragement and love that my mother, Graciela, my father, Angel, my sister, Graciela, my brother Néstor and my little sister Cecilia give me, have been invaluable through all these years of studies. I cannot find words to really express how much they all mean to me.

Abstract

Entanglement is a key resource in the emerging field of Quantum Information. The strong correlations between systems described by an entangled state allow us to perform certain tasks more efficiently than it would be possible by using only classical resources. This is why the characterization of entanglement is one of the most important problems in Quantum Information.

In this thesis, we analyze several aspects of entanglement. First, we introduce a new family of criteria to determine if a bipartite mixed state is entangled or not. This family consists of a sequence of tests that can be implemented efficiently, and has the property that all entangled states can be detected by some test in the sequence.

Each test in the family can be stated as a semidefinite program, which is a class of convex optimization problems. The duality structure of these programs allows us to explicitly construct an entanglement witness that proves entanglement of a state, whenever the state fails one of the tests in the sequence. The entanglement witnesses constructed in this manner have well-defined algebraic properties that can be used to give a characterization of the interior of the set of all possible entanglement witnesses, as well as the set of strictly positive bihermitian forms and the set of strictly positive maps.

We also study deterministic transformations of three-qubit pure state when only local operations and classical communication (LOCC) are allowed. We derive strong constraints that the operations and states involved must satisfy, and we apply these results to characterize the set of real states that can be obtained from the GHZ state by LOCC.

Contents

List of Figures

Chapter 1

Introduction

Entanglement has been one of the most striking features of quantum mechanics since the theory reached its maturity in the late 1920s. After developing his wave equation, Schröedinger himself noted that the linear structure of the space of quantum states led to a very strange behavior when a composite system was considered. He formulated his observations (and worries) in a *gedanken* (thought) experiment involving a cat in a box, that has become one of the most famous animals in science, widely known as *Schrödinger's cat*. In this experiment, a cat is confined inside a box that also contains a closed jar filled with poison. A mechanism containing a radioactive atom will break the jar if the atom decays, killing the cat. If the atom does not decay, the jar remains undamaged and the cat lives. Treated quantum mechanically, the system cat-atom is described by a coherent superposition of two states, one in which the atom decayed and the cat is dead, and another with no decay and a living cat. In quantum mechanics, we say that this state is *entangled*. Schrödinger and many scientists at the time were puzzled by these weird states that the new theory predicted, but described a world very different from their experiences in every day life.

In their famous paper of 1935 [19], Einstein, Podolsky and Rosen tried to use the strange behavior of entangled states to argue that the quantum mechanical description of nature was incomplete. Their analysis led them to the conclusion that either the wave function did not yield a complete description of a physical system, or subsystems that were spatially separated had some kind of nonlocal connection, what Einstein used to call a "spooky action at a distance." Since they truly believed in the

locality of physical laws, they concluded that the wave function did not have all the information about the state of the system. The existence of classical "hidden" variables that completed the description and maybe brought physics back to the realm of determinism became an appealing idea.

But in 1964, John Bell showed [4] that theories that involved classical hidden variables and were required to be local gave predictions that were very different from those of quantum mechanics. His proof took the form of a set of inequalities that the outcomes of measurements had to satisfy for any local hidden variable theory, but were violated by the predictions of quantum mechanics. This result allowed the construction of experiments to test whether nature admitted a local classical hidden variable model or not. The results of these experiments have confirmed that nature is quantum mechanical.

For many years, entanglement was just a strange trait of quantum mechanics. But in the 1980s, following ideas by Feynman [22] and Deutsch [15], physicist began to look at quantum mechanics not just as a means for describing the world, but also as a tool to perform certain tasks, like information processing and computing. Maybe the power of the "weird" laws of quantum mechanics could be harnessed and exploited. This was the start of the Quantum Information era.

Since the late 1980s, many interesting and useful applications of Quantum Information were developed: teleportation of an unknown quantum state [6], superdense coding of classical information [7], quantum cryptographic protocols [5, 20], Shor's algorithm for efficiently factoring prime numbers on a quantum computer [44] and quantum error correcting codes [45, 46], to name a few. Most of these applications share a common ingredient: they rely on the use of *entangled states*.

In Quantum Information, entanglement is no longer just a strange characteristic of the theory. It has become a very precious *resource*. Many applications rely entirely on entanglement while others can be made more efficient if entanglement is available. Then, it becomes clear that quantifying and characterizing entanglement should be one of the main tasks in Quantum Information Theory.

The first step in this study should be, of course, identifying which states are en-

tangled. In the case of pure states this is a remarkably simple task. But for mixed states, this simple and fundamental question seems very hard to answer, and a lot of effort has been devoted to it. Several criteria have been developed to help identify entangled states. However, these criteria are either incomplete, in the sense that they give no conclusive answer for some states, or they do not provide an algorithmic procedure to check them. This is a somewhat uncomfortable situation not only from a theoretical point of view but also from a practical point of view, since the states generated in the laboratory for practical applications of quantum information processing are invariably mixed states.

Since determining which pure states are entangled is simple, a natural next step is to compare the entanglement of two different states and try to quantify it. This can be done by defining measures of entanglement, but also by studying what other states can be obtained from a given entangled state by applying only local operations and classical communication. Since entanglement cannot be created by local actions, this gives us a way of quantifying it. For bipartite pure states this problem has been completely solved, but the case of multipartite entanglement still has many open questions.

In this thesis, we will explore some of these interesting questions regarding entanglement. In Chapter 2, we will briefly introduce the basic mathematical tools used in describing quantum states and some useful mathematical concepts that will help us in our study of entanglement. In Chapter 3, we will introduce a new family of separability criteria that allows us to identify *all bipartite entangled mixed states*. This new tool consists of a sequence of tests that can be implemented efficiently, since they can be stated as semidefinite programs. In Chapter 4, we will show that the duality of semidefinite programs can be exploited to construct a "certificate of entanglement," in the form of an entanglement witness, whenever a state fails one of the tests in the sequence. This allows us to give a complete characterization of the interior of the set of all possible entanglement witnesses, the set of strictly positive biquadratic bihermitian forms and the set of strictly positive maps. We will also discuss in detail some examples where we apply this technique to detect entangled states. In Chapter

5, we will analyze the deterministic transformations of a pure state of three qubits, when only local operations and classical communication are allowed. We show that under this type of transformations the GHZ class of states breaks into a continuum of subclasses. We study under what conditions a 2-outcome POVM can be used in deterministic transformations, and derive a set of constraints that the state involved and the POVM must satisfy. Finally, we apply these results to characterize a set of states that can be obtained from the GHZ state by local operations and classical communication.

Chapter 2

Preliminary concepts

In this chapter we will briefly review some basic mathematical tools used in the description of quantum states. We will be interested in the representation of quantum states as vectors and hermitian matrices on a Hilbert space. This will also help us fix the notation that will be used throughout this thesis. We will also introduce several concepts and operations that are particular to the case of composite systems. We will mention how measurements are represented in quantum mechanics and also we will introduce a few mathematical concepts that have useful applications in the study of entanglement.

2.1 Quantum states

In quantum mechanics we associate a Hilbert space $\mathcal{H}$ to every physical system. We then proceed to describe the properties of this system in terms of mathematical objects defined on its Hilbert space.

A *pure state* is represented by a normalized vector in $\mathcal{H}$ which we will write in Dirac's notation as $|\psi\rangle$. This vector represents everything we can possibly know about the state of the system, and we can use it to compute any of the system's physical properties. To the same state, we also associate a linear functional denoted by $\langle\psi|$, defined on vectors in $\mathcal{H}$. The normalization condition then takes the form

$$\langle\psi|\psi\rangle = 1. \tag{2.1}$$

If $\{|i\rangle\}_{i=1}^{d}$ is an orthonormal basis of $\mathcal{H}$, any state can be expanded as

$$|\psi\rangle = \sum_{i=1}^{d} x_i |i\rangle, \tag{2.2}$$

where the x_i are complex coefficients that satisfy $\sum_i |x_i|^2 = 1$. We will denote a Hilbert space of dimension d by $\mathcal{H}_d$.

In many cases we do not have complete information about which pure state describes the system. Instead, we only know that there is a set of vector $\{|\psi_i\rangle\}$ such that the system is in the pure state $|\psi_i\rangle$ with some probability p_i. When this happens, we say the system is in a *mixed state*. This type of state is represented by a positive semidefinite hermitian matrix ρ of trace 1, operating on the Hilbert space of the system, that can be written as

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{2.3}$$

where $|\psi_i\rangle\langle\psi_i|$ is a projector into a one dimensional subspace spanned by $|\psi_i\rangle$. This matrix is called a *density matrix* and it represents the most general description of the state of a quantum system. Note that a pure state can be represented by a density matrix of rank 1, since in this case the right-hand side (RHS) of (2.3) consists of only one term, and there is no uncertainty about which pure state describes the system.

An *observable* is a hermitian operator that represents a physical property of the system. The possible values that we can obtain when measuring this property are given by the eigenvalues of the observable. If the system is in the state ρ and we measure an observable A, the mean value $\langle A\rangle$ of these measurements can be computed by

$$\langle A\rangle = \mathrm{Tr}[A\rho], \tag{2.4}$$

with Tr representing the usual trace of a matrix. If the state is pure, we can write

$\rho = |\psi\rangle\langle\psi|$ for some vector $|\psi\rangle$, and the mean value takes the form

$$\begin{aligned} \langle A \rangle &= \mathrm{Tr}[A|\psi\rangle\langle\psi|] \\ &= \langle\psi|A|\psi\rangle. \end{aligned} \tag{2.5}$$

2.2 Composite systems

Sometimes we are interested in studying a system not only as a whole, but also in terms of two or more subsystems. This is typically the case when we consider physical systems that are spatially separated and we are interested in correlations between their properties, or when the system of interest interacts with an environment that we cannot access or control.

If we have k subsystems A_i, $i = 1, \ldots, k$, each one described by a Hilbert space $\mathcal{H}_{A_i}$ of dimension d_{A_i}, the Hibert space associated with the whole system is just the tensor product

$$\mathcal{H}_{A_1 \ldots A_k} = \mathcal{H}_{A_1} \otimes \ldots \otimes \mathcal{H}_{A_k}. \tag{2.6}$$

If $\{|j_i\rangle_{A_i}\}$, $j_i = 1, \ldots, d_{A_i}$, is a basis of $\mathcal{H}_{A_i}$, all the vectors of the form

$$|j_1\rangle_{A_1} \otimes \ldots \otimes |j_k\rangle_{A_k}, \tag{2.7}$$

form a basis of $\mathcal{H}_{A_1 \ldots A_k}$, which has dimension $d_{A_1} \times \cdots \times d_{A_k}$. To simplify the notation, we will also write a state of the form (2.7) as

$$|j_1 \ldots j_k\rangle, \tag{2.8}$$

where we dropped the tensor product sign and the subindex identifying the subsystems, and we use the convention that the i^{th} symbol corresponds to a state in the i^{th} space on the tensor product. The most general state of a composite system will then be represented by a density matrix, that is a positive semidefinite hermitian matrix operating on $\mathcal{H}_{A_1 \ldots A_k}$, as in the case of a single system.

In a composite system we can define an operation called the *partial trace with respect to subsystem* A_i of an operator Z in $\mathcal{H}_{A_1 \ldots A_k}$ by

$$\mathrm{Tr}_{A_i}[Z] = \sum_{j}^{d_{A_i}} {}_{A_i}\langle j|Z|j\rangle_{A_i}. \tag{2.9}$$

The result of this partial trace is an operator defined on the tensor product of the remaining subsystems.

If ρ is the density matrix of the system in the space $\mathcal{H}_{A_1 \ldots A_k}$, we can define a *reduced density matrix* ρ_{A_1} by

$$\rho_{A_1} = \mathrm{Tr}_{A_2 \ldots A_k}[\rho], \tag{2.10}$$

which represents the physical state of subsystem A_1. In the same way we can define the reduced density matrix of any other subsystem, by taking the partial trace over the subsystems excluded.

2.3 Pure entangled states

A *pure product state* $|\Psi\rangle$ is a vector in $\mathcal{H}_{A_1 \ldots A_k}$ of the form

$$|\Psi\rangle = |\psi_1\rangle \otimes \ldots \otimes |\psi_k\rangle, \tag{2.11}$$

that is, the tensor product of pure states corresponding to the subsystems. When the system is in a pure product state, we have maximal knowledge of both the state of the system *and the state of all of its subsystems.*

If a pure state of a composite system cannot be written as a tensor product of pure states, we say that it is an *entangled state.* For example, the state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \tag{2.12}$$

is an entangled state in $\mathcal{H}_2 \otimes \mathcal{H}_2$. The existence of these states, which is a consequence

of the linear structure of the set of states, is one of the most strange characteristics of quantum mechanics since these states describe correlations between the systems that cannot be explained classically. They are essential in many applications of Quantum Information.

2.3.1 Bipartite pure states

The case of pure states in a bipartite system (only two subsystems, A and B) has been extensively studied, and most of the questions about the properties and characteristics of entanglement in this case have been answered. One of the facts that has facilitated many of these results is the existence of the *Schmidt decomposition*, that states that any bipartite pure state $|\Psi\rangle$ can be transformed by the application of local unitary transformations $U_A \otimes U_B$ (where U_A and U_B are unitary transformations acting on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively), into a canonical form given by

$$\sum_{i=1}^{\min\{d_A,d_B\}} \lambda_i \, |i\rangle_A \otimes |i\rangle_B, \tag{2.13}$$

where $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$ are orthonormal vectors in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The scalars λ_i are real and nonnegative, and are called the *Schmidt coefficients*. The number of nonzero Schmidt coefficients is called the *Schmidt number*. Since entanglement cannot be changed by local unitary operations, studying the canonical form (2.13) is sufficient to understand the entanglement of any bipartite pure state. This decomposition is also very easy to compute since the nonzero Schmidt coefficients are the nonzero eigenvalues of the reduced density matrices $\rho_A = \mathrm{Tr}_B[|\Psi\rangle\langle\Psi|]$ and $\rho_B = \mathrm{Tr}_A[|\Psi\rangle\langle\Psi|]$.

2.4 Measurements

A *projective (Von Neumann) measurement* is represented by a set of orthogonal projectors P_i that form a partition of the identity. They satisfy

1. $P_i P_j = P_i \delta_{ij}$.
2. $\sum_{i=1}^{n} P_i = \mathbb{1}$,

where $\mathbb{1}$ is the identity matrix. The number n must be equal to the dimension of the Hilbert space of the system. If the system is originally in the state ρ, after the measurement is performed the system can be in one of several possible states, depending on the outcome of the measurement. The outcome associated with the projector P_i is obtained with probability

$$\text{Prob}(i) = \text{Tr}[P_i \rho], \tag{2.14}$$

and in this case the state after the measurement is given by

$$\rho_i = \frac{P_i \rho P_i}{\text{Tr}[P_i \rho]}. \tag{2.15}$$

A *generalized measurement* is represented by a positive operator valued measure (POVM). A POVM is a set of operators E_i that satisfy

1. E_i is positive semidefinite.
2. $\sum_{i}^{m} E_i^\dagger E_i = \mathbb{1}$,

with $E_i^\dagger$ the hermitian conjugate of E_i. The number m of operators in a POVM can be greater, equal or smaller than the dimension of the Hilbert space. Note that there is no orthogonality requirement, so different outcomes may not be mutually exclusive. A generalized measurement can always be realized as a projective measurement in a larger Hilbert space. The outcome associated with the operator E_i is obtained with probability

$$\text{Prob}(i) = \text{Tr}[E_i \rho E_i^\dagger], \tag{2.16}$$

and in this case the state after the measurement is given by

$$\rho_i = \frac{E_i \rho E_i^\dagger}{\text{Tr}[E_i \rho E_i^\dagger]}. \tag{2.17}$$

2.5 Mathematical concepts

We will now review a few mathematical concepts that have proven very useful in the study and characterization of entanglement.

2.5.1 Majorization

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be two vectors in $\mathbb{R}^n$ whose components are positive and satisfy $\sum_{i=1}^{n} x_i = 1$ and $\sum_{i=1}^{n} y_i = 1$. Denote by $x^{\downarrow}$ the vector obtained from x by arranging the components x_i in decreasing order, $x_1^{\downarrow} \geq x_2^{\downarrow} \geq \ldots \geq x_n^{\downarrow}$. We will say that x *is majorized by* y, which we will note $x \prec y$, if

$$\begin{aligned} x_1^{\downarrow} &\leq y_1^{\downarrow} \\ x_1^{\downarrow} + x_2^{\downarrow} &\leq y_1^{\downarrow} + y_2^{\downarrow} \\ &\vdots \\ x_1^{\downarrow} + \ldots + x_{n-1}^{\downarrow} &\leq y_1^{\downarrow} + \ldots + y_{n-1}^{\downarrow}. \end{aligned} \tag{2.18}$$

If the two vectors have different lenghts, we can still compare them by padding the shorter one with zeros to make them both the same length. The idea of majorization aims at making more rigorous the notion of a string of numbers being "more disordered" than another.

2.5.2 Positive and completely positive maps

Let us denote by $\mathcal{A}_A$ and $\mathcal{A}_B$ the set of linear operators acting on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. We will call $\mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$, the set of linear maps from $\mathcal{A}_A$ to $\mathcal{A}_B$. We say that a map $\Lambda \in \mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$ is *positive* if

$$\forall A \in \mathcal{A}_A, A \geq 0 \Rightarrow \Lambda(A) \geq 0, \tag{2.19}$$

where $A \geq 0$ means that the operator A is positive semidefinite. A map Λ is said to be *completely positive* (CP) if the induced map

$$\Lambda_n = \Lambda \otimes \mathbb{1}_n : \mathcal{A}_A \otimes \mathcal{A}_n \to \mathcal{A}_B \otimes \mathcal{A}_n, \tag{2.20}$$

is positive for all n, with $\mathcal{A}_n$ being the space of operators in a Hilbert space of dimension n, and $\mathbb{1}_n$ the identity map on $\mathcal{A}_n$. Completely positive maps have very important applications in characterizing the set of physically meaningful evolutions of a quantum state.

Chapter 3

New separability criteria

In this chapter we will introduce a new family of separability criteria for finite dimensional bipartite quantum states. This family has a natural, hierarchical structure, with each test being at least as powerful as all the previous ones. Using techniques from convex optimization, each of these tests can be implemented efficiently. This infinite family of tests has the very important property that it can detect any entangled state in a finite number of steps, giving a complete characterization of bipartite entanglement. All the results presented in the following two chapters have been obtained in collaboration with Andrew Doherty and Pablo Parrilo [16, 17].

Before presenting these new separability criteria, we will introduce the main concepts regarding the separability problem, present several separability criteria that have been developed so far, and briefly point out their advantages and short comings.

3.1 Introduction

Pure state entanglement is very easy to recognize. A bipartite entangled pure state is defined as a state that cannot be written as the tensor product of two pure states. We can find out if a state is entangled by computing the Schmidt decomposition. If the Schmidt number is greater than one, the state is entangled. However, there is no such a thing as a Schmidt decomposition for bipartite mixed states, and the simple question of asking if a given mixed state is entangled becomes really hard to answer. First of all, we need to specify what is it meant by an "entangled mixed state", since

the pure state definition clearly does not apply.

A bipartite mixed state is said to be *separable* [56] (not entangled) if it can be written as a convex combination of pure product states

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|, \tag{3.1}$$

where $|\psi_i\rangle$ and $|\phi_i\rangle$ are state-vectors on the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ of subsystems A and B, respectively, and $p_i > 0, \sum_i p_i = 1$. This definition can be extended to the multipartite case in a straightforward manner. From this expression it is easy to see that parties A and B can generate such a state by performing local operations and exchanging classical information, which makes clear the fact that this state cannot have stronger than classical correlations, and hence posseses no entanglement. Since entanglement is such a useful resource in Quantum Information, the importance of having a procedure that allows us to determine whether a state is entangled or separable becomes evident. Even though the definition given by (3.1) does not provide us with such a procedure, it allows us to develop several criteria that can be helpful to distinguish between entangled and separable states.

3.2 Separability criteria

A *separability criterion* is usually based on *a certain property that can be shown to hold for all separable states*. To make the criterion useful in practice, this property should be easy to check. Given a bipartite state, if it does not satisfy the property we can conclude that the state cannot be separable, and hence must be entangled. However, if the property is satisfied, no valid conclusion can be extracted from the criterion. It is clear then that separability criteria give usually *necessary but not sufficient* conditions for separability.

3.2.1 Positive partial transpose criterion

One of the first and most famous separability criteria was introduced by Peres [38], and it is based on a very simple observation. Given a state ρ in $\mathcal{H}_A \otimes \mathcal{H}_B$, we define the *partial transpose of ρ with respect to subsystem A*, which we will denote by ρ^{T_A}, as the operator whose matrix elements satisfy

$$ {}_A\langle i| \otimes {}_B\langle k|\rho^{T_A}|j\rangle_A \otimes |l\rangle_B = {}_A\langle j| \otimes {}_B\langle k|\rho|i\rangle_A \otimes |l\rangle_B. \tag{3.2} $$

In a similar manner, we can define the partial transpose of a multipartite state with respect to any subset of its subsystems. If ρ is a separable state, then using equation (3.1) it is easy to see that

$$ \begin{aligned} \rho^{T_A} &= \sum p_i \left(|\psi_i\rangle\langle\psi_i|\right)^T \otimes |\phi_i\rangle\langle\phi_i| \\ &= \sum p_i |\psi_i^*\rangle\langle\psi_i^*| \otimes |\phi_i\rangle\langle\phi_i|, \end{aligned} \tag{3.3} $$

where we used the hermiticity of $|\psi_i\rangle\langle\psi_i|$. Since $|\psi_i^*\rangle$ is a pure state in $\mathcal{H}_A$ and $p_i \geq 0, \sum_i p_i = 1$, equation (3.3) tells us that ρ^{T_A} is a valid physical state for the system. Then, ρ^{T_A} must be a positive semidefinite (PSD) matrix, and we can state the following separability criterion.

Positive Partial Transpose (PPT) Criterion *Let ρ be a separable state; then the matrix ρ^{T_A} must be PSD.*

This criterion has the advantage that it is computationally very easy to check, since it only involves computing the eigenvalues of a certain hermitian matrix. Furthermore, it was shown by Horodecki et al. [29] to be both necessary and sufficient for separability in $\mathcal{H}_2 \otimes \mathcal{H}_2$ and $\mathcal{H}_2 \otimes \mathcal{H}_3$. However, in higher dimensions, there are PPT states that are nonetheless entangled, as was first shown in [32]. These states are called *bound entangled states*, because they have the peculiar property that no entanglement can be distilled from them by local operations [30]. It is worthy to note that even though the definition of partial transpose given by Equation (3.2) depends on the basis used,

the criterion still holds since the positivity requirement is independent of the basis.

3.2.2 Range criterion

Another useful separability criterion that has been used to show entanglement of PPT states is the *range criterion* [32].

Range Criterion *Let ρ be a separable state; then there exists a set of product states $\{|\psi_i\rangle|\phi_i\rangle\}$ that span the range of the matrix ρ. Furthermore, the set $\{|\psi_i^*\rangle|\phi_i\rangle\}$ spans the range of the matrix ρ^{T_A}.*

The validity of this criterion is evident from Equations (3.1) and (3.3). Unfortunately, the criterion does not provide a way of finding the vectors $\{|\psi_i\rangle|\phi_i\rangle\}$, and whether the criterion is useful to show entanglement of a particular state, strongly depends on the state considered. The range criterion is independent of the PPT criterion, since it can be shown that there are PPT entangled states that violate the range criterion, but also that there non PPT states that satisfy it.

3.2.3 Reduction criterion

This criterion is very interesting since its violation implies distillability of the state [28, 11].

Reduction Criterion *Let ρ be a separable state, ρ_A and ρ_B the reduced density matrices. Then the matrices $\mathbb{1}_A \otimes \rho_B - \rho$ and $\rho_A \otimes \mathbb{1}_B - \rho$ are both PSD.*

Checking this criterion is easy since, like the PPT criterion, it only involves computing eigenvalues of hermitian matrices. The reduction criterion coincides with the PPT criterion for $\mathcal{H}_2 \otimes \mathcal{H}_2$ and $\mathcal{H}_2 \otimes \mathcal{H}_3$, and hence gives also a sufficient condition for separability in these two cases.

3.2.4 Majorization criterion

Entangled states have the property that they seem more disordered locally than globally. When we analyze separately the states of each subsystem of a composite quantum system, we lose all the information about the quantum correlations of the state. This property can be used to state the following separability criterion [37].

Majorization Criterion *Let ρ be a separable state, $\lambda(\rho)$ the vector of its eigenvalues, $\lambda(\rho_A)$ and $\lambda(\rho_B)$ the vectors of eigenvalues of the reduced density matrices ρ_A and ρ_B, respectively. Then $\lambda(\rho) \prec \lambda(\rho_A)$ and $\lambda(\rho) \prec \lambda(\rho_B)$.*

The majorization criterion is easy to check, but it turns out to be weaker than the PPT criterion.

3.2.5 Positive maps

All the criteria discussed above have the disadvantage that they are, in general, necessary but not sufficient to prove entanglement of a state. There is a criterion that gives a necessary and sufficient condition for separability that is based on the use of positive maps [29].

Positive Map Criterion *Let $\mathcal{A}_A$ and $\mathcal{A}_B$ be the algebra of linear operators acting on the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Then a state ρ in $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable, if and only if, for any positive map $\Lambda : \mathcal{A}_B \to \mathcal{A}_A$, the operator $(\mathbb{1}_A \otimes \Lambda)(\rho)$ is PSD.*

Although very important from a theoretical point of view, this criterion fails to provide us with a practical tool to detect the entanglement of a given state. The problem lies in our lack of a complete operational characterization of the set of all positive maps, which we would need to apply the test to a given state. This characterization has been known only in two cases, when the Hilbert spaces of both subsystems A and B are equal to $\mathcal{H}_2$, and when one is equal to $\mathcal{H}_2$ and the other is equal to $\mathcal{H}_3$.

The positive map criterion can be used to generate new criteria that give only

necessary conditions for separability. If Λ is a certain positive map that is not completely positive, then if $(\mathbb{1}_A \otimes \Lambda)(\rho)$ is not PSD for some state ρ, this state must be entangled. Both the PPT criterion and the reduction criterion are examples of this. The positive non CP maps involved are the transposition map $\sigma \to \sigma^T$ for the PPT criterion, and the map $\sigma \to \mathrm{Tr}[\sigma]\mathbb{1} - \sigma$ for the reduction criterion.

In summary, there seems to be a gap in our arsenal of tools to address the separability problem. On one side we have efficiently computable criteria that are incomplete, and on the other side, complete criteria that we do not know how to compute. In the next section we will introduce a new set of separability criteria that bridges this gap by providing a sequence of tests that can be efficiently implemented and are guaranteed to detect all entangled states.

3.3 A new family of separability criteria

To state our new separability criteria, we first need to introduce the idea of a *PPT symmetric extension of a state* ρ. Let $\{|i\rangle\}_{i=1}^{d_A}$ be a basis of the space $\mathcal{H}_A$, with d_A the dimension of $\mathcal{H}_A$. Then the set $\{|i_1 i_2 \dots i_k\rangle\}$, with $i_l = 1, \dots, d_A$, for $l = 1, \dots, k$, will be a basis of the space $\mathcal{H}_A^{\otimes k}$, which is the Hilbert space associated with k copies of system A. We define a set of operators $\{P_{mn}\}$ on $\mathcal{H}_A^{\otimes k}$, $n > m$, $m = 1, \dots, k$, by

$$P_{mn}|i_1 i_2 \dots i_m \dots i_n \dots i_k\rangle = |i_1 i_2 \dots i_n \dots i_m \dots i_k\rangle. \tag{3.4}$$

These operators correspond to *swapping* two copies of system A. We will now introduce the central concept in our separability criteria.

Definition 1 *Let ρ be a state in $\mathcal{H}_A \otimes \mathcal{H}_B$. We will say that a state $\tilde{\rho}$ in $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B$ is a PPT symmetric extension of ρ to k copies of subsystem A, if $\tilde{\rho}$ satisfies the following properties:*

1. *$\tilde{\rho}$ is PPT.*

2. $\tilde{\rho}$ *is invariant under swaps of the copies of* A*, i.e.,*

$$\tilde{\rho} = (P_{mn} \otimes \mathbb{1}_B)\tilde{\rho}(P_{mn} \otimes \mathbb{1}_B), \tag{3.5}$$

for all $m = 1, \ldots, k$*,* $n > m$*.*

3. $\mathrm{Tr}_{A_2 \ldots A_k}[\tilde{\rho}] = \rho$.

The first property means that $\tilde{\rho}$ must remain positive under partial transpositions with respect to any subset of subsystems in $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B$. For an arbitrary state in $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B$ this will require checking positivity of $(2^k - 1)$ partial transposes, which scales exponentially with k. The requirement of invariance under swaps of copies of A allows us to drastically reduce the number of independent partial transposes. Any two of them that involve the same number of copies of A, irrespective to its order, will be identical, provided that they also agree on transposing with respect to system B. The number of independent partial transposes for a swap invariant state in $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B$ is just k, which scales only linearly with respect to the number of copies of A. This will be very important when we discuss the resources required to implement our separability criteria. Also note that even though the last property, which we will refer to as the *extension property*, requires tracing out the last $(k-1)$ copies of A, the swap invariance tells us that we can actually trace out *any* $(k-1)$ copies and the result will still be ρ.

The importance of the concept of a PPT symmetric extension in the construction of new separability criteria is given by the following theorem.

Theorem 1 *Let* ρ *be a separable state in* $\mathcal{H}_A \otimes \mathcal{H}_B$*. Then* ρ *has a PPT symmetric extension to* k *copies of system* A *for any value of* k*.*

Proof: Since ρ is a separable state, we know that it can be written as a convex combination of product states, so we have

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|. \tag{3.6}$$

Now consider the state $\tilde{\rho}$ defined on $\mathcal{H}_A^{\otimes 2} \otimes \mathcal{H}_B$, given by

$$\tilde{\rho} = \sum_i p_i \, |\psi_i\rangle\langle\psi_i|^{\otimes k} \otimes |\phi_i\rangle\langle\phi_i|. \tag{3.7}$$

We claim that $\tilde{\rho}$ is a PPT symmetric extension of ρ to k copies of A. We need to show that it satisfies the three properties required in Definition 1. First, we can see from its definition in (3.7) that $\tilde{\rho}$ is a separable state, and so in particular it must be PPT. Second,

$$\begin{aligned}
(P_{mn} \otimes \mathbb{1}_B)\tilde{\rho}(P_{mn} \otimes \mathbb{1}_B) &= \sum_i p_i \left(P_{mn}|\psi_i\rangle\langle\psi_i|^{\otimes k}P_{mn}\right) \otimes |\phi_i\rangle\langle\phi_i| \\
&= \sum_i p_i \, |\psi_i\rangle\langle\psi_i|^{\otimes k} \otimes |\phi_i\rangle\langle\phi_i| \\
&= \tilde{\rho},
\end{aligned} \tag{3.8}$$

where the second equality comes from the fact that $|\psi_i\rangle\langle\psi_i|^{\otimes k} = (|\psi_i\rangle)^{\otimes k}(\langle\psi_i|)^{\otimes k}$, and $P_{mn}(|\psi_i\rangle)^{\otimes k} = (|\psi_i\rangle)^{\otimes k}$, since $(|\psi_i\rangle)^{\otimes k}$ is obviously invariant under swaps of copies of A. And finally,

$$\begin{aligned}
\mathrm{Tr}_{A_2 \ldots A_k}[\tilde{\rho}] &= \sum_i p_i \, \mathrm{Tr}_{A_2 \ldots A_k}[|\psi_i\rangle\langle\psi_i|^{\otimes k} \otimes |\phi_i\rangle\langle\phi_i|] \\
&= \sum p_i \, \mathrm{Tr}_{A_2 \ldots A_k}[|\psi_i\rangle\langle\psi_i|^{\otimes k-1}]|\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i| \\
&= \sum p_i \, |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i| \\
&= \rho,
\end{aligned} \tag{3.9}$$

since $\mathrm{Tr}_{A_2 \ldots A_k}[|\psi_i\rangle\langle\psi_i|^{\otimes k-1}] = \prod_{j=2}^{k} \mathrm{Tr}_A[|\psi_i\rangle\langle\psi_i|] = 1$, because $|\psi_i\rangle$ is a normalized state. □

Since we have identified a property that is satisfied by all separable states, we can use the result of Theorem 1 to construct a new family of separability criteria, which is one of the main contributions of this thesis.

PPT symmetric extension to k copies criterion *Let ρ be a separable state in $\mathcal{H}_A \otimes \mathcal{H}_B$; then a PPT symmetric extension of ρ to $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B$ must exist.*

Every value of k defines a different criterion, so we have a countably infinite family of separability criteria. In particular, we can interpret the criterion corresponding to $k = 1$ as the usual PPT criterion.

These criteria are not completely independent of each other; they actually have a natural hierarchical structure as the following theorem shows.

Theorem 2 *Let ρ be a state in $\mathcal{H}_A \otimes \mathcal{H}_B$ such that it has a PPT symmetric extension to n copies of subsystem A ($n \geq 2$); then ρ has a PPT symmetric extension to $(n-1)$ copies of subsystem A.*

Proof: Let $\tilde{\rho}_n$ be a PPT symmetric extension of ρ to n copies of subsystem A. Let $\tilde{\rho}_{n-1} = \mathrm{Tr}_A[\tilde{\rho}_n]$, where A represents one of the copies of A. It is easy to see that $\tilde{\rho}_{n-1}$ will inherit from $\tilde{\rho}_n$ the property of being symmetric under interchanges of copies of party A, since we have just removed one of the copies. It is also clear that $\tilde{\rho}_{n-1}$ is an extension of ρ to $(n-1)$ copies of A. Let us assume that it is not PPT. Then there is a subset $\mathcal{I}$ of the parties such that $\tilde{\rho}_{n-1}^{T_\mathcal{I}}$ has a negative eigenvalue, where $T_\mathcal{I}$ represents the partial transpose with respect to all the parties in subset $\mathcal{I}$. Let $|e\rangle$ be the corresponding eigenvector and let $\{|i\rangle\}_{i=1}^{d_A}$ be a basis of the system A over which the partial trace was performed. Since $\tilde{\rho}_n$ is PPT, then $\langle e|\langle i|\tilde{\rho}_n^{T_\mathcal{I}}|e\rangle|i\rangle \geq 0$, for all i. Then

$$\sum_{i=1}^{d_A} \langle e|\langle i|\tilde{\rho}_n^{T_\mathcal{I}}|e\rangle|i\rangle = \langle e|\mathrm{Tr}_A[\tilde{\rho}_n^{T_\mathcal{I}}]|e\rangle \geq 0. \tag{3.10}$$

Since we performed the partial trace over a party that is not included in $\mathcal{I}$, we can commute the trace and the partial transpose, and using $\tilde{\rho}_{n-1} = \mathrm{Tr}_A[\tilde{\rho}_n]$, we have $\langle e|\tilde{\rho}_{n-1}^{T_\mathcal{I}}|e\rangle \geq 0$, which contradicts the fact that $|e\rangle$ is an eigenvector of $\tilde{\rho}_{n-1}^{T_\mathcal{I}}$ with negative eigenvalue. Then $\tilde{\rho}_{n-1}$ is a PPT symmetric extension of ρ to $(n-1)$ copies of subsystem A. □

We have then a natural ordering of this family as a *hierarchy of tests*, indexed by the number of copies of subsystem A considered. The first test, corresponding to

$k = 1$, is just the PPT criterion; the second test corresponds to checking whether ρ has a PPT symmetric extension to two copies A; and in general, the k^{th} test searches for a PPT symmetric extension to k copies of A. The previous theorem shows that each test in the hierarchy is *at least as powerful as all the preceding ones* in detecting entanglement.

This hierarchical structure leads naturally to an operational procedure to study entanglement of bipartite states (see Figure 3.1). To check whether a given state

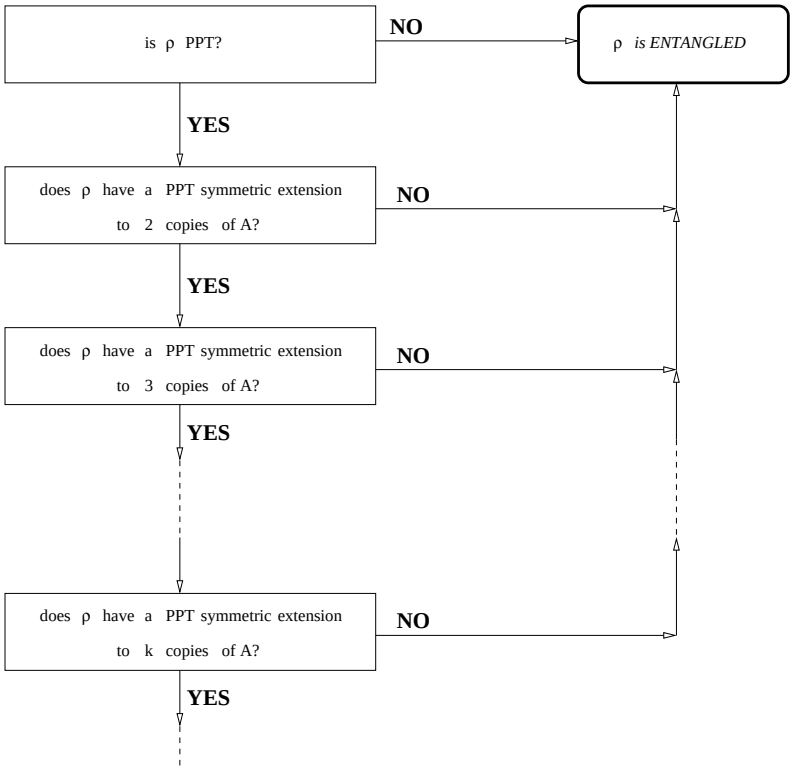


Figure 3.1: The hierarchy of separability tests.

ρ is entangled, we just apply the tests in sequence. First, we check if ρ is PPT; if the test fails (ρ is not PPT), the state must be entangled. If the test is passed, no conclusion can be extracted and we need to apply the second test in the hierarchy. If this second test fails (ρ has no PPT symmetric extension to two copies of A), the state is entangled. Again, if the test is passed, the state could be separable or entangled, and we need to apply the next test. At any point, if a test is failed, the state must

be entangled and the process stops.

This hierarchy of tests has the two properties that are most desirable on a practical tool to determine if a state is entangled. First of all, each test can be *efficiently implemented* for any state ρ. This relies on the fact that searching for PPT symmetric extensions can be formulated as a *semidefinite program* (SDP), which is a class of convex optimization problems that can be efficiently solved. And second, this hierarchy is *complete*, in the sense it can be guaranteed that any entangled state will fail one of the tests at some finite point in the hierarchy. The remaining of this chapter will be devoted to proving and discussing these two important properties.

3.4 Semidefinite programs and searching for PPT symmetric extensions

In this section we will introduce and discuss the structure of a semidefinite program and we will show explicitly how to apply it to the problem of searching for a PPT symmetric extension.

3.4.1 Semidefinite programs

A semidefinite program (SDP) is a particular type of a convex optimization problem [51, 50]. A SDP corresponds to the optimization of a linear function subject to a linear matrix inequality (LMI). A typical SDP has the form

$$\begin{aligned} &\text{minimize} && c^T\mathbf{x} \\ &\text{subject to} && F(\mathbf{x}) \geq 0, \end{aligned} \tag{3.11}$$

where c is a given vector, $\mathbf{x} = (x_1, \ldots, x_n)$, and $F(\mathbf{x}) = F_0 + \sum_i x_i F_i$, for some fixed hermitian matrices F_i. The inequality in the second line means that the matrix $F(\mathbf{x})$ must be positive semidefinite. The minimization is performed over the vector $\mathbf{x}$, whose components are the variables of the problem.

In the particular case in which $c = 0$, there is no fuction to minimize and the problem reduces to whether or not the LMI can be satisfied for some value of the vector $\mathbf{x}$. In this case, the SDP is refered to as a *feasibility problem*. The convexity of the SDP has made it possible to develop sophisticated and reliable analytical and numerical methods to solve them [51].

A very important property of a SDP, both from the theoretical and applied points of view, is its *duality structure*. To any SDP of the form (3.11), which is usually called the *primal problem*, there is associated another SDP, called the *dual problem*, that can be stated as

$$\begin{aligned} \text{maximize} \quad & -\text{Tr}[F_0 Z] \\ \text{subject to} \quad & Z \geq 0, \\ & \text{Tr}[F_i Z] = c_i, \end{aligned} \tag{3.12}$$

where the matrix Z is hermitian and is the variable over which the maximization is performed. This corresponds to the maximization of a linear functional, subject to linear constraints and a LMI.

The duality structure has very useful consequences. Let $\mathbf{x}$ and Z be any two feasible solutions of the primal and dual problems, respectively, which means that they satisfy the required constraints and LMIs. Then we have the following relationship

$$c^T \mathbf{x} + \text{Tr}[F_0 Z] = \text{Tr}[F(\mathbf{x}) Z] \geq 0, \tag{3.13}$$

where the last inequality follows from the fact that both $F(\mathbf{x})$ and Z are positive semidefinite. From (3.11) and (3.12) we can see that the left-hand side of (3.13) is just the difference between the objective functions of the primal and dual problem. The inequality in (3.13) tells us that the value of the primal objective function evaluated on *any feasible* vector $\mathbf{x}$, is always greater or equal than the value of the dual objective function evaluated on *any feasible* matrix Z. This property is called *weak duality*. So we can use any feasible $\mathbf{x}$ to compute an upper bound for the optimum of $-\text{Tr}[F_0 Z]$,

and we can also use any feasible Z to compute a lower bound for the optimum of $c^T\mathbf{x}$.

If the feasibility constraints on both the primal and dual problems are satisfied for some $Z > 0$ and $\mathbf{x}$ such that $F(\mathbf{x}) > 0$, the problems are termed *strictly feasible*, and the optimum values of the primal and dual forms are actually equal. This property is known as *strong duality*. Furthermore, there is a feasible pair $(\mathbf{x}_{\text{opt}}, Z_{\text{opt}})$ achieving the optimum. In this case it can be shown [51] that $\text{Tr}\,[F(\mathbf{x}_{\text{opt}})Z_{\text{opt}}] = 0$ and thus $F(\mathbf{x}_{\text{opt}})Z_{\text{opt}} = 0$, so the Hermitian matrices $F(\mathbf{x}_{\text{opt}})$ and Z_{opt} have orthogonal ranges. This is known as the *complementary slackness* condition.

Equation (3.13) has another important application. Consider the particular case of a feasibility problem (i.e., $c = 0$). Then, Equation (3.13) will read

$$\text{Tr}[F_0 Z] \geq 0, \tag{3.14}$$

and this must hold for *any feasible solution* of the dual problem. This property can be used to give a *certificate of infeasibility* for the primal problem: *if there exists* Z *such that* $Z \geq 0$ *and* $\text{Tr}[F_i Z] = 0$*, that satisfies* $\text{Tr}[F_0 Z] < 0$*, then the primal problem must be infeasible.* We will show later that for the particular case of our hierarchy of separability tests, whenever a PPT symmetric extension of ρ cannot be found (primal problem is infeasible), the certificate provided by the dual problem is nothing but an entanglement witness for the state ρ.

3.4.2 Separability tests as semidefinite programs

Each of the tests in the hierarchy of separability criteria introduced in Section 3.3 involves searching for a PPT symmetric extension of a certain state ρ. This extension is just a hermitian matrix that is required to satisfy certain linear constraints imposed by the extension property, and some positivity conditions imposed by the PPT requirement. This is exactly what a semidefinite program does, it tries to minimize a linear function *subject to certain positivity conditions on a hermitian matrix.* Implementing our criteria reduces to constructing a SDP in which the LMI encodes all the requirements that a PPT symmetric extension must satisfy.

The main task is to determine how to construct the matrices F_i in (3.11) for each one of the tests in the hierarchy. We will now proceed to illustrate this construction in detail for the second test which corresponds to searching for PPT symmetric extensions of a given state ρ in $\mathcal{H}_A \otimes \mathcal{H}_B$, to two copies of system A, represented by the Hilbert space $\mathcal{H}_A^{\otimes 2} \otimes \mathcal{H}_B$.

3.4.2.1 The second test

Let $\{\sigma_i^A\}_{i=1}^{d_A^2}, \{\sigma_j^B\}_{j=1}^{d_B^2}$ be bases for the space of hermitian matrices on $\mathcal{H}_A$ and $\mathcal{H}_B$, of dimensions d_A and d_B, respectively, such that they satisfy

$$\mathrm{Tr}[\sigma_i^X \sigma_j^X] = \alpha_X \delta_{ij} \quad \text{and} \quad \mathrm{Tr}[\sigma_i^X] = \delta_{i1}, \tag{3.15}$$

where X stands for A or B, and α_X is some constant—the generators of SU(n) (with $n = d_A, d_B$) could be used to form such a basis. This requirement just simplifies the algebra required, and it is not essential to the construction. We can then expand ρ in the basis $\{\sigma_i^A \otimes \sigma_j^B\}$, and write

$$\rho = \sum_{ij} \rho_{ij}\, \sigma_i^A \otimes \sigma_j^B, \tag{3.16}$$

with the expansion coefficients given by

$$\rho_{ij} = \alpha_A^{-1} \alpha_B^{-1}\, \mathrm{Tr}[\rho\, \sigma_i^A \otimes \sigma_j^B]. \tag{3.17}$$

The matrices $\{\sigma_i^A\}$ and $\{\sigma_j^B\}$ can be also used to construct a basis of the space of hermitian matrices in $\mathcal{H}_A^{\otimes 2} \otimes \mathcal{H}_B$, whose elements are of the form $(\sigma_i^A \otimes \sigma_k^A \otimes \sigma_j^B)$. The extension $\tilde{\rho}$ we are looking for is a hermitian matrix in $\mathcal{H}_A^{\otimes 2} \otimes \mathcal{H}_B$ that satisfies certain properties. The most general hermitian matrix in this space can be written as

$$\tilde{\rho} = \sum_{ikj} \tilde{\rho}_{ikj}\, (\sigma_i^A \otimes \sigma_k^A \otimes \sigma_j^B). \tag{3.18}$$

Our objective is to find whether it is possible to find coefficients $\tilde{\rho}_{ikj}$ that make $\tilde{\rho}$ satisfy all the properties required to be a PPT symmetric extension of ρ.

From (3.18) it is easy to see that the swapping invariance condition implies that the coefficients $\tilde{\rho}_{ikj}$ must be symmetric with respect to the first and second indices, so (3.18) reduces to

$$\tilde{\rho} = \sum_{\substack{ijk \\ i<k}} \tilde{\rho}_{ikj} \{\sigma_i^A \otimes \sigma_k^A \otimes \sigma_j^B + \sigma_k^A \otimes \sigma_i^A \otimes \sigma_j^B\} + \sum_{kj} \tilde{\rho}_{kkj}\, \sigma_k^A \otimes \sigma_k^A \otimes \sigma_j^B. \tag{3.19}$$

To satisfy the extension condition we need to impose

$$\mathrm{Tr}_{A_2}[\tilde{\rho}] = \rho. \tag{3.20}$$

Using (3.15) and the fact that the matrices $\{\sigma_i^A \otimes \sigma_j^B\}$ form a basis of of the set of hermitian matrices in $\mathcal{H}_A \otimes \mathcal{H}_B$, Equation (3.20) applied to (3.19) implies that

$$\tilde{\rho}_{i1j} = \rho_{ij}. \tag{3.21}$$

This fixes some of the coefficients in (3.19). The remaining coefficients are free variables.

In order for $\tilde{\rho}$ to be a PPT symmetric extension, it also has to be a *state*, which requires $\tilde{\rho}$ to be positive semidefinite and have trace 1. The trace condition is already implied by the fact that $\tilde{\rho}$ is an extension of ρ (and ρ has trace 1), but the positivity condition needs to be imposed on $\tilde{\rho}$. If we define

$$\begin{aligned}
G_0 &= \sum_j \rho_{1j}\, \sigma_1^A \otimes \sigma_1^A \otimes \sigma_j^B + \sum_{i=2,j=1} \rho_{ij} \{\sigma_i^A \otimes \sigma_1^A \otimes \sigma_j^B + \sigma_1^A \otimes \sigma_i^A \otimes \sigma_j^B\}, \\
G_{iji} &= \sigma_i^A \otimes \sigma_i^A \otimes \sigma_j^B\ , \qquad\qquad i \geq 2, \\
G_{ijk} &= (\sigma_i^A \otimes \sigma_k^A \otimes \sigma_j^B + \sigma_k^A \otimes \sigma_i^A \otimes \sigma_j^B), \quad k > i \geq 2,
\end{aligned} \tag{3.22}$$

we can write the PSD condition $\tilde{\rho} \geq 0$ as

$$\tilde{\rho} = G(\mathbf{x}) = G_0 + \sum_J x_J G_J \geq 0, \tag{3.23}$$

where we have collected all the subindices in (3.22) into one subindex J and replaced the free coefficients in (3.19) by x_J for notational convenience. This shows that the positivity condition on $\tilde{\rho}$ can be written as a LMI with hermitian matrices G_J, which is exactly the form of the constraint appearing on the semidefinite program (3.11). The variables x_i are just the coefficients of $\tilde{\rho}$ that have not been fixed by the swapping invariance condition and the extension property.

The last requirement on $\tilde{\rho}$ is that it must be PPT. As we discussed in the previous section, the swap invariance property reduces the number of independent partial transposes that can be applied to $\tilde{\rho}$. In this case, in which we have only two copies of A, there are only two independent partial transposes. These can be taken to be the partial tranpose with respect to the second copy of A and the partial transpose with respect to system B. Then we can write the PPT requirements as

$$\begin{aligned} \tilde{\rho}^{T_{A_2}} &= G^{T_{A_2}}(\mathbf{x}) = G_0^{T_{A_2}} + \sum_J x_J G_J^{T_{A_2}} \geq 0, \\ \tilde{\rho}^{T_B} &= G^{T_B}(\mathbf{x}) = G_0^{T_B} + \sum_J x_J G_J^{T_B} \geq 0, \end{aligned} \tag{3.24}$$

which again can be written as LMIs, with hermitian matrices $G_J^{T_{A_2}}$ and $G_J^{T_B}$ that can be obtained from (3.22) by applying the appropriate partial transposes.

We can combine the LMIs in (3.23) and (3.24) by defining a block-diagonal matrix F given by

$$F(\mathbf{x}) = \begin{pmatrix} G(\mathbf{x}) & 0 & 0 \\ 0 & G^{T_{A_2}}(\mathbf{x}) & 0 \\ 0 & 0 & G^{T_B}(\mathbf{x}) \end{pmatrix}. \tag{3.25}$$

Since a block-diagonal matrix $C = \left(\begin{smallmatrix} C_1 & 0 \\ 0 & C_2 \end{smallmatrix}\right)$ is positive semidefinite if and only if, both

C_1 and C_2 are positive semidefinite, we can use the LMI

$$F(\mathbf{x}) = F_0 + \sum_J x_J F_J \geq 0, \tag{3.26}$$

where,

$$F_0 = \begin{pmatrix} G_0 & 0 & 0 \\ 0 & G_0^{T_{A_2}} & 0 \\ 0 & 0 & G_0^{T_B} \end{pmatrix}, \quad F_J = \begin{pmatrix} G_J & 0 & 0 \\ 0 & G_J^{T_{A_2}} & 0 \\ 0 & 0 & G_J^{T_B} \end{pmatrix}, \tag{3.27}$$

to ensure the positivity of both $\tilde{\rho}$ and its partial transposes.

We could state the search for a PPT symmetric extension of ρ to two copies of A in the form of a SDP by setting $c = 0$ in (3.11) and imposing the LMI $F(\mathbf{x}) \geq 0$. If the extension does not exist, this will translate into the SDP being infeasible. However, due both to numerical and theoretical reasons, it is always convenient to work with strictly feasible problems. We can easily turn the search of PPT symmetric extensions into a strictly feasible problem. Consider the SDP

$$\begin{aligned} &\text{minimize} && t \\ &\text{subject to} && F(\mathbf{x}) + t\mathbb{1}_{AAB} \geq 0. \end{aligned} \tag{3.28}$$

It is clear that this problem is always strictly feasible, since we can strictly satisfy the LMI by choosing a value of t that is large enough. If the LMI $F(\mathbf{x}) \geq 0$ can be satisfied, then the optimum value of the objective function must satisfy $t_{\text{opt}} \leq 0$. On the other hand, if $t_{\text{opt}} > 0$, then $F(\mathbf{x}) \geq 0$ cannot be satisfied for any value of the variables $\mathbf{x}$, and hence no PPT symmetric extension exists. As we can see, the SDP (3.28) replaces the feasibility condition by a threshold value on the objective function. One of the advantages of this formulation is that it allows us to use the strong duality property of semidefinite programs, which will prove very useful when we discuss how to construct entanglement witnesses in the next chapter.

3.4.2.2 The k^{th} test

Implementing an arbitrary test in the hierarchy follows the same principles discussed in the previous section. We can use the bases $\{\sigma_i^A\}_{i=1}^{d_A^2}$ and $\{\sigma_j^B\}_{j=1}^{d_B^2}$ to construct a basis of hermitian matrices in $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B$ by taking tensor products, and write the most general hermitian matrix in this basis as

$$\tilde{\rho} = \sum_{\{i_l\}_{l=1}^{k+1}} \tilde{\rho}_{i_1 \ldots i_k i_{k+1}} \, \sigma_{i_1}^A \otimes \ldots \otimes \sigma_{i_k}^A \otimes \sigma_{i_{k+1}}^B. \tag{3.29}$$

Then we use the swap invariance requirement to impose constraints between the coefficients of this expansion. Any two coefficients whose indices corresponding to the copies of A are related by a permutation, must be equal, i.e.,

$$\tilde{\rho}_{i_1 \ldots i_k i_{k+1}} = \tilde{\rho}_{i_{\pi(1)} \ldots i_{\pi(k)} i_{k+1}}, \tag{3.30}$$

where π is any permutation of k elements. Note that the $(k+1)^{th}$ index corresponds to subsystem B and it is not part of the symmetrization. Imposing the extension property fixes the values of some of the remaining coefficients, giving

$$\tilde{\rho}_{i1 \ldots 1j} = \rho_{ij}. \tag{3.31}$$

Note that both (3.30) and (3.31) are not basis-independent statements, since they rely on the tensor product structure of the basis elements $(\sigma_{i_1}^A \otimes \ldots \otimes \sigma_{i_k}^A \otimes \sigma_{i_{k+1}}^B)$ and the properties of σ_i^A and σ_j^B given in (3.15), even though the swapping invariance and the extension property are basis-independent constraints.

The coefficients that have not been fixed by the swap invariance and extension property, will play the role of the variables in the SDP. Then $\tilde{\rho}$ will again take the form $G_0 + \sum_J x_J G_J$. The matrices G_0 and G_J are just linear combinations of the basis matrices $(\sigma_{i_1}^A \otimes \ldots \otimes \sigma_{i_k}^A \otimes \sigma_{i_{k+1}}^B)$. By construction, they are invariant under

swaps of copies of A, and they satisfy

$$\begin{aligned} \mathrm{Tr}_{A_2 \ldots A_k}[G_0] &= \rho, \\ \mathrm{Tr}_{A_2 \ldots A_k}[G_J] &= 0. \end{aligned} \tag{3.32}$$

This can be easily understood if we notice that the extension condition given by $\mathrm{Tr}_{A_2 \ldots A_k}[\tilde{\rho}] = \rho$ is just an inhomogeneous system of simultaneous linear equations. The matrix G_0 is a particular solution of the system, while the matrices G_J form a basis of the space of solutions of the associated homogeneous system.

As we mentioned before, the swapping invariance reduces the number of independent partial transposes that can be applied on $\tilde{\rho}$. To identify them, let us concentrate on the k copies of A for a moment. Because of the swapping symmetry, different partial transposes are specified *only by the number of copies* of A that are transposed. This gives us k different partial transposes. Consider the set of partial transposes given by $\{T_{A_1 \ldots A_l}, l = 1, \ldots, k\}$. We claim that positivity with respect to this set implies positivity with respect to any partial transpose. Let $T_{\mathcal{I}}$ represent the partial transpose with respect to some subset $\mathcal{I}$ of the subsystems, that satisfies $\mathcal{I} \neq \emptyset$ and $\bar{\mathcal{I}} \neq \emptyset$, where $\bar{\mathcal{I}}$ is the complement of $\mathcal{I}$. If $B \notin \mathcal{I}$, then $\mathcal{I}$ involves only some number l, between 1 and k, of copies of A. Because of the swapping symmetry, we can take these copies to be the first l copies, and then $\tilde{\rho}^{T_{\mathcal{I}}} = \tilde{\rho}^{T_{A_1 \cdots A_l}}$. If $B \in \mathcal{I}$ we can use the fact that

$$\tilde{\rho}^{T_{\mathcal{I}}} \geq 0 \Longleftrightarrow \left(\tilde{\rho}^{T_{\mathcal{I}}}\right)^T \geq 0. \tag{3.33}$$

But $\left(\tilde{\rho}^{T_{\mathcal{I}}}\right)^T = \tilde{\rho}^{T_{\bar{\mathcal{I}}}}$. But then $B \notin \bar{\mathcal{I}}$, and we have $\tilde{\rho}^{T_{\bar{\mathcal{I}}}} = \tilde{\rho}^{T_{A_1 \cdots A_l}}$ for some l,$1 \leq l \leq k$, as shown above. The case $\bar{\mathcal{I}} = \emptyset$ can be reduced, using (3.33), to the case $\mathcal{I} = \emptyset$, which corresponds to applying no partial transposes to $\tilde{\rho}$ at all.

The only partial transposes for which we need to impose positivity are given then by the set $\{T_{A_1 \ldots A_l}, l = 1, \ldots, k\}$. Together with the positivity condition on $\tilde{\rho}$ itself, we have a total of $(k+1)$ LMIs, which can be encoded in a block-diagonal matrix

$F(\mathbf{x})$ with $(k+1)$ blocks, in the form of (3.26), with

$$\begin{aligned} F_0 &= G_0 \oplus \left(\bigoplus_{l=1}^{k} G_0^{T_{A_1 \cdots A_l}} \right), \\ F_J &= G_J \oplus \left(\bigoplus_{l=1}^{k} G_J^{T_{A_1 \cdots A_l}} \right). \end{aligned} \tag{3.34}$$

Thus, we can implement the k^{th} test by plugging the matrices (3.34) in the SDP given by (3.28).

3.4.3 Resources needed to implement the tests

Stating our separability criteria as semidefinite programs has the advantage of allowing us to use the very efficient algorithms available to solve them. Since we are interested in employing these criteria as a practical tool, we need to study in detail the resources required in their implementation.

One possible approach to numerically solve a SDP involves the solution of a series of least squares problems [51]. If m is the number of variables (the number of components of the vector $\mathbf{x}$, or in our case the number of free coefficients in $\tilde{\rho}$), and the matrices F_J are $(n \times n)$ hermitian matrices, each least squares problem requires a number of operations that scales with problem size as $O(m^2 n^2)$. If the matrices F_J have a block-diagonal structure (as in our case), the problem breaks into idependent parts each requiring a number of operations that scales as before, but with n given by the size of the blocks, which lowers the computational resources required. The number of iterations required, i.e., the number of least squares problems that need to be solved, is known to scale no worse than $O(n^{1/2})$. Then, solving a SDP scales at most as $O(m^2 n^{5/2})$.

Consider the k^{th} test in the hierarchy. The number of variables is given by

$$m = \left[\binom{d_A^2 + k - 1}{k} - d_A^2 \right] d_B^2, \tag{3.35}$$

with d_A, d_B being the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$. The combinatorial number gives the number of independent coefficients after imposing the swap invariance, while the d_A^2 term takes into account the coefficients that are fixed by the extension property. The size of the matrices F_J is given by

$$n = d_A^{2k} d_B, \tag{3.36}$$

so the resources required scale at most as $O(d_A^{9k})$, which is polynomial on the system size for k fixed, but exponential on the number of copies of A. This is a rather undesirable behavior, since in practice we would like to apply these tests to detect entanglement of a given state (which fixes the size of the system), and we will be interested in how do the resources required grow if the state passes a given test in the hierarchy and we need to apply the next one. The scaling with respect to the number of copies seems to be the most important from a practical point of view. We will show in the next section that we could actually impose a stronger symmetry requirement on the extension $\tilde{\rho}$ that brings the scaling down to polynomial in the number of copies of A.

3.5 Exploiting the symmetry

As we pointed out before, any separable state in $\mathcal{H}_A \otimes \mathcal{H}_B$ of the form (3.1) has a PPT symmetric extension to $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B$, that we can explicitly write as

$$\tilde{\rho} = \sum p_i \, |\psi_i\rangle\langle\psi_i|^{\otimes k} \otimes |\phi_i\rangle\langle\phi_i|. \tag{3.37}$$

This extension is obviously invariant under swaps of copies of A, and we used this property to restrict the form of the matrices F_J in the LMI of our SDP. However, $\tilde{\rho}$ is invariant under a larger group of transformations, which can be used to restrict its form even further.

The symmetric subspace of $\mathcal{H}_A^{\otimes k}$, which we will note by $\mathcal{H}_{Sym(k,A)}$, has dimension

$$d_{S_k} = \binom{d_A + k - 1}{k}. \tag{3.38}$$

Let Π_k be the projector into $\mathcal{H}_{Sym(k,A)}$, which is given by

$$\Pi_k = \frac{1}{\sqrt{k!}} \sum_{\pi_k} P_{\pi_k}, \tag{3.39}$$

where the sum is over all permutations π_k of k elements, and P_{π_k} is the operator defined by

$$P_{\pi_k} |i_1 i_2 \dots i_k\rangle = |i_{\pi_k(1)} i_{\pi_k(2)} \dots i_{\pi_k(k)}\rangle. \tag{3.40}$$

Note that this generalizes the swap operators defined in (3.4) to all permutations of k elements. According to (3.40) we have the identity

$$P_{\pi_k} |\psi_i\rangle^{\otimes k} = |\psi_i\rangle^{\otimes k}, \tag{3.41}$$

which implies that

$$\Pi_k (|\psi_i\rangle\langle\psi_i|^{\otimes k}) \Pi_k = |\psi_i\rangle\langle\psi_i|^{\otimes k}. \tag{3.42}$$

Thus, the extension $\tilde{\rho}$ in (3.37) satisfies

$$(\Pi_k \otimes \mathbb{1}_B) \tilde{\rho} (\Pi_k \otimes \mathbb{1}_B) = \tilde{\rho}. \tag{3.43}$$

Equation (3.43) states that for any separable state ρ, *we can construct a PPT extension $\tilde{\rho}$ such that both its support and range are contained in $\mathcal{H}_{Sym(k,A)} \otimes \mathcal{H}_B$*. For an arbitrary ρ, we can now restrict our search to extensions that satisfy this property.

If $\{S_i^A\}$ is a basis of hermitian matrices having support and range in the symmetric subspace of $\mathcal{H}_A^{\otimes k}$, the constraint (3.43) implies that we only need to consider matrices G in (3.23) of the form $G = S_i^A \otimes \sigma_j^B$. Since a change of basis does not affect the positive semidefiniteness of a matrix, we could use this freedom to greatly simplify

the form of the matrices G. By transforming to a basis whose first elements are the basis vectors of $\mathcal{H}_{Sym(k,A)}$ tensored with the vectors of some basis of $\mathcal{H}_B$, the matrices G_J will take the block-diagonal form

$$G_J = \begin{pmatrix} G_J^{sym} & 0 \\ 0 & 0 \end{pmatrix}, \tag{3.44}$$

where G_J^{sym} has size $(d_{S_k} d_B)^2$, which scales at most as $O(k^{(d_A-1)})$ for fixed dimensions. This drastically reduces the size of the LMI $G_0 + \sum_J x_J G_J \geq 0$, since we only need to check positivity of the nonzero block.

The LMI $G_0 + \sum_J x_J G_J \geq 0$ corresponds to only one of the $(k+1)$ blocks in the matrix $F(\mathbf{x})$. However, we can show that a similar reduction in size occurs for all blocks. Consider the case of the block that corresponds to applying partial transposes to the first l copies of A. The LMI encoded by this block is

$$G_0^{T_{A_1 \ldots A_l}} + \sum_J x_J G_J^{T_{A_1 \ldots A_l}} \geq 0. \tag{3.45}$$

Since the matrices G_J have been chosen to satisfy $(\Pi_k \otimes \mathbb{1}_B) G_J (\Pi_k \otimes \mathbb{1}_B) = G_J$, in particular they satisfy

$$(\Pi_l \otimes \Pi_{k-l} \otimes \mathbb{1}_B) G_J (\Pi_l \otimes \Pi_{k-l} \otimes \mathbb{1}_B) = G_J, \tag{3.46}$$

with Π_l the projector onto the symmetric subspace of the first l copies of A, and Π_{k-l} the projector onto the symmetric subspace of the $(k-l)$ remaining copies. If we apply partial transposes with respect to the first l copies in (3.46), we get

$$(\Pi_l^T \otimes \Pi_{k-l} \mathbb{1}_B) G_J^{T_{A_1 \ldots A_l}} (\Pi_l^T \otimes \Pi_{k-l} \mathbb{1}_B) = G_J^{T_{A_1 \ldots A_l}}. \tag{3.47}$$

Π_l^T is still a projector onto a subspace of dimension d_{S_l}, although it does not have to be the symmetric subspace of l copies. But the key point is that Equation (3.47) tells us that *the matrices $G_J^{T_{A_1 \ldots A_l}}$ have range and support on the tensor product of*

two subspaces of dimension $d_{S_l} d_B$ *and* $d_{S_{k-l}} d_B$. By the same reasoning discussed above, we can perform a change of basis that will take the matrices $G_J^{T_{A_1 \cdots A_l}}$ into a block-diagonal form, whose only nonzero block has size $(d_{S_l} d_{S_{k-l}} d_B^2)^2$. Thus, the effective size of the block scales at most as $O(k^{2(d_A-1)})$. The number of variables is now $m = \left[\binom{d_A+k-1}{k}^2 - d_A^2 \right] d_B^2$, and the size of the matrix F in (3.28) scales no worse than $O(k^{2d_A-1})$, since the number of blocks is linear in k. Then the scaling of the resources needed to solve the SDP corresponding to the k^{th} test is no worse than $O(k^{(6d_A-4)})$, which is polynomial on the number of copies of party A.

3.6 Completeness of the hierarchy of tests

One of the most important properties of this new hierarchy of separability tests is that it can be shown to be *complete*. Any entangled state is guaranteed to fail one of the tests at some finite point in the hierarchy. This result allows us for the first time to have an algorithm that will detect an entangled state in a finite number of steps, although this number may be high for some states.

Even though the hierarchy is a new result, the proof of its completeness is not, since it can be obtained as a corollary of an already known result regarding the characterization of the possible equilibrium states of a system that interacts with a thermal bath. This result was obtained independently by Raggio et al. [39] and Fannes et al. [21]. It was noted by Werner [55] that this result could be interpreted as a characterization of separable states as the *only* states admitting symmetric extensions to any number of copies of one of its subsystems (with no PPT requirement). The same idea was independently rediscovered by Schumacher [43]. This characterization is very interesting from the theoretical point of view, and coupled with the efficient implementation of our separability tests as semidefinite programs, it becomes also very important from a practical point of view by closing the gap between efficient and complete separability criteria.

For the sake of completeness of this presentation, we will include a proof of this result that follows the one in [21], applied to the case of bipartite mixed states on

finite dimensional Hilbert spaces, and using some results more familiar to Quantum Information Theory. Before stating and proving the theorem, we need to introduce some useful concepts.

A density matrix $\tilde{\rho}_k$ in $\mathcal{H}_A^{\otimes k}$ is said to be *exchangeable* [10] if it is invariant under any permutation of the copies of $\mathcal{H}_A$, and for any $n > 0$ there is another density matrix $\tilde{\rho}_{(k+n)}$ in $\mathcal{H}_A^{\otimes(k+n)}$ that is also invariant under permutations of copies of A, and satisfies

$$\tilde{\rho}_k = \mathrm{Tr}_{A_{k+1}\ldots A_{k+n}}[\tilde{\rho}_{(k+n)}]. \tag{3.48}$$

This is the central concept in the following result [10, 41]

Theorem 3 (Quantum de Finetti Theorem) *Let $\tilde{\rho}_k$ be an exchangeable density matrix in $\mathcal{H}_A^{\otimes k}$. Then, there exists a unique probability measure $P(\varrho)$ on the space D_A of states in $\mathcal{H}_A$ such that*

$$\tilde{\rho}_k = \int_{D_A} \varrho^{\otimes k} P(\varrho) d\varrho. \tag{3.49}$$

We can see from this result that the exchangeability property strongly constraints the form of the state $\tilde{\rho}_k$. In fact, it restricts the state to be *separable* on the space $\mathcal{H}_A^{\otimes k}$, since (3.49) gives an explicit expansion of $\tilde{\rho}_k$ as a convex combination of product states. With this result, we can now present the proof of the following theorem.

Theorem 4 (Fannes et al., 1988) *Let ρ be a bipartite mixed state in $\mathcal{H}_A \otimes \mathcal{H}_B$. Then ρ has a symmetric extension to k copies of subsystem A for any k, if and only if, ρ is separable.*

Proof: One of the implications is trivial and follows the same reasoning presented in Theorem 1. Assume ρ is separable. Then we can write

$$\rho = \sum p_i \, |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|. \tag{3.50}$$

From this expression, we can write down explicitly a symmetric extension $\tilde{\rho}$ for any value of k, namely

$$\tilde{\rho} = \sum p_i \, |\psi_i\rangle\langle\psi_i|^{\otimes k-1} \otimes |\phi_i\rangle\langle\phi_i|, \tag{3.51}$$

and this completes the first part of the proof.

To prove the other implication, the idea is to use the existence of the extensions to construct a set of states in $\mathcal{H}_A^{\otimes k}$ that can be shown to be separable by using the Quantum de Finetti Theorem, and then show that this implies that the extensions themselves have to be separable. Let ρ be a state in $\mathcal{H}_A \otimes \mathcal{H}_B$ such that for any n, there is a symmetric extension of ρ in $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B$, which we will call $\tilde{\rho}_n$. Let us pick a fixed value k for the number of copies of party A. Let the set $\{b_i\}_{i=1}^{d_B^2}$ be a basis for the set hermitian operators in $\mathcal{H}_B$, such that $b_i > 0$ for all i (i.e., all these operators are positive definite), and in particular let us choose $b_1 = \mathbb{1}_B$, the identity in $\mathcal{H}_B$. Now we define the operator

$$\bar{\rho}_{b_i,k} = \mathrm{Tr}_B \left[(\mathbb{1}_{A^{\otimes k}} \otimes b_i) \tilde{\rho}_k \right], \tag{3.52}$$

where $\mathbb{1}_{A^{\otimes k}}$ is the identity on the k copies of party A. The operator $\bar{\rho}_{b_i,k}$ is positive semidefinite (PSD) and nonzero since all the operators b_i were taken to be positive. Then $\bar{\rho}_{b_i,k}$ is proportional to a state in $\mathcal{H}_A^{\otimes k}$, since it is hermitian and PSD. We can choose the operators b_i such that $\mathrm{Tr}[\bar{\rho}_{b_i,k}] = 1$, so that (3.52) is actually a normalized state in $\mathcal{H}_A^{\otimes k}$. The key point in constructing these states is that they are *exchangeable*. This can be easily seen from the fact that, by hypothesis, the state ρ has symmetric extensions for any number of copies, and by using (3.52) for these extensions we can generate states $\bar{\rho}_{b_i,(k+l)}$ for any $l > 0$, that are symmetric and satisfy

$$\bar{\rho}_{b_i,k} = \mathrm{Tr}_{A_{k+1} \ldots A_l} [\bar{\rho}_{b_i,(k+l)}], \tag{3.53}$$

which is the definition of an exchangeable state. Then, the state $\bar{\rho}_{b_i,k}$ satisfies the hypothesis of the Quantum de Finetti Theorem, and so we know there is a unique probability measure function $P_{b_i}(\varrho) \geq 0$, such that

$$\begin{aligned} \bar{\rho}_{b_i,k} &= \int_{D_A} \varrho^{\otimes k} P_{b_i}(d\varrho) \\ &= \int_{D_A} \varrho^{\otimes k} P_{b_i}(\varrho) d\varrho, \end{aligned} \tag{3.54}$$

where D_A represents the space of states in $\mathcal{H}_A$ (i.e., the set of hermitian, positive semidefinite operators of trace 1).

For each ϱ, we can think of $P_{b_i}(\varrho)$ as a functional applied to the operators b_i, which we will note F_ϱ, defined as $F_\varrho(b_i) = P_{b_i}(\varrho)$. This functional is *linear* on convex combinations of positive operators. To see this, let $\mu > 0$. Then $F_\varrho(\mu b_i + (1-\mu)b_j) = P_{\mu b_i+(1-\mu)b_j}(\varrho)$, where $P_{\mu b_i+(1-\mu)b_j}$ is the unique probability density that satisfies

$$\begin{aligned}
\bar{\rho}_{(\mu b_i+(1-\mu)b_j),k} &= \int_{D_A} \varrho^{\otimes k} P_{\mu b_i+(1-\mu)b_j}(\varrho) d\varrho \\
&= \mathrm{Tr}_B\left[(\mathbb{1}_{A^{\otimes k}} \otimes (\mu b_i + (1-\mu)b_j))\tilde{\rho}_k\right] \\
&= \mu\,\mathrm{Tr}_B\left[(\mathbb{1}_{A^{\otimes k}} \otimes b_i)\tilde{\rho}_k\right] + (1-\mu)\,\mathrm{Tr}_B\left[(\mathbb{1}_{A^{\otimes k}} \otimes b_j)\tilde{\rho}_k\right] \\
&= \int_{D_A} \varrho^{\otimes k} \left(\mu P_{b_i}(\varrho) + (1-\mu)P_{b_j}(\varrho)\right) d\varrho. \qquad (3.55)
\end{aligned}$$

The second equality in (3.55) holds because we are considering a convex combination of the operators b_i, which guarantees that $\mathrm{Tr}_B[(\mathbb{1}_{A^{\otimes k}} \otimes (\mu b_i + (1-\mu)b_j))\tilde{\rho}_k]$ is normalized. Then, by the uniqueness of the probability density in the Quantum de Finetti Theorem, we must have

$$P_{\mu b_i+(1-\mu)b_j}(\varrho) = \mu P_{b_i}(\varrho) + (1-\mu)P_{b_j}(\varrho), \qquad (3.56)$$

which translates into

$$F_\varrho(\mu b_i + (1-\mu)b_j) = \mu F_\varrho(b_i) + (1-\mu)F_\varrho(b_j). \qquad (3.57)$$

Then F_ϱ is a linear functional on convex combinations of positive states in $\mathcal{H}_B$.

Since F_ϱ is defined on a basis, then by linearity, there is a unique way of extending this functional to the whole space of operators in $\mathcal{H}_B$. So we have a linear, positive and continuous functional on a finite dimensional Hilbert space, and it is a well known result that any such functional can be written as

$$F_\varrho(b) = \mathrm{Tr}_B[\bar{\sigma}_\varrho b] \quad \forall b, \qquad (3.58)$$

for some *unique* positive semidefinite operator $\bar{\sigma}_\varrho$ in $\mathcal{H}_B$. This operator might not be a state in $\mathcal{H}_B$ since it needs not be normalized. We can then define a function

$$P(\varrho) = \mathrm{Tr}[\bar{\sigma}_\varrho], \tag{3.59}$$

that is nonnegative. If $P(\varrho)$ is nonzero, we can define $\sigma_\varrho = \bar{\sigma}_\varrho / P(\varrho)$. Then (3.58) takes the form

$$P_b(\varrho) = F_\varrho(b) = \mathrm{Tr}_B[\sigma_\varrho b] P(\varrho) \quad \forall b. \tag{3.60}$$

Note that since σ_ϱ is normalized, $P(\varrho) = P_{\mathbb{1}_B}(\varrho)$, which shows that $P(\varrho)$ is a probability density, since $P_{\mathbb{1}_B}$ is by construction. Using (3.60) in (3.54), we get

$$\begin{aligned} \bar{\rho}_{b_i,k} &= \int_{D_A} \varrho^{\otimes k} \,\mathrm{Tr}_B[\sigma_\varrho b_i]\, P(\varrho) d\varrho \\ &= \mathrm{Tr}_B \left[(\mathbb{1}_{A^{\otimes k}} \otimes b_i) \int_{D_A} \varrho^{\otimes k} \otimes \sigma_\varrho \, P(\varrho) d\varrho \right]. \end{aligned} \tag{3.61}$$

If $P(\varrho) = 0$ for some ϱ, we can define σ_ϱ arbitrarily, since it would not contribute to the integral in (3.61). Since (3.61) is valid for all the elements b_i of a basis of hermitian matrices in $\mathcal{H}_B$, by comparing the expression in the second line with (3.52), we can deduce that

$$\tilde{\rho}_k = \int_{D_A} \varrho^{\otimes k} \otimes \sigma_\varrho \, P(\varrho) d\varrho. \tag{3.62}$$

This means that $\tilde{\rho}_k$ is a separable state, since (3.62) is an explicit decomposition as a convex combination of product states. Furthermore, since $\tilde{\rho}_k$ is an extension of our original state ρ, we have

$$\begin{aligned} \rho &= \mathrm{Tr}_{A_2 \ldots A_k}[\tilde{\rho}_k] \\ &= \int_{D_A} \varrho \otimes \sigma_\varrho \, P(\varrho) d\varrho, \end{aligned} \tag{3.63}$$

which shows that ρ has to be a separable state. This concludes the proof of the theorem. □

Since a PPT symmetric extension is also just a symmetric extension, we have the

following corollary.

Corollary 1 *The only states that have PPT symmetric extensions to k copies of subsystem A for any k are the separable states.*

Thus, an entangled state cannot have infinite PPT extensions, and so it must fail one of the tests in the hierarchy at some finite point. This implies that the hierarchy is complete.

3.6.1 Other complete hierarchies

It is interesting to note that the PPT requirement is not essential for the completeness of the hierarchy. The existence of symmetric extensions is the key property that allows us to apply the Quantum de Finetti Theorem and show that the state must be separable. Then, we could generate another family of separability criteria in which each test searches for symmetric extensions of a state ρ without imposing any constraints on the partial transposes, and Theorem 4 proves that this hierarchy is *also* complete. We could still implement these tests using semidefinite programs. Moreover, these SDPs will require less resources, since not requiring positivity of the partial transposes reduces the size of the LMI. However, the PPT requirement seems to be more appealing in practice. First of all, it makes the second test in the hierarchy at least as powerful as the PPT criterion. And even though the PPT tests require more resources than the non-PPT tests, they are much more powerful in detecting entanglement, as we will discuss in the next chapter.

3.7 Computational complexity

Another interesting question about the separability problem involves determining its *computational complexity*, i.e., the resources needed to solve it in general (see [23]). The completeness of the hierarchy provides us with a tool that guarantees detection of any entangled state, and since we have analyzed the resources required to implement each test in the sequence, it seems that we have the right information to give an

answer about the computational complexity of the problem. However, we are missing a very important piece of information. Even though each test have been shown to scale polynomially with the number of copies, for fixed dimensions, we do not have any bounds on how high in the hierarchy we have to go to detect the entanglement of a given state. The completeness theorem tells us that any entangled will fail a test at some finite point k in the sequence, but it does not give any information about this value, so this approach is not very well suited to answer questions about complexity.

By using a different approach, it has been recently proven [27] that the separability problem is actually NP-hard, which means that solving it in general is at least as hard as solving any NP problem. This result puts our hierarchy into a new light. Even though solving separability is hard in general, the sequence of tests allows us to, in some sense, "order" the instances of the problem according to their difficulty, with the easiest ones being detected by the first tests, since they require less resources, and the more difficult requiring to go higher in the hierarchy. So even though we know that there have to be states for which we need to go arbitrarily high in the hierarchy to detect them, we still have many states for which the easiest tests are sufficient. In the next chapter we will discuss evidence that in fact, the lower tests seem to be very powerful at least for low dimensions.

3.8 Summary

We have introduced a new family of separability criteria. The criteria are based on the fact that bipartite separable states have an extension to any number of copies of one of its subsystems that is symmetric under swaps of these copies, and remains positive under all partial transposes. We can then construct a sequence of tests to study the separability of a state. We start by checking if the state is PPT (which can be considered as the search for a PPT extension to only one copy). If the state passes the test, we search for a PPT extension to two copies, and so on. Anytime a test is passed, no information can be obtained about the separability of the state, and we need to apply the next test in the sequence. But if a test is failed, the state cannot

be separable, and thus it must be entangled.

One of the advantages of this approach is that the search for these extensions can be stated as a semidefinite program, which is a type of convex optimization problem. Semidefinite programs have been extensively studied, and many efficient algorithms to solve them have been constructed. In particular they make the resources required to apply the tests scale polynomially on the number of copies, when the dimensions of the subsystems are fixed. The other important property of this family of tests is its completeness. Every entangled state has to fail one of the tests at some finite point in the sequence, which will depend on the sate. These two properties make this approach very appealing from both the theoretical and practical point of view, by providing us with a new characterization of separable states and a sequence of easily implementable tests that detect all entangled states.

Chapter 4

Characterization of entanglement witnesses and positive maps

In this chapter we will show how the duality structure of a semidefinite program can be exploited to generate a certificate of entanglement whenever a state fails one of the tests in the hierarchy introduced in the previous chapter. These certificates take the form of hermitian operators that have very interesting algebraic properties. We can exploit the connection between positive semidefinite hermitian operators with positive maps to give a characterization of the subset of strictly positive maps. We will also discuss concrete examples where we applied the hierarchy of separability criteria to analyze the entanglement of bipartite mixed states.

4.1 Introduction

4.1.1 Entanglement witnesses

Another approach to distinguishing separable and entangled states involves the concept of an *entanglement witness* [49, 29].

Definition 2 *An entanglement witness (EW) for a state ρ is a hermitian operator W that satisfies*

$$\mathrm{Tr}[\rho W] < 0 \quad \text{and} \quad \mathrm{Tr}[\rho_{sep} W] \geq 0, \tag{4.1}$$

where ρ_{sep} is any separable state.

From this definition it is clear that if (4.1) is satisfied, then the state ρ cannot be separable, and W gives a proof of that fact. We will say that W detects or "witness" the entanglement of the state ρ. Since an EW is an observable, it also provides a physical way of determining if a state is entangled. We can just measure W on a given state, and if the mean value of this measurement (given by $\mathrm{Tr}[\rho W]$) is less than zero, then the state must be entangled.

The properties of an EW have a very nice geometric interpretation in terms of properties of convex sets (see appendix A for a review of useful concepts in convexity). A very important result in convex analysis is the Hahn-Banach Theorem [42], which states that any two disjoint convex subsets of a vector space can be separated by an hyperplane that divides the vector space in two half spaces, where separation means that each subset is contained in a different half space. We will only need a particular case of this theorem.

Theorem 5 (Hahn-Banach) *Let S be a convex subset of a vector space V, and let p be a point in V such that $p \notin S$. Then there is an hyperplane H that separates S and p.*

Consider the vector space of hermitian operators. The set of separable states is a convex set in this space, since all its elements can be written as convex combinations of pure product states, which are then the extremal points of the set. An entangled state ρ is just a point in this vector space that does not belong to the set of separable states. Then, by the Hahn-Banach Theorem, there must be a separating hyperplane. We can associate with this hyperplane its normal vector, which is some hermitian operator that we can call W. We can see now that the equations in (4.1) use the inner product between hermitian matrices to state that ρ and the set of separable states belong to the different half spaces determined by the hyperplane associated with the hermitian operator W. This shows that the existence of entanglement witnesses is just a reflection of the geometric properties of the set of separable states, as we can see in Figure 4.1. From this geometric point of view, it is clear that we could give, in principle, a complete characterization of separability by means of entanglement

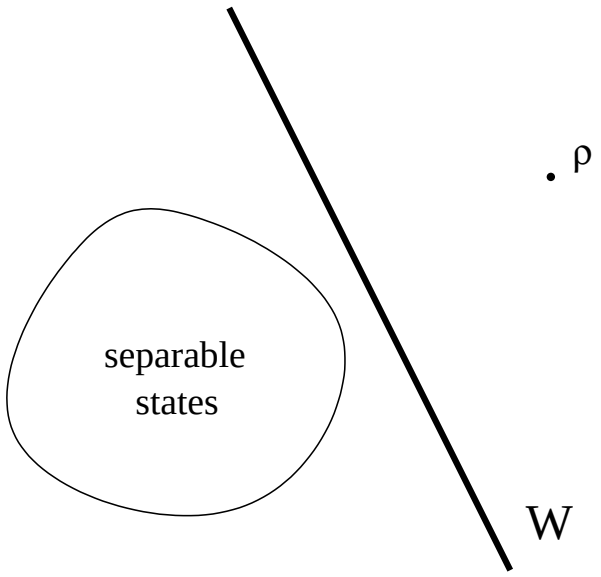


Figure 4.1: Hahn-Banach Theorem.

witnesses. A state is entangled, *if and only if*, there is an EW that detects the entanglement. Then, we could just determine if a state ρ is entangled or not by computing $\mathrm{Tr}[\rho W]$ for every entanglement witness W. Unfortunately, the lack of a complete characterization of the set of EWs in the general case, makes this approach not very useful in practice. This is analogous to the positive map approach to the separability problem discussed in Section 3.2.5, which gave necessary and sufficient conditions for separability, but was not a practical tool. This analogy is not a coincidence, since there is actually an isomorphism between entanglement witnesses and positive maps. We will discuss this in more detail later in this chapter.

4.1.2 Bihermitian form associated with an entanglement witness

Let $\{|i\rangle\}$ and $\{|j\rangle\}$ be bases of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, and let $|x\rangle = \sum_i x_i|i\rangle$ and $|y\rangle = \sum_j y_j|j\rangle$ be some arbitrary pure states, where x_i and y_j are complex numbers, satisfying $\sum_i |x_i|^2 = \sum_i |y_i|^2 = 1$. To every entanglement witness W we associate a

biquadratic bihermitian form given by

$$\begin{aligned} E_W(x,y) = \langle xy|W|xy\rangle &= \mathrm{Tr}[|x\rangle\langle x| \otimes |y\rangle\langle y|W] \\ &= \sum_{ijkl} W_{ijkl} x_i^* y_j^* x_k y_l, \end{aligned} \tag{4.2}$$

where the coefficients of the form are defined by

$$W_{ijkl} = \langle ij|W|kl\rangle. \tag{4.3}$$

The function $E_W(x,y)$ is just the mean value of the observable W on the pure product state $|xy\rangle$. Any entanglement witness W must satisfy $\mathrm{Tr}[\rho_{sep}W] \geq 0$. Let us recall that any separable state can be written as a convex combination of projectors into pure product states

$$\rho_{sep} = \sum_i p_i |x\rangle\langle x| \otimes |y\rangle\langle y|. \tag{4.4}$$

From this equation, it is not difficult to see that $\mathrm{Tr}[\rho_{sep}W] \geq 0$, if and only if, $\mathrm{Tr}[|x\rangle\langle x| \otimes |y\rangle\langle y|W] \geq 0$ for any pure product state $|x\rangle\langle x| \otimes |y\rangle\langle y|$. From (4.2) we can see that this condition translates into *a positivity requirement on the associated form* $E_W(x,y)$.

4.1.3 Decomposable entanglement witnesses

An entanglement witness W is called *decomposable* if it can be written as

$$W = P + Q^{T_A}, \tag{4.5}$$

were both P and Q are PSD operators. We can expand both these operators in the bases of their corresponding eigenvectors $\{|\psi_p\rangle\}$ and $\{|\phi_p\rangle\}$, which yields

$$\begin{aligned} P &= \sum_p \kappa_p |\psi_p\rangle\langle\psi_p| \\ Q &= \sum_p \lambda_p |\phi_p\rangle\langle\phi_p|, \end{aligned}$$

where the eigenvalues κ_p and λ_p must be nonnegative because of the positivity of both P and Q. The form associated with W is then

$$\begin{aligned} E_W(x,y) &= \langle xy|(P+Q^{T_A})|xy\rangle \\ &= \mathrm{Tr}[|x\rangle\langle x|\otimes|y\rangle\langle y|\,P] + \mathrm{Tr}[|x\rangle\langle x|\otimes|y\rangle\langle y|\,Q^{T_A}] \\ &= \mathrm{Tr}[|x\rangle\langle x|\otimes|y\rangle\langle y|\,P] + \mathrm{Tr}[(|x\rangle\langle x|)^T\otimes|y\rangle\langle y|\,Q] \\ &= \mathrm{Tr}[|x\rangle\langle x|\otimes|y\rangle\langle y|\,P] + \mathrm{Tr}[(|x^*\rangle\langle x^*|)\otimes|y\rangle\langle y|\,Q] \\ &= \sum_p |\sqrt{\kappa_p}\langle\psi_p|xy\rangle|^2 + \sum_p |\sqrt{\lambda_p}\langle\phi_p|x^*y\rangle|^2 \\ &= \sum_p |\sqrt{\kappa_p}\sum_{ij}\psi_{ij}^p x_i y_j|^2 + \sum_p |\sqrt{\lambda_p}\sum_{ij}\phi_{ij}^p x_i^* y_j|^2, \end{aligned} \tag{4.6}$$

with $|\psi_p\rangle = \sum_{ij}\psi_{ij}^p|ij\rangle$ and $|\phi_p\rangle = \sum_{ij}\phi_{ij}^p|ij\rangle$. On the third line of (4.6) we used the fact that $\mathrm{Tr}[MN^{T_X}] = \mathrm{Tr}[M^{T_X}N]$ (where X stands for any of the subsystems), and on the fourth line we used the hermiticity of the operator $|x\rangle\langle x|$ to replace its transpose by its complex conjugate, i.e., $(|x\rangle\langle x|)^T = |x^*\rangle\langle x^*|$, where $|x^*\rangle = \sum_i x_i^*|i\rangle$. We will make use of these results again later in this chapter.

From the last line of (4.6), we see that the form $E_W(x,y)$ has a very interesting property: it can be written as a *sum of squared magnitudes (SOS)*. This trivially proves that $E_W(x,y)$ is positive, which is equivalent to the property of W having a positive expectation value on all separable states, as discussed in the previous subsection.

This type of EW is closely related to entangled states that are non PPT. Let W be a decomposable EW for a certain entangled state ρ. Then we must have

$$\begin{aligned} 0 > \mathrm{Tr}[W\rho] &= \mathrm{Tr}[(P+Q^{T_A})\rho] \\ &= \mathrm{Tr}[P\rho] + \mathrm{Tr}[Q^{T_A}\rho] \\ &= \mathrm{Tr}[P\rho] + \mathrm{Tr}[Q\rho^{T_A}]. \end{aligned} \tag{4.7}$$

Then $\mathrm{Tr}[Q\rho^{T_A}]$ must be negative, since $\mathrm{Tr}[P\rho] \geq 0$ due to the fact that both P and ρ are PSD. But since Q is also PSD, we can conclude that ρ^{T_A} cannot be PSD: *a*

decomposable entanglement witness can only detect states that are not PPT.

There is also a converse to this result: *all entangled states that are not PPT can be detected by entanglement witnesses that are decomposable.* This can be seen as follows. Let ρ be an non PPT entangled state. Then ρ^{T_A} must have a negative eigenvalue associated with a certain eigenvector $|\omega\rangle$. Consider the observable $W = (|\omega\rangle\langle\omega|)^{T_A}$. Then

$$\begin{aligned} \mathrm{Tr}[W\rho] &= \mathrm{Tr}[(|\omega\rangle\langle\omega|)^{T_A}\rho] \\ &= \mathrm{Tr}[|\omega\rangle\langle\omega|\rho^{T_A}] \\ &= \langle\omega|\rho^{T_A}|\omega\rangle < 0. \end{aligned} \tag{4.8}$$

On the other hand,

$$\begin{aligned} E_W(x,y) &= \langle xy|W|xy\rangle \\ &= \mathrm{Tr}[|x\rangle\langle x| \otimes |y\rangle\langle y|(|\omega\rangle\langle\omega|)^{T_A}] \\ &= \mathrm{Tr}[|x^*\rangle\langle x^*| \otimes |y\rangle\langle y|(|\omega\rangle\langle\omega|)] \\ &= |\langle\omega|x^*y\rangle|^2 \geq 0, \end{aligned} \tag{4.9}$$

which proves that W is positive on pure product states, and hence on all separable states. From Equations (4.8) and (4.9) we can see that W is an entanglement witness for the state ρ, and since $(|\omega\rangle\langle\omega|)$ is obviously PSD, W is decomposable. The duality structure of semidefinite programs will allow us to use the hierarchy of separability tests to generalize this connection, and show that the set of entangled states breaks into different classes, each one related to entanglement witnesses whose associated forms have well-defined algebraic properties.

4.2 Duality structure and the construction of entanglement witnesses

In the previous chapter we introduced a family of separability tests that allows us to detect any entangled state. One of the most appealing characteristics of this hierarchy of tests was the fact that each test could be stated in the form of a semidefinite program. This fact allows us to employ the very efficient algorithms that have been developed to solve this type of problem. But there is another important advantage of this formulation that has to do with exploiting the duality structure of a semidefinite program.

4.2.1 Dual solutions and entanglement witnesses

Consider the SDP (3.28), and let us focus on the second test of the hierarchy, i.e., searching for PPT symmetric extensions to two copies of party A. In this case, the dual problem takes the form

$$\begin{aligned} \text{maximize} \quad & -\mathrm{Tr}[F_0 Z] \\ \text{subject to} \quad & Z \geq 0, \\ & \mathrm{Tr}[F_i Z] = 0, \\ & \mathrm{Tr}[Z] = 1, \end{aligned} \tag{4.10}$$

where F_0 has three blocks, associated with the extension and its two independent partial transposes, and from (3.25) we can see that it has the block-diagonal form

$$F_0 = \begin{pmatrix} G_0 & 0 & 0 \\ 0 & G_0^{T_{A_2}} & 0 \\ 0 & 0 & G_0^{T_B} \end{pmatrix}, \tag{4.11}$$

and so do the matrices F_i. Due to this block structure, we can restrict the search over Z in the dual program, to hermitian matrices that have the same form, so we

can take

$$Z = \begin{pmatrix} Z_0 & 0 & 0 \\ 0 & Z_1^{T_{A_2}} & 0 \\ 0 & 0 & Z_2^{T_B} \end{pmatrix}, \tag{4.12}$$

where the Z_i are operators in $\mathcal{H}_A^{\otimes 2} \otimes \mathcal{H}_B$. The positivity condition on Z in (4.10), translates into a positivity requirements for each of the blocks in (4.12). Using this structure we can write

$$\begin{aligned} \mathrm{Tr}[F_0 Z] &= \mathrm{Tr}[G_0 Z_0 + G_0^{T_{A_2}} Z_1^{T_{A_2}} + G_0^{T_B} Z_2^{T_B}] \\ &= \mathrm{Tr}[G_0 Z_0] + \mathrm{Tr}[G_0^{T_{A_2}} Z_1^{T_{A_2}}] + \mathrm{Tr}[G_0^{T_B} Z_2^{T_B}] \\ &= \mathrm{Tr}[G_0 Z_0] + \mathrm{Tr}[G_0 Z_1] + \mathrm{Tr}[G_0 Z_2] \\ &= \mathrm{Tr}[G_0 (Z_0 + Z_1 + Z_2)], \end{aligned} \tag{4.13}$$

since $\mathrm{Tr}[G_0^{T_X} Z_i^{T_X}] = \mathrm{Tr}[G_0 Z_i]$, for $i = 1, 2$ and $X = A, B$. We defined G_0 in Equation (3.22) as a linear function of ρ, so we can write $G_0 = \Lambda(\rho)$, where Λ is a linear map from hermitian matrices in $\mathcal{H}_A \otimes \mathcal{H}_B$ to hermitian matrices in $\mathcal{H}_A^{\otimes 2} \otimes \mathcal{H}_B$, whose action on an arbitrary operator Y is given by

$$\Lambda(Y) = Y \otimes \frac{\mathbb{1}_A}{d_A} + P\left(Y \otimes \frac{\mathbb{1}_A}{d_A}\right) P - \frac{\mathbb{1}_A}{d_A} \otimes \frac{\mathbb{1}_A}{d_A} \otimes \mathrm{Tr}_A[Y], \tag{4.14}$$

where P is the swap operator defined by $P|i\rangle_A \otimes |j\rangle_A \otimes |k\rangle_B = |j\rangle_A \otimes |i\rangle_A \otimes |k\rangle_B$. The adjoint map Λ^* acts in the opposite direction, mapping hermitian matrices in $\mathcal{H}_A^{\otimes 2} \otimes \mathcal{H}_B$ into hermitian matrices in $\mathcal{H}_A \otimes \mathcal{H}_B$, and its action on an operator V is given by

$$\Lambda^*(V) = \frac{1}{d_A}\left(\mathrm{Tr}_{A_2}[V] + \mathrm{Tr}_{A_2}[PVP] - \frac{\mathbb{1}_A}{d_A} \otimes \mathrm{Tr}_{A_1 A_2}[V]\right). \tag{4.15}$$

We can use this adjoint map to define an operator on $\mathcal{H}_A \otimes \mathcal{H}_B$, defined by

$$\tilde{Z} = \Lambda^*(Z_0 + Z_1 + Z_2). \tag{4.16}$$

We can now combine (4.13) and (4.16) to obtain

$$\begin{aligned} \mathrm{Tr}[\rho\tilde{Z}] &= \mathrm{Tr}[\rho\Lambda^*(Z_0 + Z_1 + Z_2)] \\ &= \mathrm{Tr}[\Lambda(\rho)(Z_0 + Z_1 + Z_2)] \\ &= \mathrm{Tr}[G_0(Z_0 + Z_1 + Z_2)] \\ &= \mathrm{Tr}[F_0 Z]. \end{aligned} \tag{4.17}$$

This equation allows us to establish a connection between the objective function of the dual program (4.10) and the expectation value of an observable $\tilde{Z}$ on the state ρ.

Let ρ_{sep} be any separable state. Then we know that there is a PPT symmetric extension of ρ_{sep}, or equivalently, the optimum value of the objective function of the primal problem (3.28) satisfies $t_{\mathrm{opt}} \leq 0$. From the weak duality property (3.13), we have

$$t + \mathrm{Tr}[F_0 Z] \geq 0, \tag{4.18}$$

for any feasible values of t and Z. In particular, this equation must hold for the optimum value t_{opt}, which means that

$$\mathrm{Tr}[F_0 Z] \geq -t_{\mathrm{opt}} \geq 0. \tag{4.19}$$

By combining this result with Equation (4.17) we get

$$\mathrm{Tr}[\rho_{sep}\tilde{Z}] \geq 0, \tag{4.20}$$

which holds *for any $\tilde{Z}$ obtained from a feasible dual solution Z.* This means that any operator $\tilde{Z}$ constructed in this way, satisfies one of the two properties required in (4.1), and is therefore a candidate for an entanglement witness.

Now consider the case in which the state ρ has no PPT symmetric extension to two copies of A, which implies that the state is entangled. In this case, the optimum value of t in (3.28) must satisfy $t_{\mathrm{opt}} > 0$. Since both the primal and dual problems are strictly feasible, we can use the strong duality property that implies that an optimal

dual solution Z_{opt} exists and satisfies

$$-\text{Tr}[F_0 Z_{\text{opt}}] = t_{\text{opt}} > 0. \tag{4.21}$$

We can use the adjoint map Λ^* to define an observable

$$\tilde{Z}_{EW} = \Lambda^*(Z_{\text{opt}}), \tag{4.22}$$

on the space $\mathcal{H}_A \otimes \mathcal{H}_B$. By using Equations (4.17) and (4.21) we can see that this observable satisfies

$$\text{Tr}[\rho \tilde{Z}_{EW}] < 0. \tag{4.23}$$

But since this observable was obtained from *a feasible solution* of the dual problem, Equation (4.20) tells us that it must *also* satisfy

$$\text{Tr}[\rho_{sep} \tilde{Z}_{EW}] \geq 0, \tag{4.24}$$

for *any* separable state ρ_{sep}. These last two equations prove that, if no PPT extension exists, *the optimal dual solution Z_{opt} can be used to construct an explicit entanglement witness $\tilde{Z}_{EW} = \Lambda^*(Z_{\text{opt}})$ for the state ρ.*

Even though we have shown the calculation explicitly only for the second test of the hierarchy, a similar reasoning can be applied to all tests to show that if the appropriate PPT symmetric extension does not exist, the optimal dual solution can be used to construct an entanglement witness for the state ρ. The EWs obtained in this way for each of the tests have very well-defined and interesting algebraic properties, that can also be used to interpret each step in the hierarchy as a search for EWs of a particular form.

4.2.2 Algebraic properties of the entanglement witnesses

For any EW there is an associated biquadratic bihermitian form given by (4.2). We have shown that the requirement that an entanglement witness W is positive on all

separable states, is equivalent to requiring the associated form $E_W(x, y)$ to be positive.

The first test in our hierarchy of separability criteria corresponds to the PPT criterion. In Section 4.1.3 we showed that all the entanglement witnesses that detect states that fail the first test, i.e., those that are not PPT, are decomposable. We also noted that the bihermitian form associated with these EWs had the property that it could be written as a SOS.

Now imagine that we have a state ρ that is PPT entangled, whose entanglement is detected by the second test of the hierarchy (ρ does not have a PPT symmetric extension to two copies of party A). In the previous section we have shown that the dual SDP will provide us with an entanglement witness $\tilde{Z}_{EW}$ for this state. Let us concentrate on the properties of $\tilde{Z}_{EW}$. First, it is clear that this EW cannot be decomposable, since decomposable EWs can only detect states that are not PPT. By setting $\rho_{sep} = |xy\rangle\langle xy|$ in (4.20), we have that

$$\begin{aligned} \mathrm{Tr}[|xy\rangle\langle xy|\tilde{Z}_{EW}] &= \langle xy|\tilde{Z}_{EW}|xy\rangle \\ &= E_{\tilde{Z}_{EW}}(x, y) \geq 0. \end{aligned} \tag{4.25}$$

According to Equation (4.17), we have

$$\mathrm{Tr}[|xy\rangle\langle xy|\tilde{Z}_{EW}] = \mathrm{Tr}[\Lambda(|xy\rangle\langle xy|)(Z_0 + Z_1 + Z_2)]. \tag{4.26}$$

The operator Λ maps a state ρ in $\mathcal{H}_A \otimes \mathcal{H}_B$ into an operator in $\mathcal{H}_A^{\otimes 2} \otimes \mathcal{H}_B$ that is invariant under swaps of the two copies of A and yields the original state ρ when one of the copies of A is traced out, but is in general not positive semidefinite. Now consider the state $|xxy\rangle\langle xxy|$. This state is invariant under swaps of copies of system A and also satisfies $\mathrm{Tr}_{A_2}[|xxy\rangle\langle xxy|] = |xy\rangle\langle xy|$. Then we know that there must exist some coefficients a_J such that

$$|xxy\rangle\langle xxy| = \Lambda(|xy\rangle\langle xy|) + \sum_J a_J G_J, \tag{4.27}$$

since the G_J form a basis of the space of matrices M satisfying the swapping symmetry and $\mathrm{Tr}_{A_2}[M] = 0$. According to (4.10) we have $\mathrm{Tr}[G_J Z_i] = 0$, and hence we can rewrite (4.26) as

$$\mathrm{Tr}[|xy\rangle\langle xy|\tilde{Z}_{EW}] = \mathrm{Tr}[|xxy\rangle\langle xxy|(Z_0 + Z_1 + Z_2)]. \tag{4.28}$$

Combining (4.25) and (4.28), we have

$$\langle xy|\tilde{Z}_{EW}|xy\rangle = \langle xxy|(Z_0 + Z_1 + Z_2)|xxy\rangle. \tag{4.29}$$

Since we are working with normalized states, we know that $\langle x|x\rangle = 1$, so we can multiply the left-hand side (LHS) of (4.29) by this factor without changing the equality, obtaining

$$E_{\tilde{Z}_{EW}}(x, y)\langle x|x\rangle = \langle xxy|(Z_0 + Z_1 + Z_2)|xxy\rangle. \tag{4.30}$$

This equation is, in principle, only valid when the variables x_i and y_i correspond to a normalized state, i.e., when they satisfy $\sum_i |x_i|^2 = 1$ and $\sum_i |y_i|^2 = 1$. However, since both sides of (4.30) are *homogeneous polynomials* of degree 2 on the x_i and the x_j^*, and of degree 1 on the y_i and the y_j^*, we can extend this equality to all values of the variables, and interpret (4.30) as an equality between two forms *that is satisfied everywhere*. But we can now rewrite the RHS of (4.30) as

$$\langle xxy|(Z_0 + Z_1 + Z_2)|xxy\rangle = \langle xxy|Z_0|xxy\rangle + \langle xx^*y|Z_1^{T_{A_2}}|xx^*y\rangle + \langle xxy^*|Z_2^{T_B}|xxy^*\rangle, \tag{4.31}$$

where we used the same properties discussed below Equation (4.6). Since $Z_0, Z_1^{T_{A_2}}$ and $Z_2^{T_B}$ are positive by construction, because they are obtained from a feasible solution of the SDP (4.10), this equation can be shown to give an explicit sum of squares (SOS) decomposition of the RHS of (4.30) in the same way as we did in Equation (4.6).

We can summarize these results as follows. The bihermitian form $E_{\tilde{Z}_{EW}}(x, y)$ must be positive since $\tilde{Z}_{EW}$ is an EW, but it cannot be a SOS because that would

imply that this EW is decomposable. However, Equations (4.30) and (4.31) show that $E_{\tilde{Z}_{EW}}(x,y)$ *can be written as a SOS when multiplied by the form* $\sum_i |x_i|^2$. This property holds for *any* entanglement witness obtained from the second test in the hierarchy.

We can perform a similar analysis if we consider the k^{th} test in the hierarchy. From the point of view of the SDP, the only difference is that the matrices F_J in (4.10) have $(k+1)$ blocks that correspond to the $(k+1)$ independent partial transposes as discussed in Section 3.4.2.2. In the same way as before we can define a map Λ mapping hermitian matrices in $\mathcal{H}_A \otimes \mathcal{H}_B$ to hermitian matrices in $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B$ that satisfies $G_0 = \Lambda(\rho)$, and use the adjoint map Λ^* to associate an entanglement witness $\tilde{Z}_{EW} = \Lambda^*(Z_{\text{opt}})$ with the optimal dual solution of the SDP (4.10), where Z_{opt} will also have a block diagonal structure with $(k+1)$ blocks, so we can write

$$Z_{\text{opt}} = Z_0 \oplus \left(\bigoplus_{l=1}^{k} Z_l^{T_{A_1} \ldots T_{A_l}} \right), \tag{4.32}$$

with each block being PSD. By studying the associated bihermitian form of this EW, we will obtain an analogous to Equation (4.29) of the form

$$\langle xy|\tilde{Z}_{EW}|xy\rangle = \langle x|^{\otimes k} \otimes \langle y| \left(\sum_{l=0}^{k} Z_l \right) |x\rangle^{\otimes k} \otimes |y\rangle. \tag{4.33}$$

We can multiply the LHS by $\langle x|x\rangle^{k-1} = 1$ without changing the equality, and this factor transforms the LHS into an homogeneous polynomial on the variables (x_i, x_j^*, y_k, y_l^*) of the same degrees as the RHS. We can then interpret the equation

$$E_{\tilde{Z}_{EW}}(x,y)\langle x|x\rangle^{k-1} = \langle x|^{\otimes k} \otimes \langle y| \left(\sum_{l=0}^{k} Z_l \right) |x\rangle^{\otimes k} \otimes |y\rangle, \tag{4.34}$$

as an identity between forms valid everywhere. By using the same properties of traces and partial transposes we used before, and the relation between partial transpose of a hermitian matrix and complex conjugation, we can rewrite the RHS of (4.34) to

obtain

$$\begin{aligned} E_{\tilde{Z}_{EW}}(x,y)\langle x|x\rangle^{k-1} &= \langle x|^{\otimes k} \otimes \langle y|Z_0|x\rangle^{\otimes k} \otimes |y\rangle + \\ &+ \sum_{l=1}^{k} \langle x^*|^{\otimes l} \otimes \langle x|^{\otimes k-l} \otimes \langle y|Z_l^{T_{A_1}\cdots T_{A_l}}|x^*\rangle^{\otimes l} \otimes |x\rangle^{\otimes k-l} \otimes |y\rangle. \end{aligned} \tag{4.35}$$

And as before, we can use the positivity of the matrices $Z_l^{T_{A_1}\cdots T_{A_l}}$, $l = 1, \ldots, k$, to see that the RHS of (4.35) gives an explicit decomposition of the LHS of (4.34) as a SOS. We can summarize these results in the following proposition.

Proposition 1 *The biquadratic bihermitian form associated with an EW obtained from the k^{th} test of the hierarchy, can be written as a SOS when multiplied by the SOS form $\langle x|x\rangle^{k-1} = \left(\sum_i |x_i|^2\right)^{k-1}$.*

We will say then that these EWs *satisfy the SOS property.*

As we discussed in Chapter 3, searching for symmetric extensions with no PPT requirement generates another complete family of separability criteria. For this family, Equation (4.30) takes the form

$$E_{\tilde{Z}_{EW}}(x,y)\langle x|x\rangle = \langle xxy|Z_0|xxy\rangle, \tag{4.36}$$

since now the LMI has only one block, corresponding to the positivity requirement on the extension. Since Z_0 is PSD, the RHS of (4.36) is also a SOS, so we will still say that $\tilde{Z}_{EW}$ satisfies the SOS property. The main difference between (4.36) and (4.31) is in the type of terms that appear in the sum of squares decomposition. Note that (4.36) involves only squares of polynomials in the variables (x_i, y_j) while the second and third terms on the RHS of (4.31) correspond to squares of polynomials in the (x_i^*, y_j, x_k) and (x_i, y_j^*) variables respectively. This situation extends to all the steps of the hierarchy. The SOS decomposition generated by the PPT family involves the squared magnitudes of all possible polynomials in the variables (x_i, y_j) *and their conjugates* that are compatible with the symmetry requirements, while the

SOS decomposition obtained from the non-PPT family involves squared magnitudes of polynomials involving *only* the variables (x_i, y_j). Thus, for any EW obtained from any of the two families, the associated bihermitian form becomes a SOS when multiplied by a certain power of the SOS form $(\sum_i |x_i|^2)$. However, the value of the power required need not be the same. The power required in the non-PPT case will be in general higher than for the PPT case, since the latter provides a decomposition that uses the same terms as the former plus more general terms.

4.3 A characterization of entanglement witnesses

We have shown that the duality structure of semidefinite programs allows us to construct an EW whenever a certain state ρ fails a test in our hierarchy of criteria, i.e., when ρ fails to have a PPT symmetric extension to a certain number of copies of subsystem A. We have seen that the EWs generated in this way have a very distinct algebraic property.

The completenes of the hierarchy proven in Theorem 4 guarantees that all entangled states must fail one of the tests at some point in the sequence. By using the duality structure, we can translate this result into a statement regarding entanglement witnesses.

Proposition 2 *All entangled states are detected by an entanglement witness that satisfies the SOS property.*

This result tells us that, of all possible entanglement witnesses, the subset that satisfies the SOS property is *sufficient* to detect *all* entangled states.

We presented our family of separability criteria as the search for an extension of the original state ρ that satisfied certain symmetries and had positive partial transposes, and showed that this search could be put in the primal form of a SDP. By considering the corresponding dual programs and the properties of the EWs generated by them, we can give the hierarchy a new interpretation. Given a state ρ, we try to prove its entanglement by searching for an entanglement witness. Since we cannot do a search

over all possible entanglement witnesses, because we lack a complete characterization of them, we split the search into a countably infinite family of different types of EWs, each class defined by the smallest value of k such that multiplication by $\langle x|x\rangle^{k-1} = (\sum_i |x_i|^2|)^{k-1}$ makes the associated bihermitian form a SOS. We can do these searches in sequence, increasing the value of k in each step, and implement them as a SDP.

The completeness result tells us that searching over the EWs that have the SOS property is enough to prove entanglement of any entangled state. This raises a very interesting question: *do all EWs have the SOS property*? Or, in other words, is the characterization of EWs provided by the properties of the associated form complete? We can use some basic properties of convex sets to show that most EWs satisfy the SOS property, and the ones that may not satisfy it are those that are extremal in the sense that their associated hyperplane touches the set of separable states. These are the *optimal* EWs introduced in [8].

This question is better addressed by using some concepts and results from convex analysis, that are reviewed in appendix A. Let S be the set of all unnormalized separable states, which is just the cone generated by the set of separable states. S is actually a closed convex cone. Its dual cone is $S^* = \{Z \,:\, \mathrm{Tr}[Z\rho_{sep}] \geq 0, \forall \rho_{sep} \in S\}$, which contains the set of all entanglement witnesses. Note that S^* is not exactly the set of entanglement witnesses, since it is not required that its elements detect some entangled state. An observable X that satisfies $\mathrm{Tr}[X\rho] \geq 0$ for all states, is in S^* but it is not an EW. If $(S^*)^o$ notes the *interior* of S^*, we have $(S^*)^o = \{Z \,:\, \mathrm{Tr}[Z\rho_{sep}] > 0, \forall \rho_{sep} \in S\}$. Then, we have the following result.

Theorem 6 *Let W be an entanglement witness such that $W \in (S^*)^o$. Then W has the SOS property, i.e., $\exists k$ such that $E_W(x,y)(\sum_i |x_i|^2)^k = SOS$.*

Proof: Let $S_k^* = \{Z \,:\, E_Z(x,y)(\sum_i |x_i|^2)^k = SOS\}$. These sets are closed convex cones. Clearly, $S_k^* \subset S_{k+1}^*$ and $S_k^* \subset S^*$. Now we define the set

$$O = \bigcup_{k=1}^{\infty} S_k^*. \tag{4.37}$$

O is a convex cone, although it may not be closed. We will now show that the dual of this cone is the set S. Let $\rho_{sep} \in S$. For any $Z \in O$, $\exists k$ such that $Z \in S_k^*$. But then $Z \in S^*$, so $\mathrm{Tr}[Z\rho_{sep}] \geq 0$, which means that $\rho_{sep} \in O^*$, so we have

$$S \subset O^*. \tag{4.38}$$

Now, let $\rho \in O^*$. Then, $\forall Z \in O$ we have $\mathrm{Tr}[Z\rho] \geq 0$. Since $S_k^* \subset O$ for all k, then we have in particular that $\mathrm{Tr}[Z\rho] \geq 0, \forall Z \in S_k^*$, which means that $\rho \in (S_k^*)^*$. We claim that this implies $\rho \in S$. To see this, assume $\rho \notin S$; then ρ is an entangled state. By the completeness of the hierarchy of separability tests, we know that there is a value of k for which $\mathrm{Tr}[Z\rho] < 0$ for some $Z \in S_k^*$, and then we must have $\rho \notin (S_k^*)^*$, which is a contradiction. Then

$$O^* \subset S. \tag{4.39}$$

From (4.38) and (4.39), we have $S = O^*$. Then we can use (A.9) to state that $S^* = \mathrm{cl}(O)$, which means

$$(S^*)^o \subset O. \tag{4.40}$$

If $W \in (S^*)^o$ then by (4.37) there exists k such that $W \in S_k^*$, and hence it has the SOS property. □

4.4 The geometric picture

Theorem 6 has a very nice geometric interpretation. It says that the sequence of convex cones S_k^* approximates the convex cone S^* from the inside, giving a complete characterization of its interior in terms of the SOS property (see Figure 4.2).

Since the set of all entanglement witnesses is contained in S^*, this characterization applies to all EWs that belong to $(S^*)^o$. The theorem does not apply to the EWs that lie on the boundary of S^*, which are the ones that satisfy $\mathrm{Tr}[Z\rho_{sep}] = 0$ for some separable state ρ_{sep}. These EWs may or may not satisfy the SOS property. Geometrically, they correspond to the EWs whose associated hyperplane is tangent

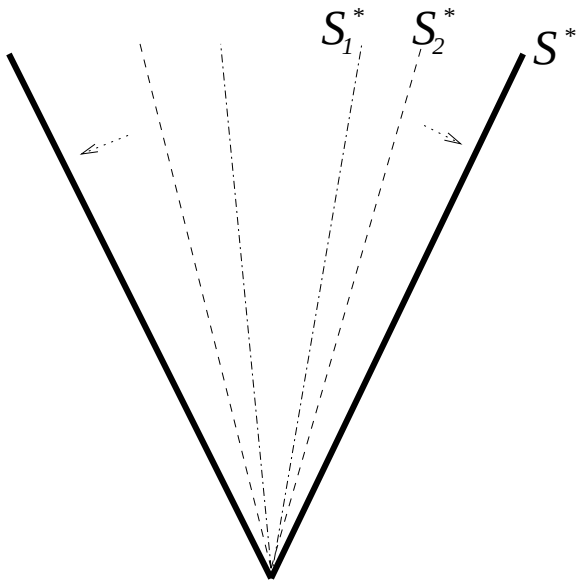


Figure 4.2: Sequence of cones approximating S^*.

to the set of separable states.

We have used concepts from convex analysis to give a nice geometric interpretation of the dual problem (4.10) in terms of the structure of the set of entanglement witnesses. We can carry out a similar analysis to give a geometric picture of the hierarchy of separability tests.

Let D_k be the set of states that have a PPT symmetric extension to k copies of subsystem A. It is easy to see that D_k is a convex set. Then, the cone generated by D_k, $C_k = \text{cone}(D_k)$ is a convex cone. Since a state that has a PPT symmetric extension to k copies, also has one to $(k-1)$ copies, we have $C_k \subseteq C_{k-1}$. The completeness theorem tells us that the only states having these extensions for any value of k are exactly the separable states. Then the convex cone S of unnormalized separable states satisfies

$$S = \bigcap_{k=1}^{\infty} C_k. \tag{4.41}$$

This means that the convex cone S is approximated *from the outside* by the convex cones C_k, as seen in Figure 4.3. Figures 4.3 and 4.2 reflect the duality of the SDP. The primal problem characterizes the cone S by generating a sequence of cones that ap-

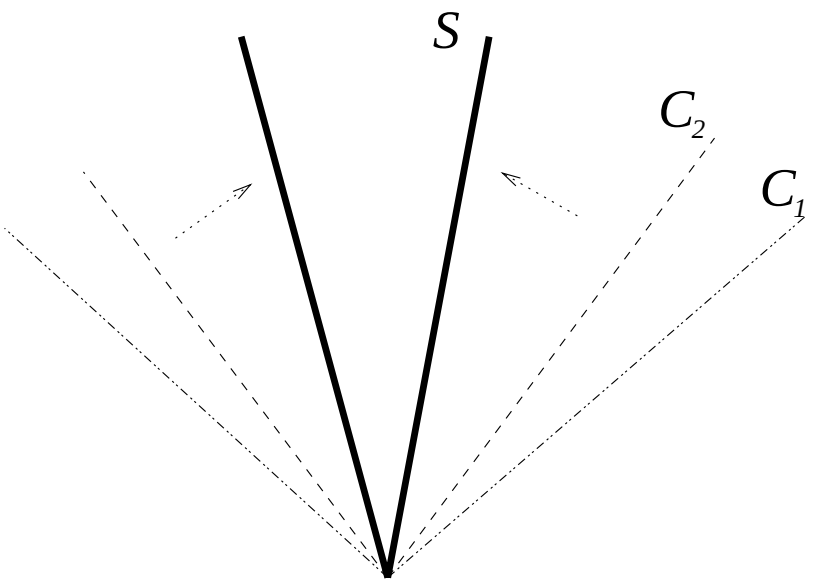


Figure 4.3: Sequence of cones approximating S.

proximate S from the outside, while the dual problem gives another characterization of it in terms of its dual cone S^* by generating a sequence of cones that approximate S^* from the inside.

4.5 Positive maps

It has been known for quite some time that there is a close relationship between entanglement witnesses, positive bihermitian forms and positive maps [12, 57]. In particular, this relationship was exploited in [29] to give a complete characterization of the separability problem in terms of positive maps. We will now show how to translate the properties of the entanglement witnesses generated by our hierarchy of separability tests into a characterization of the set of strictly positive maps.

Let us recall the definition of a positive map. Let $\mathcal{A}_A$ and $\mathcal{A}_B$ be the set of linear operators acting on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, and $\mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$ the set of linear maps from $\mathcal{A}_A$ to $\mathcal{A}_B$. We say that a map $\Lambda \in \mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$ is *positive*, if for any operator $A \in \mathcal{A}_A$, $A \geq 0$ implies $\Lambda(A) \geq 0$. A *completely positive* (CP) map, is a map Λ such

that the induced map Λ_n

$$\Lambda_n = \Lambda \otimes \mathbb{1}_n : \mathcal{A}_A \otimes \mathcal{A}_n \to \mathcal{A}_B \otimes \mathcal{A}_n, \tag{4.42}$$

is positive for all n, with $\mathcal{A}_n$ being the space of operators in a Hilbert space of dimension n and $\mathbb{1}_n$ the identity map on that space.

It is clear that any CP map is also a positive map. However, there are positive maps that are not CP. This has very important consequences on the study of entanglement of quantum states. In particular, there is a one to one correspondence [29] between entanglement witnesses and positive non-CP maps. Since the hierarchy of separability tests offers a characterization of the interior of the set of entanglement witnesses, it is not difficult to translate this characterization to the set of positive non-CP maps. To do this, we use the fact that for any linear operator $L \in \mathcal{A}_A \otimes \mathcal{A}_B$, we can define a map $\Lambda \in \mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$ by

$$\langle k|\Lambda(|i\rangle\langle j|)|l\rangle = \langle i| \otimes \langle k|L|j\rangle \otimes |l\rangle. \tag{4.43}$$

Conversely, Equation (4.43) can be used to uniquely construct the operator A from the map Λ. Equivalently, we can write [33]

$$\Lambda(\rho) = \mathrm{Tr}_A \left[L(\rho^T \otimes \mathbb{1}_B) \right], \tag{4.44}$$

where ρ is any operator in $\mathcal{A}_A$. Note that the same operator $L \in \mathcal{A}_A \otimes \mathcal{A}_B$ can be used to define two different maps, one in $\mathcal{L}(\mathcal{A}_A, \mathcal{A}_B)$ and one in $\mathcal{L}(\mathcal{A}_B, \mathcal{A}_A)$. It has been shown [33] that this relationship gives in fact a one to one correspondence between entanglement witnesses, i.e., hermitian operators that are positive on separable states but have a negative eigenvalue, and positive non-CP maps. It also gives a correspondence between CP maps and PSD matrices. By using (4.44) it is not dificult to see that the interior of the set of entanglement witnesses, which correspond to those Z that satisfy $\mathrm{Tr}[Z\rho_{sep}] > 0$ for any separable state ρ_{sep}, is mapped onto the set of positive maps that map any nonzero positive semidefinite operator into a *positive*

definite operator. Our characterization of entanglement witnesses will translate into a characterization of this subset of positive maps, which is the set of strictly positive maps. The maps that are left out are those that send at least one PSD operator that is not positive definite into a another PSD operator that is not positive definite.

Theorem 6 showed that any Z in the interior of the cone S^* (which contains all entanglement witnesses) has the SOS property. Since they correspond to strictly positive maps (the ones that map any nonzero PSD operator into a positive definite operator), we can characterize these maps by associating a biquadratic bihermitian form directly to the map, using Equation (4.43). Then we can state that a map is strictly positive only if the form

$$\begin{aligned} E_\Lambda(x,y) &= \langle y|\Lambda(|x^*\rangle\langle x^*|)|y\rangle \\ &= \sum_{ijkl}(\langle k|\Lambda(|i\rangle\langle j|)|l\rangle)x_i^* y_k^* x_j y_l \end{aligned} \tag{4.45}$$

has the SOS property.

We can also give a characterization in a language that only involves statements about maps, without reference to the associated forms. To do this we need to analyze in more detail some of the properties of the EWs generated by the SDP. Let us consider the family of separability criteria that searches for symmetric extensions of a certain state, but does not require positive partial transposes. In this case we have

$$\langle xxy|(Z_{EW}\otimes \mathbb{1}_A)|xxy\rangle = \langle xxy|Z_0|xxy\rangle, \tag{4.46}$$

for all states $|x\rangle$ and $|y\rangle$, with $Z_0 \geq 0$. This is just an equivalent form of Equation (4.36). It is not difficult to show that this equality implies that the operators $Z_{EW}\otimes\mathbb{1}_A$ and Z_0 actually *coincide* when they are restricted to the subspace given by $\mathcal{H}_{Sym_{(k,A)}}\otimes \mathcal{H}_B$. Furthermore, this is true for any number of copies of system A. If we denote by Π_k the projector onto $\mathcal{H}_{Sym_{(k,A)}}$ (the symmetric subspace of $\mathcal{H}_A^{\otimes k}$), we have

$$\Pi_k\otimes\mathbb{1}_B(Z_{EW}\otimes\mathbb{1}_{A^{\otimes(k-1)}})\Pi_k\otimes\mathbb{1}_B = (\Pi_k\otimes\mathbb{1}_B)Z_0(\Pi_k\otimes\mathbb{1}_B). \tag{4.47}$$

Since Z_0 is PSD on the space $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B$, its restriction to the tensor product of $\mathcal{H}_{Sym_{(k,A)}}$ and $\mathcal{H}_B$ remains PSD, which is the RHS of (4.47). The completeness theorem of Section 3.6 then tells us that if Z_{EW} is a strictly positive entanglement witness, then there must exist a finite k for which Equation (4.47) is true.

We can now use the isomorphism defined by (4.43) to restate (4.47) in terms of properties of maps. First we use the fact that this isomorphism gives a one to one correspondence between PSD operators in $\mathcal{A}_A \otimes \mathcal{A}_B$ and CP maps in $\mathcal{L}(\mathcal{A}_B, \mathcal{A}_A)$ [33]. Let $\Lambda : \mathcal{A}_B \to \mathcal{A}_A$ be the positive non CP map associated with Z_{EW}, and let $\bar{\Lambda}_k : \mathcal{A}_A \to \mathcal{A}_{Sym(k,A)}$ be defined by $\bar{\Lambda}_k(\rho) = \Pi_k(\rho \otimes \mathbb{1}_{A^{\otimes(k-1)}})\Pi_k$. Equation (4.44) can be used to check that the map associated with the operator $\Pi_k \otimes \mathbb{1}_B(Z_{EW} \otimes \mathbb{1}_{A^{\otimes(k-1)}})\Pi_k \otimes \mathbb{1}_B$ is given by

$$\left(\bar{\Lambda}_k \circ \Lambda\right) : \mathcal{A}_B \to \mathcal{A}_{Sym(k,A)}. \tag{4.48}$$

But since the RHS of (4.47) is PSD, this map has to be *completely positive*.

On the other hand, if Λ is not a positive map, then the map $\left(\bar{\Lambda}_k \circ \Lambda\right)$ cannot be completely positive for any k. This is true because the map $\bar{\Lambda}_k$ always maps a non PSD matrix into a non PSD matrix, as we can easily show. Let $|i\rangle$ be an eigenvector of a non PSD operator σ in $\mathcal{H}_A$, with negative eigenvalue. Then $\langle i|\sigma|i\rangle < 0$. For any k, the vector $|i\rangle^{\otimes k}$ belongs to the symmetric subspace $\mathcal{H}_{Sym_{(k,A)}}$ and satisfies $\Pi_k|i\rangle^{\otimes k} = |i\rangle^{\otimes k}$. Then we have

$$\begin{aligned} \langle i|^{\otimes k}\bar{\Lambda}_k(\sigma)|i\rangle^{\otimes k} &= \langle i|^{\otimes k}\,\Pi_k(\sigma \otimes \mathbb{1}_{A^{\otimes(k-1)}})\Pi_k\,|i\rangle^{\otimes k} \\ &= \langle i|^{\otimes k}(\sigma \otimes \mathbb{1}_{A^{\otimes(k-1)}})|i\rangle^{\otimes k} \\ &= \langle i|\sigma|i\rangle < 0, \end{aligned} \tag{4.49}$$

and so $\bar{\Lambda}_k(\sigma)$ cannot be PSD. Thus, we have the following result.

Theorem 7 *If the map $\Lambda : \mathcal{A}_B \to \mathcal{A}_A$ is strictly positive, then there is a finite k such that the map $\left(\bar{\Lambda}_k \circ \Lambda\right) : \mathcal{A}_B \to \mathcal{A}_{Sym(k,A)}$ is completely positive. If for some k the map $\left(\bar{\Lambda}_k \circ \Lambda\right)$ is completely positive, then Λ is a positive map.*

4.6 Examples

We have applied the second test of the hierarchy to many bound entangled states found in the literature of dimensions up to 6 by 6. In all cases, this test has been *sufficient* to demonstrate entanglement and construct numerical (and in some cases analytical) entanglement witnesses. Even though we know that from complexity arguments that there should be entangled states that pass this test (i.e., they have a PPT symmetric extension to two copies of A), we have not been able to find an example of this type of state. This is very encouraging from the practical point of wiew, since it suggests that the second test is very powerful for low dimensions.

We present now in some detail, two examples of PPT entangled states for which we applied the second test of the hierarchy to prove entanglement and construct the appropriate entanglement witnesses. We used MATLAB to code the corresponding SDP, and used the package SEDUMI [47] to solve it.

4.6.1 $3 \otimes 3$ state.

We consider the following state, described in [31], given by

$$\rho_\alpha = \frac{2}{7}|\psi_+\rangle\langle\psi_+| + \frac{\alpha}{7}\sigma_+ + \frac{5-\alpha}{7}P\sigma_+P, \tag{4.50}$$

with $0 \leq \alpha \leq 5$, $|\psi_+\rangle = \frac{1}{\sqrt{3}}\sum_{i=0}^{2}|ii\rangle$, $\sigma_+ = \frac{1}{3}(|01\rangle\langle 01| + |12\rangle\langle 12| + |20\rangle\langle 20|)$ and P the operator that swaps the two systems (note they are both the same space). Notice that ρ_α is invariant under the simultaneous change of $\alpha \to 5-\alpha$ and interchange of the parties. The state is separable for $2 \leq \alpha \leq 3$ and not PPT for $\alpha > 4$ and $\alpha < 1$, which was proved in [12] by using a positive map that is not completely positive. Our code solved the SDP for this state in about 5 seconds on a desktop computer. From this solution, numerical entanglement witnesses can be constructed for ρ_α in the range $3+\epsilon < \alpha \leq 4$ (and $1 \leq \alpha < 2-\epsilon$) with $\epsilon \geq 10^{-8}$. By examining the numerical form of the witnesses in the limit $\alpha \to 3^+$, we extracted a witness that

shows entanglement for all $\alpha > 3$, that is given by

$$\begin{aligned}\tilde{Z}_{EW} &= 2\left(|00\rangle\langle 00| + |11\rangle\langle 11| + |22\rangle\langle 22|\right) + \\ &\quad + |02\rangle\langle 02| + |10\rangle\langle 10| + |21\rangle\langle 21| - 3|\psi_+\rangle\langle\psi_+|.\end{aligned}$$

From this entanglement witness, the Choi form [12], which is actually the basis for constructing the state (4.50), can be recovered. Since this observable is obtained from the dual program corresponding to the second test of the hierarchy, it satisfies the SOS property, and can be shown to be explicitly nonnegative on separable states by the identity

$$\begin{aligned}4\langle xy|\tilde{Z}_{EW}|xy\rangle\langle x|x\rangle &= |2\,x_0x_1y_2^* - x_2x_0y_1^* - x_1x_2y_0^*|^2 \\ &+ |2x_0x_0^*y_0 - 2x_1x_0^*y_1 + x_1x_1^*y_0 - x_2x_0^*y_2|^2 \\ &+ |2x_0x_0^*y_2 - 2x_1x_2^*y_1 + x_2x_2^*y_2 - x_0x_2^*y_0|^2 \\ &+ |2x_0x_1^*y_0 - 2x_2x_2^*y_1 + x_2x_1^*y_2 - x_1x_1^*y_1|^2 \\ &+ 3\,|x_2x_0y_1^* - x_1x_2y_0^*|^2 + 3\,|x_1x_1^*y_0 - x_2x_0^*y_2|^2 \\ &+ 3\,|x_2x_2^*y_2 - x_0x_2^*y_0|^2 + 3\,|x_2x_1^*y_2 - x_1x_1^*y_1|^2 \geq 0.\end{aligned}$$

The expected value of this observable on the original state is $\mathrm{Tr}[\tilde{Z}_{EW}\rho_\alpha] = \frac{1}{7}(3-\alpha)$, which demonstrates entanglement for all $\alpha > 3$. Applying the non-PPT hierarchy to this state fails to show entanglement for $\alpha \leq 3.84$, even if we apply the sixth test in this hierarchy, showing that it is considerable weaker than the PPT hierarchy.

4.6.2 $4 \otimes 4$ state

We consider next the $4 \otimes 4$ state given by

$$\rho_\alpha = \frac{1}{2+\alpha}(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| + \alpha\cdot\sigma), \quad \alpha \geq 0, \tag{4.51}$$

where

$$\begin{aligned}
\psi_1 &= \frac{1}{2}(|00\rangle + |11\rangle + \sqrt{2}\,|22\rangle), \\
\psi_2 &= \frac{1}{2}(|01\rangle + |10\rangle + \sqrt{2}\,|33\rangle), \\
\sigma &= \frac{1}{8}(|02\rangle\langle 02| + |03\rangle\langle 03| + |12\rangle\langle 12| + |13\rangle\langle 13| + \\
&\quad + |20\rangle\langle 20| + |21\rangle\langle 21| + |30\rangle\langle 30| + |31\rangle\langle 31|).
\end{aligned}$$

Applying the PPT criterion yields provable entanglement only for those states with $\alpha < 2\sqrt{2} \approx 2.82843$. It was suspected [26] that the state was actually entangled for all nonnegative values of α. Again, using the second test, we showed that this is indeed the case and provided an explicit entanglement witness. Using essentially the same approach as in the example above, from the dual solution of the semidefinite program we can identify a particular witness

$$\begin{aligned}
W &= (|22\rangle - |00\rangle)(\langle 22| - \langle 00|) + (|22\rangle - |11\rangle)(\langle 22| - \langle 11|) + \\
&\quad + (|33\rangle - |01\rangle)(\langle 33| - \langle 01|) + (|33\rangle - |10\rangle)(\langle 33| - \langle 10|) + \\
&\quad + |23\rangle\langle 23| + |32\rangle\langle 32| - |22\rangle\langle 22| - |33\rangle\langle 33|.
\end{aligned}$$

This witness is nonnegative on all product states, as the following identity certifies.

$$\begin{aligned}
\langle xy|W|xy\rangle\langle x|x\rangle &= |x_0x_0^*y_0 + x_1x_1^*y_0 - x_2x_0^*y_2 - x_3x_1^*y_3|^2 + \\
&\quad |x_0x_0^*y_1 + x_1x_1^*y_1 - x_2x_1^*y_2 - x_3x_0^*y_3|^2 + \\
&\quad |x_2x_2^*y_2 + x_3x_3^*y_2 - x_0x_2^*y_0 - x_1x_2^*y_1|^2 + \\
&\quad |x_2x_2^*y_3 + x_3x_3^*y_3 - x_1x_3^*y_0 - x_0x_3^*y_1|^2 + \\
&\quad |x_1x_3y_2^* - x_0x_2y_3^*|^2 + |x_0x_3y_2^* - x_1x_2y_3^*|^2 + \\
&\quad |x_1x_2y_0^* - x_0x_2y_1^*|^2 + |x_0x_3y_0^* - x_1x_3y_1^*|^2 \geq 0.
\end{aligned}$$

Applying the witness W to the state (4.51), we obtain $\mathrm{Tr}[W\rho_\alpha] = -\frac{2(\sqrt{2}-1)}{2+\alpha} < 0$, therefore certifying entanglement for *all* values of α in the allowable range.

4.7 Summary

We have seen that the duality structure of the SDP used to implement the separability tests introduced in Chapter 3 provides us with an explicit construction of an entanglement witness for a state ρ, that has been shown to be entangled by one of the tests. The entanglement witnesses generated in this way have a very nice algebraic property: their associated bihermitian form becomes a sum of squared magnitudes when multiplied by a certain positive form that it is also a SOS. This property can be used as an explicit proof for the positivity of the form, which is equivalent to the requirement that the corresponding EW must have a nonnegative expectation value on all separable states.

This property of the entanglement witnesses generated by the dual program, and the hierarchichal structure of the separability tests, allows us to give an interpretation of this approach to the separability problem in terms of entanglement witnesses. To detect the entanglement of a state, we just search for an entanglement witness for it, but we do it in a sequence of searches, each one restricted to entanglement witnesses of a certain form, which is determined by the properties of the associated bihermitian form. The key points are that searching over these restricted classes can be implemented as a semidefinite program, and these classes of EWs are sufficient to detect entanglement of any state.

We have applied this approach to many PPT entangled states found in the literature. For all cases tested so far, with dimensions of up to 6 by 6, the second test of the hierarchy has been sufficient to show entanglement. By studying the numerical EWs constructed by the dual program, we can also extract an EW that can show entanglement for a parameterized family of states. This is very useful, since every EW that we construct can be added to our entanglement toolbox, since it may help to show entanglement for some other family of states.

The connection of the separability problem with other important problems in algebraic geometry and linear algebra, allowed us to translate important results from one setting to another and develop a sort "mapping" between characterizations of

entangled states, positive bihermitian forms and positive maps. The completeness of the hierarchy implies in the case of bihermitian forms, an extension to the complex case of the positive solution to Hilbert's 17^{th} problem [40], which states that all positive real forms can be written as a quotient of positive forms that are a sum of squares. Our result implies that the same is true for strictly positive bihermitian forms. And for maps, it provides a characterization of strictly positive maps in terms of their extendability to completely positive maps in a larger space, as well as in terms of an associated bihermitian form.

Chapter 5

Local manipulations of three-qubit pure states

In this chapter we will study deterministic local transformations of three-qubit pure states. We will be interested in characterizing the set of states that can be obtained from a given state by letting the three parties A, B and C (which following the usual quantum information convention we will refer to as Alice, Bob and Charlie) apply only local operations, such as local unitaries and local measurements, and communicate through a classical channel, colectively known as LOCC (local operations and classical communication).

5.1 Introduction

The study of the transformations that are possible when using only local operations and classical communication (LOCC) is very useful since it allows us to classify entangled states and it can be used as one way of quantifying this resource. Two states that are related by local unitary transformations are considered equivalent as far as entanglement is concerned, since both states can be reversibly obtained from each other, and local operations cannot increase entanglement. The action of the group of local unitaries then breaks the space of states into *orbits* [34]. Then, to transform a pure state into another state in a different orbit by local operations, we need to allow each party to apply a local generalized measurement, i.e., a POVM, on their part of the state.

For bipartite pure states, the problem of deterministically transforming one state into another has been solved by Nielsen [36], who gave necessary and sufficient conditions for a given transformation to be achievable with probability 1. Later Vidal [53] extended this result by calculating the maximal probability of success of any LOCC transformation of bipartite pure states. For more than two parties, this problem is still unsolved. The bipartite case seems to be very special due to the existence of the Schmidt decomposition. As we briefly discussed in Chapter 2, any pure bipartite state can be transformed, by applying local unitaries, into a state of the form

$$|\psi\rangle = \sum_{i}^{n} \lambda_i |ii\rangle, \tag{5.1}$$

where the λ_i are positive real numbers, $|ii\rangle = |i\rangle_A \otimes |i\rangle_B$, and $\{|i\rangle_A\}$,$\{|i\rangle_B\}$ are orthonormal vectors on each of the subsystems. This greatly simplifies the analysis of LOCC transformations: it gives a canonical expression for states in a given orbit, and allows the reduction of an arbitrary LOCC protocol to a protocol in which one party applies local unitaries and local POVMs, and the other party only has to apply a local unitary, conditional on the results obtained by the first party [35]. For multipartite states with three parties or more there is no known reduction of LOCC protocols.

For a system of three qubits, several Schmidt-like decompositions have been proposed [9, 1], all based on the idea of using local unitaries to get rid of as many coefficients as possible. One interesting property that emerges from these decompositions is that in general it is not possible to make all the coefficients real. In particular there are states that have at least one coefficient that is complex for any local basis, and this has as a consequence that these states are not locally unitarily equivalent to their conjugates (the states obtained by taking the complex conjugate of the coefficients). This contrasts with the bipartite case in which, since the Schmidt decomposition has only real coefficients, every state is in the same orbit as its conjugate.

A POVM applied to a state has, in general, outcomes that belong to different orbits. However, a protocol that transforms a state into another with probability 1, *has to include at least one* POVM for which all outcomes are in the same orbit. For

instance, this has to be the case for the last POVM of the protocol: if its outcomes are not in the same orbit, then the protocol has not achieved the transformation with probability 1. We will call a POVM with this property a *deterministic* POVM, because we can use such a POVM and suitable local unitaries, to obtain any state in the orbit of the outcomes with probability 1, attaining a deterministic transformation. Since any local POVM can be replaced by a sequence of 2-outcome POVMs [3], it is then interesting to study the case of a deterministic 2-outcome POVM.

In the rest of this chapter, we will study some properties of deterministic LOCC protocols and deterministic POVMs applied to three-qubit pure states. We will only be interested in transformations between states that have genuine tripartite entanglement (i.e., all three reduced density matrices have rank 2), since other cases can be reduced to the bipartite case.

5.2 General properties of LOCC transformations of three-qubit pure states

Pure states of three qubits with 3-particle entanglement are divided in two inequivalent classes: the GHZ class and the W class [18]. States in the GHZ class can be transformed by means local unitaries into a state that is a superposition of only two pure product states. States in the W class always require at least three pure product states in any local basis. These two classes have the property that any local POVM applied to a state in a given class, can only have as outcomes states in the same class. The states in the W class form a set of measure zero in the space of all possible pure states of three qubits. In particular, a state in this class can always be transformed by local unitary operations, into a state with real coefficients. We will call a state *real* if it is locally unitarily equivalent (LUeq) to a state with real coefficients. States in the GHZ class can be either real or complex.

Any state in the GHZ class is LUeq to a state of the (essentially unique) form

$$|\psi\rangle = \mu|000\rangle + \nu e^{i\gamma}|\varphi_A\rangle|\varphi_B\rangle|\varphi_C\rangle, \tag{5.2}$$

where $\mu \geq \nu > 0$ are real numbers, $\gamma \in [0, 2\pi)$ and $|\varphi_X\rangle = \cos\delta_X|0\rangle + \sin\delta_X|1\rangle$ with $\delta_X \in (0, \frac{\pi}{2}]$ and $X = A, B, C$ [18]. We will assume that the state $|\psi\rangle$ is normalized, so only five of the six parameters in (5.2) are independent. If we write $|\psi\rangle = |\mu\rangle + |\nu\rangle$ where $|\mu\rangle$ and $|\nu\rangle$ correspond to the first and second term in (5.2), respectively, we can construct an invariant quantity

$$\Omega(|\psi\rangle) = \langle\mu|\nu\rangle = \mu\nu e^{i\gamma}\cos\delta_A\cos\delta_B\cos\delta_C. \tag{5.3}$$

If $\mu = \nu$, the sign of the phase γ is not well defined, since in this case there is an ambiguity with respect to which product state in (5.2) is $|\mu\rangle$, and hence we can interchange $|\mu\rangle$ and $|\nu\rangle$ by local unitaries, and transform the state into its conjugate, which changes the sign of γ. As shown in [2] this means that the state is real, although we need to use complex coefficients if we want to write it in the particular form given by (5.2). Aside from this ambiguity, this decomposition is unique. If $\mu > \nu$ then the state $|\psi\rangle$ is complex if and only if $\Im m(\Omega(|\psi\rangle)) \neq 0$, where $\Im m(z)$ is the imaginary part of the complex number z. If $\Im m(\Omega(|\psi\rangle)) = 0$, then either γ is equal to 0 or π (and in both cases all the coefficients are real, so the state is real), or $\delta_X = \frac{\pi}{2}$ for some X. If this is the case, we can get rid of the phase by applying the local unitary

$$U = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\gamma} \end{pmatrix}, \tag{5.4}$$

to party X, which makes all the coefficients real.

Let $\{A_i\}, i = 1, \ldots, n$, represent a local POVM applied by Alice. If we apply it to a state $|\psi\rangle$ we can write the normalized outcomes as $|\phi_i\rangle = q_i^{-\frac{1}{2}} A_i \otimes \mathbb{1} \otimes \mathbb{1}|\psi\rangle$, where $q_i = \langle\psi|A_i^\dagger A_i \otimes \mathbb{1} \otimes \mathbb{1}|\psi\rangle$ is the probability of outcome i, and $\mathbb{1}$ is the 2×2 identity matrix. Let us consider the case in which none of the operators A_i corresponds to

a projective measurement (i.e., they all have rank 2). If we apply this POVM to a state with genuine tripartite entanglement, all the outcomes will still have 3-particle entanglement. To understand why this is true, suppose that there is an operator A_j of the POVM such that its corresponding outcome $|\phi_j\rangle$ has no 3-particle entanglement. Then $|\phi_j\rangle$ has to be the product of a pure state of one of the parties, let us call it X, and a pure state (possibly entangled) of the remaining two parties, so party X is completely disentangled from the other two. Since we are assuming that A_j is invertible (it is a rank two, 2 by 2 matrix), we can construct a local POVM with operators $\{A_j^{-1}, \sqrt{\mathbb{1} - (A_j^{-1})^\dagger A_j^{-1}}\}$ that when applied to $|\phi_j\rangle$ has at least one outcome that has 3-particle entanglement (the one corresponding to $A_j^{-1} \otimes \mathbb{1} \otimes \mathbb{1}|\phi_j\rangle$), that occurs with nonzero probability (because $(A_j^{-1})^\dagger A_j^{-1}$ also has rank two). Then we would have a protocol that with finite probability and only applying local operations, allows us to create entanglement between party X and the other two, starting from a state in which party X was disentangled, and this is clearly not possible.

Let us consider a state $|\psi\rangle$ in the GHZ class and let Alice apply a local POVM to it. Then all the outcomes $|\phi_i\rangle$ have to be in the GHZ class too, so we know that we can apply local unitaries to them such that

$$(U_{A(i)} \otimes U_{B(i)} \otimes U_{C(i)})|\phi_i\rangle = |\mu_i\rangle + |\nu_i\rangle, \tag{5.5}$$

where

$$\begin{aligned} |\mu_i\rangle &= \mu_i|000\rangle, \\ |\nu_i\rangle &= \nu_i e^{i\gamma_i}|\varphi_{A(i)}\rangle|\varphi_{B(i)}\rangle|\varphi_{C(i)}\rangle. \end{aligned} \tag{5.6}$$

Since $|\mu_i\rangle, |\nu_i\rangle$ and $|\mu\rangle, |\nu\rangle$ are product states, and the action of the POVM and any local unitaries is still local, for every outcome i we must have either

$$\begin{aligned} \sqrt{q_i}|\mu_i\rangle &= (U_{A(i)} \otimes U_{B(i)} \otimes U_{C(i)})(A_i \otimes \mathbb{1} \otimes \mathbb{1})|\mu\rangle, \\ \sqrt{q_i}|\nu_i\rangle &= (U_{A(i)} \otimes U_{B(i)} \otimes U_{C(i)})(A_i \otimes \mathbb{1} \otimes \mathbb{1})|\nu\rangle, \end{aligned} \tag{5.7}$$

or

$$\begin{aligned}\sqrt{q_i}|\mu_i\rangle &= (U_{A(i)} \otimes U_{B(i)} \otimes U_{C(i)})(A_i \otimes \mathbb{1} \otimes \mathbb{1})|\nu\rangle, \\ \sqrt{q_i}|\nu_i\rangle &= (U_{A(i)} \otimes U_{B(i)} \otimes U_{C(i)})(A_i \otimes \mathbb{1} \otimes \mathbb{1})|\mu\rangle. \end{aligned} \tag{5.8}$$

To decide which one is the case, we note that decomposition (5.2) requires that $\mu_i \geq \nu_i$, and μ_i, ν_i are the norms of the states $|\mu_i\rangle$ and $|\nu_i\rangle$, respectively. Then, if $\langle\mu|A_i^\dagger A_i \otimes \mathbb{1} \otimes \mathbb{1}|\mu\rangle \geq \langle\nu|A_i^\dagger A_i \otimes \mathbb{1} \otimes \mathbb{1}|\nu\rangle$ (which is equivalent to $\langle\mu_i|\mu_i\rangle \geq \langle\nu_i|\nu_i\rangle$), we have that (5.7) must hold. Otherwise, (5.8) holds. Using $\sum_i A_i^\dagger A_i = \mathbb{1}$, since the A_i are the elements of a POVM, we can then write

$$\begin{aligned}\Re e(\Omega(|\psi\rangle)) = \langle\mu|\nu\rangle + \langle\nu|\mu\rangle &= \sum_i q_i(\langle\mu_i|\nu_i\rangle + \langle\nu_i|\mu_i\rangle) \\ &= \sum_i q_i \Re e(\Omega(|\phi_i\rangle)), \end{aligned} \tag{5.9}$$

with $\Re e(z)$ the real part of z. This result is due to Vidal [52]. It puts a strong constraint on deterministic LOCC protocols, as we show in the following theorem.

Theorem 8 *Let $|\psi\rangle$ and $|\xi\rangle$ be two states in the GHZ class and assume there is a LOCC protocol that transforms $|\psi\rangle$ into $|\xi\rangle$ with probability 1. Then,*

$$\Re e(\Omega(|\psi\rangle)) = \Re e(\Omega(|\xi\rangle)), \tag{5.10}$$

i.e., the quantity $\Re e(\Omega)$ is invariant under deterministic LOCC transformations. Furthermore, it must be invariant for every local POVM in the protocol, that is, if the POVM is applied to a state $|\chi\rangle$ and has outcomes $|\phi_i\rangle$, then

$$\Re e(\Omega(|\chi\rangle)) = \Re e(\Omega(|\phi_i\rangle)), \tag{5.11}$$

for all i.

Proof: The most general LOCC protocol is a sequence of local unitaries, local POVMs and classical communication between all the parties. Local unitaries can-

not change $\Re e(\Omega)$ because $\Omega(|\psi\rangle)$ is an invariant of the orbit. Thus, it can only be changed by applying POVMs. Consider the first POVM of the protocol, that takes the state $|\psi\rangle$ into one of its possible outcomes $|\phi_i\rangle$, each occurring with probability q_i. Then, according to Equation (5.9) (and because $q_i > 0$), either all outcomes $|\phi_i\rangle$ satisfy $\Re e(\Omega(|\phi_i\rangle)) = \Re e(\Omega(|\psi\rangle))$ or there are at least two outcomes $|\phi_1\rangle$ and $|\phi_2\rangle$ that satisfy $\Re e(\Omega(|\phi_1\rangle)) < \Re e(\Omega(|\psi\rangle)) < \Re e(\Omega(|\phi_2\rangle))$. It is easy to see that in the latter case, at any stage in the protocol, we will have two outcomes $|\phi_j\rangle$ and $|\phi_k\rangle$ that will satisfy $\Re e(\Omega(|\phi_j\rangle)) < \Re e(\Omega(|\phi_k\rangle))$. This will be true in particular for the last stage of the protocol. But that would mean that $|\phi_j\rangle$ and $|\phi_k\rangle$ are in different orbits (because Ω is invariant under local unitaries), and that contradicts the fact that the protocol is deterministic. Thus, the only possibility is that all the outcomes of the first POVM have the same value of $\Re e(\Omega)$. We can apply exactly the same reasoning to all the POVMs in the protocol, and then conclude that all the final outcomes satisfy $\Re e(\Omega(|\phi_i\rangle)) = \Re e(\Omega(|\psi\rangle))$. Since this is a deterministic protocol that transforms $|\psi\rangle$ into $|\xi\rangle$, then all these outcomes should be in the same orbit as $|\xi\rangle$, and so we have $\Re e(\Omega(|\xi\rangle)) = \Re e(\Omega(|\phi_i\rangle)) = \Re e(\Omega(|\psi\rangle))$.□

This theorem tells us that under deterministic LOCC transformations the class of GHZ states breaks into an infinite number of subclasses that are labeled by the real part of the complex invariant Ω. Two states in different subclasses cannot be transformed one into the other with probability 1 by means of local operations and classical communication. From Equation (5.3) and from the range of the parameters, we see that the set of these subclasses is isomorphic to the open segment $(-\frac{1}{2}, \frac{1}{2})$. The subclass that contains the GHZ state, $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, corresponds to the center of the segment, and it is defined by $\Re e(\Omega) = 0$. Note that all subclasses contain both real and complex states.

This result gives a broad description of how a state can be transformed in the space of orbits with probability 1. Tighter constraints can be obtained from studying the behavior of entanglement monotones [54], which usually introduce some necessary conditions that must be satisfied in order for a transformation to be possible to be implemented locally. To find sufficient conditions we have to be able to show that a

protocol exists that accomplishes the transformation. A first step in that direction is to study deterministic POVMs.

5.3 Deterministic 2-outcome POVM

In this section we will study under what conditions a 2-outcome POVM is a deterministic POVM (i.e., both outcomes are in the same orbit). A general three-qubit state can be written as

$$|\psi\rangle = \sum_{ijk=0}^{1} t_{ijk}|ijk\rangle, \tag{5.12}$$

where the complex coefficients t_{ijk} satisfy $\sum_{ijk} |t_{ijk}|^2 = 1$. Following [1], we can define matrices T_0 and T_1, where

$$(T_i)_{jk} = t_{ijk}. \tag{5.13}$$

The group of Local Unitary (LU) transformations of three qubits is locally isomorphic (i.e., has the same Lie algebra) to $U(1) \times [SU(2)]^3$. Under a LU transformation performed only by Bob and Charlie with matrices U_B and U_C, the matrices T_i transform according to

$$T_i \to U_B T_i U_C, \tag{5.14}$$

while if the transformation is performed by Alice, we have

$$\begin{aligned} T_0 &\to u^A_{00} T_0 + u^A_{01} T_1 \\ T_1 &\to u^A_{10} T_0 + u^A_{11} T_1, \end{aligned} \tag{5.15}$$

where u^A_{ij} are the matrix elements of U_A.

It has been shown [48, 25] that the orbits of three-qubit pure states can be parameterized with 5 continuous invariants plus a discrete invariant, since in general a three-qubit state is not LUeq to its complex conjugate. There are many ways of

choosing these invariants [18, 9, 1]. For our analysis we will use the following set

$$\begin{aligned}
I_1 &= \sum_{ijkmpq} t_{kij} t^*_{mij} t_{mpq} t^*_{kpq} = \mathrm{Tr}[\rho_A^2], \\
I_2 &= \sum_{ijkmpq} t_{ikj} t^*_{imj} t_{pmq} t^*_{pkq} = \mathrm{Tr}[\rho_B^2], \\
I_3 &= \sum_{ijkmpq} t_{ijk} t^*_{ijm} t_{pqm} t^*_{pqk} = \mathrm{Tr}[\rho_C^2], \\
I_4 &= |\sum_{ijklmnopqrst} t_{ijk} t_{lmn} t_{opq} t_{rst} \epsilon_{il} \epsilon_{or} \epsilon_{jm} \epsilon_{ps} \epsilon_{kq} \epsilon_{nt}|, \\
I_5 &= \sum_{ijklmnopq} t_{ijk} t^*_{ilm} t_{nlo} t^*_{pjo} t_{pqm} t^*_{nqk},
\end{aligned} \tag{5.16}$$

where ϵ_{ij} is the antisymmetric symbol, ρ_X is the reduced density matrix of subsystem X ($X = A, B, C$), and all the indices are summed from 0 to 1. I_4 is the 3-tangle introduced in [13]. As shown in [48] these 5 invariants are algebraically independent. However, since they are all real and invariant under complex conjugation of the coefficients t_{ijk}, they cannot distinguish between a state and its conjugate. To fix this ambiguity we use the complex invariant [24]

$$\begin{aligned}
I_6 = \sum_{i_l j_l k_l} & t_{i_1 j_1 k_1} t_{i_2 j_2 k_2} t_{i_3 j_3 k_3} t_{i_4 j_4 k_4} t_{i_5 j_5 k_5} t_{i_6 j_6 k_6} \times \\
& t^*_{i_1 j_1 k_3} t^*_{i_2 j_2 k_4} t^*_{i_3 j_4 k_5} t^*_{i_4 j_3 k_1} t^*_{i_5 j_6 k_2} t^*_{i_6 j_5 k_6},
\end{aligned} \tag{5.17}$$

where again all indices are summed from 0 to 1. To completely specify an orbit we need the value of I_1 through I_5 plus the sign of the imaginary part of I_6. It is worth noting that $1 - I_1$, $1 - I_2$, $1 - I_3$ and I_4 are decreasing entanglement monotones [54], while I_5 is not an entanglement monotone [24].

We will consider the case of a 2-outcome POVM applied by Alice on a pure state $|\psi\rangle$ of three qubits. The most general POVM is given by operators A_0 and A_1 of the

form

$$
\begin{aligned}
A_0 &= V_0 \begin{pmatrix} \sqrt{x} & 0 \\ 0 & \sqrt{y} \end{pmatrix} U, \\
A_1 &= V_1 \begin{pmatrix} \sqrt{1-x} & 0 \\ 0 & \sqrt{1-y} \end{pmatrix} U,
\end{aligned} \tag{5.18}
$$

where V_0, V_1 and U are unitary matrices and $0 \leq x, y \leq 1$. This decomposition can be understood in the following way: A_i are positive semidefinite operators, and by performing a singular value decomposition we know that there are unitary matrices V_i and U_i such that $V_i^\dagger A_i U_i^\dagger$ are positive semidefinite diagonal matrices. The matrices U_i can be used to diagonalize the hermitian matrices $A_i^\dagger A_i$. But since we have the constraint that $A_0^\dagger A_0 + A_1^\dagger A_1 = \mathbb{1}$, and $\mathbb{1}$ is already a diagonal matrix, it is easy to see that we can take $U_0 = U_1 = U$.

It is easy to check that the operators in (5.18) satisfy $A_0^\dagger A_0 + A_1^\dagger A_1 = \mathbb{1}$. When we apply this POVM to a state $|\psi\rangle$, we obtain two outcomes $|\phi_0\rangle$ and $|\phi_1\rangle$ given by

$$
|\phi_i\rangle = \frac{1}{\sqrt{q_i}} (A_i \otimes \mathbb{1} \otimes \ \mathbb{1} |\psi\rangle) \quad , \quad i = 0, 1, \tag{5.19}
$$

where q_i is the probability of outcome i. From (5.18) and (5.19) we can see that the action of this POVM on $|\psi\rangle$ is equivalent to applying a local unitary transformation first given by U, applying a diagonal and real POVM and finally applying a local unitary V_i conditional on the outcome of the POVM. This last local unitary cannot change the orbit of the outcome $|\phi_i\rangle$. Since we are considering two states in the same orbit to be equivalent, we can take this unitary to be the identity without loss of generality.

Let us consider first the case in which $U = \mathbb{1}$ in (5.18). Then both elements of the POVM reduce to real and diagonal matrices

$$
E_0 = \begin{pmatrix} \sqrt{x} & 0 \\ 0 & \sqrt{y} \end{pmatrix} \quad , \quad E_1 = \begin{pmatrix} \sqrt{1-x} & 0 \\ 0 & \sqrt{1-y} \end{pmatrix}. \tag{5.20}
$$

From now on, we will take $0 < x, y < 1$, since when x or y are equal to zero or one, the POVM becomes a projective measurement, which destroys three particle entanglement. We can write explicit expressions for both outcomes of the POVM

$$\begin{aligned} |\phi_0\rangle &= \frac{1}{\sqrt{q_0}} \sum_{jk} (\sqrt{x}\ t_{0jk}|0jk\rangle + \sqrt{y}\ t_{1jk}|1jk\rangle), \\ |\phi_1\rangle &= \frac{1}{\sqrt{q_1}} \sum_{jk} (\sqrt{1-x}\ t_{0jk}|0jk\rangle + \sqrt{1-y}\ t_{1jk}|1jk\rangle). \end{aligned} \tag{5.21}$$

Now we compute the invariants I_1 through I_5 for $|\phi_0\rangle$ as a function of x and y

$$\begin{aligned} I_1(x,y) &= \frac{x^2a^2 + 2xy\ \mathrm{Tr}[T_0T_1^\dagger]\ \mathrm{Tr}[T_1T_0^\dagger] + y^2b^2}{(ax+by)^2}, \\ I_2(x,y) &= \frac{x^2F_0 + 2xy\ \mathrm{Tr}[T_0T_0^\dagger T_1T_1^\dagger] + y^2F_1}{(ax+by)^2}, \\ I_3(x,y) &= \frac{x^2F_0 + 2xy\ \mathrm{Tr}[T_0T_1^\dagger T_1T_0^\dagger] + y^2F_1}{(ax+by)^2}, \\ I_4(x,y) &= \frac{xy\ I_4(|\psi\rangle)}{(ax+by)^2}, \\ I_5(x,y) &= \frac{x^3\ G_{00} + 3x^2y\ G_{01} + 3xy^2\ G_{10} + y^3\ G_{11}}{(ax+by)^3}, \end{aligned} \tag{5.22}$$

where the matrices T_i are as defined in (5.13), $a = \mathrm{Tr}[T_0T_0^\dagger]$, $b = \mathrm{Tr}[T_1T_1^\dagger]$, $a + b = 1$ for a normalized $|\psi\rangle$, $F_i = \mathrm{Tr}[(T_iT_i^\dagger)^2]$ and $G_{ij} = \mathrm{Tr}[T_iT_j^\dagger T_iT_i^\dagger T_jT_i^\dagger]$. The invariants for $|\phi_1\rangle$ are obtained from (5.22) by replacing x by $1-x$ and y by $1-y$. For the two outcomes to be in the same orbit, we need the five invariants to take the same values for both states, i.e.,

$$I_i(x,y) = I_i(1-x, 1-y) \quad , \quad i = 1, \ldots, 5. \tag{5.23}$$

If these conditions are satisfied, then either $|\phi_0\rangle$ is LUeq to $|\phi_1\rangle$, or $|\phi_0\rangle$ is LUeq to $|\phi_1\rangle^*$. To determine which one is the case, we need to compute the sign of the imaginary part of the complex invariant I_6. For now, let us concentrate on the equations in (5.23). These equations have a common solution with $0 < x, y < 1$ if

and only if the following conditions are satisfied (see appendix B)

$$a^2 \text{ Tr}[(T_1T_1^\dagger)^2] = b^2 \text{ Tr}[(T_0T_0^\dagger)^2], \tag{5.24}$$

$$a \text{ Tr}[T_1T_0^\dagger T_1T_1^\dagger T_0T_1^\dagger] = b \text{ Tr}[T_0T_1^\dagger T_0T_0^\dagger T_1T_0^\dagger], \tag{5.25}$$

$$a^2x(1-x) = b^2y(1-y). \tag{5.26}$$

Furthermore, the solution satisfies $I_5(|\phi_i\rangle) < I_5(|\psi\rangle)$. This is worth noting because I_5 is not an entanglement monotone, but behaves monotonically under this particular class of POVMs. Equations (5.24) and (5.25) are real valued polynomial constraints on the coefficients of the state, and in general are not satisfied for an arbitrary state. From (5.14) and (5.15) we can see that these constraints are invariant under LU transformations applied by Bob and Charlie, while they are not invariant under local unitaries by Alice. Equation (5.26) is a constraint on the parameters of the POVM that depends on the state we are transforming through the values of a and b.

Now let U in (5.18) be any unitary matrix, so our POVM takes the form $\{E_0U, E_1U\}$, with E_0, E_1 given by (5.20). This is equivalent to applying the local unitary U to Alice's part of the state, followed by a diagonal POVM, and we already know the conditions that need to be satisfied in this last stage for the outcomes to be in the same orbit. So we can reduce the problem to finding a local unitary performed by Alice that would transform the original state $|\psi\rangle$ into a state that satisfies (5.24) and (5.25). Then we can choose a POVM that satisfies (5.26), where now a and b are computed using the coefficients of the transformed state $U \otimes \mathbb{1} \otimes \mathbb{1}|\psi\rangle$. We will consider the cases of real and complex states separately.

5.3.1 Real states

To characterize the orbit of a real state $|\psi\rangle$ we only need four parameters instead of the five needed for an arbitrary state. First, note that, by our definition, any real state can be transformed by means of local unitary transformations, into a state with only real coefficients. Of the (at most) eight coefficients of this state, only seven are

independent if we are considering a normalized state, and we can get rid of three more by applying local real unitary (orthogonal) transformations on each of the three qubits. Since $I_i, i = 1, \ldots, 4$, are algebraically independent, we can use this set to parameterize the orbits of real states. This greatly simplifies our analysis because, as seen in appendix B, (5.24) is enough to assure that $I_i, i = 1, \ldots, 4$, have the same values for both outcomes of our POVM. So, given a real state, we need to find a U such that $|\psi'\rangle = U \otimes \mathbb{1} \otimes \mathbb{1}|\psi\rangle$ satisfies (5.24). Let

$$U(\alpha) = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}. \tag{5.27}$$

In terms of the matrices T_i, which group the coefficients t_{ijk} of the state, this transformation can be written

$$\begin{aligned} T'_0 &= \cos\alpha\ T_0 + \sin\alpha\ T_1\ , \\ T'_1 &= -\sin\alpha\ T_0 + \cos\alpha\ T_1. \end{aligned} \tag{5.28}$$

If we plug this into (5.24), take out a common factor $\cos^8\alpha$, introduce the variable $z = \tan\alpha$ and move all terms to one side, we can write (5.24) as a polynomial $p_1(z)$ of degree 8 with real coefficients, of the form

$$p_1(z) = A(1 - z^8) + B(z + z^7) + C(z^2 - z^6) + D(z^3 + z^5) = 0. \tag{5.29}$$

If z_0 is a real root of p_1, then $U(\alpha_0)$, with $\alpha_0 = \arctan(z_0)$ is the unitary matrix we are looking for. Now it is easy to check that $p_1(1) = -p_1(-1)$, so p_1 has at least one real root in $[-1, 1]$, which means that we can always find a unitary U, such that $|\psi'\rangle = U \otimes \mathbb{1} \otimes \mathbb{1}|\psi\rangle$ satisfies (5.24). Now we can apply to $|\psi'\rangle$ a diagonal POVM that satisfies (5.26), and we are certain that both outcomes have the same values of the four invariants $I_i, i = 1, \ldots, 4$. But in the case of real states this is enough to completely specify the orbit, since $|\psi\rangle$ real implies $|\psi'\rangle$ is real, since U was chosen to be real, and the outcomes of the POVM, $|\phi_0\rangle$ and $|\phi_1\rangle$, are also real, due to the fact

that the POVM itself is real. In this case we do not have to worry about the value of the complex invariant. Finally, since $|\phi_0\rangle$ and $|\phi_1\rangle$ are in the same orbit, we can apply local unitaries to transform them into any state in the same orbit. So the net result of this protocol is to transform any state in the orbit of $|\psi\rangle$ into any state in the orbit of $|\phi_0\rangle$, with probability 1. The results presented so far show that for any real state, there is some set of orbits that can be reached deterministically from that state, although we have not yet characterized this set. We will discuss this problem in Section 5.4.

5.3.2 Complex states

The analysis of complex states turns out to be more complicated, because now we need to find U such that $|\psi'\rangle$ satisfies *both* (5.24) and (5.25). We can write any unitary U as

$$e^{i\phi}\begin{pmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix}\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} e^{i\zeta} & 0 \\ 0 & e^{-i\zeta} \end{pmatrix}. \tag{5.30}$$

The phase and the matrix on the left will commute with the diagonal matrices of the POVM, so their action is equivalent to applying a local unitary to the outcomes of the POVM. But we know that this action will not change the orbit of the outcome state, so we can fix them to be the identity. So U will take the state $|\psi\rangle$ with matrices T_0 and T_1 to a state $|\psi'\rangle$ with matrices

$$\begin{aligned} T_0' &= \cos\alpha\ e^{i\zeta}\ T_0 + \sin\alpha\ e^{-i\zeta}\ T_1\ , \\ T_1' &= -\sin\alpha\ e^{i\zeta}\ T_0 + \cos\alpha\ e^{-i\zeta}\ T_1. \end{aligned} \tag{5.31}$$

We can substitute (5.31) into the homogeneous form of (5.24) and (5.25), again divide by $\cos^8\alpha$ and introduce the variable $z = \tan\alpha$, so both conditions are expressed as polynomials in z equal to zero, with real coefficients, of the form

$$p_i(z) = A_i(1 - z^8) + B_i(z + z^7) + C_i(z^2 - z^6) + D_i(z^3 + z^5) = 0, \quad i = 1, 2, \tag{5.32}$$

with the coefficients given by

$$\begin{aligned} A_i &= a_{0i} \ , \\ B_i &= b_{1i}\cos(2\zeta) + b_{2i}\sin(2\zeta) \ , \\ C_i &= c_{0i} + c_{1i}\cos(4\zeta) + c_{2i}\sin(4\zeta) \ , \\ D_i &= d_{1i}\cos(2\zeta) + d_{2i}\sin(2\zeta) + d_{3i}\cos(6\zeta) + d_{4i}\sin(6\zeta), \end{aligned} \tag{5.33}$$

where $a_{0i}, b_{ji}, c_{ji}, d_{ji}$ are real valued polynomials on the coefficients of $|\psi\rangle$, whose exact form can be computed from regrouping the terms obtained after substituting (5.31) into (5.24) and (5.25).

Finding a local unitary performed by Alice on $|\psi\rangle$ that would yield a state that satisfies (5.24) and (5.25) is equivalent to finding values z and ζ (which parameterize the unitary) such that both polynomials p_1 and p_2 vanish simultaneously. We can think of ζ as a parameter for these polynomials, and what we are looking for is a value of ζ such that p_1 and p_2 have a common real root.

The polynomials p_i have certain useful symmetries. First of all, because their coefficients are real, complex roots appear in conjugate pairs. Also, because of the particular symmetry of the coefficients (i.e., the coefficient of z^8 is equal to minus the independent term, the coefficient of z^7 is equal to the coefficient of z, and so on), if z_0 is a root of p_i, so is $-\frac{1}{z_0}$ (this corresponds to $\alpha + \frac{\pi}{2}$ being also a solution if so is α, and this is related to the fact that (5.24) and (5.25) are symmetric under the interchange of 0 and 1). Since $p_i(1) = -p_i(-1)$, p_i has a real root in $[-1, 1]$. To simplify the problem, we can extract a factor $z^2 + 1$ from p_i, so we reduce the problem to two polynomials of degree 6, that have the same symmetry properties discussed above. If we introduce the variable $w = (\frac{1}{z} - z)$ we can further reduce the two polynomials of degree 6 to two polynomials $g_i(w), i = 1, 2$, of degree 3, given by

$$g_i(w) = A_i w^3 + B_i w^2 + (C_i + 2A_i)w + (D_i + B_i), \tag{5.34}$$

with the property that if w is a root of g_i, the corresponding z's given by $w = (\frac{1}{z} - z)$

(which are real if and only if w is real) are roots of p_i. So we reduced the problem to finding a common real root of g_1 and g_2. The resultant [14] of the two polynomials g_1 and g_2 is a function of ζ and takes the form

$$\mathrm{Res}(g_1, g_2)(\zeta) = \sum_{k=0}^{4} (r_k \cos[(2+4k)\zeta] + s_k \sin[(2+4k)\zeta]), \tag{5.35}$$

where r_k and s_k are polynomials on the coefficients of $|\psi\rangle$. We can see that this resultant vanishes several times in $[0, 2\pi]$, which is the range of ζ, and this is useful because *the resultant of two polynomials vanishes if and only if they have a common factor*. This falls short of saying that we can find ζ such that g_1 and g_2 have a common real root, because there is in principle the possibility that the common factor is a polynomial of degree 2 irreducible over the real numbers, so g_1 and g_2 have a common root but it is complex. However, after checking this procedure with many randomly generated states, we found that the common factor *always corresponds to a real root.*

Let us assume that in fact, we can always find a value ζ_0 such that p_1 and p_2 have a common real root z_0. Then we know that if we apply $U(\alpha_0, \zeta_0) \otimes \mathbb{1} \otimes \mathbb{1}$ (where $\alpha_0 = \arctan(z_0)$) to $|\psi\rangle$, we obtain a state $|\psi'\rangle$ that satisfies (5.24) and (5.25). Then, we can choose a POVM that satisfies (5.26), and we can be sure that both outcomes of this POVM, when applied to $|\psi'\rangle$, will have the same values of $I_i, i = 1, \ldots, 5$. However, as we pointed out before, this is still not enough to say that both outcomes are in the same orbit. There is still the possibility that they are in orbits that are conjugate to each other, since we are dealing with complex states, which are not LUeq to their conjugates. To decide which one is the case, we can compute the sign of the imaginary part of I_6 for both outcomes. Unfortunately, the expression of I_6 for both outcomes is too complicated and it is not possible to extract the sign of the imaginary part analytically for an arbitrary state, although it is very easy to compute it numerically for a given state. We analyzed randomly generated states, and found that we can *always* find a value of ζ for which both outcomes are indeed in the same orbit (although there are other values of ζ for which the outcomes are in conjugate orbits). We will refer to states with this property as *gate states*, since we can use

them as a gate to leave one orbit and move to another with probability 1.

5.4 The transformation in the space of orbits

We can now use the results of the previous section to give a characterization of the states that can be obtained from $|\psi\rangle$ by applying a 2-outcome deterministic POVM. Let us assume that the state $|\psi\rangle$ is a gate state. We will also assume that $a < b$ (if it is not, we apply a bit flip on Alice's qubit, which interchanges the matrices T_0 and T_1, and hence a and b). We can use the invariants evaluated for $|\phi_0\rangle$ (given by (5.22)) to characterize the orbit of the outcomes. These equations are homogeneous of degree zero in x and y, so we can write them in terms of only one parameter $\lambda = \frac{y}{x}$

$$\begin{aligned} I_i(\lambda) &= \alpha_i + \beta_i \frac{\lambda}{(a+b\lambda)^2}, \qquad i = 1, \ldots, 4 \ , \\ I_5(\lambda) &= \alpha_5 + \frac{\lambda(\beta_5 + \gamma_5 \lambda)}{(a+b\lambda)^3}, \end{aligned} \tag{5.36}$$

where

$$\begin{aligned} \alpha_1 &= 1 \ , \ \alpha_2 = \alpha_3 = \frac{\mathrm{Tr}[(T_0 T_0^\dagger)^2]}{a^2} \ , \ \alpha_4 = 0 \ , \\ \alpha_5 &= \frac{\mathrm{Tr}[(T_0 T_0^\dagger)^3]}{a^3} \ , \\ \beta_1 &= 2(\mathrm{Tr}[T_0 T_1^\dagger] Tr[T_1 T_0^\dagger] - ab) \ , \\ \beta_2 &= 2(\mathrm{Tr}[T_0 T_0^\dagger T_1 T_1^\dagger] - b\frac{\mathrm{Tr}[(T_0 T_0^\dagger)^2]}{a}) \ , \\ \beta_3 &= 2(\mathrm{Tr}[T_0 T_1^\dagger T_1 T_0^\dagger] - b\frac{\mathrm{Tr}[(T_0 T_0^\dagger)^2]}{a}) \ , \\ \beta_4 &= I_4(|\psi\rangle) \ , \\ \beta_5 &= 3(\mathrm{Tr}[T_0 T_1^\dagger T_0 T_0^\dagger T_1 T_0^\dagger] - \frac{b\mathrm{Tr}[(T_0 T_0^\dagger)^3]}{a}) \ , \\ \gamma_5 &= 3(\mathrm{Tr}[T_1 T_0^\dagger T_1 T_1^\dagger T_0 T_1^\dagger] - \frac{b^2\mathrm{Tr}[(T_0 T_0^\dagger)^3]}{a^2}). \end{aligned} \tag{5.37}$$

The range of λ is $[1, +\infty)$ (when $a < b$), with $\lambda = 1$ corresponding to no transformation ($E_0 \propto \mathbb{1}$), so we have $I_i(\lambda = 1) = I_i(|\psi\rangle)$, and $\lambda = +\infty$ corresponding to

a projective measurement ($y = 1, x = 0$) that destroys any 3-particle entanglement. From (5.36) we can see that the set of orbits we can reach from $|\psi\rangle$ by applying a deterministic 2-outcome POVM can be described as a one parameter family $\{I_i(\lambda)\}$ that corresponds to a curve in the space of orbits, that starts at state $|\psi\rangle$ and ends on a state that has no tripartite entanglement.

It is possible for some orbits to have more than one gate state. The values of the coefficients (5.37) will be in general different for different gate states. Since these coefficients determine the curve $\{I_i(\lambda)\}$, we will be able to transform to different sets of orbits depending on which gate state we use. We can also reach a different family of orbits if we let Bob or Charlie apply a deterministic POVM instead of Alice. This is because the matrices T_i, are different for different parties, and so will give in general different gate states.

If we fix the sign of the imaginary part of I_6, we can use the set of invariants $\{I_i, i = 1, \ldots, 5\}$ as coordinates for the orbits. All the previous results can be summarized in the following picture. Every point in this space (which represents the orbit of some state $|\psi\rangle$) is the starting point of a finite number of curves, each representing a set of orbits that can be obtained from $|\psi\rangle$ with probability 1 with a local 2-outcome POVM.

More orbits can be reached if several rounds of deterministic POVMs are allowed. The general protocol will be something like this: (i) starting with the state $|\psi\rangle$, Alice applies a local unitary to transform it into a gate state; (ii) she applies a POVM on her part of the system, that satisfies (5.26); (iii) according to the outcome she obtains, she communicates to Bob and Charlie the state $|\psi'\rangle$ they are sharing after the measurement; (iv) they decide which one will apply the next POVM and repeat the same steps, now starting with the state $|\psi'\rangle$. A simplified pictorial representation of this transformation is given in Figure 5.1. The transformation occurs in the 5-dimensional space defined by the invariants I_i, but for simplicity, we represent only two of them (I_4 and I_5). We start with a gate state $|\psi\rangle$ and we apply a deterministic 2-outcome POVM (with some parameter λ_0), that transforms it into state $|\psi'\rangle$. The solid curve connecting $|\psi\rangle$ and $|\psi'\rangle$ represents all the orbits that can be reached from

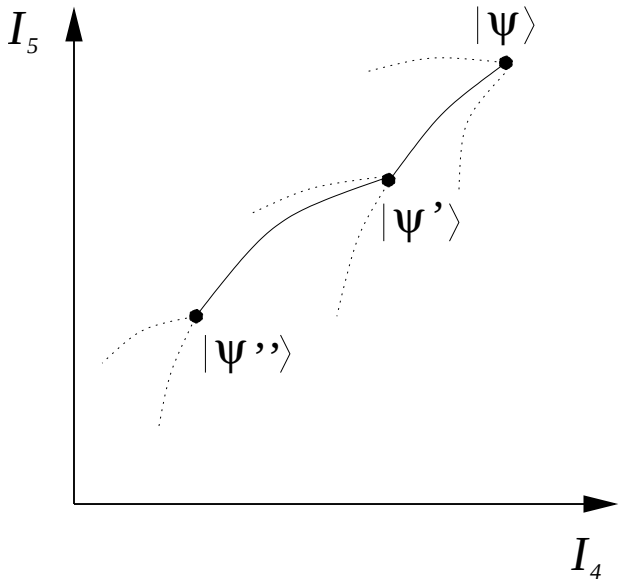


Figure 5.1: Transformation of states in the space of orbits.

$|\psi\rangle$ by applying a POVM with parameter λ between 1 and λ_0. The dotted lines originating at $|\psi\rangle$ represent the set of orbits that can be reached from the same orbit, but using a gate state different from $|\psi\rangle$ (that is still in the same orbit as $|\psi\rangle$ so it is represented by the same point in the plot). In the actual space of orbits, these curves extend until they reach an orbit that represents a state with no 3-particle entanglement, that corresponds to the point where the POVM becomes a projective measurement (i.e., $\lambda = +\infty$). For clarity, we are only plotting the beginning of these curves. After deterministically transforming $|\psi\rangle$ into $|\psi'\rangle$, the parties can choose again from several gate states to apply the next POVM. This will determine which party will apply this POVM, because in general, a state is a gate state only for a particular party. In Figure 5.1, the full line represents a POVM that transforms $|\psi'\rangle$ into $|\psi''\rangle$, while again, the dotted lines correspond to other possible deterministic transformations that can be applied to $|\psi'\rangle$. By applying many deterministic POVMs with different parameters, we can reach many different orbits.

5.5 Transformation of the GHZ state

As an example of the use of 2-outcome deterministic POVMs, we will now study the particular case of the state $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. As it was mentioned in Section 5.2, this state belongs to the subclass of states that satisfy $\Re e(\Omega) = 0$. We will show that it can be transformed with probability 1 into any real state in that subclass.

First, we need to identify the real states that satisfy $\Re e(\Omega) = 0$. From (5.3), clearly we must have that either $\Omega(|\psi\rangle)$ is zero or pure imaginary. In the former case, this means that $\langle\mu|\nu\rangle = 0$, and then decomposition (5.2) takes one of the following forms:

$$\begin{aligned} \mu|000\rangle &+ \nu|1\rangle|\varphi\rangle|\varphi'\rangle, \\ \mu|000\rangle &+ \nu|\varphi\rangle|1\rangle|\varphi'\rangle, \\ \mu|000\rangle &+ \nu|\varphi\rangle|\varphi'\rangle|1\rangle. \end{aligned} \tag{5.38}$$

If $\Omega(|\psi\rangle)$ is pure imaginary (but nonzero), then the only case in which $|\psi\rangle$ is actually a real state is the case in which $\mu = \nu$, as discussed in Section 5.2. In this case, the state takes the form

$$\frac{1}{\sqrt{2}}(|000\rangle \pm i|\varphi\rangle|\varphi'\rangle|\varphi''\rangle), \tag{5.39}$$

where none of the states in the second term can be equal to $|0\rangle$ or $|1\rangle$, and we obtain $\mu = \frac{1}{\sqrt{2}}$ by imposing normalization of the state. The two states in (5.39) (corresponding to the two possible signs of the second term) are LUeq to each other.

Since the GHZ state is symmetric under a permutation of the parties, it is clear that if we find a protocol that transforms it into the first state in (5.38), then we can also transform it into the other two. Now we will use the results of Section 5.3 to explicitly construct protocols that transform the GHZ state into the state

$$|\phi\rangle = \mu|000\rangle + \nu|1\rangle|\varphi\rangle|\varphi'\rangle, \tag{5.40}$$

or the state

$$\frac{1}{\sqrt{2}}(|000\rangle + i|\varphi''\rangle|\varphi\rangle|\varphi'\rangle), \tag{5.41}$$

for all allowed values of $\mu, \nu, |\varphi\rangle, |\varphi'\rangle$ and $|\varphi''\rangle$. These protocols will be divided into three steps. First, Charlie applies a local deterministic POVM that transforms $|GHZ\rangle$ into $\frac{1}{\sqrt{2}}(|000\rangle + |11\rangle|\varphi'\rangle)$. Then, Bob applies another local POVM that takes the state to $\frac{1}{\sqrt{2}}(|000\rangle + |1\rangle|\varphi\rangle|\varphi'\rangle)$. Finally, Alice applies the last POVM, which she can choose to take the state to $\mu|000\rangle + \nu|1\rangle|\varphi\rangle|\varphi'\rangle$ or $\frac{1}{\sqrt{2}}(|000\rangle + i|\varphi''\rangle|\varphi\rangle|\varphi'\rangle)$.

Step 1. The T_i matrices for the GHZ state are given by

$$T_0 = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 \end{pmatrix} \quad , \quad T_1 = \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{pmatrix}, \tag{5.42}$$

and they have the same form for all parties. If Charlie applies a local unitary U on its qubit, where

$$U = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \tag{5.43}$$

the T_i' matrices for the state $|\psi'\rangle = \mathbb{1} \otimes \mathbb{1} \otimes U|GHZ\rangle$ are

$$T_0' = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad T_1' = \frac{1}{2} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{5.44}$$

It is very easy to check that these matrices satisfy Equation (5.24), so the state $|\psi'\rangle$ is a gate state. Thus, Charlie can apply a deterministic POVM to it. In particular, this state satisfies $b' = a' = \mathrm{Tr}[T_0'^{\dagger} T_0'] = \frac{1}{2}$, so according to Equation (5.26) we have $y = 1 - x$, so Charlie can apply a deterministic POVM of the form

$$E_0 = \begin{pmatrix} \sqrt{x} & 0 \\ 0 & \sqrt{1-x} \end{pmatrix} \quad , \quad E_1 = \begin{pmatrix} \sqrt{1-x} & 0 \\ 0 & \sqrt{x} \end{pmatrix}, \tag{5.45}$$

where $x \in [\frac{1}{2}, 1)$. The normalized state corresponding to the outcome zero is

$$\begin{aligned} |\phi_0\rangle &= \sqrt{2}(\mathbb{1} \otimes \mathbb{1} \otimes E_0)|\psi'\rangle \\ &= \sqrt{2}(\mathbb{1} \otimes \mathbb{1} \otimes E_0 U)|GHZ\rangle \\ &= |00\rangle\,(E_0 U|0\rangle) + |11\rangle\,(E_0 U|1\rangle) \\ &= \langle 0|U^\dagger E_0^\dagger E_0 U|0\rangle^{\frac{1}{2}}\,|00\rangle|0'\rangle + \langle 1|U^\dagger E_0^\dagger E_0 U|1\rangle^{\frac{1}{2}}\,|11\rangle|1'\rangle, \end{aligned} \tag{5.46}$$

where

$$|0'\rangle = \frac{E_0 U|0\rangle}{\langle 0|U^\dagger E_0^\dagger E_0 U|0\rangle^{\frac{1}{2}}} \quad , \quad |1'\rangle = \frac{E_0 U|1\rangle}{\langle 1|U^\dagger E_0^\dagger E_0 U|1\rangle^{\frac{1}{2}}}, \tag{5.47}$$

are normalized states. A straightforward calculation shows that $\langle 0|U^\dagger E_0^\dagger E_0 U|0\rangle = \langle 1|U^\dagger E_0^\dagger E_0 U|1\rangle = \frac{1}{2}$, so we can write

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle|0'\rangle + |11\rangle|1'\rangle). \tag{5.48}$$

This state can be taken to the canonical form (5.2) by letting Charlie apply a local (real) unitary on his qubit, that takes the state $|0'\rangle$ into $|0\rangle$, and $|1'\rangle$ into $|\varphi'\rangle = \cos\delta'|0\rangle + \sin\delta'|1\rangle$. Thus, $\langle 0|\varphi'\rangle = \langle 0'|1'\rangle$ and then we have

$$\begin{aligned} \cos\delta' &= \langle 0'|1'\rangle \\ &= 2\langle 0|U^\dagger E_0^\dagger E_0 U|1\rangle \\ &= 2x - 1. \end{aligned} \tag{5.49}$$

We can see that for any $\delta' \in (0, \frac{\pi}{2}]$, we can find $x \in [\frac{1}{2}, 1)$ that satisfies this equation. This means that we can transform $|GHZ\rangle$ into $\frac{1}{\sqrt{2}}(|000\rangle + |11\rangle|\varphi'\rangle)$ with probability 1, for any $|\varphi'\rangle$.

Step 2. In this step Bob applies a deterministic POVM to transform the state $|\phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |11\rangle|\varphi'\rangle)$ into $\frac{1}{\sqrt{2}}(|000\rangle + |1\rangle|\varphi\rangle|\varphi'\rangle)$. The T_i matrices for $|\phi\rangle$ from

Bob's point of view are given by

$$T_0 = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 \end{pmatrix}, \quad T_1 = \begin{pmatrix} 0 & 0 \\ \frac{1}{\sqrt{2}}\cos\delta' & \frac{1}{\sqrt{2}}\sin\delta' \end{pmatrix}. \tag{5.50}$$

First, Bob applies the local unitary U from (5.43) to his qubit, obtaining the state $|\phi'\rangle = \mathbb{1} \otimes U \otimes \mathbb{1}|\phi\rangle$, characterized by matrices T_i' given by

$$T_0' = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ \cos\delta' & \sin\delta' \end{pmatrix} \quad , \quad T_1' = \frac{1}{2}\begin{pmatrix} -1 & 0 \\ \cos\delta' & \sin\delta' \end{pmatrix}. \tag{5.51}$$

Again, it is easy to show that T_i' satisfy (5.24), so $|\phi'\rangle$ is a gate state. We also have that $a' = b' = \mathrm{Tr}[T_0' T_0'^{\dagger}] = \frac{1}{2}$, so Bob can apply the POVM of Equation (5.45) to his qubit and obtain two outcomes in the same orbit. We can apply the same analysis we did in Step 1 to the outcome $|\chi_0\rangle$ of Bob's POVM, and show that

$$|\chi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0'\rangle|0\rangle + |1\rangle|1'\rangle|\varphi'\rangle), \tag{5.52}$$

where the normalized states $|0'\rangle$ and $|1'\rangle$ are also given by (5.47). It should be clear from Step 1 that, again, we can choose x and a suitable local unitary on Bob's qubit to transform this state into

$$|\chi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |1\rangle|\varphi\rangle|\varphi'\rangle) \tag{5.53}$$

for any $|\varphi\rangle = \cos\delta|0\rangle + \sin\delta|1\rangle$, with $\delta \in (0, \frac{\pi}{2}]$.

Step 3. Now Alice has to choose between two local POVMs depending on whether she wants to obtain (5.40) or (5.41). Consider first the case in which she wants to transform $|\chi\rangle$ into $\mu|000\rangle + \nu|1\varphi\varphi'\rangle$. The T_i matrices for $|\chi\rangle$ from Alice's point of view are

$$T_0 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \ , \ T_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} \cos\delta\cos\delta' & \cos\delta\sin\delta' \\ \sin\delta\cos\delta' & \sin\delta\sin\delta' \end{pmatrix}. \tag{5.54}$$

These matrices already satisfy Equation (5.24) and since $a = \mathrm{Tr}[T_0 T_0^\dagger] = \frac{1}{2}$, Alice can apply the deterministic POVM given by (5.45). The state corresponding to outcome zero is

$$\begin{aligned} |\xi\rangle &= \sqrt{x}|000\rangle + \sqrt{1-x}|1\varphi\varphi'\rangle \\ &= \mu|000\rangle + \nu|1\varphi\varphi'\rangle, \end{aligned} \tag{5.55}$$

where we set $\mu = \sqrt{x}$ and $\nu = \sqrt{1-x}$. Since $x \in [\frac{1}{2}, 1)$, we have $\mu \geq \nu$. The state in (5.55) is the same as in (5.40).

Consider now the case in which Alice wants to obtain $\frac{1}{\sqrt{2}}(|000\rangle + i|\varphi''\rangle|\varphi\rangle|\varphi'\rangle)$ from $|\chi\rangle$. In this case we can construct the appropriate POVM $\{A_0, A_1\}$ by inspection. If $|\varphi''\rangle = \cos\delta''|0\rangle + \sin\delta''|1\rangle$, we define

$$A_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i\cos\delta'' \\ 0 & i\sin\delta'' \end{pmatrix} \ , \ A_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i\cos\delta'' \\ 0 & -i\sin\delta'' \end{pmatrix}. \tag{5.56}$$

It is easy to verify that they satisfy $A_0^\dagger A_0 + A_1^\dagger A_1 = \mathbb{1}$, and that the probabilities of both outcomes are equal to $\frac{1}{2}$. The normalized state that corresponds to outcome zero is

$$\frac{1}{\sqrt{2}}(|000\rangle + i|\varphi''\rangle|\varphi\rangle|\varphi'\rangle), \tag{5.57}$$

while the one corresponding to outcome 1 is just the complex conjugate of (5.57). But we know that these two states are actually in the same orbit, so we can transform outcome 1 into (5.57) by local unitaries, so we obtain (5.57) with probability 1. The state in (5.57) is the same as in (5.41). This concludes the protocol. □

Note that all three steps involve only local unitaries and deterministic POVMs, so these protocols allow Alice, Bob and Charlie to transform the GHZ state into any other real state that belongs to the subclass defined by $\Re e(\Omega) = 0$ with probability 1, using only local operations and classical communication. This is then a complete characterization of the real states that can be obtained from the GHZ state, since by Theorem 8 we know that we cannot reach real states that belong to a different

subclass. It is interesting to note that it does not seem to be that easy to find a deterministic protocol to transform the GHZ state into any complex state in the same subclass. Whether this is actually possible is still an open question.

5.6 Summary and conclusions

In this chapter, we studied the properties of deterministic LOCC transformations of three-qubit pure states with tripartite entanglement. We showed that the set of states in the GHZ class breaks into an infinite number of disjoint subclasses, characterized by the real part of a complex function $\Omega(|\psi\rangle)$. Two states that belong to different subclasses cannot be transformed one into the other with probability one, by means of local operations and classical communication. This quantity is not only invariant under deterministic transformations, but it also must be conserved by any local POVM that is part of a deterministic protocol. This imposes a strong constraint on the POVMs that can be used for deterministically transforming a given state.

It is interesting to point out that the invariance of $\Re e(\Omega)$ under deterministic LOCC transformations (and its invariance under any local POVM that is part of such a transformation) follows from the invariance of Ω under local unitaries and the very particular form of Equation (5.9). In the language of entanglement monotones, we can say that $\Re e(\Omega)$ is both an increasing and decreasing entanglement monotone. Any function of the states that is invariant under local unitaries and satisfies an equation like (5.9) for an arbitrary local POVM, will be invariant under deterministic LOCC protocols, and hence will break the set of states into inequivalent classes that will be labeled by that function. This will be true even in the multipartite case, so identifying quantities with these properties could be very useful in the study of deterministic transformations of entanglement.

We also discussed the case of a deterministic 2-outcome POVM. We showed that for this POVM to exist, both the state and the parameters of the POVM have to satisfy certain polynomial conditions. In particular the coefficients of the state have to satisfy two polynomial constraints. To be able to apply a deterministic POVM to

a given state, we need to find a local unitary that will transform our original state into another state that satisfies the two constraints. For real states, the problem actually simplifies and only one constraint has to be satisfied. In this case, it was proven in general that the necessary local unitary could be found, allowing us to apply a local 2-outcome POVM that would send the state to some other orbit with probability 1. For complex states we found some analytical evidence that the unitary could be found, but a rigorous proof of this fact is still an open problem. However, it is important to stress that of all random numerical examples analyzed, the algorithm discussed in Section 5.3 never failed to find a gate state for complex states. We also discussed how several rounds of POVMs and local unitaries applied in sequence by all the parties allow us to reach a larger set of orbits than the one we get from only one POVM. There is a lot of freedom in choosing the order in which the parties apply a POVM and which POVM they choose. Although it is in general difficult to study this procedure analytically, in order to characterize the set of states that can be obtained from $|\psi\rangle$ (except for states with high symmetry like the GHZ state), a numerical analysis is easy to implement, and can be used to study general properties of this set, that could help us to have a better understanding of deterministic transformations.

Finally, we combined the two main results of this chapter to give a complete characterization of the real states that can be obtained from the GHZ state with probability 1. First we used the results of Section 5.2 to characterize the subclass of states that could in principle be obtained deterministically from it, and then we constructed an explicit protocol that allows the three parties to transform the GHZ state into any real state in that subclass. Finding a protocol to transform it to a complex state in the same subclass does not seem to be as easy, and thus whether this transformation is possible or not is still an open question.

Appendix A

Convex sets

A set $C \subseteq \mathbb{R}^n$ is said to be a *convex set* if it satisfies

$$x, y \in C, 0 \leq \lambda \leq 1 \Rightarrow \lambda\, x + (1 - \lambda)\, y \in C. \tag{A.1}$$

This property simply states that if two points belong to the set, so do all the points in the segment that connects them.

A point $y \in \mathbb{R}^n$ is said to be a *convex combination* of a set of points $\{x_i\}_{i=1}^m \subseteq \mathbb{R}^n$ if

$$y = \sum_{i=1}^{m} p_i x_i, \tag{A.2}$$

where the coefficients p_i satisfy $p_i \geq 0$ and $\sum_{i=1}^m p_i = 1$. We can use this concept to define the *convex hull* of a set S, which we will denote by $\mathrm{Co}(S)$, as

$$\mathrm{Co}(S) = \{y : y = \sum_{i=1}^{m} p_i x_i,\ \{x_i\}_{i=1}^m \subseteq S,\ p_i \geq 0,\ \sum_{i=1}^{m} p_i = 1\}. \tag{A.3}$$

The convex hull of a set S is equal to the intersection of all convex sets that contain the set S, so it can also be interpreted as the *smallest* convex set containing S.

A point x of a convex set $S \subseteq \mathbb{R}^n$ is said to be *extremal* if

$$x = \lambda y_1 + (1 - \lambda) y_2,\ \ y_1, y_2 \in S \Rightarrow (x = y_1 \wedge \lambda = 1) \vee (x = y_2 \wedge \lambda = 0). \tag{A.4}$$

Geometrically, it means that an extremal point does not belong to any proper segment

defined by two distinct elements of S. If E is the set of extremal points of S, then $S = \mathrm{Co}(E)$.

A set $K \subseteq \mathbb{R}^n$ is said to be a *cone* if it satisfies

$$x \in K, \lambda \geq 0 \Rightarrow \lambda x \in K. \tag{A.5}$$

For any given set S, we define the *cone generated by* S as

$$\mathrm{cone}(S) = \{y : y = \lambda x,\ \lambda \geq 0,\ x \in S\}. \tag{A.6}$$

A set $K \subseteq \mathbb{R}^n$ is a *convex cone* if

$$x, y \in K, \lambda, \mu \geq 0 \Rightarrow \lambda x + \mu y \in K. \tag{A.7}$$

If an inner product $\langle , \rangle$ is defined, we can associate with any cone its *dual cone*, noted by K^* and defined by

$$K^* = \{y : \langle y, x \rangle \geq 0, \forall x \in K\}. \tag{A.8}$$

Note, that this definition depends on the inner product considered. First of all, it is easy to see that K^* is in fact a convex cone. It is always a closed set, even if the cone K is not closed. A very important property (see [42]) is that

$$(K^*)^* = \mathrm{cl}(K), \tag{A.9}$$

where $\mathrm{cl}(K)$ represents the closure of K.

Appendix B

Solution of $\mathbf{I}_i(x,y) = \mathbf{I}_i(1-x,1-y)$

We want to know under which conditions does (5.23) have a nontrivial solution (i.e., $x \neq y$ and $x, y \neq 0, 1$). We will consider only states that have 3-particle entanglement, which means that $a, b \neq 0, 1$. First, let us note that we can write $I_1(x,y)$ as

$$I_1(x,y) = 1 + \frac{2xy(\mathrm{Tr}[T_0T_1^\dagger]\mathrm{Tr}[T_1T_0^\dagger] - ab)}{(ax+by)^2}, \tag{B.1}$$

where $(\mathrm{Tr}[T_0T_1^\dagger]\mathrm{Tr}[T_1T_0^\dagger] - ab) \neq 0$ if $|\psi\rangle$ has 3-particle entanglement. Then $I_1(x,y) = I_1(1-x,1-y)$ has a solution if and only if

$$\frac{xy}{(ax+by)^2} = \frac{(1-x)(1-y)}{(a(1-x)+b(1-y))^2}, \tag{B.2}$$

which is the same as

$$a^2x(1-x) = b^2y(1-y). \tag{B.3}$$

This also implies that $I_4(x,y) = I_4(1-x,1-y)$. Both I_2 and I_3 have the form

$$I_i(x,y) = \frac{F_0x^2 + F_1y^2 + 2C_ixy}{(ax+by)^2}, \quad i = 2,3. \tag{B.4}$$

We can use (B.2) to write $I_i(x,y) = I_i(1-x,1-y), i = 2,3$, as

$$\frac{F_0 + F_1z^2}{(a+bz)^2} = \frac{F_0 + F_1w^2}{(a+bw)^2}, \tag{B.5}$$

where we introduced the variables $z = \frac{y}{x}$ and $w = \frac{(1-y)}{(1-x)}$. From (B.3) we see that these variables are not independent, and satisfy the condition $zw = (\frac{a}{b})^2$. Furthermore, both z and w are positive, since x and y are between 0 and 1. If we expand (B.5) and use the relationship between z and w, we have

$$(F_0 b^2 - F_1 a^2)(z\frac{(a^2+b^2)}{a^2} + 2\frac{a}{b}) = 0, \tag{B.6}$$

and since z has to be positive (and a and b are positive), we have the condition

$$a^2 F_0 = b^2 F_1, \tag{B.7}$$

which is Equation (5.24).

To study the equation $I_5(x,y) = I_5(1-x, 1-y)$ we can assume that both (B.7) and (B.3) are satisfied, since we are looking for a *simultaneous* solution of (5.23). Let $\mu = I_5(x,y)$. Introducing $z = \frac{y}{x}$ and using (5.22) we can write

$$G_{00} + 3G_{01}z + 3G_{10}z^2 + G_{11}z^3 = \mu(a+bz)^3, \tag{B.8}$$

where $G_{ij} = \mathrm{Tr}[T_i T_j^\dagger T_i T_i^\dagger T_j T_i^\dagger]$, and we can expand this into

$$(G_{00} - \mu a^3) + 3(G_{01} - \mu a^2 b) + 3(G_{10} - \mu a b^2)z^2 + (G_{11} - \mu b^3) = 0. \tag{B.9}$$

A root of this cubic polynomial represents an operator of a POVM for which the value of I_5 for the outcome of that operator is μ. We are looking for two operators whose outcomes have the same value of I_5, but that also satisfy Equation (B.3). That is the same as finding two roots z_0 and z_1 of (B.9), that satisfy the condition

$$z_0 z_1 = \frac{a^2}{b^2}. \tag{B.10}$$

Let z_2 be the third root of (B.9). From elementary algebra we know that the product of the three roots is equal to minus the quotient of the independent and the cubic

coefficients, so we can write

$$z_0 z_1 z_2 = -\frac{G_{00} - \mu a^3}{G_{11} - \mu b^3} = -\frac{a^3}{b^3}\frac{\frac{G_{00}}{a^3} - \mu}{\frac{G_{11}}{b^3} - \mu}. \tag{B.11}$$

Using (B.7) and the Cayley-Hamilton theorem, it can be shown that

$$\frac{G_{00}}{a^3} = \frac{G_{11}}{b^3}, \tag{B.12}$$

so (B.11) reduces to

$$z_0 z_1 z_2 = -\frac{a^3}{b^3}. \tag{B.13}$$

If we want (B.10) to be satisfied we need $z_2 = -\frac{a}{b}$. If we plug this into (B.9), we find that z_2 is actually a root if and only if

$$b\ G_{01} = a G_{10}, \tag{B.14}$$

which is Equation (5.25). There is one more detail we need to check. We need $z_0 = \frac{y}{x}$ and $z_1 = \frac{1-y}{1-x}$ to be positive numbers, because x and y are between 0 and 1, and only one of them should be greater than 1 (which can be seen from their explicit form in terms of x and y). We know that the other root $z_2 = -\frac{a}{b}$ is negative, so the condition for only one of them to be greater than 1 can be written

$$(z_0 - 1)(z_1 - 1)(z_2 - 1) > 0. \tag{B.15}$$

Expanding this inequality we get

$$z_0 z_1 z_2 - (z_0 z_1 + z_0 z_2 + z_1 z_2) + (z_0 + z_1 + z_2) - 1 > 0. \tag{B.16}$$

All the symmetric polynomials on the roots of a polynomial equation can be written in terms of the coefficients of that polynomial, so we can rewrite this inequality as

$$-\frac{(G_{00} - \mu a^3)}{(G_{11} - \mu b^3)} - 3\frac{(G_{01} - \mu a^2 b)}{(G_{11} - \mu b^3)} - 3\frac{(G_{10} - \mu a b^2)}{(G_{11} - \mu b^3)} - 1 > 0. \tag{B.17}$$

Expanding this and using $a + b = 1$ we get

$$G_{00} + 3\ G_{01} + 3\ G_{10} + G_{11} > \mu. \tag{B.18}$$

But the left-hand side is just the value of I_5 for the state $|\psi\rangle$, while μ is the value of I_5 for the transformed state $|\phi_0\rangle$ (or $|\phi_1\rangle$). So this condition is telling us that under a deterministic 2-outcome POVM, I_5 behaves monotonically, even though it is not an entanglement monotone in general.

Bibliography

[1] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach. Generalized Schmidt decomposition and classification of three-quantum-bit states. *Phys. Rev. Lett.*, 85:1560, 2000.

[2] A. Acín, A. Andrianov, E. Jané, and R. Tarrach. Three-qubit pure-state canonical forms. *J. Phys. A: Math. Gen.*, 34:6725, 2001.

[3] A. Acín, E. Jané, W. Dür, and G. Vidal. Optimal distillation of a GHZ state. *Phys. Rev. Lett.*, 85:4811, 2000.

[4] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195, 1964.

[5] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE, New York, 1984.

[6] C. H. Bennett, G. Brassard, C. Crépeau, R Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[7] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[8] D. Bruss, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera. Reflections upon separability and distillability. *J. Mod. Opt.*, 49:1399–1418, 2002.

[9] H. Carteret, A. Higuchi, and A. Sudbery. Multipartite generalisation of the Schmidt decomposition. *J. Math. Phys.*, 41:7932, 2000.

[10] C. M. Caves, C. A. Fuchs, and R. Schack. Unknown quantum states: The quantum de Finetti representation. *Journal of Mathematical Physics*, 43:4537–4559, 2002.

[11] N. J. Cerf, C. Adami, and R. M. Gingrich. Reduction criterion for separability. *Phys. Rev. A*, 60:898, 1999.

[12] M.-D. Choi. Positive semidefinite biquadratic forms. *Linear Algebra and Its Applications*, 12:95–100, 1975.

[13] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:52306, 2000.

[14] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer, New York, 1992.

[15] D. Deutsch. Quantum theory, the Church-Turing Principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97, 1985.

[16] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Distinguishing separable and entangled states. *Phys. Rev. Lett.*, 88(18):187904, 2002.

[17] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. A complete family of separability criteria. In preparation, 2003.

[18] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62:62314, 2000.

[19] A. Einstein, B. Podolsky, and N. Rosen. Can quantum mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[20] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[21] M. Fannes, J. T. Lewis, and A. Verbeure. Symmetric states of composite systems. *Letters in mathematical physics*, 15:255–260, 1988.

[22] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467, 1982.

[23] M. R. Garey and D. S. Johnson. *Computers and intractability: A guide to the Theory of NP-Completeness.* W. H. Freeman, San Francisco, 1980.

[24] R. M. Gingrich. Private communication.

[25] R. M. Gingrich. Properties of entanglement monotones of three-qubit pure states. *Phys. Rev. A*, 65:52302, 2002.

[26] N. Gisin. Private communication. For the intuition behind this state, see N. Gisin and S. Wolf, "Linking classical and quantum key agreement: Is there bound information?" Advances in cryptology – Proceedings of Crypto 2000, Lecture Notes in Computer Science, 1880, 482-500, 2000; R. Renner and S. Wolf, "New bounds in secret-key agreement: the gap between information and secrecy extraction," to appear in Proceedings of EUROCRYPT '03.

[27] L. Gurvits. Quantum matching theory with new complexity theoretic, combinatorial and topological insights on the nature of quantum entanglement. Los Alamos electronic archive, `quant-ph/0201022`, 2002.

[28] M. Horodecki and P. Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Phys. Rev. A*, 59:4206, 1999.

[29] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1, 1996.

[30] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Phys. Rev. Lett.*, 80(24):5239–5242, 1998.

[31] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and quantum communication. Los Alamos electronic archive, `quant-ph/0109124`, 2001.

[32] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232:333, 1997.

[33] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, 3:275, 1972.

[34] N. Linden and S. Popescu. On multi-particle entanglement. *Fortsch. Phys.*, 46:567, 1998.

[35] H-K. Lo and S. Popescu. Concentrating entanglement by local actions: Beyond mean values. *Phys. Rev. A*, 63:022301, 2001.

[36] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83:436, 1999.

[37] M. A. Nielsen and J. Kempe. Separable states are more disordered globally than locally. *Phys. Rev. Lett.*, 86:5184, 2001.

[38] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77(8):1413–1415, 1996.

[39] G. A. Raggio and R. F. Werner. Quantum statistical mechanics of general mean field systems. *Helvetica Physica Acta*, 62:980–1003, 1989.

[40] B. Reznick. Some concrete aspects of Hilbert's 17th problem. In *Contemporary Mathematics*, volume 253, pages 251–272. American Mathematical Society, 2000.

[41] E. Størmer. Symmetric states of infinite tensor products of C^*-algebras. *J. Func. Anal.*, 3:48, 1969.

[42] R. T. Rockafellar. *Convex Analysis.* Princeton University Press, Princeton, NJ, 1970.

[43] B. Schumacher. Private communication.

[44] P. W. Shor. Algorithms for quantum computation: Discrete logarithm and factoring. In S. Goldwasser, editor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, page 124. IEEE Computer Society, Los Alamitos, 1994.

[45] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4):2493–2496, 1995.

[46] A. M. Steane. Multiple particle interference and quantum error correction. *Phys. Rev. Lett.*, 77:793, 1996.

[47] J. Sturm. Sedumi version 1.05. available from http://fewcal.kub.nl/sturm/software/sedumi.html, 2001.

[48] A. Sudbery. On local invariants of pure three-qubit states. *J. Phys. A*, 34:643, 2001.

[49] Barbara M. Terhal. Bell inequalities and the separability criterion. *Phys. Lett. A*, 271(5–6):319–326, 2000.

[50] L. Vandenberghe and S. Boyd. Convex optimization. http://www.stanford.edu/~boyd/cvxbook.html.

[51] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.

[52] G. Vidal. Private communication.

[53] G. Vidal. Entanglement of pure states for a single copy. *Phys. Rev. Lett.*, 83:1046, 1999.

[54] G. Vidal. Entanglement monotones. *J. Mod. Opt.*, 47:355, 2000.

[55] R. F. Werner. An application of Bell's inequalities to a quantum state extension problem. *Lett. Math. Phys.*, 17:359, 1989.

[56] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40(8):4277–4281, 1989.

[57] S. L. Woronowicz. Positive maps of low dimensional matrix algebras. *Rep. in Math. Phys.*, 10:165–183, 1976.