A Discourse on Entanglement and its Detection in Finite Dimensions

Thiago de Oliveira Maciel

August 2011

A Discourse on Entanglement and its Detection in Finite Dimensions

Thiago de Oliveira Maciel

Orientador:

Prof. Dr. Reinaldo Oliveira Vianna

Dissertação apresentada à UNIVERSIDADE FEDERAL DE MINAS GERAIS - UFMG, como requisito parcial para a obtenção do grau de MESTRE EM FÍSICA.

Belo Horizonte
Brasil
Agosto de 2011

Dedicate

To my grandfather Mário Gaspar Maciel: which is — and always will be — my greatest *exempli*.

Agradecimentos

Não há como não agradecer, primeiramente, à minha família: a meu pai Ademar e à minha mãe Nara, eles são, simplesmente, os melhores pais que eu poderia ter; à minha irmã Velise, que — graças à ela — pude ir e voltar todos os dias da universidade; à minha irmã Taísa, que me ajuda tanto — nem sei se um dia conseguirei retribuir tudo (*cf.* esta dissertação escrita toda em inglês: obrigado, mana) —; às minhas tias (Delourdes e Izabel) e tios (Paulo e Sérgio, do lado do pai e Jorge, por parte da mãe), primas (Ceres, Cibele, Jaqueline, Caroline, Gabriela, Daniele, Pâmella e, agora, Gisele), primos (Bruno, Charles, Fábio, Alex, Deivid, Michel, Marcos e, agora, Marcus), agregados e agregadas — que geram todo o meu contexto familiar que me faz ser quem sou e onde as bases para o que ainda posso ser foram construídas — e, claro, ao meu avo Mário Gaspar Maciel: a quem dedico esta dissertação.

Em especial, agradeço ao pessoal do Infoquant (Reinaldo, André Tanus, Debarba e Fernando) e as *ladies* e *gentlemen* (Geraldo, Campô, Mário Mazzoni, Michelle, Ana Paula, Monique e Luciana Cambraia), mas, independente de qualquer coisa, sempre serei grato aos meus amigos e amigas, que sempre tento cultivar da melhor forma possível: Geraldo, Campô, André Tanus, André Arruda, Michelle, Debarba, Fernando, Ana Paula, Jaque, Ingrid, Julia, Luciana Cambraia, Monique, Mateus, Marco Túlio, Érico, Gláucia, Amanda, Junior, Hobbit, Léo, Gabi, Gabi, Denise, Wanderson, Alex Bueno, Gustavão, Marina, Breno Rotelli, Simone Boff, Isabel Sager, Badaia, Bárbara morena, Bárbara ruiva, Camila, Farley, Palhacinho, Guilherme Almeida, Guilherme (André Matos), Hayssa, Lígia, Lídia, Emílson, Henrique Elias, Lilí, Peter Jaques, Zé Geraldo, Adriani Simonete, Narciso Hansen, Linei Rocha, Reinaldo Portanova, Atos e os Bandidos[i]. Sem a ajuda do meu amigo π[ii], não saberia da minha primeira oportunidade de bolsa de iniciação científica com o Reinaldo, portanto, agradeço a ele por isso. Agradeço, também, a Izabella Amim Gomes: que conheço há uns dez anos e por quem tenho um carinho muito especial.

Separo um parágrafo para agradecer a Cyntia, que — na falta de verbetes adequados — digo que preenche os espaços da minha vida com belíssimos interlúdios.

Agradeço, também, ao meu professor e amigo Mário Mazzoni: grande parte do que aprendi sobre física fora ensinado por ele. Também, ao Sebastião

[i] Enumerar pessoas é sempre uma tarefa inglória, perdoem-me caso tenha deixado de citar alguém.

[ii] Que, escrito assim, não preciso truncar.

de Pádua e ao C. H. Monken, que — devido às grandes discussões e ensinamentos — entendo, hoje, que o que acontece no laboratório é muito diferente de calcular traços de produtos de operadores hermiteanos.

E, claro, agradeço ao meu orientador, professor e amigo Reinaldo Oliveira Vianna: sem a oportunidade de trabalhar com ele, nenhuma palavra estaria escrita neste discurso. Obrigado por me dar a oportunidade de enxergar a mecânica quântica dessa belíssima forma e que, hoje, gera esta dissertação.

Esta dissertação teve o apoio financeiro direto e indireto da **CAPES**, **FAPEMIG** e **CNPq**.

Abstract

We explore procedures to detect entanglement of unknown mixed states, which can be experimentally viable. The heart of the method is a hierarchy of semi-definite programs, which provides sufficient conditions to entanglement. Our numerical investigations indicate that the entanglement is detected with a cost which is much lower than full state tomography. The procedure is applicable to both free and bound entanglements and involves only single copy measurements. The discourse involves density matrices and its properties, quantum manipulations, entanglement and its detection.

Keywords

entanglement, quantum information, quantum maps, positive maps, completely positive maps, positive operators, block positive operators, semidefinite programs, SDP, entanglement witness, decomposable maps, Kraus operators, Choi operators, Choi map, detecting entanglement, convex sets, density matrices, MUBs.

Resumo

Desenvolvemos um método a fim de explorar a detecção do emaranhamento em estados desconhecidos sem tomografia completa. O coração do método está na hierarquia de programação semi-definida. Temos evidências numéricas que indicam que detectar emaranhamento com informação incompleta é possível e tem um custo menor que uma tomografia completa de estado. O método é aplicável tanto ao emaranhamento livre, quanto preso e envolve medições simples. O discurso aborda matrizes densidades, operações quânticas, caracterização e medição de emaranhamento.

Palavras-chave

emaranhamento, informação quântica, operações quânticas, mapas positivos, mapas completamente positivos, operadores positivos, operadores bloco-positivos, programação semidefinida, SDP, testemunhas de emaranhamento, mapas decomponíveis, operadores de Kraus, operadores de Choi, mapa de Choi, detecção de emaranhamento, conjuntos convexos, matriz densidade, MUBs.

Contents

List of Figures

List of Tables

CHAPTER 1

Preface: why do we study entanglement?!

> "Entanglement is not *one* but rather *the* characteristic trait of quantum mechanics".
>
> - Erwin Schrödinger

One of the challenges of understanding nowadays physics is that some of the concepts seem quite abstract when we are discussing about microscopic objects outside the realm of everyday experience. Conventional knowledge holds that quantum mechanics is hard and tough to learn: which is more or less correct — often overstated though —. However, the necessity of abandoning conventional ways of thinking about the world and finding a radically new way — the *quantum mechanical* way — may be understood by any curious person willing to spend some mathematics and time concentrating hard. Conveying that understanding is the purpose of this discourse, in particular, we focus on — as Schrödinger said — *the* characteristic trait of quantum mechanics: *entanglement*[i]. This exclusive property of quantum systems — which keeps coming back to haunt us — leads the main road of the discourse.

The standard explanation is based on the historical development of quantum mechanics. During that time there were a series of crises to describe the microscopical world in physics. The pattern was that each time some experimental fact would be noticed that seemed hard to explain with the old "classical" way of viewing the world. Each time, physicists would bandage over the old classical thinking with an *ad hoc* bandaid. This happened over and over again until, in the mid-1920s, the sick patient of classical physics of microscopical world finally keeled over completely and was replaced with the new framework of quantum mechanics.

[i] Originally called by Schrödinger *verschränkung*: which underlines an intrinsic order of statistical relations between subsystems of compound quantum systems.

The problem with this style of explanation, and what makes it confusing, is that none of those early crises was entirely clearcut. In each case, there were physicists who argued that the new experimental results could be explained pretty well with a conventional classical picture.

Imagine one tossing a coin and checking whether is heads or tails. This process of figuring out whether the coin is heads or tails is what physicists call a *measurement process*. In physicists' language, what is going on when we look at the coin is that we are *measuring* a two-valued or *binary property* of the coin. This usage of the term measurement is somewhat different from everyday usage, where, *e.g.*, we might measure something with a ruler. But the basic idea is the same: a measurement is a process that determines a physical property — whether it be the length of an object, or the side a coin has landed —.

All this language may seem pedantic: we are just looking at a coin! But it comes in handy when we move from the conventional concepts to standard knowledge. At this point, looking to the quantum mechanics scenario, it is worth quote[ii] Reinaldo Vianna: "In the end, what really matters is the 'click' on the detector.". We believe that no one will look to quantum mechanics in a 'spooky' way following this spirit.

The present-day entanglement theory has its roots in the key discoveries: quantum cryptography with Bell theorem; quantum dense coding and quantum teleportation — including teleportation of entanglement of EPR pairs (so-called entanglement swapping) —. All such effects are based on entanglement and all of them have been demonstrated in pioneering experiments. In fact, all these results — including the idea of quantum computation — were a basis for a new interdisciplinary domain called *quantum information*: which have entanglement as a central notion.

Although the reason why we study entanglement is the outstanding applications of this property as resource, it is still a property of quantum compound systems: which needs to be studied carefully and deeply. We will dissect it keenly — with aid of powerful mathematical tools —.

To explore the subject in this keenly fashion, we assume that the reader has the standard lore in quantum mechanics. One remark should be done though: most of the material here has been presented before — this is true for all the literature review and most of the original work —. We just fit it in the main road.

Now, let us explain the road to entanglement presented here in this discourse. In the chapter *Nice to meet you, density matrix!*, we intent to expose and unravel aspects of a density matrix which is forgotten in the standard lore: the concepts of convex sets and positivity of Hermitian matrices.

In the chapter *Let entanglement be your puppet: manipulations of quantum states*, we gave a unified mathematical representation for quantum manipulations. We are pretty sure that — after reading this chapter — the reader will be able to comprehend a vast part of the nowadays literature in the subject.

In the chapter *Entang' what?! Entanglement as a quantum property of compound systems*, we present entanglement as a property in its full glory, with

[ii] Which became the chapter's *A 'click' on the detector: measuring entanglement* epigraph.

aid of separability criterions, entanglement witness, (un)decomposable maps and describe how we characterize entanglement in a numerical approach.

Finally, equipped with all mathematical tools of the previous chapters, in the last one, *A 'click' on the detector: measuring entanglement*, we make use of them and present our — Thiago O. Maciel *et al.* — work on the subject: checking entanglement with incomplete information about the state — *cf.* [1] —.

We hope you enjoy it!

CHAPTER 2

Nice to meet you, density matrix!

> "[...] the most universal picture which remains after the details are forgotten is that of a convex set.".
>
> - Bogdan Mielnik

Following the spirit of this discourse, we will start the discussion of properties of the object which we used to describe quantum states: *the density matrix*. One might be satisfied with the standard lore of the subject [2, 3][i] in the context of quantum mechanics — but we will explore a little bit further[ii] —. One *bona fide* density matrix should satisfy the following conditions:

$$(i) \quad \textit{Hermitian,} \qquad \rho = \rho^{\dagger}; \tag{2.1}$$

$$(ii) \quad \textit{positive semi-definite,} \qquad \rho \geq 0; \tag{2.2}$$

$$(iii) \quad \textit{normalized,} \qquad tr(\rho) = \|\rho\|_1 = 1. \tag{2.3}$$

But the trace one positive semidefiniteness of the density matrix ρ yields (mathematical) properties which should be unraveled to a careful reader. We start exploring the convex properties of the set of states and, then, go through the conditions *(i)* and *(ii)*: whereas *(ii)* implies *(i)* for complex Hermitian matrices.

2.1 The space of density matrices as a convex set

Let us state some general facts and definitions (*cf.* [5]). There is a restriction that arises naturally in quantum mechanics[iii]: the states set must be a *convex set*. A set in which one may form 'mixtures' of any points in the set.

[i] And so many others.

[ii] *Cf.* [4] and the section 2.2 for more details.

[iii] In classical statistics also.

In a geometric point of view, the mixture of two states may be defined as one point on the segment of the straight line between the two points that represent what we want to mix. In a convex set, all mixtures of this type generates one state belonging to the same set. But, before we see how this restricts the set of the states, we must define what we mean by *straight lines*.

An *affine space* is just like a flat Euclidean space $\mathcal{E}^N$ of dimension N, except that no special choice of origin is assumed. Thus, one *straight line* through the two points ρ_1 and ρ_2 is defined by

$$\rho = p_1\rho_1 + p_2\rho_2, \quad p_1 + p_2 = 1. \tag{2.4}$$

If we choose one origin in ρ_0, we see that this generates one plane spanned by the vectors $\rho_1 - \rho_0$ and $\rho_2 - \rho_0$. Then, one K-dimensional plane is obtained by taking $K+1$ generic points (with $K < N$). We call this plane as a *hyperplane*. For $K = N$, we describe the entire space $\mathcal{E}^N$.

An *affine map* is a transformation that takes lines to lines and preserves the relative length of line segments lying on parallel lines, *i.e.*, a linear transformation described by one matrix Λ with a translation along a constant vector σ ($\Lambda\rho + \sigma$) where Λ is an invertible matrix.

We define a subset of this affine one as a *convex set* if, for any pair of points ρ_1 and ρ_2 belonging to the set, it is true that the *mixture* ρ belongs to the set also, *i.e.*,

$$\rho = p_1\rho_1 + p_2\rho_2, \quad p_1 + p_2 = 1, \quad p_1, p_2 \geq 0. \tag{2.5}$$

The requirement $p_1, p_2 \geq 0$ restricts ρ to belong to the segment of the line lying between the pair of points. The generalization to more points follows from the definition.

We used an affine space as the 'container' for the convex sets since convexity properties are preserved by general affine transformations, which are common in quantum mechanics.

Given any subset of the affine space, we define the *convex hull* of this subset as the smallest convex set that contains the set. The convex hull of a finite set of points is called a *convex polytope*. if we take $p+1$ points that are not confined to any $(p-1)$-dimensional subspace, then the convex polytope is called a *p-simplex*, *i.e.*,

$$\rho = p_1\rho_1 + \cdots + p_p\rho_p, \quad \sum_{i=1}^{p} p_i = 1, \quad p_i \geq 0. \tag{2.6}$$

The *dimension* of a convex set is the largest number N such that the set contains an N-simplex. A closed and bounded convex set that has an interior is known as a *convex body*. Convex bodies always contain some special points that cannot be obtained as mixtures of other points: these points are called *pure points*, while non-pure points are called *mixed*.

Let us quote two useful theorems:

Theorem 1 (Minkowski [6])**.** *Any convex body is the convex hull of its pure points.*

Theorem 2 (Carathéodory [7]). *If X is a subset of $\mathbb{R}^d$, then any point in the convex hull of X can be expressed as a convex combination of at most $d+1$ points in X.*

Thus, any point ρ of a convex body S may be expressed as a *convex combination* of pure points, *i.e.*,

$$\rho = \sum_{i=1}^{p} p_i \rho_i, \quad \sum_{i=1}^{p} p_i = 1, \quad p_i \geq 0, \quad p \leq d+1. \tag{2.7}$$

Take $\mathcal{L}(\mathcal{H})$ as the space of linear Hermitian operators on $\mathcal{H}$: this is a real vector space of dimension $d = N^2 - 1$. The set $\mathcal{L}_+(\mathcal{H})$ of positive operators is a convex cone in this space. The set of strictly positive operators is denoted $\mathcal{L}_{++}(\mathcal{H})$. It is an open set in $\mathcal{L}(\mathcal{H})$ and is a convex cone, also. We will find much use for the concept of *convex functions*. If f is a map of $\mathcal{L}(\mathcal{H})$ into itself, we say f is *convex* if

$$f((1-\alpha)\rho + \alpha\sigma) \leq (1-\alpha) f(\rho) + \alpha f(\sigma) \tag{2.8}$$

for all ρ and $\sigma \in \mathcal{L}(\mathcal{H})$ and $0 \leq \alpha \leq 1$. If f is continuous, then f is convex if, and only if,

$$f\left(\frac{\rho+\sigma}{2}\right) \leq \frac{f(\rho)+f(\sigma)}{2} \tag{2.9}$$

for all ρ and σ. We say f is *monotone* if $f(\rho) \geq f(\sigma)$ whenever $\rho \geq \sigma$, *i.e.*, $\rho - \sigma \geq 0$ is positive semidefinite.

As ρ is Hermitian, any density matrix can be diagonalized: the set of density matrices that are diagonal in a given basis $\{|e_i\rangle\}$ can be written as

$$\rho = \sum_{i=1}^{N} \lambda_i |e_i\rangle\langle e_i|, \quad \rho|e_i\rangle = \lambda_i |e_i\rangle \quad \text{and} \quad \sum_{i=1}^{N} \lambda_i = 1. \tag{2.10}$$

This set is known as *eigenensemble*, or as the *eigenvalue simplex*[iv]. It forms a particular $(N-1)$-dimensional cut through the set of density matrices — and every density matrix are placed in some eigenvalue simplex —.

The *rank* of a point in a convex set is the minimum number r of pure points that are needed to express it as a convex combination of pure states. Thus, a density matrix of matrix rank r may be written as a convex sum of no less than r projectors — obviously, when diagonalized —. Hence, the maximal rank of a mixed state is equal to N, which is much less than the upper bound N^2 given by the Carathéodory's theorem 2.

But this is not every possible mixture, *e.g.*, the maximally mixed state $\rho_\star$ may be obtained as a mixture of pure states by setting equal weights. We may obtain $\rho_\star$ in many other ways. A similar non-uniqueness afflicts all mixed states: interestingly, this may be expressed in a precise way as follows:

Theorem 3 (Schrödinger's mixture theorem [8]). *A density matrix ρ, having the diagonal form*

$$\rho = \sum_{i=1}^{N} \lambda_i |e_i\rangle\langle e_i|,$$

[iv] It is a simplex since the eigenvalues are positive and sum to one.

may be written in the form

$$\rho = \sum_{i=1}^{M} p_i |\psi_i\rangle\langle\psi_i|, \quad \sum_{i=1}^{M} p_i = 1, \quad p_i \geq 0$$

if, and only if, there exist a unitary $M \times M$ matrix U such that

$$|\psi_i\rangle = \frac{1}{\sqrt{p_i}} \sum_{j=1}^{N} U_{ij} \sqrt{\lambda_i} |e_i\rangle.$$

Here, all states are normalized to unit length but they need not be orthogonal to each other.

2.2 Positive Semidefinite Matrices

The theory of positive definite matrices, positive definite functions and positive linear maps is rich in content. It offers many beautiful theorems that are simple and yet ingenious in their proof, diverse as well powerful in their application. We start with a glimpse of some of the basic properties of positive matrices. This will lead us to main road of the line of thinking followed through the discourse. We will bring mathematical tools in their full glory to dissect the desired properties in the quantum context.

2.2.1 Characterizations

Let $\mathcal{H}^N$ be the N-dimensional Hilbert space $\mathbb{C}^N$. The inner product between two vectors $|\psi\rangle$ and $|\phi\rangle$ is written as $\langle\psi|\phi\rangle$[v]. We denote by $\mathcal{L}(\mathcal{H})$ the space of all linear operators on $\mathcal{H}$ — sometimes, just a subspace: the space of $N \times N$ matrices of complex entries —. Every element ρ of $\mathcal{L}(\mathcal{H})$ can be identified with its matrix with respect to the standard (canonical) basis $\{|i\rangle\}$ of $\mathbb{C}^N$. We say ρ is *positive semidefinite* if

$$\langle\psi|\rho|\psi\rangle \geq 0 \quad \text{for all} \quad |\psi\rangle \in \mathcal{H}, \tag{2.11}$$

and *positive definite* if, in addition,

$$\langle\psi|\rho|\psi\rangle > 0 \quad \text{for all} \quad |\psi\rangle \in \mathcal{H}. \tag{2.12}$$

A positive semidefinite matrix is positive definite if, and only if, it is invertible.

For the sake of simplicity, we use the term *positive* matrix for a positive semidefinite — or a positive definite — matrix. Sometimes, if we want to emphasize that the matrix is positive definite, we say that it is *strictly positive*. We use the notation $\rho \geq 0$ to mean that ρ is positive and $\rho > 0$ to mean it is strictly positive.

There are some conditions that characterize positive matrices. Some of them are listed below.

[v] Adopting the convention that the inner product is conjugate linear in the first variable and linear in the second.

(i) ρ is positive if, and only if, it is Hermitian — *i.e.* , $\rho = \rho^\dagger$ — and all its eigenvalues are nonnegative; ρ is strictly positive if, and only if, all its eigenvalues are positive;

(ii) ρ is positive if, and only if, it is Hermitian and all its principal minors are nonnegative; ρ is strictly positive if, and only if, all its principal minors are positive;

(iii) ρ is positive if, and only if, $\rho = AA^\dagger$ for some matrix A; ρ is strictly positive if, and only if, A is nonsingular;

(iv) ρ is positive if, and only if, $\rho = T^\dagger T$ for some upper triangular matrix T. Further, T can be chosen to have nonnegative diagonal elements. If ρ is strictly positive, then T is unique. This is called *Cholesky decomposition* of ρ; ρ is strictly positive if, and only if, T is nonsingular;

(v) ρ is positive if, and only if, $\rho = A^2$ for some positive matrix A. Such a A is unique. We write $A = \rho^{1/2}$ and call it the (positive) square root of ρ; ρ is strictly positive if, and only if, A is strictly positive;

(vi) ρ is positive if, and only if, there exist $|\psi_1\rangle, \dots, |\psi_n\rangle \in \mathcal{H}^N$ such that

$$\rho_{ij} \equiv \langle \psi_i | \psi_j \rangle;$$

ρ is strictly positive if, and only if, the vectors $|\psi_j\rangle$, $1 \leq j \leq n$, are linearly independent.

To illustrate the last condition, let $|\psi_1\rangle, \dots, |\psi_n\rangle$ be any n vectors in *any* Hilbert space. Then, the $N \times N$ matrix

$$G(|\psi_1\rangle, \dots, |\psi_n\rangle)_{ij} \equiv \langle \psi_i | \psi_j \rangle \tag{2.13}$$

is positive — being of the form $AA^\dagger$ —. It is strictly positive if, and only if, $|\psi_1\rangle, \dots, |\psi_n\rangle$ are linearly independent. The matrix G is called *Gram matrix* associated with the vectors $|\psi_1\rangle, \dots, |\psi_n\rangle$.

2.2.2 Some theorems

In this section, we present some theorems on positive matrices[vi]. Some concepts presented here are not that common in quantum literature — but may be useful at some point —. One remark should be done though: we will not make use of these following theorems — in this section and in the next one —- explicitly in this discourse. We present and illustrate them to *enforce* the symmetry conditions imposed by positivity in Hermitian matrices. Positive matrices are one special kind of matrix: which will be clear in the last chapter *A 'click' on the detector: measuring entanglement*.

Let ρ be a positive operator on $\mathcal{H}$. If X maps a Hilbert space $\mathcal{H}$ into $\mathcal{H}'$, then the operator $X\rho X^\dagger$ on $\mathcal{H}'$ is positive also. On the other hand, if X is an invertible operator — and $X\rho X^\dagger$ is positive —, then ρ is positive.

[vi] Details and proofs are can be founded in [4, 9, 10].

Take ρ and σ: two operators on $\mathcal{L}(\mathcal{H})$. We say that ρ is *congruent* to σ (and write $\rho \sim \sigma$) if there exists an invertible operator X on $\mathcal{L}(\mathcal{H})$ such that $\sigma = X\rho X^\dagger$. Congruence is an equivalence relation on $\mathcal{L}(\mathcal{H})$. If X is unitary, we say ρ is *unitarily equivalent* to σ (and write $\rho \simeq \sigma$).

If ρ is Hermitian, the *inertia* of ρ is the triple of nonnegative integers

$$In(\rho) \equiv (\pi(\rho), \zeta(\rho), \nu(\rho)), \tag{2.14}$$

where $\pi(\rho), \zeta(\rho)$ and $\nu(\rho)$ are the number of positive, zero and negative eigenvalues of ρ (counted with multiplicity).

The *Sylvester's law of inertia*[11, 12] says that $In(\rho)$ is a complete invariant for congruence on the set of Hermitian matrices — *i.e.*, two Hermitian matrices are congruent if, and only if, they have the same inertia —.

Let $\mathcal{H}'$ be a subspace of $\mathcal{H}$ and let P be the orthogonal projection onto $\mathcal{H}'$. If we choose an orthonormal basis in which $\mathcal{H}'$ is spanned by the first k vectors, then we can write an operator ρ on $\mathcal{H}$ as a block matrix

$$\rho = \begin{bmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{bmatrix}$$

and

$$P\rho P = \begin{bmatrix} \rho_{11} & 0 \\ 0 & 0 \end{bmatrix}.$$

If X is the one-to-one map of $\mathcal{H}'$ into $\mathcal{H}$, then $X\rho X^\dagger = \rho_{11}$. We say that ρ_{11} is the *compression* of ρ to $\mathcal{H}'$.

If ρ is (strictly) positive, then all its compressions are (strictly) positive. Conversely, if all the principal subdeterminants of ρ are nonnegative, then the coefficient in the characteristic polynomial of ρ alternate in sign. Hence — by the *Descartes' rule of signs*[vii] — ρ has no negative root.

Take $\rho_{[j]}$ denoting the $j \times j$ (for $1 \leq j \leq N$) block in the top left corner of the matrix ρ. We call this the *leading* $j \times j$ submatrix of ρ and its determinant, subdeterminant. If all the leading subdeterminants of a Hermitian matrix ρ are positive, then ρ is strictly positive[viii]. Positivity of other principal minors follows as a consequence.

We denote by $\rho \otimes \sigma$ the tensor product of two operators ρ and σ — acting possibly on different Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ —. As we already know from standard quantum lore[ix], if ρ and σ are positive, then $\rho \otimes \sigma$ is positive also.

If ρ and σ are $N \times N$ matrices, we write $\rho \circ \sigma$ for their entrywise product — *i.e.*, for the matrix which the entries are given by $\rho_{ij}\sigma_{ij}$ —. We call this *Schur*

[vii] The rule states that if the terms of a single-variable polynomial with real coefficients are ordered by descending variable exponent, then the number of positive roots of the polynomial is either equal to the number of sign differences between consecutive nonzero coefficients, or is less than it by a multiple of 2. Multiple roots of the same value are counted separately.

[viii] The example $\rho = \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix}$ is a clear example that non-negativity of the two leading subdeterminants is not adequate to ensure positivity of ρ

[ix] *Cf.* chapter *Let entanglement be your puppet: manipulations of quantum states.*

product[x]. If ρ and σ are positive, the so is $\rho \circ \sigma$. One way of seeing this is by observing that $\rho \circ \sigma$ is a principal submatrix of $\rho \otimes \sigma$[xi].

Take ρ and σ Hermitian — or positive — operators, then the sum $\rho + \sigma$ is positive also; their product $\rho\sigma$ is, however, Hermitian if, and only if, $[\rho,\sigma] = 0$: *i.e.*, ρ and σ commute. Let us take the *symmetrized product*, which reads

$$\mathrm{Y} = \rho\sigma + \sigma\rho. \tag{2.15}$$

Now, if both ρ and σ are Hermitian, then Y is Hermitian also. However, if ρ and σ are positive, then Y need not be positive: *e.g.*, the matrices

$$\rho = \begin{bmatrix} 1 & 0 \\ 0 & \alpha \end{bmatrix} \quad \text{and} \quad \sigma = \begin{bmatrix} 1 & \beta \\ \beta & 1 \end{bmatrix}$$

are positive if $\alpha > 0$ and $0 < \beta < 1$, but Y is not positive when α is close to zero and β is close to one. The fact that if Y is positive and ρ strictly positive, then σ is positive might be considered surprising: that is why we need to clarify.

Proposition 4. *Let ρ and σ be Hermitian and suppose ρ strictly positive. If the symmetrized product $\mathrm{Y} = \rho\sigma + \sigma\rho$ is (strictly) positive, then σ is (strictly) positive.*

Proof. Choose an orthonormal basis in which σ is diagonal: *i.e.*, $diag(\varsigma_1, \cdots, \varsigma_n)$. Then $\mathrm{Y}_{ii} = 2\varsigma_i\rho_{ii}$. Now, observe that the diagonal entries of a (strictly) positive matrix are (strictly) positive. □

An amusing corollary of Proposition 4 is a simple proof of the operator monotonicity of the map $\rho \mapsto \rho^{1/2}$ on positive matrices.

If ρ and σ are Hermitian, we say that $\rho \geq \sigma$ if $\rho - \sigma \geq 0$; and $\rho > \sigma$ if $\rho - \sigma > 0$.

Proposition 5. *If ρ and σ are positive and $\rho > \sigma$, then $\rho^{1/2} > \sigma^{1/2}$*

Proof. Using the identity

$$\rho^2 - \sigma^2 = \frac{(\rho+\sigma)(\rho-\sigma) + (\rho-\sigma)(\rho+\sigma)}{2}, \tag{2.16}$$

if ρ and σ are strictly positive, then $\rho + \sigma$ is positive also, so, if $\rho^2 - \sigma^2$ is positive, then $\rho - \sigma$ is positive — by Proposition 4 —. □

Remember that if $\rho \geq \sigma$, then we not always have $\rho^2 > \sigma^2$: *e.g.*, consider

$$\rho = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad \sigma = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

[x] Also called the *Hadamard product*.

[xi] $\left(\rho_{ij} \circ \sigma_{ij}\right)_{ij} = \left(\left(\rho_{ij} \otimes \sigma_{kl}\right)_{kl}\right)_{ij}$.

2.2.3 Block matrices

In pursuit of properties yielded by (non-)separable density matrices, the study of block matrices arises as by-product. Although not very common in quantum literature, we present some useful theorems.

We will see that simple 2×2 block matrices play remarkable role in the study of positive matrices.

Let ρ be a block matrix with entries A, B, C and D, $N \times N$ matrices: as $\rho = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$. So, ρ is an element of $\mathcal{L}(\mathcal{H}^{2N})$ — or $\mathcal{L}(\mathcal{H}^N \oplus \mathcal{H}^N)$ —. We will see that several properties of ρ can be obtained from those of a block matrix in which A is one of the entries.

We denote $A = UP$ for the *polar decomposition* of A, where U is unitary and P is positive. P can be read $P = (A^\dagger A)^{1/2}$: this is called the *positive part* — or the *absolute value* — of A and is written as $|A|$. We have $A^\dagger = PU^\dagger$ and

$$|A^\dagger| = (AA^\dagger)^{1/2} = (UP^2U^\dagger)^{1/2} = UPU^\dagger.$$

A is said to be normal if $AA^\dagger = A^\dagger A$. This condition is equivalent to $UP = PU$ and $|A| = |A^\dagger|$.

We write $A = USV$ for *singular value decomposition* (SVD) of A, where U and V are unitary and S is diagonal with nonnegative diagonal entries $s_1 \geq \cdots \geq s_N$: these are the singular values of A — or the eigenvalues of $|A|$ —.

The symbol $\|A\|$ will denote, in this section, the norm of A as a linear operator on the Hilbert space $\mathcal{L}(\mathcal{H})$, *i.e.*

$$\|A\| \equiv \sup_{\||\psi\rangle\|=1} \|A|\psi\rangle\| = \sup_{\||\psi\rangle\|\leq 1} \|A|\psi\rangle\|.$$

It is easy to see that $\|A\| = s_1$.

Some important properties of this norm are the following[xii]:

$$\|AB\| \leq \|A\|\|B\|; \tag{2.17}$$

$$\|A\| = \left\|A^\dagger\right\|; \tag{2.18}$$

$$\|A\| = \|UAV\|, \tag{2.19}$$

for all unitary U and V. This last property is called *unitary invariance*. Finally,

$$\left\|A^\dagger A\right\| = \|A\|^2. \tag{2.20}$$

There are other norms on $\mathcal{L}(\mathcal{H}^N)$ that satisfy the first three properties. It is the condition (2.20) that makes the operator norm $\|\cdot\|$ very special.

We say A is *contractive*, or A is a *contraction*, if $\|A\| \leq 1$.

Proposition 6. *The operator A is contractive if, and only if, the operator $\begin{bmatrix} \mathbb{1} & A \\ A^\dagger & \mathbb{1} \end{bmatrix}$ is positive.*

[xii] *Cf.* [4, 9]

Proof. Let $A = USV$, then

$$\begin{aligned}\begin{bmatrix} \mathbb{1} & A \\ A^\dagger & \mathbb{1} \end{bmatrix} &= \begin{bmatrix} \mathbb{1} & USV \\ V^\dagger S U^\dagger & \mathbb{1} \end{bmatrix} \\ &= \begin{bmatrix} U & O \\ O & V^\dagger \end{bmatrix} \begin{bmatrix} \mathbb{1} & S \\ S & \mathbb{1} \end{bmatrix} \begin{bmatrix} U^\dagger & O \\ O & V \end{bmatrix}\end{aligned}$$

This matrix is unitarily equivalent to $\begin{bmatrix} \mathbb{1} & S \\ S & \mathbb{1} \end{bmatrix}$, which in turn is unitarily equivalent to the direct sum

$$\begin{bmatrix} 1 & s_1 \\ s_1 & 1 \end{bmatrix} \oplus \begin{bmatrix} 1 & s_2 \\ s_2 & 1 \end{bmatrix} \oplus \cdots \begin{bmatrix} 1 & s_N \\ s_N & 1 \end{bmatrix},$$

where $s_1, \cdots, s_N$ are the singular values of A. These 2×2 matrices are all positive if, and only if, $s_1 \leq 1$ (*i.e.*, $\|A\| \leq 1$). □

Proposition 7. *Take A and B positive matrices, then the matrix $\begin{bmatrix} A & X \\ X^\dagger & B \end{bmatrix}$ is positive if, and only if, $X = A^{1/2} K B^{1/2}$ for some contraction K.*

Proof. Assume first that A and B are strictly positives. Thus allow us to use the congruence

$$\begin{aligned}\begin{bmatrix} A & X \\ X^\dagger & B \end{bmatrix} &\sim \begin{bmatrix} A^{-1/2} & O \\ O & B^{-1/2} \end{bmatrix} \begin{bmatrix} A & X \\ X^\dagger & B \end{bmatrix} \begin{bmatrix} A^{-1/2} & O \\ O & B^{-1/2} \end{bmatrix} \\ &= \begin{bmatrix} \mathbb{1} & A^{-1/2} X B^{-1/2} \\ B^{-1/2} X A^{-1/2} & \mathbb{1} \end{bmatrix}.\end{aligned}$$

Let $K = A^{-1/2} X B^{-1/2}$, then by Proposition 6, this block matrix is positive if, and only if, K is a contraction. This proves the proposition when A and B are strictly positive. The general case follows by continuity argument. □

One may see that, from Proposition 7, if $\begin{bmatrix} A & X \\ X^\dagger & B \end{bmatrix}$ is positive, then the range of X is a subspace of the range of A and the range of $X^\dagger$ is a subspace of the range of B. The rank of X may not exceed either the rank of A, or the rank of B.

Theorem 8. *Let A and B be strictly positive matrices, then the block matrix $\begin{bmatrix} A & X \\ X^\dagger & B \end{bmatrix}$ is positive if, and only if, $A \geq X B^{-1} X^\dagger$.*

Proof. Using the congruence

$$\begin{aligned}\begin{bmatrix} A & X \\ X^\dagger & B \end{bmatrix} &\sim \begin{bmatrix} \mathbb{1} & -XB^{-1} \\ O & \mathbb{1} \end{bmatrix} \begin{bmatrix} A & X \\ X^\dagger & B \end{bmatrix} \begin{bmatrix} \mathbb{1} & O \\ -B^{-1} X^\dagger & \mathbb{1} \end{bmatrix} \\ &= \begin{bmatrix} A - XB^{-1}X^\dagger & O \\ O & B \end{bmatrix}.\end{aligned}$$

Which is clearly positive if, and only if, $A \geq XB^{-1}X^\dagger$. □

Lemma 9. *The matrix A is positive if, and only if,* $\begin{bmatrix} A & A \\ A & A \end{bmatrix}$ *is positive.*

Proof. We may write

$$\begin{bmatrix} A & A \\ A & A \end{bmatrix} = \begin{bmatrix} A^{1/2} & O \\ A^{1/2} & O \end{bmatrix} \begin{bmatrix} A^{1/2} & A^{1/2} \\ O & O \end{bmatrix},$$

which is positive being of the form $XX^\dagger$. □

Corolarium 10. *Let A be any matrix, then the matrix* $\begin{bmatrix} |A| & A^\dagger \\ A & |A^\dagger| \end{bmatrix}$ *is positive.*

Proof. Use the polar decomposition $A = UP$, thus

$$\begin{aligned} \begin{bmatrix} |A| & A^\dagger \\ A & |A^\dagger| \end{bmatrix} &= \begin{bmatrix} P & PU^\dagger \\ UP & UPU^\dagger \end{bmatrix} \\ &= \begin{bmatrix} \mathbb{1} & O \\ O & U \end{bmatrix} \begin{bmatrix} P & P \\ P & P \end{bmatrix} \begin{bmatrix} \mathbb{1} & O \\ O & U^\dagger \end{bmatrix}, \end{aligned}$$

and, then, use the Lemma 9. □

CHAPTER 3

Let entanglement be your puppet: manipulations of quantum states

> "[...] quantum phenomena do not occur in a Hilbert space, they occur in a laboratory".
>
> - Asher Peres

To acquire the full glory of the entanglement as resource, one definitely needs some manipulations of quantum states and — in some cases — classical communication.This chapter intend to give a unified mathematical representation for these manipulations: the so-called Kraus formalism [13–15].

This chapter is organized as follows: first we present a general overview of quantum operations, then we will explore a little bit further and present the whole quantum maps framework — where the knowledge of the content in the appendix *In the toolbox: matrix reshaping and reshuffling* is assumed —. Finally, we separate quantum operations in classes where increasing degrees of communication are allowed.

3.1 General quantum operations

We can construct the formalism of general quantum operations in two ways [3, 16]. In the former, we have an axiomatic point of view: we restrict ourselves to a class of linear maps Λ which maps a state ρ acting on $\mathcal{H}_1$ into $\tilde{\rho}$ on $\mathcal{H}_2$, *i.e.*, $\Lambda : \mathcal{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2)$, in addition to some physically motivated constraints and define the remaining manipulations as quantum operations; in the latter, the approach is constructive and the set of quantum operations is defined as the one which can be obtained by combining operations from a certain set of elementary operations. They are both equivalent[i].

In the standard lore of quantum operations, there are basically four types of manipulations:

(O1) Unitary transformations: $\rho \to U\rho U^\dagger$, with $UU^\dagger = \mathbb{1}$;

(O2) Adding an uncorrelated ancilla: $\varrho \to \rho \otimes \sigma$, with σ a density operator;

(O3) Tracing out part of the system: $\rho_1 \to tr_{\mathcal{H}_2}(\rho)$ with ρ acting on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$;

(O4) Projective measurements and postselection: $\rho \to \sum_{i=1}^{k} P_i \rho P_i$, with P_i pairwise orthogonal projectors such that $\sum_{i=1}^{n} P_i = \mathbb{1}$ with $k \leq n$.

It is easy to see that operations (O1)-(O3) can be represented as trace preserving completely positive maps — or CP-map, for short —. The inverse holds also, *i.e.*, any trace preserving CP-map can be executed by means of the quantum manipulations (O1)-(O3). This result follows from the Stinespring dilation theorem [13, 16, 18, 21].

Now, with aid of the Choi-Kraus representation, any CP-map Λ can be written as $\Lambda(\rho) = \sum_i E_i \rho E_i^\dagger \; \forall \, \rho \in \mathcal{L}(\mathcal{H})$. The operators E_i are commonly called the Kraus operators. For a trace preserving CP-map, we have $\sum_{i=1} E_i^\dagger E_i = \mathbb{1}$, but, in the case we allow (O4), we need to relax this constraint to $\sum_i E_i^\dagger E_i \leq \mathbb{1}$ and renormalize the state[ii]. Thus we may summarize this as follows (*cf.* [13]):

Theorem 11. *A quantum operation Λ can be decomposed into operations of the form (O1)-(O4) if and only if Λ acts as a CP non-increasing map: $\Lambda(\rho) = \sum_i E_i \rho E_i^\dagger$, with $\sum_i E_i^\dagger E_i \leq \mathbb{1}$.*

3.2 Positive and completely positive maps

With a carefully study of the previous section, one should be able to get the idea presented in most of quantum protocols in the literature. But there are lots of things to say when dealing with quantum operations. To explore quantum maps in their full glory, we need a consistent framework: that is what we will explain in this section — we remark here that, at this point, one *should* understand the content in the appendix *In the toolbox: matrix reshaping and reshuffling* —. So, let's start with the 'indices juggling'!

We are particularly interested in a class of maps Λ which maps a state ρ acting on $\mathcal{H}^N$ into $\tilde{\rho}$ on $\mathcal{H}^N$, $\Lambda : \mathcal{L}(\mathcal{H}^N) \to \mathcal{L}(\mathcal{H}^N)$. So, what conditions need to be fulfilled by a map Λ to represent a physical operation?

As the linearity of quantum mechanics is assumed here in this discourse[iii], our first constraint on Λ is that the map should be a linear one, *i.e.*, we postulate the existence of a *linear superoperator* Λ,

$$\tilde{\rho} = \Lambda \rho \quad \text{or} \quad \tilde{\rho}_{m\mu} = \Lambda_{\substack{m\mu \\ n\nu}} \rho_{n\nu}, \tag{3.1}$$

[i] It was introduced, in physics, by Kraus [17] — based on an earlier theorem by Stinespring [18] — and, independently, by Sudarshan *et al.* [19]. *Cf.* [14] and [20] also.

[ii] We can also maintain $\sum_i E_i^\dagger E_i = \mathbb{1}$ but allowing postselection on the outcomes of i.

[iii] Non-linear quantum mechanics is a lively field of research though.

where summation over repeated indices is understood throughout this section. One may understand the first equality in Eq. (3.1) as $(\Lambda\,\rho_{\downarrow})_{\Box}$, *i.e.*, a superoperator acting on the reshaped ρ (as a column vector) and, then, reshaped back to de square form. This form includes inhomogeneous maps also, $\tilde{\rho} = \Lambda\rho + \sigma$ reads

$$\Lambda_{\substack{m\mu\\n\nu}}\,\rho_{n\nu} + \sigma_{m\mu} \equiv (\Lambda_{\substack{m\mu\\n\nu}} + \sigma_{m\mu}\delta_{n\nu})\rho_{n\nu} = \tilde{\Lambda}_{\substack{m\mu\\n\nu}}\,\rho_{n\nu} \tag{3.2}$$

directly from the fact that $tr(\rho) = 1$, *i.e.*, we are dealing with affine maps of density matrices.

Now that we dealt with linearity, we should take into account the preservation of the density matrices properties of the image $\tilde{\rho}$: (i) Hermiticity; (ii) trace equals one and (iii) positivity. These requirements impose three constraints on the matrix Λ:

$$(i) \quad \tilde{\rho} = \tilde{\rho}^{\dagger} \quad \Leftrightarrow \quad \Lambda_{\substack{m\mu\\n\nu}} = \Lambda^{*}_{\substack{\mu m\\\nu n}} \quad \text{so} \quad \Lambda^{*} = \Lambda^{S}; \tag{3.3}$$

$$(ii) \quad tr(\tilde{\rho}) = 1 \quad \Leftrightarrow \quad \Lambda_{\substack{mm\\n\nu}} = \delta_{n\nu} \quad ; \tag{3.4}$$

$$(iii) \quad \tilde{\rho} \geq 0 \quad \Leftrightarrow \quad \Lambda_{\substack{m\mu\\n\nu}}\,\rho_{n\nu} \geq 0 \quad \text{when} \quad \rho \geq 0. \tag{3.5}$$

Which, presented this way, is not *that* illuminating.

To unravel these constraints in a clear way, we may reshuffle Λ — as in Eq. (A.12) — and define the *dynamical matrix*[iv]

$$D_{\Lambda} \equiv \Lambda^{R} \quad \text{so that} \quad D_{\substack{mn\\\mu\nu}} = \Lambda_{\substack{m\mu\\n\nu}}. \tag{3.6}$$

The dynamical matrix D_{Λ} uniquely determines the map Λ. Which obeys

$$D_{a\Lambda+b\Phi} = aD_{\Lambda} + bD_{\Phi}, \tag{3.7}$$

i.e., it is a linear function of the map.

Now we are able to write the three conditions as

$$(i) \quad \tilde{\rho} = \tilde{\rho}^{\dagger} \quad \Leftrightarrow \quad D_{\substack{mn\\\mu\nu}} = D^{\dagger}_{\substack{mn\\\mu\nu}} \quad \text{so} \quad D_{\Lambda} = D^{\dagger}_{\Lambda}; \tag{3.8}$$

$$(ii) \quad tr(\tilde{\rho}) = 1 \quad \Leftrightarrow \quad D_{\substack{mn\\m\nu}} = \delta_{n\nu} \quad ; \tag{3.9}$$

$$(iii) \quad \tilde{\rho} \geq 0 \quad \Leftrightarrow \quad D_{\substack{mn\\\mu\nu}}\,\rho_{n\nu} \geq 0 \quad \text{when} \quad \rho \geq 0. \tag{3.10}$$

Which gives us a better picture. The condition (i) holds if, and only if, D_{Λ} is Hermitian; condition (ii) takes a familiar form also:

$$D_{\substack{mn\\m\nu}} = \delta_{n\nu} \quad \Leftrightarrow \quad tr_{A}(D_{\Lambda}) = \mathbb{1}, \tag{3.11}$$

i.e., the partial trace with respect to the first subsystem is equal the identity operator for the second subsystem; only the condition (iii) needs further explanation.

[iv] This idea was introduced by Sudarshan *et al.* [19] and earlier — in the mathematics literature — by Schatten [22].

This requirement stands for the positivity of the map, *i.e.*, Λ should map positive matrices to positive matrices — so (iii) must holds —. Consider the original density matrix be a pure one, so that $\rho_{n\nu} = z_n z_\nu^*$. Then its image will be positive if, and only if, for all vectors x_m,

$$x_m \, \tilde{\rho}_{n\nu} \, x_\mu^* \; = \; x_m \, z_n \, D_{\substack{mn \\ \mu\nu}} \, x_\mu^* \, z_\nu^* \quad \geq 0. \tag{3.12}$$

In the usual notation, one reads this equation as

$$\langle x|\tilde{\rho}|x\rangle = \langle x|\otimes\langle z|D_\Lambda|x\rangle\otimes|z\rangle \; \geq 0. \tag{3.13}$$

But note that, juggling indices, is an easier way to show the equality. The equations (3.12) and (3.13) mean that the dynamical matrix itself must be positive when acts on product states in $\mathcal{H}^{N^2}$. This property is called *block-positivity*. Which lead us to the following theorem (*cf.* [23]):

Theorem 12 (Jamiołkowski). *A linear map $\Lambda : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is positive if, and only if, the corresponding dynamical matrix D_Λ is block-positive.*

The converse holds also, since (3.12) is strong enough to ensure that (3.10) holds for all mixed states ρ as well.

Some remarks about the positivity condition should be done: first, it is difficult to work with — since must holds for *all* product vectors acting on $\mathcal{H}^{N^2}$ —; another point is that any quantum state ρ may be extended by an ancilla to a state $\rho \otimes \sigma$ of larger composite system. This simple point lead us to check rather the map $\Lambda \otimes \mathbb{1}$ remains positive. Since the map leaves the ancilla unaffected, this may seem like a foregone conclusion. Classically it is so, but quantum mechanically it is not. So, we must introduce the concept of *K-positivity*: a K-positive map is a positive map such that the induced map

$$\Lambda \otimes \mathbb{1}^K, \quad \text{where} \quad \mathcal{L}(\mathcal{H}^N) \to \mathcal{L}(\mathcal{H}^N \otimes \mathcal{H}^K), \tag{3.14}$$

is positive for $k \geq 1$. Λ is said *a completely positive map* if, and only if, is K-positive for *all* $k \geq 1$. But, check for all possible extensions looks non-operational, so, let us call the dynamical matrix properties of the map to unravel this. Since D_Λ is an Hermitian operator acting on $\mathcal{H}^{N^2}$, it admits a spectral decomposition

$$D_\Lambda = \sum_{i=1}^{r} \lambda_i \, |\xi_i\rangle\langle\xi_i| \quad \text{so that} \quad D_{\substack{mn \\ \mu\nu}} = \sum_{i=1}^{N^2} \lambda_i \, \Xi^i_{mn} (\Xi^i_{\mu\nu})^*, \tag{3.15}$$

where r is the rank of D_λ; the eigenvalues λ_i are real and the matrices Ξ^i_{mn} are reshaped vectors in $\mathcal{H}^{N^2}$.

Now we are able to check the positivity of the induced map $\Lambda \otimes \mathbb{1}$ when it acts on matrices in $\mathcal{L}(\mathcal{H}^{NK}) = \mathcal{L}(\mathcal{H}^N \otimes \mathcal{H}^K)$. We pick an arbitrary vector $z_{nn'}$ in $\mathcal{H}^{NK}$ and act with our map on the corresponding pure state:

$$\tilde{\rho}_{mm'\mu\mu'} = \Lambda_{\substack{m\mu \\ n\nu}} \, \delta_{\substack{m'\mu' \\ n'\nu'}} \, z_{nn'} \, z^*_{\nu\nu'} = D_{\substack{mn \\ \mu\nu}} \, z_{nm'} \, z^*_{\nu\mu'} = \sum_i \lambda_i \, \Xi^i_{mn} \, z_{nm'} (\Xi^i_{\mu\nu} \, z_{\nu\mu'})^*. \tag{3.16}$$

Let us pick another arbitrary vector $x_{mm'}$ and test whether $\tilde{\rho}$ is a positive operator:

$$x_{mm'}\,\tilde{\rho}_{mm'\mu\mu'}\,x^{*}_{\mu\mu'} = \sum_{i} \lambda_i\,|\Xi^{i}_{mn}\,x_{mn'}\,z_{nm'}|^2 \geq 0, \tag{3.17}$$

which must hold for arbitrary $x_{mm'}$ and $z_{mm'}$, thus all the eigenvalues λ_i must be non-negative. This leads us to Choi's theorem:

Theorem 13 (Choi #2)**.** *A linear map Λ is completely positive if, and only if, the corresponding dynamical matrix D_Λ is positive.*

It is remarkable that we are able to check complete positiveness of the map by looking to the non-negative eigenvalues of the dynamical matrix[v].

The set of complete positive maps is isomorphic to the set of positive matrices D_Λ of size N^2. When the map is trace preserving also, we need to add the condition (3.11), which implies that $tr(D_\Lambda) = N$. We may think of the set of trace preserving completely positive maps as a subset of the set of density matrices in $\mathcal{L}(\mathcal{H}^{N^2})$, with a unusual normalization though[vi].

So, the dynamical matrix is positive if, and only if, it may be written in the form

$$D_\Lambda = \sum_i |E_i\rangle\langle E_i| \quad \text{so that} \quad D_{\substack{mn\\ \mu\nu}} = \sum_i E^{i}_{mn}(E^{i}_{\mu\nu})^{*}, \tag{3.18}$$

where the vectors $|E_i\rangle$ are arbitrary to an extent given by Schrödinger's mixture theorem. Thus, we arrive at an alternative characterization of completely positive maps. They are the maps that may be written in the *operator sum representation*:

Theorem 14 (Choi #1)**.** *A linear map Λ is completely positive if, and only if, it is of the form*

$$\Lambda(\rho) = \sum_i E_i\,\rho\,E_i^{\dagger}. \tag{3.19}$$

This also known as the *Kraus* or *Stinespring form*, since its existence follows from the *Stinespring dilation theorem*[vii]. The operators E_i are known as *Kraus operators*. The map will be *trace preserving* if, and only if, the condition (3.9) holds, which reads

$$\sum_i E_i^{\dagger} E_i = \mathbb{1}. \tag{3.20}$$

Trace preserving completely positive maps go under various names: *deterministic* or *proper quantum operations*, *quantum channels*, or *stochastic maps*. This is the most general class that we need to consider.

The convex set of proper quantum operations is denoted $\mathcal{CP}^N$. To find its dimension, we note that the dynamical matrices belong to the positive cone in the space of Hermitian matrices of size N^2 (*i.e.*, $N^2 \times N^2$), which

[v] *Cf.* [24] for further explanation.

[vi] We will explore this further later when presenting the duality between maps and states.

[vii] It was introduced, in physics, by Kraus [17] — based on an earlier theorem by Stinespring [18] — and, independently, by Sudarshan *et al.* [19]. *Cf.* [14] and [20] also.

has dimension N^4 (*i.e.*, N^4 linearly independent parameters); the dynamical matrix corresponds to a trace preserving map if, and only if, (3.11) holds, *i.e.*, the partial trace is the identity operator, so it is subject to N^2 conditions. Thus, the dimension of $\mathcal{CP}^N$ equals $N^4 - N^2$.

Since the operator sum representation does not determine the Kraus operators uniquely, we would like to bring it to a canonical form. The problem is quite similar to that of introducing a canonical form for a density matrix: its eigenstates. Such a decomposition of the dynamical matrix was given in Eq. (3.15). A set of canonical Kraus operators may be obtained by setting $E_i = \sqrt{\lambda_i}\,\Xi_i$. Which leads us to the following results:

Definition 15 (Canonical Kraus form)**.** *A completely positive map $\Lambda : \mathcal{L}(\mathcal{H}^N) \to \mathcal{L}(\mathcal{H}^N)$ may be represented as*

$$\Lambda(\rho) = \sum_{i=1}^{r\leq N^2} \lambda_i\, \Xi_i\, \rho\, \Xi_i^\dagger = \sum_{i=1}^{r} E_i\, \rho\, E_i^\dagger, \tag{3.21}$$

where

$$tr(E_i^\dagger\, E_j) = \sqrt{\lambda_i\, \lambda_j} \langle \xi_i | \xi_j \rangle = \lambda_i\, \delta_{ij}. \tag{3.22}$$

If the map is trace preserving also, then

$$\sum_i E_i^\dagger E_j = \mathbb{1} \quad \Rightarrow \quad \sum_i \lambda_i = d^2. \tag{3.23}$$

If D_Λ is non-degenerate, the canonical form is unique up to phase choice for the Kraus operators. The *Kraus rank* of the map is the number of Kraus operators that appear in the canonical form and equals the rank r of the dynamical matrix.

As in Eq. (A.7), the operator sum representation may be written as

$$\Lambda = \sum_{i=1}^{N^2} E_i \otimes E_i^* = \sum_{i=1}^{N^2} \lambda_i\, \Xi_i \otimes \Xi_i^*. \tag{3.24}$$

The canonical operator sum representation may be considered as a Schmidt decomposition (A.9) of Λ — with Schmidt coefficients $\lambda^i_{schmidt} = \lambda_i$ —.

We will continue the discussion of positive maps and the duality maps *vs.* states in the next chapter.

In the next subsections we will describe the most common classes of quantum operations in the bipartite case $\mathcal{H}_A \otimes \mathcal{H}_B$ (Alice and Bob) without loss of generality in the multipartite case. The extension to more parties, *e.g.*, Clarice, David, Eve, *etc.* [viii] is straightforward. We now review these classes of operations: where increasing degrees of communication are allowed [13, 25–27].

[viii] To avoid prejudiced labeling, we kept the track female, male, female, male, *etc.*.

3.2.1 Local operations

Local operations are the most simple manipulations that we are able to perform. This class is generated by the Kraus operators of the form $A_i \otimes \mathbb{1}$ and $\mathbb{1} \otimes B_i$, with $\sum_i A_i^\dagger A_i = \sum_i B_i^\dagger B_i = \mathbb{1}$. In this case, the parties are not allowed to communicate and the operations are non-measuring. Blending them, we are able to describe local operations as follows:

$$\Lambda(\rho) = \sum_{i,j} (A_i \otimes B_j)\rho(A_i \otimes B_j)^\dagger. \tag{3.25}$$

3.2.2 1-local operations

Now communication starts to play a few roles: suppose we allow *local operations and one-way communication* from Alice to Bob. Now Alice performs a generalized measurement on her subsystem, with Kraus operators $A_i \otimes \mathbb{1}$, with $\sum_i A_i^\dagger A_i = \mathbb{1}$. If the result of her operation is i, the operation on the state acts as[ix]

$$(\Lambda_i \otimes \mathbb{1})(\rho) = (A_i \otimes \mathbb{1})\rho(A_i \otimes \mathbb{1})^\dagger.$$

Alice is able to pick up the phone[x] and tell Bob that she found result i, and, depending on that outcome, he decides which trace preserving operation (defined by B_{ji} operators with $\sum_j B_{ji}^\dagger B_{ji} = \mathbb{1}$) he will perform. The index i denotes the operation Bob implements depends on the result that he got from Alice. The global state now reads

$$(\Lambda_i^A \otimes \Lambda_{ji}^B)(\rho) = \sum_j (\mathbb{1} \otimes B_{ji})(A_i \otimes \mathbb{1})\rho(A_i^\dagger \otimes \mathbb{1})(\mathbb{1} \otimes B_{ji}^\dagger).$$

If they continue this protocol on many particles, the total ensemble will change as

$$\Lambda^{AB}(\rho) = \sum_{i,j} (A_i \otimes B_{ji})\rho(A_i \otimes B_{ji})^\dagger. \tag{3.26}$$

Obviously, postselection for certain i may occur in some terms of this expression. The equation (3.26) describes the local operations and one-way communication. The quantum teleportation protocol is the most famous case of this scheme: where Alice performs a Bell measurement.

3.2.3 2-local operations: the paradigm of LOCC

The general *local operations and classical communication* (LOCC) paradigm was first formulated in [28]. Distant parties (in this case we consider Alice and Bob) are allowed to perform arbitrary local quantum manipulations and communicate classically. Note that *no* quantum communication is allowed, *i.e.*, no transfer of quantum systems between the parties can be done.

[ix] Notice that is a trace decreasing operation — as it will occur only with a certain probability —.

[x] Just an allegory to refer classical communication.

The mathematical description of the local operations and two-way communication is quite complicated and the notation tends to be cumbersome, but we will try to explain in a clear way. In this situation it is useful to do alternating measurements and communications. We follow the same strategy of 1-local, focus on one particular outcome and do the summation at the end.

Alice starts the protocol and make her measurement, she finds i_1 as result, therefore the main operator here is $A_{i_1} \otimes \mathbb{1}$. Now she pick up the phone and tells her result to Bob, he will then perform $\mathbb{1} \otimes B_{j_1}(i_1)$ — which is a function of Alice's i_1 outcome — and communicate his result to Alice. She decides then execute $A_{i_2}(i_1,j_1) \otimes \mathbb{1}$ — which is function of Bob's outcome (which is function of Alice's first outcome)[xi]—. All these operators satisfy similar normalization properties (sum the products to identity).

In the end of the LOCC protocol (for the total ensemble) we have

$$\Lambda(\rho) = \sum_k (A_k \otimes B_k)\rho(A_k \otimes B_k)^\dagger, \tag{3.27}$$

with k={i_1,i_2,...,i_n,j_1,j_2,...,j_n} and

$$\begin{aligned} A_k &= A_{in}(i_1,i_2,\ldots,i_{n-1};j_1,j_2,\ldots,j_{n-1})\ldots A_{i_2}(i_1,j_1)A_{i_1} \\ B_k &= B_{jn}(i_1,i_2,\ldots,i_n;j_1,j_2,\ldots,j_{n-1})\ldots B_{j_2}(i_1,i_2,j_1)B_{j_1}(i_1). \end{aligned}$$

Postselection can be done also for particular choices of $i_1,i_2,\ldots,i_n, j_1,j_2,\ldots, j_{n-1}$.

3.2.4 Separable operations

This class of quantum manipulations was considered in [27, 29]. Separable operations are defined as any operation which can be written as

$$\Lambda(\rho) = \sum_i (A_i \otimes B_i)\rho(A_i \otimes B_i)^\dagger, \tag{3.28}$$

where each A_i and B_i are arbitrary operations — measurements included — with the usual normalization condition $\sum_i (A_i \otimes B_i)^\dagger (A_i \otimes B_i) = \mathbb{1}$. It follows that any LOCC is also separable, but the reverse is generally not true [25]. However, we do have the following theorem (*cf.* [26]):

Theorem 16. *It is* always *possible to simulate a separable operation using only LOCC, but with probability possibly smaller than one.*

Proof. Suppose Alice and Bob have two sets of operators A_i and B_i such that $\sum_i (A_i \otimes B_i)^\dagger (A_i \otimes B_i) = \mathbb{1}$ and a state ρ. Generally, we have $\sum_{i=1} A_i^\dagger A_i \neq \mathbb{1}$ and $\sum_{i=1} B_i^\dagger B_i \neq \mathbb{1}$. So we are able to rescale the operators to $\tilde{A}_i = aA_i$ and $\tilde{B}_i = bB_i$ so that $\sum_{i=1} A_i^\dagger A_i \leq \mathbb{1}$ and $\sum_{i=1} B_i^\dagger B_i \leq \mathbb{1}$. Alice and Bob then will perform a LOCC and will obtain two outcomes: k_A e k_B. Their strategy is to maintain the state only if the outcomes coincide ($k_A = k_B$). Without keeping track of the outcomes, ρ is mapped into

$$\Lambda(\rho) = N \sum_i p_i \frac{(\tilde{A}_i \otimes \tilde{B}_i)\rho(\tilde{A}_i \otimes \tilde{B}_i)^\dagger}{tr((\tilde{A}_i \otimes \tilde{B}_i)\rho(\tilde{A}_i \otimes \tilde{B}_i)^\dagger)} = \sum_i (A_i \otimes B_i)\rho(A_i \otimes B_i)^\dagger, \tag{3.29}$$

[xi] Note the cascading pattern here.

with $p_i \equiv tr((\tilde{A}_i \otimes \tilde{B}_i)\rho(\tilde{A}_i \otimes \tilde{B}_i)^\dagger)$ and N a normalization factor. □

3.2.5 PPT-preserving operations

This class of quantum manipulations does what its name says: maps ancilla PPT states into PPT states. We can follow the Rains' definition [30, 31], operations Λ such that the induced map

$$\mathbb{1} \otimes \Lambda : \rho \to \Lambda(\rho^{T_B})^{T_B}$$

is completely positive (with T_B stands for partial transposition in the Bob subsystem). We remark here that all separable operations are PPT-preserving (*cf.* [16])

$$\left[(A \otimes B)\rho(A \otimes B)^\dagger\right]^{T_B} = \left[(A \otimes (B^\dagger)^T)\rho^{T_B}(A^\dagger \otimes B)\right]^{\text{xii}}.$$

Note that PPT-preserving operations are the first class of operations which can be regarded as non-local[xiii]. The key result on this class is that they may be implemented probabilistically by means of LOCC when both parties share a specific entangled PPT state. This was first realized in [26] by Cirac *et al.*. They characterized completely general quantum operations (in particular entangling ones) on bipartite systems by means of a generalized Jamiołkowski isomorphism.

3.2.6 Entangling operations

The Jamiołkowski isomorphism [23] is an isomorphism between a linear map from an input space to an output space and an operator defined over the tensor product of these two spaces. This correspondence is useful when the map acts on one part of a bipartite system, but, on compound systems, it is not so clear how to interpret this duality. The physical interpretation came in a very elegant way in [26].

Suppose one have two systems, A and B, each consisting of two d-level subsystems $A = A_1,A_2$ and $B = B_1,B_2$ respectively. We will establish an isomorphism between a CP-map $\Lambda = \Lambda_{A_1,B_1} : \mathcal{L}(\mathcal{H}_{A_1,B_1}) \to \mathcal{L}(\mathcal{H}_{A_1,B_1})$ and an operator $\mathcal{O} = \mathcal{O}_{A_1,A_2,B_1,B_2}$ acting on the total system $\mathcal{H}_A \otimes \mathcal{H}_B$. The isomorphism reads

$$\mathcal{O} \equiv \mathbb{1}_{A_2,B_2} \otimes \Lambda_{A_1,B_1}(P_{A_1,A_2} \otimes P_{B_1,B_2}), \tag{3.30}$$

where Λ acts only on the systems A_1 and B_1. Here P_{A_1,A_2} is the projector on the maximally entangled state $|\psi\rangle_{A_1,A_2} \equiv \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle_{A_1,A_2}$ (analogously for P_{B_1,B_2}). Equivalently, we have

$$\Lambda(\rho_{A_1,B_1}) \equiv d^2 tr_{A_2,B_2}(\mathcal{O}\rho^T_{A_2,B_2}) \equiv d^4 tr_{A_2,A_3,B_2,B_3}(\mathcal{O}\rho_{A_3,B_3}P_{A_2,A_3}P_{B_2,B_3}).$$

[xii] This equation may be written in more concise way, with aid of the four index notation. *Cf.* the appendix *In the toolbox: matrix reshaping and reshuffling*.

[xiii] *E.g.*, creation of an entangled PPT state is a PPT-preserving operation.

From (3.30) it follows that $\mathcal{O}$ is the result of the action of Λ on two systems A_1 and B_1 which are prepared in a maximally entangled state with two acillary systems.

The second form has an equally simple interpretation: if both parties share a state $\mathcal{O}$, then they may implement the map Λ probabilistically on a certain state ρ_{A_1,B_1} by simultaneously projecting and postselecting ρ_{A_3,B_3}, and $\mathcal{O}$ on the maximally entangled states of A_2A_3 and B_2B_3 with the probability of $p = \frac{1}{d}$ — where d is the dimension of the Hilbert space —. From this isomorphism one can easily deduce the following correspondences:

1. Λ is a separable operation if $\mathcal{O}$ is separable, and conversely Λ is an entangling operation if $\mathcal{O}$ is entangled — with respect to A and B —;
2. Λ is a PPT-preserving operation if and only if $\mathcal{O}^{T_A} \geq 0$. Thus any PPT-preserving operation may be implemented probabilistically locally with aid of a shared PPT state.

This isomorphism has a large number of applications (*cf.* [26, 32]) which we will not explore further. A simple application is the classification of global unitaries according to their entangling power on composite systems [33–35]. Entangling power of a unitary is defined as the average entanglement a unitary creates on product states. When Λ is a unitary map, $\mathcal{O}$ is a pure state and there exists a closed expression of the entangling power in terms of the entanglement of this state vector. Using this, Lieven *et al.* showed that the unitaries with highest entangling power are special kinds of permutations (*cf.* [36]).

CHAPTER 4

Entang' what?! Entanglement as a quantum property of compound systems

> "Thus one disposes provisionally (until the entanglement is resolved by actual observation) of only a **common** description of the two in that space of higher dimension. This is the reason that knowledge of the individual systems can decline to the scantiest, even to zero, while that of the combined system remains continually maximal. Best possible knowledge of a whole does **not** include best possible knowledge its parts — and this is what keeps coming back to haunt us.".
>
> - Erwin Schrödinger

There is no manner to introduce entanglement without a brief historical overview[i]. Starting with EPR *gedanken* experiment [37, 38], from the 1930's, entanglement was vastly explored in the scenario of the completeness of quantum mechanics: which was put in solid mathematical grounds in the 1960's — by the striking works of Gleason [39], Kochen and Specker [40] and Bell [41, 42]. Bell's work dealt directly with th EPR *gedanken* experiment and is of a major importance as it showed that entanglement is incompatible with a certain local hidden variable model (LHV) hypothesis. For deep treatments on Bell's inequalities, *cf.* [43, 44].

Nowadays, the problem of completeness seems well proposed and considerable effort has been put into understanding the mathematical structure of entanglement: which lead us to the spirit of this discourse. The first problem is: given an arbitrary quantum state, determine whether it is entangled, or not.

[i] Actually, it is possible, but it is not preferable. That is why we will do that just briefly.

The study of this problem came together with the realisation that Bell-like inequalities are pretty weak tests for entanglement. The breakthrough came when notions from convex analysis and C^*-algebras[ii] were applied to the problem (*cf.* [46, 47]). We will review these results leading to the general framework of entanglement witnesses and its dual formulation in terms of positive maps. We introduce the so-called PPT entangled states and relate them to classical problems in linear algebra. The separability problem has been shown to be NP-hard [48], therefore, there is no hope of finding a simple analytical method and no efficient algorithm which is able to distinguish all entangled states from all separable ones (*cf.* [49, 50]). Thus, interest has grown in finding good numerical heuristics in tackling the problem in low dimensions. We will apply tools from semidefinite programming to the separability problem. In particular, we focus on the work by Brandão and Vianna [51–53].

For reviews of entanglement versus separability problem from different viewpoints, *cf.* [16, 54–61].

4.1 Characterizing entanglement

In spite of the fact that violation of Bell-like inequalities reveals that quantum correlations may be greater than classical ones, it will be clear that Bell inequalities are a poor test of non-classical behavior. It is possible to show that, for any entangled pure state shared by an arbitrary number of parties, there exists a Bell inequality which is violated [62, 63]. For mixed states, this story has lots of complications and open problems, but it has been shown that although a state might not violate any Bell-like inequalities, it still may be useful for teleportation — using entanglement as resource — [64, 65]. In other scenarios, there are some states which only violate some inequality after a certain local generalized measurement [66, 67]; other states only show a violation when multiple copies are measured collectively [68].

So, given the difficulties of check entanglement with inequalities, it is convenient to characterize the set of entangled mixed states with some reasonable mathematical definitions. The advantage of this approach is to have a workable definition of what is entangled — and what is not —.

Let us present the definition of entanglement for bipartite systems — the generalization to multipartite is straightforward —, starting with pure states [69, 70]. Let $\mathcal{H}$ be a Hilbert space such that $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, as we said in chapter *Nice to meet you, density matrix!*, we denote by $\mathcal{H}^d$ the Hilbert space of dimension d which is $\cong \mathbb{C}^d$, thus, let $\mathcal{H}^d = \mathcal{H}^{d_a} \otimes \mathcal{H}^{d_b}$, where $d = d_a \times d_b \geq 4$,

Definition 17. *A pure state $|\psi\rangle \in \mathcal{H}^d$ shared by two parties, Alice and Bob, is called separable if, and only if, it may be written as*

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle,$$

with $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$, i.e.*, belongs to the Cartesian product $\mathcal{H}_A \times \mathcal{H}_B \subset \mathcal{H}_A \otimes \mathcal{H}_B$. Otherwise, we call $|\psi\rangle$* entangled*.*

[ii] *Cf.* [45].

There is a simple manner of determining whether a pure state is entangled: the *Schmidt decomposition*.

Theorem 18 (Schmidt decomposition [71][iii]). *Every pure state* $|\psi\rangle \in \mathcal{H} = \mathcal{H}^{d_a} \otimes \mathcal{H}^{d_b}$ *may be expressed in the form*

$$|\psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}\, |e_i\rangle \otimes |f_i\rangle, \tag{4.1}$$

where $\{|e_i\rangle\}_{i=1}^{d_a}$ *is an orthonormal basis for* $\mathcal{H}_A$*;* $\{|f_i\rangle\}_{i=1}^{d_b}$ *is an orthonormal basis for* $\mathcal{H}_B$ *and* $d \leq min\{d_a, d_b\}$*.*

One may found surprising that there is only a single sum — at first thought, it is natural thinking of something like

$$|\psi\rangle = \sum_{i=1}^{d_a} \sum_{j=1}^{d_b} \Lambda_{ij}\, |\tilde{e}_i\rangle \otimes |\tilde{f}_j\rangle, \tag{4.2}$$

where Λ is some complex-valued matrix and the bases are arbitrary —. Let us make a constructive proof: which is useful for our daily work.

Proof. Assume, without loss of generality, that $d_a \leq d_b$. Thus, one observe that we may write Eq. (4.2) by introducing the states $|\tilde{\phi}_i\rangle = \sum_j \Lambda_{ij} |\tilde{f}_j\rangle$: which will not be orthonormal states, but they certainly exist and permit us to write the global state as

$$|\psi\rangle = \sum_{i=1}^{d_a} |\tilde{e}_i\rangle \otimes |\tilde{\phi}_i\rangle. \tag{4.3}$$

Let $\rho \equiv |\psi\rangle\langle\psi|$ and take the partial trace over the second subsystem, it reads

$$\rho_A = tr_B(\rho) = \sum_{i=1}^{d_a} \sum_{j=1}^{d_a} \langle\tilde{\phi}_j|\tilde{\phi}_i\rangle\, |\tilde{e}_i\rangle\langle\tilde{e}_j|. \tag{4.4}$$

Here comes the trick: we can always diagonalize $\rho_A \in \mathcal{L}(\mathcal{H}_A)$, so it takes the form

$$\rho_A = \sum_{i=1}^{d_a} \lambda_i\, |e_i\rangle\langle e_i|, \tag{4.5}$$

where the coefficients λ_i are real and non-negative. Finally, we go back and repeat the argument, using this basis from the start. Put the tildes off, we have

$$\langle\phi_j|\phi_i\rangle = \lambda_i \delta_{ij}\,, \tag{4.6}$$

i.e., we can set $|\phi_i\rangle = \sqrt{\lambda_i}\,|f_i\rangle$. □

Definition 19. *The real numbers* $\sqrt{\lambda_i}$ *in the Schmidt decomposition* (4.1) *are called* Schmidt coefficients *and they obey*

$$\sum_i \lambda_i = 1, \quad \lambda_i \geq 0. \tag{4.7}$$

[iii] For further reading, *cf.* [3, 5, 69].

The number r of non-vanishing λ_i is called Schmidt rank *of the state $|\psi\rangle$ ($S(|\psi\rangle) \equiv r$) and it is equal to the rank of the reduced density matrix. The state $|\psi\rangle$ is separable if, and only if $S(|\psi\rangle) = 1$, otherwise, $|\psi\rangle$ is entangled.*

The set of all possible vectors $\vec{\lambda}$ forms a $(d-1)$-dimensional simplex, known as *Schmidt simplex*.

Moving, now, to mixed states. As we said in chapter *Nice to meet you, density matrix!* we denote by $\mathcal{L}(\mathcal{H}) = \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ the set of linear operators on $\mathcal{H}$: which, in finite dimensions, is the space of complex matrices of order $d = d_a \times d_b$.

Definition 20. *A bipartite state $\rho \in \mathcal{L}(\mathcal{H}) = \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is called separable if, and only if, it may be written as a convex sum of pure product states,* i.e.*,*

$$\rho = \sum_i p_i \left|\psi_i^A\right\rangle\left\langle\psi_i^A\right| \otimes \left|\psi_i^B\right\rangle\left\langle\psi_i^B\right|, \tag{4.8}$$

with $p_i > 0$, $\sum_i p_i = 1$, $|\psi_i^A\rangle \in \mathcal{H}_A$ and $|\psi_i^B\rangle \in \mathcal{H}_B$. Otherwise, the state ρ is called entangled[iv].

Let us define the set of separable states as $\mathcal{S}$ and, thus, may be identified with the convex hull[v] of the normalized positive operators in $\mathcal{L}_+(\mathcal{H}_A) \otimes \mathcal{L}_+(\mathcal{H}_B) \subsetneq \mathcal{L}_+(\mathcal{H}_A \otimes \mathcal{H}_B)$. If such a decomposition exist, then — from Carathéodory theorem (*cf.* Theorem 2) — follows that we may always replace it with a decomposition of, at most, d^2 terms, where $d = d_a \times d_b = dim(\mathcal{H})$[vi]. The physical idea behind it is that a separable state may always be constructed by two independent parties by LOCC[vii], but — as usual — physical justification came later.

4.1.1 Entanglement witnesses

We saw that to check whether a pure state is entangled, it is sufficient to expand it in its Schmidt decomposition. For mixed states, the problem is tougher as no such canonical decomposition may be obtained in a straightforward manner. But we make use of the inglory definition of entanglement — which negates the separable — and exploit the convexity and compactness of the set of separable states in our favor.

The following theorem gives us a geometrical characterization of the problem of determining whether $\rho \in D$ is contained in a certain convex subset $C \subset D$:

Theorem 21. *Let $C \subset D$ be a convex set of states in a Hilbert-Schmidt space $\mathcal{L}(\mathcal{H})$, then, for each $\rho \notin C$, there exists a Hermitian operator $A \in \mathcal{L}(\mathcal{H})$ such that*

$$tr(A\,\rho) < 0 \quad and \quad tr(A\,\sigma) \geq 0$$

for convex sets C, D and all *$\sigma \in C$.*

[iv] If there is no summation in Eq. (4.8), it is called *product state*.

[v] *Cf.* chapter *Nice to meet you, density matrix!*.

[vi] This definition was first presented independently by Werner and Primas in 1983, but was popularized in [72].

[vii] *Cf.* chapter *Let entanglement be your puppet: manipulations of quantum states*.

This theorem is an immediate consequence of theorems in functional analysis [73, 74]. The Hahn-Banach theorem states that a convex set and a point lying outside it can be separated by a hyperplane W; and the Riesz-Frecht representation theorem then characterizes such hyperplanes. The hyperplane W are called *witnesses* [60]: they witness states outside C.

Corolarium 22 (Horodeki *et al.* [47])**.** *A state $\rho \in \mathcal{L}(\mathcal{H})$ is entangled if, and only if, there exists one Hermitian operator W which $tr(W\rho) < 0$ and such that $tr(W\sigma) \geq 0$ for all $\sigma \in \mathcal{S}$. Such operators W will be referred to as* entaglement witnesses.

To illustrate what we mean, consider the well known CHSH entanglement witness

$$W_{CHSH} = 2\mathbb{1} - \left[\vec{a}\cdot\vec{\sigma}\otimes(\vec{b}+\vec{b}')\cdot\vec{\sigma} + \vec{a}'\cdot\vec{\sigma}\otimes(\vec{b}-\vec{b}')\cdot\vec{\sigma}\right], \tag{4.9}$$

which is an entanglement witness [60, 75]. Here, $\vec{\sigma} = (X, Y, Z)$ is a vector containing the Pauli spin matrices. Note, also, that a general entanglement witness W can be measured locally: by decomposing it as (non-convex) sum of product states. The problem of finding an optimized decomposition both in the optimal number of projectors on product vectors and in the optimal number of settings of the detectors has been partially solved — *cf.* [76, 77] — assuming that we are able to find an optimized decomposition of witness operators into local operators.

Let us give more examples of entanglement witnesses to enrich the context. The first one is the so-called swap — or flip — operator F, which acts on state vectors as $F|\psi_A\rangle|\psi_B\rangle = |\psi_B\rangle|\psi_A\rangle$, or, in basis $\{|ij\rangle\}$ of $\mathcal{H}$,

$$F_d = \sum_{i,j=1}^{d} |ij\rangle\langle ji|. \tag{4.10}$$

One may check the block positivity (3.12) of the operator (4.10). The swap operator is an entanglement witness because F has negative eigenvalues and, therefore, the result of $F\rho F^{\dagger}$ is a state with at least one negative eigenvalue for some states[viii]. The flip operator is an entanglement witness for the Werner states [72]: which we will mention in the next chapter.

Another example is given by

$$W_R = \mathbb{1} - dP^{+}, \tag{4.11}$$

where P^{+} is the projector of the maximally entangled state $|\psi^{+}\rangle = \dfrac{1}{\sqrt{d}}\displaystyle\sum_{i=1}^{d}|ii\rangle$. Since the maximum overlap of a separable state with P^{+} is $1/d$ and W has negative eigenvalues, it is an entanglement witness — *e.g.*, for $|\psi^{+}\rangle$ —. We will connect (4.11) with the *reduction criterion* map in the next section.

The value $\min_W tr(W\rho)$ may be associated with the distance of ρ to the set of separable states and — in some way — is related to the degree

[viii] *E.g.*, for $|\psi^{-}\rangle$, we have $F|\psi^{-}\rangle = -|\psi^{-}\rangle$.

of entanglement of ρ. However, as the set of entanglement witnesses is unbounded, such minimum may be ill-defined. This may be overcomed by imposing suitable constraints on the entanglement witness W and it turns out that, in this way, a variety of geometrical entanglement measures may be obtained [52, 78].

4.1.2 Duality between maps and states

Now we will continue the discussion about maps — *cf.* chapter *Let entanglement be your puppet: manipulations of quantum states* —; introduce the concept of duality — maps *vs.* states — and put it in the context of entanglement witnesses. We will present the Jamiołkowski isomorphism [23]. Let $\mathcal{CP}^d$ denote the convex set of all trace preserving completely positive maps $\Lambda : \mathcal{L}(\mathcal{H}^d) \to \mathcal{L}(\mathcal{H}^d)$. Any such map may be uniquely represented by its dynamical matrix D_Λ of size[ix] d^2: it is a positive matrix and its trace is equal to d. Hence, the rescaled matrix $\rho_\Lambda \equiv D_\Lambda / d$ represents a mixed state in $\mathcal{L}(\mathcal{H}^{d^2})$. In fact, rescaled dynamical matrices form only a subspaces of this set — determined by the trace preserving conditions (3.11) —: which impose d^2 constraints. Let us denote this $(d^4 - d^2)$-dimensional set by $\mathcal{L}_{\mathbb{1}}(\mathcal{H}^{d^2})$. Since any trace preserving CP map has a dynamical matrix — and vice versa — the correspondence between maps in $\mathcal{CP}^d$ and states in $\mathcal{L}_{\mathbb{1}}(\mathcal{H}^{d^2})$ is one-to-one.

So, let us find the dynamical matrix for the identity operator:

$$\mathbb{1}_{\substack{m\mu \\ n\nu}} = \delta_{mn}\delta_{\mu\nu} \quad \text{so that} \quad D^{\mathbb{1}}_{\substack{m\mu \\ n\nu}} = (\mathbb{1}_{\substack{m\mu \\ n\nu}})^R = \delta_{m\mu}\delta_{n\nu} = dP^+_{\substack{m\mu \\ n\nu}}, \tag{4.12}$$

where $P^+ \equiv |\phi^+\rangle\langle\phi^+|$ represents the projector of the maximally entangled state of the composite system, which reads

$$|\phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \otimes |i\rangle. \tag{4.13}$$

This state is written in its Schmidt decomposition (4.1) and all its Schmidt coefficients are equal, *i.e.*, $\lambda_1 = \cdots = \lambda_d = 1/d$. Thus, we have found that the identity operator corresponds to the maximally entangled pure state $|\phi^+\rangle\langle\phi^+|$ of the composite system. Interestingly, this correspondence may be extended for other operations, or — in general — for arbitrary linear maps. The *Jamiołkowski isomorphism*

$$\Lambda : \mathcal{L}(\mathcal{H}^d) \to \mathcal{L}(\mathcal{H}^d) \quad \longleftrightarrow \quad \rho_\lambda \equiv \frac{D_\Lambda}{d} = [\Lambda \otimes \mathbb{1}](|\phi^+\rangle\langle\phi^+|) \tag{4.14}$$

allows us to associate a linear map Λ acting on the space of mixed states $\mathcal{L}(\mathcal{H}^d)$ with an operator acting in the enlarged Hilbert state $\mathcal{H}^d \otimes \mathcal{H}^d$. To show this relation, write the operator $\Lambda \otimes \mathbb{1}$ as an eight-indices matrix[x] and

[ix] Note that we use N, or d interchangeably for space's sizes.

[x] An analogous operation $\mathbb{1} \otimes \Lambda$ acting on P^+ leads to the matrix D^S: which has the same spectrum.

explore its action on the state P^+ expressed by two Kronecker's deltas as in (4.12),

$$\Lambda_{\substack{mn \\ m'n'}} \mathbb{1}_{\substack{\mu\nu \\ \mu'\nu'}} P^+_{\substack{m'\mu' \\ n'\nu'}} = \frac{1}{d}\Lambda_{\substack{mn \\ \mu\nu}} = \frac{1}{d}D_{\substack{m\mu \\ n\nu}}. \tag{4.15}$$

Conversely, for any positive matrix D, we find the corresponding map Λ by diagonalization. The reshaped eigenvector of D, rescaled by the roots of the eigenvalues give the canonical Kraus form (3.21) of the operation Λ. If $tr_A(\rho_\Lambda) = \mathbb{1}/d$ with $\rho_\Lambda \in \mathcal{L}_{\mathbb{1}}(\mathcal{H}^{d^2})$, then the map Λ is trace preserving.

Consider, now, a more general case in which ρ denotes a state acting on $\mathcal{H}^d \otimes \mathcal{H}^d$. Let Λ be an arbitrary map which sends $\mathcal{L}(\mathcal{H}^d)$ into itself and let $D_\Lambda = \Lambda^R$ denote its dynamical matrix of size d^2. Acting with the extended map on ρ we find its image $\tilde{\rho} = [\Lambda \otimes \mathbb{1}](\rho)$. Doing analogously as (4.15) we obtain

$$(\tilde{\rho})^R = \Lambda\rho^R \quad \text{so that} \quad \tilde{\rho} = (D^R_\Lambda \rho^R)^R. \tag{4.16}$$

Here, the standard multiplication of square matrices takes place: in contrast to Eq. (3.1), in which the state ρ acts on a simple Hilbert space and is treated as a vector.

Note that Eq. (4.14) may be obtained as a special case of (4.16): just take for ρ the maximally entangled state (4.13) — for which $(P^+)^R = \mathbb{1}/d$ —. Formula (4.16) provides a useful application of the dynamical matrix corresponding to a map Λ, which acts on a subsystem. Since the normalization of matrices does not influence positivity, this result implies the following reshuffling lemma:

Lemma 23. *Consider two Hermitian matrices A and B of the same size N.*

$$\textit{If} \quad A \geq 0 \quad \textit{and} \quad B \geq 0, \quad \textit{then} \quad (A^R B^R)^R \geq 0. \tag{4.17}$$

For a proof, *cf.* [79].

Formula (4.14) may be used to find operators D associated with positive maps Λ which are neither trace preserving, nor complete positive also. The Jamiołkowski isomorphism, thus, relates the set of positive linear maps with dynamical matrices acting in the composite space and positive on product states.

Expressing the maximally entangled state $|\psi^+\rangle$ in (4.14) by its Schmidt form (4.13), we may compute the matrix elements of D_Λ in the product basis consisting of the states $|i\rangle \otimes |j\rangle$. Due to the factorization of the right-hand side, we see that the double sum describing $\rho_\Lambda = D_\Lambda/d$ drops out and the result reads

$$\langle k| \otimes \langle i|D_\Lambda|l\rangle \otimes |j\rangle = \langle k|\Lambda(|i\rangle\langle j|)|l\rangle. \tag{4.18}$$

This equation may be understood as a definition of a map Λ related to the linear operator D_Λ. Its special case — $k = l$ and $i = j$ — proves the isomorphism that, if D_Λ is block positive, then the corresponding map Λ sends positive projection operators $|i\rangle\langle i|$ into positive operators [23]. That is where entanglement witnesses $W \equiv D_\Lambda$ play important roles.

Thus, we are in position of starting the main result of the section: which was first published in [47] — note that it can be extended to multipartite case, *cf.* [80] —.

Theorem 24. *A density operator ρ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable if, and only if*

$$[\mathbb{1} \otimes \Lambda](\rho) \geq 0,$$

for all positive maps $\Lambda : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_A)$.

Proof. With each linear map $\Lambda : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_A)$ there is associated an adjoint maps $\Lambda^\dagger : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ defined by

$$tr\big(A\,\Lambda(B)\big) = tr\big(\Lambda^\dagger(A)\,B\big)$$

for all operators A and B. It is easy to verify that the adjoint map of a positive map is positive also. Suppose, now, that ρ is entangled, then — from Corolarium 22 — follows that there exists an entanglement witness W such that $tr(W\rho) < 0$. By virtue of the Jamiołkowski isomorphism and Theorem 12, it is equivalent to

$$tr\big([\mathbb{1} \otimes \Lambda_W](P^+)\rho\big) = tr\big([\mathbb{1} \otimes \Lambda_W^\dagger](\rho)P^+\big) < 0$$

and — since P^+ is positive — it follows that $[\mathbb{1} \otimes \Lambda_W^\dagger](\rho) \ngeq 0$. Conversely, let $\Lambda_W^\dagger$ be a positive map such that $[\mathbb{1} \otimes \Lambda_W^\dagger](\rho)$ has a negative eigenvalue with corresponding eigenvector $|\phi\rangle = A \otimes \mathbb{1}|\psi^+\rangle$. Thus, we have

$$\left\langle \phi \middle| \mathbb{1} \otimes \Lambda_W^\dagger(\rho) \middle| \phi \right\rangle = tr\big((A \otimes \mathbb{1})W(A^\dagger \otimes \mathbb{1})\rho\big) < 0.$$

Since W is positive on separable states, the same applies to $(A \otimes \mathbb{1})W(A^\dagger \otimes \mathbb{1})$. This shows that ρ must be entangled. □

The proof of the Theorem 24 reveals two important facts about the relation between entanglement witness and positive maps. Namely, given an entanglement witness W, the corresponding positive map $\Lambda_W^\dagger$ will always detect more states than the witness: as it detects all states detected by the class of witnesses $(A \otimes \mathbb{1})W(A^\dagger \otimes \mathbb{1})$ for all operators A. Furthermore, if a certain positive map Λ_W is negative on a state ρ, the proof shows us how to construct an operator A such that the local transformation[xi]

$$\rho \quad \longrightarrow \quad (A^\dagger \otimes \mathbb{1})\rho(A \otimes \mathbb{1})$$

will yield a state that can be detected by the entanglement witness W.

In the previous section, we introduce the witness (4.11) — $W_R = \mathbb{1} - dP^+$ —. The map associated with this witness is given by $\Lambda(A) = \mathbb{1}tr(A) - A$. From this, follows that all separable states ρ satisfy

$$\rho_A \otimes \mathbb{1} - \rho \geq 0 \quad \text{and} \quad \mathbb{1} \otimes \rho_B - \rho \geq 0, \tag{4.19}$$

where this is not necessarily the case for entangled states: the associated separability criterion is called *reduction criterion* [81, 82]. One may prove the positivity of the map directly.

[xi] *Cf.* chapter *Let entanglement be your puppet: manipulations of quantum states.*

Another entanglement witness was given by the swap operator F. One may see that the associated map is given by the transposition. For a separable state $\rho = \sum_i p_i \left|\psi_i^A\right\rangle\left\langle\psi_i^A\right| \otimes \left|\psi_i^B\right\rangle\left\langle\psi_i^B\right|$, we have that $[\mathbb{1} \otimes T](\rho) \geq 0$, while this is not necessarily in the case of entangled states. We denote $[\mathbb{1} \otimes T](\rho) \equiv \rho^{T_B}$ and call this operation *partial transpose*. When $\rho^{T_B} \geq 0$, we say that the state has a *Positive Partial Transpose* (PPT), otherwise, the state has a *Negative Partial Transpose* (NPT). The partial transpose criterion was first discovered by Peres [46] independently of the notion of positive maps. This criterion turns out to be powerful, in particular, positivity of the partial transposition is necessary and sufficient for separability when $dim(\mathcal{H}) \leq 6$ [47]. It was subsequently shown to be necessary and sufficient for states with low rank [83]; for pure states [60]; for rank two states [84] and rank three states [83]. In general though, it is not sufficient and there exist PPT — bound — entangled states [85].

It can be shown that the reduction criterion is strictly weaker than the partial transposition [82] — except when $dim(\mathcal{H}_B) = 2$, or $dim(\mathcal{H}_A) = 2$ —.

4.1.3 Digging deeply

We present now some deeper results on maps. We saw that quantum manipulations which describe physical processes are represented by CP maps, but, in the previous section, we saw that, even when they are not CP, they provide a crucial tool in the investigation of quantum entanglement. That is why we explore them a little bit further.

Consider the transposition of a density matrix in a fixed basis, *i.e.*, $T : \rho \to \rho^T$. The super-operator entering (3.1) is the swap operator S, namely, $T_{\substack{m\mu \\ n\nu}} = \delta_{m\nu}\delta_{n\mu} = S_{\substack{m\mu \\ n\nu}}$. Hence it is symmetric with respect to reshuffling, $T = T^R = D_T$. This permutation of matrix contains N diagonal entries equal to unity and $N(N-1)/2$ blocks of size two. Thus, its spectrum consists of $N(N+1)/2$ eigenvalues equal to unity and $N(N-1)/2$ equal to -1: which is consistent with the constraint $tr(D) = N$. The matrix D_T is note positive, so, the transposition T is not CP — as we saw for the action of $[\mathbb{1} \otimes T]$ in the maximally entangled state yielding negative eigenvalues —.

The transposition of an N-dimensional Hermitian matrix changes the signs of the imaginary part of the elements of Dij. This is a reflection in an $N(N+1)/2$-dimensional hyperplane.

As discussed in the chapter *Let entanglement be your puppet: manipulations of quantum states*, a map fails to be CP if its dynamical matrix D contains at least one negative eigenvalue. Let $m \geq 1$ denote the number of the negative eigenvalues[xii]. Ordering the spectrum of D decreasingly allows us to rewrite its spectral decomposition

$$D = \sum_{i=1}^{N^2-m} \lambda_i \left|\xi_i\right\rangle\left\langle\xi_i\right| - \sum_{i=N^2-m+1}^{N^2} \left|\lambda_i\right| \left|\xi_i\right\rangle\left\langle\xi_i\right| \tag{4.20}$$

[xii] For short, *negrank*. *E.g.*, for transposition, $negrank(D_T) = N(N-1)/2$.

Thus, a not complete positive map has the canonical form

$$\tilde{\rho} = \sum_{i=1}^{N^2-m} \lambda_i \, \Xi_i \, \rho \Xi_i^\dagger - \sum_{i=N^2-m+1}^{N^2} |\lambda_i| \, \Xi_i \, \rho \Xi_i^\dagger, \tag{4.21}$$

where the Kraus operators $E_i = \sqrt{|\lambda_i|}\,\Xi_i$ form an orthogonal basis. This is analogous to the canonical form (3.21) of a CP map and it shows that a positive map may be represented as a *difference* of two completely positive maps [86]. While this is true, it does not solve the problem: taking any two CP maps and constructing a quasi-mixture[xiii] $\Lambda = (1+a)\Lambda_1^{CP} - a\Lambda_2^C P$, we do not know in advance how large is the contibuition a of the negative part might be to keep the map Λ positive.

In fact, the characterization of the set $\mathcal{P}^N$ of positive maps: $\mathcal{L}(\mathcal{H}^N) \rightarrow \mathcal{L}(\mathcal{H}^N)$ for $N > 2$ is by far not simple. By definition, $\mathcal{P}^N$ contains the set $\mathcal{CP}^N$ of all CP maps as a proper subset. To learn more about the set of positive maps, we need unravel other features of the operation of transposition T. For any transformation Λ, the modifications of the dynamical matrix induced by a composition with T may be described by the transformation of partial transpose, namely,

$$T\Lambda = \Lambda^{S_1}, \quad D_{T\Lambda} = D_\Lambda^{T_A}, \quad \text{and} \quad \Lambda T = \Lambda^{S_2}, \quad D_{\Lambda T} = D_\Lambda^{T_B}. \tag{4.22}$$

To demonstrate this, it is enough to use the explicit form of Λ_T and the observation that

$$D_{\Phi\Lambda} = \left[D_\Phi^R D_\Lambda^R \right]^R. \tag{4.23}$$

Positivity of $D_{\Phi\Lambda}$ follows from the fact that the composition of two CP maps is completely positive also. Which follows directly from the identity $[(\Phi\Lambda) \otimes \mathbb{1}] = [(\Phi \otimes \mathbb{1}) \cdot (\Lambda \otimes \mathbb{1})]$ and implies the Lemma 23.

Sandwiching Λ between two transpositions does not influence the spectrum of the dynamical matrix, *i.e.*, $T\Lambda T = \Lambda^S = \Lambda^*$ and $D_{T\Lambda T} = D_\Lambda^T = D_\Lambda^*$. Thus, if Λ is completely positive, so is $T\Lambda T$ — if D_Λ is positive, so is D_Λ^T —.

The not completely positive transposition map T allows one to introduce the following definition [87, 88]

Definition 25. *A map Λ is called* completely co-positive *(CcP) if the map $T\Lambda$ is CP.*

Properties (4.22) of the dynamical matrix imply that the map ΛT could be used instead to define the same set of CcP maps. Thus, any CcP map Λ may be written in a Kraus-like form as

$$\tilde{\rho} = \Lambda(\rho) = \sum_{i=i}^{k} E_i \, \rho^T \, E_i^\dagger. \tag{4.24}$$

Now we are able to define a *decomposable* map as follows:

[xiii] Quasi because some weights are negative.

Definition 26. *A positive map* Λ *is called* decomposable *if it may be written as a convex combination of a CP map and a CcP map,* i.e.*,*

$$\Lambda = a\Lambda_{CP}(1-a)\Lambda_{CcP}, \quad \textit{with} \quad a \in [0,1]. \tag{4.25}$$

An important characterization of the set $\mathcal{P}^2$ of positive maps acting on (complex) states of one qubit follows from [87, 89]:

Theorem 27 (Størmer-Woronowicz's)**.** *Every one-qubit positive map* $\Lambda \in \mathcal{P}^2$ *is decomposable.*

I.e., the set of $N = 2$ positive maps can be represented by the convex hull of the set of CP and CcP maps. Note that this result is not general in higher dimensions.

The first example of an undecomposable map was given by Choi [24, 88, 90]. Consider a map defined on $\mathcal{L}(\mathcal{H}^3)$: which depends on three non-negative parameters, namely,

$$\Lambda_C^{a,b,c}(\rho) = \tag{4.26}$$

$$\begin{bmatrix} (a-1)\rho_{11}+b\rho_{22}+c\rho_{33} & -\rho_{12} & -\rho_{13} \\ -\rho_{21} & c\rho_{11}+(a-1)\rho_{22}+b\rho_{33} & -\rho_{23} \\ -\rho_{31} & -\rho_{32} & b\rho_{11}+c\rho_{22}+(a-1)\rho_{33} \end{bmatrix}$$

This generalized Choi map (4.26) is positive if, and only if,

$$a \geq 1, \quad a+b+c \geq 3, \quad 1 \leq a \leq 2 \quad \Rightarrow bc \geq (2-a)^2, \tag{4.27}$$

while it is decomposable if, and only if,

$$a \geq 1, \quad 1 \leq a \leq 3 \quad \Rightarrow bc \geq (3-a)^2/4. \tag{4.28}$$

We may analyze this map in the context of entanglement, *e.g.*, in the family of states [91]

$$\rho_H = \frac{2}{7}|\phi_3^+\rangle\langle\phi_3^+| + \frac{\lambda}{7}\sigma_+ + \frac{5-\lambda}{7}\sigma_-, \quad 2 \leq \lambda \leq 5, \tag{4.29}$$

where

$$|\phi_3^+\rangle\langle\phi_3^+| = \frac{1}{\sqrt{3}}\sum_{i,j=0}^{2}|ii\rangle\langle jj| \tag{4.30}$$

is the density matrix for the maximally entangled state, and

$$\sigma_+ = \frac{1}{3}(|01\rangle\langle 01| + |12\rangle\langle 12| + |20\rangle\langle 20|), \tag{4.31}$$

$$\sigma_- = \frac{1}{3}(|10\rangle\langle 10| + |21\rangle\langle 21| + |02\rangle\langle 02|) \tag{4.32}$$

are two separable states. With these definitions, using — $[\mathbb{1} \otimes \Lambda_C^{2,0,1}](\rho_H)$ — the character of ρ_H changes with λ according to

$$\rho_H = \begin{cases} \text{separable,} & 2 \leq \lambda \leq 3, \\ \text{PPT entanglement,} & 3 < \lambda \leq 4, \\ \text{NPT entanglement,} & 4 < \lambda \leq 5. \end{cases} \tag{4.33}$$

We gave a glimpse of non-decomposable maps and its applications in the separability problem, but many others have been found and studied in the literature.

4.1.4 A numerical approach

In this section, we give an example of a numerical approach to the separability problem. Gurvits [48] reformulated the separability problem as a weak membership problem — allowing some error in the decision — and showed that, even in this scenario, the problem is NP-hard. Yet — as demonstrated by the partial transpose criterion — this does not exclude the existence of efficient algorithms for low dimensional systems. There have been several algorithmic proposals: which can be categorized in three classes:

(i) **From the outside** Here, a hierarchy of tests is devised which in every step detects entanglement of some states and provide a corresponding witness. Typically, the first tests will detect highly entangled states, while further tests will detect more weakly entangled states. Ideally, the hierarchy should be complete, *i.e.* , in the asymptotic regime every entangled state should be detected. Examples of such algorithms may be found in [51–53, 92–95];

(ii) **From the inside** In this approach, again a hierarchy of tests is devised, but — this time — able to deliver a certificate for separability. States detected in the first tests will be typically close to the maximally mixed state, while further tests will be able to detect states closer to the boundary of entangled states. The logic behind this is that, for weakly (classical) correlated states, there is more freedom in finding convex decomposition in terms of product vectors. Examples may be founded in [51–53, 96, 97];

(iii) **Distance measure** The starting point here is to take an entanglement measure $E(\rho)$ which satisfies $E(\rho) = 0$ for all separable states and $E(\rho) > 0$ for all entangled states. The algorithm, typically, works then by calculating $E(\rho)$ to a certain accuracy. For examples, see [98, 99].

The most successful algorithms as of today use of optimization theory: in particular, semidefinite programming. Semidefinite programs (SDPs) are convex optimization problems which can be written as the minimization of a linear objective function, subject to semidefinite constraints in the form of linear matrix inequalities [100]:

$$\textit{minimize } c^\dagger x$$

$$\textit{subject to} \begin{cases} F(x) = F_0 + \sum_{i=1}^{m} x_i F_i \geq 0, \end{cases} \tag{4.34}$$

where $c \in \mathbb{C}^m$, the Hermitian matrices $F_i \in \mathcal{L}(\mathcal{H}^n)$ are given and $x \in \mathbb{C}^m$ is the vector of optimization variables. $F(x) \geq 0$ means that $F(x)$ is a positive matrix. The problem has no local minima. When the unique minimum of this problem cannot be found analytically, one can resort to powerful algorithms that return the approximated answer [101]. Solving the problem could be compared to finding the eigenvalues of a Hermitian matrix. If the matrix is small enough or has very high symmetry, one can easily determine its eigenvalues on the back of an envelope, but in other cases some numerical algorithm is needed. Anyway, one never doubts that the eigenvalues of such a matrix can be determined exactly.

Semidefinite programs have two appealing features: firstly, efficient algorithms are available for solving SPDs in polynomial time with arbitrary accuracy [101]; secondly, with each (primal) SDP, there is associated a dual SDP, which reads,

$$\begin{aligned} &\textit{maximize} \quad -tr(F_0\, Z) \\ &\text{subject to} \quad \{tr(F_i\, Z) = c_i, \quad Z \geq 0, \end{aligned} \tag{4.35}$$

where $Z \geq 0$ means that Z is a positive semidefinite (Hermitian) operator. Now, one may see that $c^T x$ is always larger than $-tr(F_0\, Z)$, so that, solving the dual problem, gives a lower bound on the primal problem. It is often the case that these values coincide — in which case, the SDP have the so-called strong duality property —. Suppose, now, that $c = 0$, then the primal problem becomes a feasibility problem. Then, a positive value of $-tr(F_0\, Z)$ shows that the primal problem is not feasible. *I.e.* , the operator Z gives a certificate for the unfeasibility. Needles to say that such certificates are of the great value in decision problems such as the separability problem. The main result of this discourse use of this certificate as the heart of the method. We will present it in the next chapter.

4.2 Proprieties of entanglement measures

Now that we know what is entanglement and how to characterize it, the natural question which arises is how we may quantify it — as, in the end, we desire delight the outstanding features of entanglement as resource —. But the problem of quantifying entanglement for mixed states becomes complicated [13, 102, 103].

Let us discuss the properties that any potential measure $E(\rho)$ should satisfy, namely,

(E1) **Discriminance.** $E(\rho) = 0$ if, and only if, ρ is separable;

(E2) **Monotonicity.** $\rho \to \sum_i p_i \rho_i \Rightarrow E(\rho) \geq \sum_i p_i E(\rho_i)$ under *probabilistic* LOCC;

(E3) **Convexity.** $E(a\rho + (1-a)\sigma) \leq aE(\rho) + (1-a)E(\sigma)$, with $a \in [0,1]$;

(E4) **Asymptotic continuity.** Let ρ_m and σ_m denote sequences of states acting on m copies of the composite Hilbert space $(\mathcal{H}^N \otimes \mathcal{H}^K)^{\otimes m}$. If $\lim_{m\to\infty} \|\rho_m - \sigma_m\|_1 = 0$, then $\lim_{m\to\infty} \dfrac{E(\rho_m) - E(\sigma_m)}{m \ln(NK)}$;

(E5) **Additivity.** $E(\rho \otimes \sigma) = E(\rho) + E(\sigma)$ for any ρ and $\sigma \in \mathcal{L}(\mathcal{H}^{NK})$;

(E6) **Normalization.** $E(|\psi^+\rangle\langle\psi^+|) = 1$;

(E7) **Computability.** There exists an efficient method to compute E for any ρ.

There are alternative forms of properties (E1)-(E5):

(E1a) **Weak discriminance.** If ρ is separable, then $E(\rho) = 0$;

(E2a) **Monotonicity *under* deterministic LOCC.** $E(\rho) \geq E[\Lambda_{LOCC}(\rho)]$;

(E3a) **Pure states convexity.** $E(\rho) \leq \sum_i p_i E(|\phi_i\rangle)$, where $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$;

(E4a) **Continuity.** If $\|\rho - \sigma\|_1 \to 0$ then $|E(\rho) - E(\sigma)| \to 0$;

(E5a) **Extensivity.** $E(\rho^{\otimes n}) = nE(\rho)$;

(E5b) **Sub-additivity.** $E(\rho \otimes \sigma) \leq E(\rho) + E(\sigma)$;

(E5c) **Super-additivity.** $E(\rho \otimes \sigma) \geq E(\rho) + E(\sigma)$.

The above list of postulates deserves a few comments. The rather natural *if, and only if* condition in (E1) is very strong: it cannot be satisfied by one measure quantifying the distillable entanglement, due to the existence of bound entangled states. Hence, one often requires the weaker property (E1a) instead.

Monotonicity (E2) under probabilistic LOCC is stronger than the deterministic one: since local unitary operations are reversible, the latter property implies

(E2b) **Invariance with respect to local unitary operations.** *I.e.*,

$$E(\rho) = E(U_A \otimes U_B \, \rho \, U_A^\dagger \otimes U_B^\dagger).$$

Convexity property (E3) guarantees that one cannot increase entanglement by mixing. Following Vidal [104], we will call any quantity satisfying (E2) and (E3) an *entanglement monotone*. These fundamental postulates reflect the key idea that quantum entanglement cannot be created locally. *I.e.*, it is not possible to get any entanglement for free — one needs to invest resources for certain entangling operations —.

The postulate that any two neighboring states should be characterized by similar entanglement is made precise in (E4).

Additivity (E5) is — in the distillability scenario — a most welcome property. For certain measures one may show sub-, or super-, additivity: additivity requires both. Some authors suggest to require extensivity (E5a), which is difficult to demonstrate also. However, for any measure E one may consider the quantity

$$E_\infty(\rho) \equiv \lim_{n\to\infty} \frac{1}{n} E(\rho^{\otimes n}).$$

If such limit exists, the *regularized* measure E_∞ defined in this way satisfies (5a) by construction. The normalization property (E6) is useful to compare different quantities: which may be achieved by a trivial rescaling.

The complete wish list (E1)-(E7) is very demanding, so, it is not surprising that — instead of on ideal measure of entanglement fulfilling all required properties, the literature contains a plethora of measures, *e.g.*, [29, 54, 103] — each of them satisfying some axioms only. The pragmatic wish (E7) is an especially tough one: we have learned that even the problem of deciding the separability is a 'hard one' [48]. The quantification of entanglement cannot be easier. Instead of waiting for the discovery of a single — universal — measure, we have thus focus our attention in only one of them: which will illustrate our results in the next chapter.

The distance from an analyzed state ρ to the set of separable states $\mathcal{S}$ satisfies (E1) by construction. However, it is note simple to find the separable state σ closest to ρ with respect to a certain metric. There are several distances to choose from, we illustrate with one of them because we are able to calculate efficiently with aid of the numerical approach [51–53].

(Generalized) Robustness [105, 106]: $E_R(\rho)$ measures the endurance of entanglement by quantifying the minimal amount of mixing with any state needed to wipe out the entanglement, namely,

$$E_R(\rho) = \min_{\sigma \in \mathcal{L}(\mathcal{H})} \left(\min_{s \geq 0 \in \mathbb{R}} s : \frac{\rho + s\sigma}{1+s} \in \mathcal{S} \right). \tag{4.36}$$

We call *random robustness* the special case of $\sigma = \mathbb{1}/N$. The robustness may be interpreted as a minimal distance of ρ to the set of separable states. This construction does not depend on the boundary of the entire set of states in $\mathcal{L}(\mathcal{H})$, in contrast with the best separable approximation. Robustness is known to be convex and monotone, but is not additive [105], using log-robustness

$$E_{LR}(\rho) = \log(1 + E_R(\rho)). \tag{4.37}$$

CHAPTER 5

A ‘click’ on the detector: measuring entanglement

“In the end, what really matters is the ‘click’ on the detector.”.

- Reinaldo Vianna

At this point, we are equipped with everything we need to present the main subject of this discourse: checking entanglement with incomplete information about the state (*cf.* [1], which contains our work).

Our understanding of entanglement has largely grown in the last few years (*cf.* [61]), but the experimental detection is still a daunting challenge. So, let us present a brief overview about the subject.

Theoretically, the tool of choice to detect entanglement is an *Entanglement Witness* (EW) [47]. It consists of a Hermitian operator (W) with non-negative expectation values for all the separable states — but which can have a negative expectation value for an entangled state — in this case, the state is said to be detected by the EW. When it comes to experiments, EWs are not that good: each state has its own optimal witness and the construction of the optimal EW depends on the knowledge of the state[i]. There does not exist an EW which detects all the entangled density operators acting on a given Hilbert space. Nevertheless, an EW can detect many states on a certain region of the state space, though it will be optimal just for a restricted family of states. Therefore, when some information about the state is known, an EW can be implemented[ii].

Exploring collective measurements to estimate nonlinear functionals of quantum states, Walborn *et al.* [107, 108] have experimentally measured the concurrence of unknown pure two qubit states, using two copies of the objective state. It has also been extended to the estimation of the concurrence

[i] *E.g.*, *cf.* [51].

[ii] For examples of experimental implementations of EWs, *cf.* [61] and the references therein.

of mixed states, and implemented experimentally [109, 110]. In the case of rank-2 two-qubit states, it is also possible to measure the concurrence exactly by means of collective measurements on four copies [111].

In this chapter, we investigate measurements on single copies of unknown mixed quantum states. The method we propose is simple, and shows to be effective in low dimensions. We are advocating that using sophisticated mathematical tools to characterize entanglement in a data post-processing fashion, while keeping the experiment as simple as possible, is efficient. Therefore it is an approach in the opposite direction of works, *e.g.* , like those in [107–110], where entanglement is directly measured in a very elaborate experiment. We have performed numerical tests in systems of two qubits, one qubit and one qutrit and two qutrits. In the case of two qutrits, we have investigated both bound and free entanglement. Though we discuss just bipartite entanglement, the formalism can be straightforwardly applied to the multipartite case. The basic idea is to consider the state written in an orthonormal basis: which can be thought of as a *generalized Bloch representation*. Then the expectation values — which are the components of the *generalized Bloch vector* — are gradually measured. For each set of measurements, it is checked if there is enough information to infer entanglement. In the case of states with Negative Partial Transpose (NPT), we check if there is no state with Positive Partial Transpose (PPT) compatible with the measurements. In the general case, including entangled PPT states [85], we build an entanglement witness compatible with the measurements, using the method described in [51]. In the spirit of data post-processing, we mention the recent techniques independently introduced by Eisert *et al.* [112] and Gühne *et al.* [113], that yield bounds to certain entanglement quantifiers, based on the measurement of non-optimal EWs. We note also that Badziag *et al.* [114] and Hassan *et al.* [115] have introduced interesting entanglement criteria based on the norm of the generalized Bloch vector. In the context of Quantum Key Distribution, Curty *et al.* [116] have introduced a method to check the presence of entanglement by means of EWs built with previous measured data. Cai *et al.* [117] also propose a framework to directly detect entanglement by measuring only one copy of a state at a time, and demonstrate the benefits of the method in the case of two-qubit states.

In the next section, we introduce and illustrate our method. Later, we discuss a possible choice of informationally complete set of observables, and illustrates how our method would perform with projective measurements. In particular, that section makes clear that, compared to two qubits and two qutrits, it is not obvious how to choose the minimal amount of (or *optimal*) measurements in a $2 \otimes 3$[iii] system. The section *Estimated EW and Low-Entangled States* offers more questions than answers: we analyze the limitations of the method, studying three representative states, namely, one highly entangled and two very low entangled states. As presented in this work, our method offers a yes/no answer about the entanglement of a unknown mixed state, but our calculations suggest that a further development of it could yield a good quantitative estimator of entanglement.

[iii] Just to simplify the notation of $\mathcal{L}(\mathcal{H}^2 \otimes \mathcal{H}^3)$. We will use this freely.

5.1 Checking entanglement with incomplete information

Given a state represented by the density operator ρ, we want to check if it is entangled, without performing a full tomography. As matter of fact, we want to make the least possible number of assumptions about the state. We will present a strategy based on acquisition of partial information about the state, followed by data (post-)processing in form of Semi-Definite Programs (SDP). SDPs can be efficiently solved [100, 101, 118], and have exact solutions. As the numerical tests will show, it is effective in low dimensions. We focus on bipartite states in order to simplify the discussion, but the generalization of the formalism to multipartite states is straightforward.

A state ρ, acting on $\mathcal{L}(\mathcal{H}^d) = \mathcal{L}(\mathcal{H}^{d_a} \otimes \mathcal{H}^{d_b})$ — where $d = d_a \times d_b$ — can be written as

$$\rho = \sum_{i=0}^{d_a^2-1} \sum_{j=0}^{d_b^2-1} r_{ij} P_{ij}, \tag{5.1}$$

where the P_{ij} are observables forming a complete basis in the Hilbert-Schmidt space, and $r_{ij} = tr(\rho P_{ij}) \in \mathbb{R}$.

One possible choice for these observables is $P_{ij} = \sigma_i^{d_a} \otimes \sigma_j^{d_b}$, with the $\sigma_i^{d_s}$ being $SU(d_s)$ matrices, *i.e.*, generalizations of the Pauli matrices — where $\sigma_0^{d_s}$ stands for the identity matrix and $r_{00} = 1/d$ —. In this case, the state can also be written with explicit *local* and *non-local* parts, and we have an expression that can be thought of as a *generalized Bloch representation*, namely,

$$\rho = \frac{1}{d}\left(\mathbb{1}^{d_a} \otimes \mathbb{1}^{d_b} + \vec{r}_a \cdot \vec{\sigma}^{d_a} \otimes \mathbb{1}^{d_b} + \mathbb{1}^{d_a} \otimes \vec{r}_b \cdot \vec{\sigma}^{d_b} + \sum_{i=1}^{d_a^2-1} \sum_{j=1}^{d_b^2-1} t_{ij} \sigma_i^{d_a} \otimes \sigma_j^{d_b} \right), \tag{5.2}$$

where $\mathbb{1}^{d_s}$ is the $d_s \times d_s$ identity matrix; $\vec{\sigma}^{d_s}$ are the matrices for $SU(d_s)$; $\vec{r}_s \in \mathbb{R}^{d_s^2-1}$ and, finally, $t_{ij} \in \mathbb{R}$. Note that $\vec{r}_a$ and $\vec{r}_b$ are the local parameters, defining the reduced density matrices, namely,

$$\rho_a \equiv tr_b(\rho) = \frac{1}{d_a}(\mathbb{1}^a + \vec{r} \cdot \vec{\sigma}^{d_a}), \tag{5.3}$$

where $tr_b(\cdot)$ is the partial trace on subsystem b — analogous expression for ρ_b —. The *non-local* parameters,

$$t_{ij} = tr(\rho \sigma_i^{d_a} \otimes \sigma_j^{d_b}) = \langle T_{ij} \rangle, \tag{5.4}$$

form a real matrix T, and are responsible for the classical and quantum correlations in ρ. Note that the parameters in Eq. (5.1), or Eq. (5.2), must be real in order to ρ to be Hermitian: but it does not guarantee its positivity.

We will introduce some procedures to check the entanglement of an unknown state based on partial information about it: this partial information consists of the knowledge of some of the r_{ij} (*cf.* Eq. (5.1)) — eventually enriched with some further characteristic of the state, as the fact that it is NPT, or its marginals are known (*cf.* Eq. (5.3)) —.

As it is well known, it is harder to check the entanglement of a bound entangled state than a free entangled one. From the theoretical point of view, it is easy to know if the latter are entangled, for they have negative partial transpose: which is known as the Peres-Horodecki criterion [46, 47]. But if the state is PPT, we need an entanglement witness. The known examples of bound entangled states show very low entanglement — therefore, they will be more difficult to be checked experimentally —.

Now we present our first procedure: which checks entanglement in NPT bipartite states. The method we propose can be thought of as a way of checking the Peres-Horodecki criterion. Assuming the knowledge of n ($n \leq d^2 - 1$) of the parameters $r_k \equiv r_{ij}$ ($k = 1,2,\ldots,d^2 - 1$) in Eq. (5.1), we check the existence of a PPT state compatible with the available information. The nonexistence of such a state witnesses the entanglement of the state of interest. This can be done by means of the following very simple SDP:

$$\begin{gathered} \textit{determine } \varrho \\ \textit{subject to} \begin{cases} \varrho \geq 0 \\ tr(\varrho) = 1 \\ \varrho^{T_B} \geq 0 \\ tr(\varrho P_k) = r_k, \;\; k = 1,2,\ldots,n\,. \end{cases} \end{gathered} \tag{5.5}$$

This SDP is a *feasibility* program. ϱ^{T_B} stands for the partial transpose of ϱ. When this program is infeasible, *i.e.* , when there is no PPT state compatible with the available data, we are certain that the unknown ρ is NPT and, therefore, entangled.

It might happen that the state of interest has passed through some known decoherence channel — which restricts the state's marginals to some known form —. One example is the Werner states [72], which correspond to *depolarized* states whose marginals are maximally mixed. The program in Eq. (5.5) can be easily modified to include this additional information: which corresponds to further constraints in the SDP, namely,

$$\begin{gathered} \textit{determine } \varrho \\ \textit{subject to} \begin{cases} \varrho \geq 0 \\ tr(\varrho) = 1 \\ \varrho^{T_B} \geq 0 \\ \varrho_a = \rho_a \\ \varrho_b = \rho_b \\ tr(\varrho P_k) = r_k, \;\; k = 1,2,\ldots,n\,. \end{cases} \end{gathered} \tag{5.6}$$

Programs in Eq. (5.5) and in Eq. (5.6) determine the projection of the state of interest in a certain hyperplane (in the Hilbert-Schmidt space), and check the existence of the family of PPT states with the same projection. If there is no such state, it means that the measured state is NPT, and therefore entangled. This suffices to check entanglement in spaces $2 \otimes 2$ (qubit-qubit) and $2 \otimes 3$ (qubit-qutrit) [47]. In larger spaces, this approach still works for the

NPT states, but it will not detect entangled PPT states. Now we introduce a procedure that, in principle, can detect both free and bound entangled states.

When the state of interest is in a space which allows for bound entanglement [85], we need an entanglement witness to check if it is separable or not. If we eliminate the constraint of positivity of the partial transpose in the programs of Eqs. (5.5) and (5.6), namely, $\varrho^{T_B} \geq 0$, those programs return a state ϱ: which can be PPT — or not — compatible with the available data. We, then, build an optimal entanglement witness (W_ϱ) to ϱ and use it to estimate the entanglement of ρ, *i.e.*, $tr(W_\varrho \rho) \sim tr(W_\varrho \varrho)$. Remember that an EW is a Hermitian operator with non-negative expectation values on separable states, but which can have a negative expectation value on an entangled state, in this case, we say that the EW detects the entangled state. The optimal EW of a state yields the most negative expectation value, when compared to any other EW of the same kind, therefore $tr(W_\varrho \rho) > tr(W_\rho \rho)$. Note that EWs can be chosen to correspond to different entanglement quantifiers [52]. The EWs in this work have the constraint $tr(W) = 1$, and correspond to the random robustness [53, 105]: which measures how resilient to white noise is the entanglement.

We need an *error bar* to our entanglement estimate given by $tr(W_\varrho \varrho)$. In order to do that, we rewrite Eq. (5.1) as:

$$\varrho = \sum_{k=1}^{n} r_k P_k + \sum_{j=n+1}^{d^2} r_j P_j. \tag{5.7}$$

The first summation corresponds to the known data: let us call it ϱ_{known}. Of course, $\rho_{known} = \varrho_{known}$. The second summation is yielded either by the program in Eq. (5.5), or Eq. (5.6), and we call it $\varrho_{unknown}$. Now we can write our entanglement estimate as:

$$tr(W_\varrho \rho) = tr(W_\varrho \tilde{\varrho}) \pm |tr(W_\varrho \tilde{\varrho}_{unknown})|. \tag{5.8}$$

The techniques we use to build the optimal EW are based on SDPs, and are described in [51].

In Fig. 5.1, we show how the method performs for two qubits, one qubit and one qutrit, and two qutrits. Each graph is built out of 10^4 random NPT entangled states. We plot the *efficacy of entanglement detection* — *i.e.*, number of states detected as entangled divided by 10^4— in the sample of states, against the number of measured non-local parameters (*cf.* Eq. (5.4)). Every time the program in Eq. (5.5), or in Eq. (5.5), is infeasible for a given state, it means that the measured data were sufficient to detect entanglement. In the case of two qutrits, we also test the EW approach of Eq. (5.8). A state is considered successfully detected as entangled, when both $tr(W_\varrho \varrho) + |tr(W_\varrho \varrho_{unknown})|$ and $tr(W_\varrho \varrho) - |tr(W_\varrho \varrho_{unknown})|$ are negative. About 70% of the states are detected as entangled, with an effort which is roughly half of a full state tomography. On one hand, the less entangled is the state, more information we need to infer its entanglement. Therefore, the graphs show 100% efficacy only when all the tomographic parameters are measured. On the other hand, highly entangled states are detected with the knowledge of only a few non-local parameters.

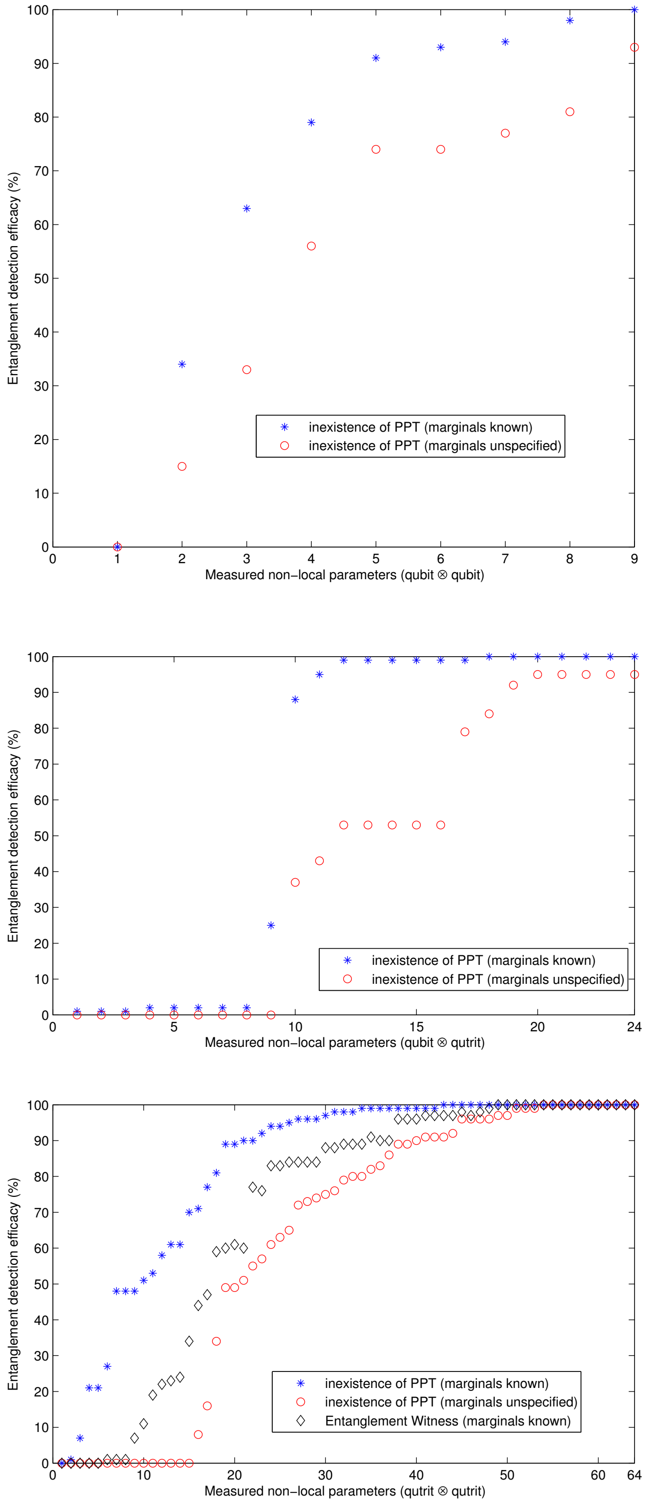

Figure 5.1: Fraction of success of entanglement detection against the number of measured non-local parameters — *cf.* Eq. (5.4)—, for a sample of 10^4 random NPT states, using the approaches described in Eqs. (5.5) and (5.6), for two qubits, one qubit and one qutrit, and two qutrits. For two qutrits, we also show the results using the EW (Eq. (5.8)).

5.2 Choosing what to measure in the laboratory

In the last section, we have described the general idea behind detecting entanglement of unknown states based on partial information. Our main goal was to show that the proposed data post-processing is effective. Now we want to discuss how our technique could be actually implemented with projective measurements: a sensible way to do this is by grouping the observables in the smallest number of maximal commuting classes. Commuting observables share a common set of eigenvectors and, consequently, can be simultaneously measured — *i.e.*, can be simultaneously diagonalized —. Therefore, such a scheme would yield the smallest number of complete projective measurements to be done.

Let us fix the basis of observables. For a Hilbert space of dimension d_s, we introduce the *shift* and *clock* operators, namely:

$$X \equiv \sum_{j=0}^{d_s-1} |j+1\rangle\langle j| \tag{5.9}$$

and

$$Z \equiv \sum_{j=0}^{d_s-1} \exp(\frac{2\pi i j}{2})|j\rangle\langle j|, \tag{5.10}$$

where $\{|j\rangle,\ j=0,\ldots,d_s-1\}$ is an orthonormal basis. For dimension 2, these operators are the usual Pauli matrices. We define also

$$Y \equiv XZ \tag{5.11}$$

and, for $d > 2$,

$$V \equiv XZ^2. \tag{5.12}$$

Two-particle observables are now defined as tensor products of powers of these operators. For two qubits, one qubit and one qutrit, and two qutrits, Table 5.1 shows the complete bases of observables, with a convenient labeling [119].

Now we can group the observables of Table 5.1 in maximally commuting classes. For two qubits, we have the 5 classes [120] shown in Table 5.2; for one qubit and one qutrit, there are 12 classes, as shown in Table 5.3; and finally, for two qutrits, there are the 10 classes [121, 122] shown in Table 5.4. Note that, for two qubits and two qutrits, the classes are disjoint sets. In each case, the simultaneous eigenvectors of each class form a set of Mutually Unbiased Bases (MUB) [123, 124], in the sense that any two vectors of different bases have the same overlap's absolute value. In the case of the $2\otimes 3$ system, the classes are neither disjoint and nor minimal. With 5 observables in each class, the minimal number of classes, for a total of 35 distinct operators, should be 7. It is the case for the systems $2\otimes 2$ and $3\otimes 3$, with 15 observables divided in 5 classes of 3 operators, and 80 observables divided in 10 classes of 8 operators, respectively. It is conjectured that there is no informationally complete set (in the tomographic sense) of MUBs for the $2\otimes 3$ system [125–127], and it is known that generalized Pauli matrices — which is our choice of observables — are not extensible to MUBs [128].

$2 \otimes 2$	I	Z	X	Y
I	0	13	14	15
Z	1	4	7	10
X	2	5	8	11
Y	3	6	9	12

$2 \otimes 3$	I	Z	X	Y
I	0	33	34	35
Z	1	9	17	25
X	2	10	18	26
Y	3	11	19	27
V	4	12	20	28
Z^2	5	13	21	29
X^2	6	14	22	30
Y^2	7	15	23	31
V^2	8	16	24	32

$3 \otimes 3$	I	Z	X	Y	V	Z^2	X^2	Y^2	V^2
I	0	73	74	75	76	77	78	79	80
Z	1	9	17	25	33	41	49	57	65
X	2	10	18	26	34	42	50	58	66
Y	3	11	19	27	35	43	51	59	67
V	4	12	20	28	36	44	52	60	68
Z^2	5	13	21	29	37	45	53	61	69
X^2	6	14	22	30	38	46	54	62	70
Y^2	7	15	23	31	39	47	55	63	71
V^2	8	16	24	32	40	48	56	64	72

Table 5.1: Complete bases of observables in Hilbert spaces of dimensions $2 \otimes 2$, $2 \otimes 3$ and $3 \otimes 3$. Each two-particle observable is the tensor product between one operator of the first line by one operator of the first column.

$$\begin{array}{llll}
C_1 = \{ & 1 & 4 & 13 \} \\
C_2 = \{ & 2 & 8 & 14 \} \\
C_3 = \{ & 3 & 12 & 15 \} \\
C_4 = \{ & 5 & 9 & 10 \} \\
C_5 = \{ & 6 & 7 & 11 \}
\end{array}$$

Table 5.2: Five maximally commuting classes of observables (*cf.* Table 5.1) for two qubits. The common eigenvectors of each class form a set of MUBs.

$C_1 = \{$	1	5	33	9	13	$\}$
$C_2 = \{$	2	6	33	10	14	$\}$
$C_3 = \{$	3	7	33	11	15	$\}$
$C_4 = \{$	4	8	33	12	16	$\}$
$C_5 = \{$	1	5	34	17	21	$\}$
$C_6 = \{$	2	6	34	18	22	$\}$
$C_7 = \{$	3	7	34	19	23	$\}$
$C_8 = \{$	4	8	34	20	24	$\}$
$C_9 = \{$	1	5	35	25	29	$\}$
$C_{10} = \{$	2	6	35	26	30	$\}$
$C_{11} = \{$	3	7	35	27	31	$\}$
$C_{12} = \{$	4	8	35	28	32	$\}$

Table 5.3: Twelve maximally commuting classes of observables (*cf.* Table 5.1) for qubit⊗qutrit.

$C_1 = \{$	1	5	73	9	13	77	41	45	$\}$
$C_2 = \{$	2	6	74	18	22	78	50	54	$\}$
$C_3 = \{$	3	7	75	27	31	79	59	63	$\}$
$C_4 = \{$	4	8	76	36	40	80	68	72	$\}$
$C_5 = \{$	10	46	33	19	32	69	60	55	$\}$
$C_6 = \{$	11	47	17	28	38	53	66	64	$\}$
$C_7 = \{$	12	48	25	34	23	61	51	70	$\}$
$C_8 = \{$	14	42	29	20	39	57	67	56	$\}$
$C_9 = \{$	15	43	37	26	24	65	52	62	$\}$
$C_{10} = \{$	16	44	21	35	30	49	58	71	$\}$

Table 5.4: Ten maximally commuting classes of observables (*cf.* Table 5.1) for two qutrits. The common eigenvectors of each class form a set of MUBs.

In Fig. 5.2, we repeat the calculations of section II, namely Eqs. (5.1), (5.5) and (5.8), but now using the MUB projectors for the two qubits and two qutrits.

Though we do not know MUBs for the $2 \otimes 3$ system, we still want to do the minimal number of projective measurements in the laboratory. To make a complete tomography, we need a set of 35 informationally complete projectors. Measuring in the basis of common eigenvectors of each of the 12 classes (*cf.* Table 5.3), the numbers of independent projective measurements extracted from each class are, respectively, 5, 4, 4, 4, 3, 2, 2, 2, 3, 2, 2, 2. These 35 projectors, which are linearly independent in the Hilbert-Schmidt space, can be sorted in 7 sets of 5, and re-orthonormalized in order to correspond to 7 complete projective measurements (7 *observables*). The results of measurements in these two different bases are shown in Fig. 5.3.

5.3 Estimated EW and Low-Entangled States

At this point, we have discussed how we could detect the entanglement of unknown NPT states, based on partial information. In particular, the method

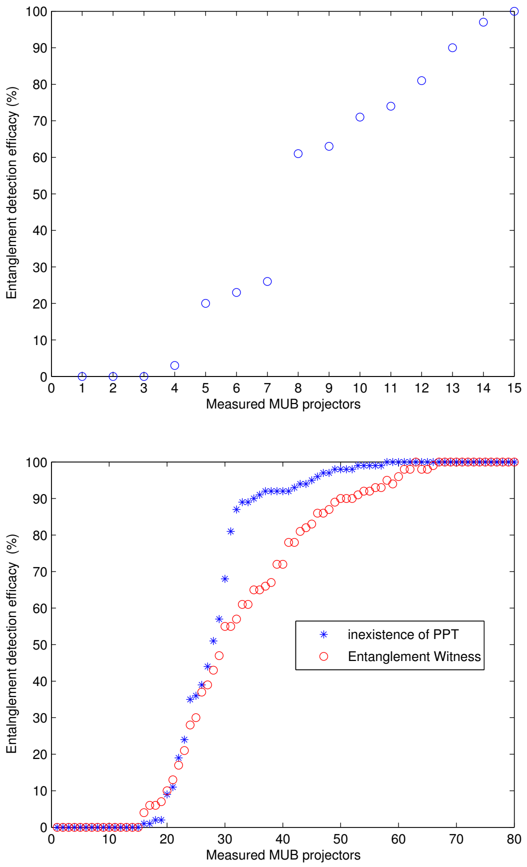

Figure 5.2: Fraction of success of entanglement detection against the number of measured MUB projectors (*cf.* Eq. (5.1)) , for a sample of 10^4 random NPT states, using the approaches described in Eq. (5.5) (Peres-Horodecki criterion), for two qubits (top), and Eqs. (5.5) and (5.8) (EW) for two qutrits (bottom).

we have proposed to check the Peres-Horodecki criterion (Eq. (5.5)) is rigorous, yields an exact answer and, according to our numerical tests, performs nicely for the systems $2 \otimes 2$, $2 \otimes 3$ and $3 \otimes 3$, as shown in Figs. 5.2 and 5.3. On the other hand, our proposed EW estimate — Eq. (5.8) — needs to be better understood. Figs. 5.1 and 5.3 are numerical evidence for the correctness of Eq. 5.8, but we are lacking a rigorous proof for the exact expression of our *error bar*. In this section, we will study the performance of Eq. 5.8 in 3 particular states, being one highly entangled two-qutrit Werner state [72] and two very low entangled states, being one of them also a two-qutrit Werner state, and the other one a two-qutrit bound entangled state [91]. It will add further evidence of the correctness of Eq. 5.8, and will show that our proposed *error bar* is too big, *i.e.* , it seems that $tr(W_\varrho \varrho)$ is a very good upper bound to $tr(W_\varrho \rho)$, much better than we expected, and there must be a tighter *error bar*, but we couldn't devise it yet. Note that $tr(W_\varrho \rho)$ is certainly an upper bound to $tr(W_\rho \rho)$.

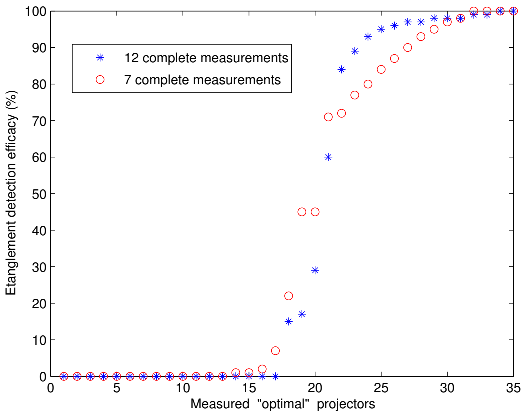

Figure 5.3: Fraction of success of entanglement detection against the number of *optimal* projectors (*cf.* Eq. (5.1) and Table 5.3) , for a sample of 10^4 random NPT states, using the approach described in Eq. (5.5) (Peres-Horodecki criterion), for the $2 \otimes 3$ system.

The two-qudit (for our purposes $d = 3$) Werner states [72] can be written as follows:

$$\rho_W = \frac{\mathbb{1}^d + \beta F_d}{d^2 + d\beta}, \tag{5.13}$$

with $-1 \leq \beta \leq 1$. ρ_W is separable for $\beta \geq -\frac{1}{d}$. F_d is a swap operator for two qudits,

$$F_d = \sum_{i,j=1}^{d} |ij\rangle\langle ji|. \tag{5.14}$$

The two-qutrit bound entangled state we use is picked up from the following family of states [91]:

$$\rho_H = \frac{2}{7}|\phi_3^+\rangle\langle\phi_3^+| + \frac{\lambda}{7}\sigma_+ + \frac{5-\lambda}{7}\sigma_-, \quad 2 \leq \lambda \leq 5, \tag{5.15}$$

where

$$|\phi_3^+\rangle\langle\phi_3^+| = \frac{1}{\sqrt{3}} \sum_{i,j=0}^{2} |ii\rangle\langle jj| \tag{5.16}$$

is the density matrix for the maximally entangled state, and

$$\sigma_+ = \frac{1}{3}(|01\rangle\langle 01| + |12\rangle\langle 12| + |20\rangle\langle 20|), \tag{5.17}$$

$$\sigma_- = \frac{1}{3}(|10\rangle\langle 10| + |21\rangle\langle 21| + |02\rangle\langle 02|) \tag{5.18}$$

are two separable states. With these definitions, the character of ρ_H changes with λ according to

$$\rho_H = \begin{cases} \textit{separable}, & 2 \leq \lambda \leq 3, \\ \textit{bound entangled}, & 3 < \lambda \leq 4, \\ \textit{free entangled}, & 4 < \lambda \leq 5. \end{cases} \tag{5.19}$$

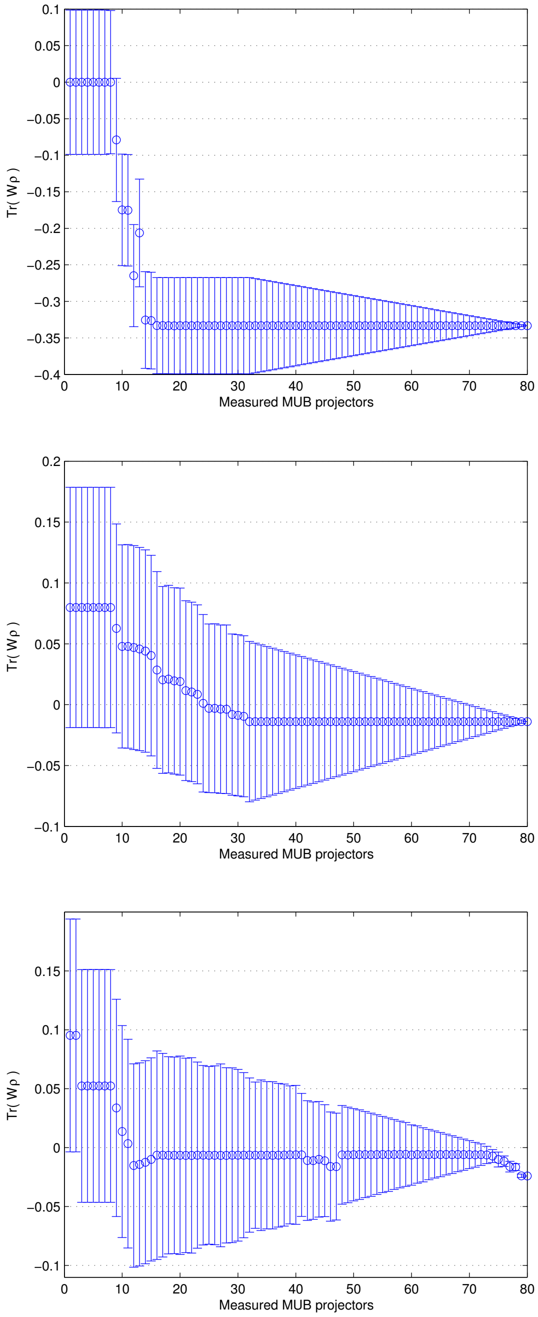

Figure 5.4: Estimated EW with its *error bar* — Eq. (5.8) — for 3 particular two-qutrit states: (top) Werner state with $\beta = -1$, (middle) Werner state with $\beta = -0.37$, (bottom) Horodecki bound entangled state with $\lambda = 3.9$. In each case, the exact value for $tr(W_\rho \rho)$ corresponds to the mark 80 in the abscissa.

In Fig. 5.4, we see the results yielded by Eq. (5.8) applied to Werner states — Eq. (5.13) — with $\beta = -1$ ($tr(W_{\rho_W}\rho_W) = -1/3$) and $\beta = -0.37$ ($tr(W_{\rho_W}\rho_W) = -0.014$), and to the Horodecki bound entangled state — Eq. (5.15) — with $\lambda = 3.9$ ($tr(W_{\rho_H}\rho_H) = -0.024$). As we have mentioned before, a state is considered detected as entangled when the *error bar* resides entirely in the entangled region. We see that the highly entangled Werner state is detected with just 11 measurements. On the other hand, the two low entangled states are detected after the 70^{th} measurement. The Peres-Horodecki criterion — Eq. (5.5) — detects the low entangled Werner state in the 32^{nd} measurement but, of course, it is not applicable to the PPT state. Ignoring the error bar, note that the estimated EW never super-estimated the entanglement; it yielded the exact results for the Werner states after the 17^{th} measurement, for the most entangled state, and after the 32^{nd} measurement, for the low entangled state; and, finally, it detected the bound entangled state after 10 measurements.

5.4 Final remarks about the method

We discussed data post-processing strategies to characterize entanglement of unknown mixed states based on partial knowledge of the state. The method is guaranteed to work: for it *converges* to a full state tomography. We applied our method in systems of dimension $2 \otimes 2$, $2 \otimes 3$ and $3 \otimes 3$. Our numerical investigations showed that entanglement can be detected with a cost which is much lower than full state tomography — when the entanglement is not very small —. For low entangled states — including PPT ones, we presented a method to construct entanglement witnesses (EW). The EWs have an error bar that monotonically diminishes with the increase of information about the state. Our tests suggest that the error bar is too big, for ignoring it, the entanglement estimate yielded by the EW is always a lower bound to the true entanglement. Therefore we believe that a tighter error bar could be calculated, but we weren't able to prove it yet.

We also discussed the choice of observables to be measured in the laboratory. In particular, we noted that the choice is not obvious in the case of the $2 \otimes 3$ system, when one is willing to measure the smallest set of informationally complete projectors. Nevertheless, we offered a method to construct these minimal informationally complete sets, in the case of projective measurements.

The application of our approach to multipartite systems is straightforward, at the level of the formalism. As a matter of fact, we performed some tests on NPT states of three qubits, obtaining results similar to the ones we presented for the bipartite systems.

APPENDIX A

In the toolbox: matrix reshaping and reshuffling

In this appendix we will discuss about very useful tools to work with quantum maps. *Matrix reshaping* and *reshuffling* are simple algebraic transformations that one can perform on matrices — which will help to demystify and unravel some map properties (*cf.* chapter 10 of [5]) —. Here we try to explain these techniques in a simple manner, as we use them in our daily work on quantum manipulations. We also introduce a useful notation in the composite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, or in the Hilbert-Schmidt space of linear operators $\mathcal{H}_{HS}$.

Consider a rectangular matrix Ξ_{ij}, $i = 1, \dots, M$ and $j = 1, \dots, N$. It is said Ξ is *reshaped* when, row after row (lexicographical order)[i], we organize its elements into a vector $\overrightarrow{\xi}$ [ii] of size MN,

$$\overrightarrow{\xi}_k \equiv \Xi_{ij}, \quad \text{where} \quad k = (i-1)N + j, \quad i = 1, \dots, M, \quad j = 1, \dots, N. \text{[iii]} \tag{A.1}$$

As we just reorganize the matrix elements in a different fashion, it is clear that this procedure can be undone, *i.e.*, any vector $\overrightarrow{\xi}$ of length MN may be reshaped into a matrix Ξ[iv]. To illustrate, we can provide the simplest *exempli gratia*: one 2×2 matrix Ξ and its lexicographical reshaped form, which reads

[i] We can organize column after column (anti-lexicographical order). Some programs, like MATLAB, performs the reshape in anti-lexicographical way. A simple way to change between then (*e.g.*, in MATLAB) is transposing the input matrix.

[ii] When convenient, we shall use other notation: $\Xi_{\downarrow}$, or $\Xi_{\rightarrow}$ — indicating reshaped as column vector, or row vector, respectively —.

[iii] We will use this recipe in Eq.(A.1) to doubling indices extensively here.

[iv] We can also introduce a convenient notation $\vec{\xi}_{\square}$ indicating this reverse operation.

$$\Xi = \begin{bmatrix} \Xi_{11} & \Xi_{12} \\ \Xi_{21} & \Xi_{22} \end{bmatrix} \quad \leftrightarrow \quad \Xi_{\downarrow} = \begin{bmatrix} \Xi_{11} \\ \Xi_{12} \\ \Xi_{21} \\ \Xi_{22} \end{bmatrix} \quad \leftrightarrow \quad \Xi_{\rightarrow} = (\Xi_{11}, \Xi_{12}, \Xi_{21}, \Xi_{22}). \tag{A.2}$$

In a anti-lexicographical manner, one should have

$$\Xi = \begin{bmatrix} \Xi_{11} & \Xi_{12} \\ \Xi_{21} & \Xi_{22} \end{bmatrix} \quad \leftrightarrow \quad \Xi_{\downarrow} = \begin{bmatrix} \Xi_{11} \\ \Xi_{21} \\ \Xi_{12} \\ \Xi_{22} \end{bmatrix} \quad \leftrightarrow \quad \Xi_{\rightarrow} = (\Xi_{11}, \Xi_{21}, \Xi_{12}, \Xi_{22}).$$

As one might see above, *reshaping* a matrix is a really simple procedure. But now that we were able to write reshaped matrices, the first question which arises is "which properties remains in these new vectors". Well, we still are able to do everything that a well-behaved vector does in a linear vector space.

The inner product in Hilbert-Schmidt space — for instance, of size N (matrix of size N meaning a square $N \times N$ matrix) — now looks like a common inner product between two vectors of length N^2,

$$\langle \Xi | \Pi \rangle \equiv tr(\Xi^{\dagger}\Pi) = \vec{\xi}^{*} \cdot \vec{\pi} = \langle \xi | \pi \rangle \tag{A.3}$$

Thus the Hilbert-Schmidt norm of a matrix is the same as the norm of the amalgamated (corresponding) vector: $||\Xi||^2_{HS} = tr(\Xi^{\dagger}\Xi) = |\vec{\xi}|^2$.

These vectors can also be linearly transformed[v] into $\vec{\xi}' = \Phi\vec{\xi}$, where Φ is a matrix of size $MN \times MN$. In the usual notation, we denote the matrix elements by $\Phi_{kk'}$ (where k stands for the row, and k' for the column). But, now, we introduce a convenient four index notation $\Phi_{\substack{m\mu \\ n\nu}}$ — it will facilitate the description of operations in composite systems —, where $m,n = 1,\ldots,N$ and $\mu,\nu = 1,\ldots,M$[vi]. The correspondence between the two and four index notation can be clarified with a 4×4 example:

$$\Phi = \begin{bmatrix} \Phi_{11} & \Phi_{12} & \Phi_{13} & \Phi_{14} \\ \Phi_{21} & \Phi_{22} & \Phi_{23} & \Phi_{24} \\ \Phi_{31} & \Phi_{32} & \Phi_{33} & \Phi_{34} \\ \Phi_{41} & \Phi_{42} & \Phi_{43} & \Phi_{44} \end{bmatrix} \quad \leftrightarrow \quad \Phi = \begin{bmatrix} \Phi_{\substack{11\\11}} & \Phi_{\substack{11\\12}} & \Phi_{\substack{11\\21}} & \Phi_{\substack{11\\22}} \\ \Phi_{\substack{12\\11}} & \Phi_{\substack{12\\12}} & \Phi_{\substack{12\\21}} & \Phi_{\substack{12\\22}} \\ \Phi_{\substack{21\\11}} & \Phi_{\substack{21\\12}} & \Phi_{\substack{21\\21}} & \Phi_{\substack{21\\22}} \\ \Phi_{\substack{22\\11}} & \Phi_{\substack{22\\12}} & \Phi_{\substack{22\\21}} & \Phi_{\substack{22\\22}} \end{bmatrix}.$$

Here the upper pair of indices denotes the row of the matrix, while the lower pair determines its column. It is easy to see that the transposed matrix Φ^T is obtained by flipping these lines, *i.e.*, $\Phi^T_{\substack{m\mu\\n\nu}} = \Phi_{\substack{n\nu\\m\mu}}$. It looks cumbersome at the first sight, but this notation shows itself useful when representing an operator

[v] Good sniffers will smell a superoperator acting on a state!

[vi] The relation between k and m,μ; k' and n,ν can be found following the recipe in Eq. (A.1).

acting on a composite space, *e.g.*, $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. The tensor product of any two bases in the parties gives a basis in $\mathcal{H}$, *i.e.*,

$$\Phi_{\substack{m\mu \\ n\nu}} = \langle e_m \otimes f_\mu | \Phi | e_n \otimes f_\nu \rangle, \tag{A.4}$$

where Latin indices stands for the first subsystem, $\mathcal{H}_A$, and the Greek ones to the second, $\mathcal{H}_B$[vii]. The elements of the identity operator $\mathbb{1} = \mathbb{1}_A \otimes \mathbb{1}_B$ reads $\mathbb{1}_{\substack{m\mu \\ n\nu}} = \delta_{mn}\delta_{\mu\nu}$.

One can compute the trace of the matrix by $tr(\Phi) = \Phi_{\substack{m\mu \\ m\mu}}$ (summation over repeating indices is understood).

To compose systems with tensor product, *i.e.*, $\Phi = A \otimes B$, one should perform

$$\Phi_{\substack{m\mu \\ n\nu}} \equiv A_{mn} B_{\mu\nu}. \tag{A.5}$$

It should not be confused with the standard multiplication of matrices (*e.g.*, $C = A \cdot B$), which reads $C_{\substack{m\mu \\ n\nu}} \equiv A_{\substack{m\mu \\ l\lambda}} B_{\substack{l\lambda \\ n\nu}}$, with summation over repeated indices.

Another useful task is tracing out parties, *e.g.*, the partial trace over the second subsystem $\Phi^A = tr_B(\Phi)$ provides a $N \times N$ matrix — while, tracing out the first subsystem ($\Phi^B = tr_A(\Phi)$) produces one $M \times M$ matrix —, *i.e.*,

$$\Phi^A_{mn} \equiv \Phi_{\substack{m\mu \\ n\mu}} \quad \text{and} \quad \Phi^B_{\mu\nu} \equiv \Phi_{\substack{m\mu \\ m\nu}}. \tag{A.6}$$

There is one more detail to discuss about matrix multiplication. When working with states evolution, or Choi-Kraus operators, frequently we deal with product of three operators (*e.g.*, $U\varrho U^\dagger$). Now we are able to write the matrix product, for instance, $A \cdot B \cdot C$ in a different fashion:

$$A \cdot B \cdot C \equiv \left(\Phi B_\downarrow\right)_\square \quad \text{where} \quad \Phi = A \otimes C^T, \tag{A.7}$$

i.e., this triple product is equivalent to a superoperator Φ acting on the reshaped column vector of B and, then, reshaped back to the rectangular form[viii].

Now that we have unraveled the details about reshaping, we are able to start the discussion about *reshuffling matrices*.

Let U be a $N^2 \times N^2$ unitary matrix. Reshape each column $|\xi_k\rangle = U_{ik}$ of U, with $i = 1, \ldots, N^2$ into $N \times N$ matrices Ξ_k — N^2 of them —, as in Eq. (A.2). Since $\langle \xi_k | \xi_{k'} \rangle \equiv tr(\Xi_k^\dagger \Xi_{k'}) = \delta_{kk'}$, or, in double index notation[ix], $\langle \xi_{m\mu} | \xi_{n\nu} \rangle \equiv tr(\Xi^\dagger_{m\mu} \Xi_{n\nu}) = \delta_{mn}\delta_{\mu\nu}$, they form an orthonormal basis[x] for the linear operators acting on $\mathcal{L}(\mathcal{H}^N)$.

Consider X an arbitrary matrix of size N^2, *i.e.*, a $N^2 \times N^2$ one. We now use the basis in the previous paragraph to decompose X as

[vii] The extension to the multipartite case is straightforward.

[viii] Writing a simple triple product this way looks clumsy, but remember this recipe when dealing with quantum maps and Jamiołkowski isomorphism.

[ix] *Cf.* Eq.(A.1).

[x] This is a simple recipe to build complete and orthonormal bases.

$$X = \sum_{i=1}^{N^2}\sum_{j=1}^{N^2} C_{ij}\, \Xi_i \otimes \Xi_j = \sum_{m,\mu,n,\nu=1}^{N} C_{\substack{m\mu \\ n\nu}}\, \Xi_{m\mu} \otimes \Xi_{n\nu}, \tag{A.8}$$

where $C_{ij} = tr((\Xi_i \otimes \Xi_j)^\dagger X)$. As the Ξ_k matrices came from the pure $|\xi_k\rangle$ ones, the matrix X may be considered as a vector in the composite Hilbert-Schmidt space $\mathcal{H}^{N^2} \otimes \mathcal{H}^{N^2}$ and we are able to write X in the Schmidt decomposition:

$$|X\rangle = \sum_{k=1}^{N^2} \sqrt{\lambda_k}\, |\xi_k\rangle \otimes |\xi'_k\rangle, \tag{A.9}$$

where $\sqrt{\lambda_k}$ are the singular values of C — *i.e.*, the square roots of the non-negative eigenvalues of $CC^\dagger$ —. The sum of the squares is determined by the norm of the operator, $\sum_{k=1}^{N^2} \lambda_k \equiv tr(X^\dagger X) \equiv \|X\|^2_{HS}$. The trick here lives in the fact that Schmidt coefficients *do not* depend on the basis, so we can, cleverly, choose the canonical one in $\mathcal{H}^{N^2}$, *i.e.*, that from the identity matrix, $U \equiv \mathbb{1}$. Thus each of the N^2 matrices Ξ_k — reshaped column $|\xi_k\rangle$ from U — consists of only one non-zero element, which equals one: $\Xi_k \equiv \Xi_{m\mu} \equiv |m\rangle\langle\mu|$, where our usual reciprocity between one and two indices is understood. Their tensor product still form an orthonormal basis in $\mathcal{H}^N \otimes \mathcal{H}^N$ and allow us to write an arbitrary matrix X as in Eq. (A.8). This simplify enormously the matrix of coefficients C, which, now, has the form $C_{\substack{m\mu \\ n\nu}} = tr\big((\Xi_{m\mu} \otimes \Xi_{n\nu})X\big) \equiv X_{\substack{mn \\ \mu\nu}}$.

We name this reordering[xi] *reshuffling of* X: $X^R \equiv C(X)$. To dissect this algebraic detour, we illustrate with an example. First, observe that reshaping each row of an initially square matrix X of size MN — following Eq. (A.1) — into a rectangular $M \times N$ submatrix and placing, in lexicographical order, block after block, one produces the reshuffled matrix X^R. In the simplest case $M = N = 2$ — in which any row of the matrix X is reshaped into a 2×2 matrix — we have

$$C_{ij} \equiv X^R_{ij} = \left[\begin{array}{cc|cc} \mathbf{X_{11}} & \mathbf{X_{12}} & X_{21} & X_{22} \\ X_{13} & X_{14} & \mathbf{X_{23}} & \mathbf{X_{24}} \\ \hline \mathbf{X_{31}} & \mathbf{X_{32}} & X_{41} & X_{42} \\ X_{33} & X_{34} & \mathbf{X_{43}} & \mathbf{X_{44}} \end{array}\right]. \tag{A.10}$$

A remark should be done in the symmetric case (with $M = N$): N^3 elements of X — typeset **boldface** in (A.10) — do not change position during reshuffling. Thus the space of complex matrices with reshuffling symmetry $X = X^R$ is $2N^4 - 2(N^4 - N^3) = 2N^3$ dimensional.

We may summarize these last paragraphs in the following lemma:

Lemma 28 (Operator Schmidt decomposition lemma)**.** *The Schmidt coefficients of an operator X acting on a bipartite Hilbert space are equal to the squared singular values of the reshuffled matrix X^R.*

I.e., the Schmidt decomposition in (A.9) of an operator X of size MN may be enhanced by a set of three equations:

[xi] In the literature, also called *realignment*.

$$\left\{\begin{array}{ccl} \{\lambda_k\}_{k=1}^{N^2} & = & \{SV(X^R)\}^2 \quad : \quad \text{eigenvalues of } (X^R)^\dagger X^R; \\ |\xi_k\rangle & : & \quad \text{reshaped eigenvectors of } (X^R)^\dagger X^R; \\ |\xi'_k\rangle & : & \quad \text{reshaped eigenvectors of } (X^R)^\dagger X^R, \end{array}\right. \tag{A.11}$$

where SV indicates singular values and we have assumed $N \leq M$. In the case the rank of $X^R(X^R)^\dagger$ equals one, the operator can be written into a product form: $X = X_A \otimes X_B$, where $X_A = tr_B(X)$ and $X_B = tr_A(X)$.

We should remark that this reshuffling process may be performed in square matrices — in general — if their size K is not prime. The notation X^R has unique meaning if a definite decomposition of the size $K = MN$ is specified. In case of $M \neq N$, the reshuffled matrix X^R is a $N^2 \times M^2$ rectangular matrix. Since $(X^R)^R = X$, we see that we may also reshuffle rectangular matrices, provided both dimensions are squares of natural numbers[xii].

One may see that we are able to define the reshuffling operation in a different manner: in our previous example — Eq. (A.10) — we had reshaped each row of X into rectangular $M \times N$ submatrices. But we may do this in anti-lexicographical order, *i.e.*, reshaping each column instead. In our four index notation, we can compare these two forms:

$$X^R_{\substack{m\mu\\ n\nu}} = X_{\substack{mn\\ \mu\nu}} \quad \text{and} \quad X^{R'}_{\substack{m\mu\\ n\nu}} = X_{\substack{\nu\mu\\ nm}}, \tag{A.12}$$

or, in matrix form,

$$X^{R'}_{ij} = \left[\begin{array}{cc|cc} \mathbf{X_{11}} & X_{31} & X_{12} & X_{32} \\ \mathbf{X_{21}} & X_{41} & X_{22} & X_{42} \\ \hline X_{13} & X_{33} & X_{14} & \mathbf{X_{34}} \\ X_{23} & X_{43} & X_{24} & \mathbf{X_{44}} \end{array}\right]. \tag{A.13}$$

These two reshuffled matrices are equivalent up to permutation of rows and columns and transposition — keeping the singular values of X^R and $X^{R'}$ equal —.

As we had presented the four index notation in this appendix, we may also make use of indices manipulations to present other common operations. *E.g.*, the partial transpositions — with respect to the first subsystem ($T_A = T \otimes \mathbb{1}$) and with respect to the second ($T_B = \mathbb{1} \otimes T$) — takes the form

$$X^{T_A}_{\substack{m\mu\\ n\nu}} = X_{\substack{n\mu\\ m\nu}} \quad \text{and} \quad X^{T_B}_{\substack{m\mu\\ n\nu}} = X_{\substack{m\nu\\ n\mu}}. \tag{A.14}$$

Another transformation which we are able to present here is the *swap* among two subsystems:

$$X^S_{\substack{m\mu\\ n\nu}} \equiv X_{\substack{\mu m\\ \nu n}}, \tag{A.15}$$

which consists in relabelling certain rows — and columns — of the matrix, implying preservation of the spectrum. *E.g.*, for a tensor product $X = Y \otimes Z$,

[xii] *Cf.* [129, 130] for more similar realignments of matrices.

Table A.1: The discussed reorderings of a matrix X.

Transformation	Definition	Symbol	Preserves Hermiticity	Preserves spectrum
transposition	$X^{T}_{\substack{m\mu\\ n\nu}} = X_{\substack{n\nu\\ m\mu}}$	$\updownarrow\updownarrow$	yes	yes
partial	$X^{T_A}_{\substack{m\mu\\ n\nu}} = X_{\substack{n\mu\\ m\nu}}$	$\updownarrow\cdot$	yes	no
transpositions	$X^{T_B}_{\substack{m\mu\\ n\nu}} = X_{\substack{m\nu\\ n\mu}}$	$\cdot\updownarrow$	yes	no
reshuffling	$X^{R}_{\substack{m\mu\\ n\nu}} = X_{\substack{mn\\ \mu\nu}}$	⤢	no	no
reshuffling′	$X^{R'}_{\substack{m\mu\\ n\nu}} = X_{\substack{\nu\mu\\ nm}}$	⤡	no	no
swap	$X^{S}_{\substack{m\mu\\ n\nu}} = X_{\substack{\mu m\\ \nu n}}$	$\substack{\leftrightarrow\\ \leftrightarrow}$	yes	yes
partial	$X^{S_A}_{\substack{m\mu\\ n\nu}} = X_{\substack{\mu m\\ n\nu}}$	$\underset{\cdot}{\leftrightarrow}$	no	no
swaps	$X^{S_B}_{\substack{m\mu\\ n\nu}} = X_{\substack{m\mu\\ \nu n}}$	$\overset{\cdot}{\leftrightarrow}$	no	no

the swap operation implies $X^S = Z \otimes Y$. One may define a swap operator as follows

$$S \equiv \sum_{i,j=1}^{N} |i\,j\rangle\langle j\,i| \quad \text{so that} \quad S_{\substack{m\mu\\ n\nu}} = \delta_{m\nu}\delta_{n\mu}. \tag{A.16}$$

This operator is symmetric, Hermitian, unitary and the identity $X^S = SXS$ holds. We may also define *partial swaps* — $X^{S_A} = SX$ and $X^{S_B} = XS$ —.

To conclude this appendix, we summarized all these involutions — since performed twice are equal to identity — in the table A.1, with some properties of the transformations. It is not difficult to find some relations between them[xiii].

[xiii] *Cf.* [5] for some of them.

Bibliography

[1] Thiago O. Maciel and Reinaldo O. Vianna. ‘Viable entanglement detection of unknown mixed states in low dimensions’. *Phys. Rev. A* **80**, 3 (2009), p. 032325. arXiv:0907.1114.

[2] C. Cohen-Tannoudji, B. Diu and F. Lalo
"e. *Quantum mechanics*. Quantum Mechanics. Wiley, 1977. ISBN: 9782705658342.

[3] M. A. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[4] R. Bhatia. *Positive Definite Matrices*. Princeton Series in Applied Mathematics. Princeton University Press, 2007.

[5] Karol Życzkowski and Ingmar Bengtsson. *Geometry of Quantum States*. Cambridge University Press, 2006.

[6] L. Danzer, B. Grünbaum, V. Klee and Helly. ‘Helly’s theorem and its relatives’. *Convexity*. Proc. Symp. Pure Math. Providence, RI: AMS, 1963, pp. 101–179.

[7] C. Carathéodory. ‘Über den Variabilitätsbereich der Fourierschen Konstanten von positiven harmonischen Funktionen’. *Rendiconti del Circolo Matematico di Palermo* **32** (1911), pp. 193–217.

[8] E. Schrödinger. ‘Probability distributions between separated systems’. *Proceedings of the Cambridge Philosophical Society*. Vol. 32. 1936, p. 446.

[9] R. Bhatia. *Matrix Analysis*. Graduate texts in mathematics. Springer-Verlag New York, 1997.

[10] R. Horn and C. R. Johnson. *Topics in Matrix Analysis*. British Library Cataloguing in Publication applied for. Press Syndicate of the University of Cambrige, 1991.

[11] J. J. Sylvester. ‘A demonstration of the theorem that every homogeneous quadratic polynomial is reducible by real orthogonal substitutions to the form of a sum of positive and negative squares’. *Philosophical Magazine* **4**, 23 (1952), pp. 138–142.

[12] C. W. Norman. *Undergraduate algebra*. Oxford University Press, 1986.

[13] M. J. Donald, M. Horodecki and O. Rudolph. ‘The uniqueness theorem for entanglement measures’. *J. Math. Phys.* **43**, 4252 (2002). arXiv:quant-ph/0105017.

[14] K. Kraus. *States, Effects and Operations*. Lecture Notes in Physics. Springer, Berlin, Heidelberg, 1983.

[15] M. A. Nielsen, C. M. Caves, B. Schumacher and H. Barnum. 'Information-theoretic approach to quantum error correction and reversible measurement'. *Proc. R. Soc. Lond. A* **454**, 1969 (1998), pp. 277–304. arXiv:quant-ph/9706064.

[16] M. Horodecki, P. Horodecki and R. Horodecki. 'Mixed-State Entanglement and Quantum Communication'. *Quantum Information*. Ed. by G. Alber. 2001, pp. 151–195. arXiv:quant-ph/0109124.

[17] K. Kraus. 'General state changes in quantum theory'. *Annals of Physics* **64**, 2 (1971), pp. 311 –335.

[18] W. F. Stinespring. 'Positive Functions on C^*-algebras'. *Proceedings of the American Mathematical Society* **6** (1955), 211–216.

[19] E. C. G. Sudarshan, P. M. Mathews and Jayaseetha Rau. 'Stochastic Dynamics of Quantum-Mechanical Systems'. *Phys. Rev.* **121**, 3 (1961), pp. 920–924.

[20] David Evans. 'Quantum dynamical semigroups, symmetry groups, and locality'. *Acta Applicandae Mathematicae* **2** (3 1984), pp. 333–352.

[21] M. Keyl. 'Fundamentals of quantum information theory'. *Physics Reports* **5** (2002), pp. 431–548. arXiv:quant-ph/0202122.

[22] R Schatten. *A Theory of Cross-spaces*. Princeton University Press, 1950.

[23] A. Jamiołkowski. 'Linear transformations which preserve trace and positive semidefiniteness of operators'. *Rep. Math. Phys* **3**, 4 (1972), pp. 275–278.

[24] Man-Duen Choi. 'Positive semidefinite biquadratic forms'. *Linear Algebra Appl.* **12**, 2 (1975), pp. 95–100.

[25] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin and W. K. Wootters. 'Quantum nonlocality without entanglement'. *Phys. Rev. A* **59**, 2 (1999), pp. 1070–1091. arXiv:quant-ph/9804053.

[26] J. I. Cirac, W. Dür, B. Kraus and M. Lewenstein. 'Entangling Operations and Their Implementation Using a Small Amount of Entanglement'. *Phys. Rev. Lett.* **86**, 3 (2001), pp. 544–547. arXiv:quant-ph/0007057.

[27] E. M. Rains. 'Rigorous treatment of distillable entanglement'. *Phys. Rev. A* **60**, 1 (1999), pp. 173–178. arXiv:quant-ph/9809078.

[28] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters. 'Mixed-state entanglement and quantum error correction'. *Phys. Rev. A* **54**, 5 (1996), pp. 3824–3851. arXiv:quant-ph/9604024.

[29] V. Vedral and M. B. Plenio. 'Entanglement measures and purification procedures'. *Phys. Rev. A* **57**, 3 (1998), pp. 1619–1633. arXiv:quant-ph/9707035.

[30] E. M. Rains. 'Bound on distillable entanglement'. *Phys. Rev. A* **60**, 1 (1999), pp. 179–184. arXiv:quant-ph/9809082.

[31] E. M. Rains. 'Erratum: Bound on distillable entanglement [Phys. Rev. A 60, 179 (1999)]'. *Phys. Rev. A* **63**, 1 (2000), p. 019902.

[32] W. Dür and J. I. Cirac. 'Nonlocal operations: Purification, storage, compression, tomography, and probabilistic implementation'. *Phys. Rev. A* **64**, 1 (2001), p. 012317. arXiv:quant-ph/0012148.

[33] X. Wang and P. Zanardi. 'Quantum entanglement of unitary operators on bipartite systems'. *Phys. Rev. A* **66**, 4 (2002), p. 044303. arXiv:quant-ph/0207007.

[34] P. Zanardi. 'Entanglement of quantum evolutions'. *Phys. Rev. A* **63**, 4 (2001), p. 040304. arXiv:quant-ph/0010074.

[35] P. Zanardi, C. Zalka and L. Faoro. 'Entangling power of quantum evolutions'. *Phys. Rev. A* **62**, 3 (2000), p. 030301. arXiv:quant-ph/0005031.

[36] L. Clarisse, S. Ghosh, S. Severini and A. Sudbery. 'Entangling power of permutations'. *Phys. Rev. A* **72**, 1 (2005), p. 012314. arXiv:quant-ph/0502040.

[37] A. Einstein, B. Podolsky and N. Rosen. 'Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?' *Phys. Rev.* **47**, 10 (1935), pp. 777–780.

[38] N. Bohr. 'Can Quantum-Mechanical Description of Physical Reality be Considered Complete?' *Phys. Rev.* **48**, 8 (1935), pp. 696–702.

[39] A. M. Gleason. 'Measures on the closed subspaces of a Hilbert space'. *Journal of mathematics and mechanics* **6**, 6 (1957), pp. 885–893.

[40] S. Kochen and E. P. Specker. 'Problem of hidden variables in quantum mechanics'. *Journal of mathematics and mechanics* **17**, 1 (1967), pp. 59–87.

[41] J. S. Bell. 'On the Einstein Podolsky Rosen paradox'. *Physics* **1** (1964), pp. 195–200.

[42] J. S. Bell. 'On the Problem of Hidden Variables in Quantum Mechanics'. *Rev. Mod. Phys.* **38**, 3 (1966), pp. 447–452.

[43] A. Peres. *Quantum theory: concepts and methods*. Fundamental theories of physics. Kluwer Academic, 1993.

[44] M. Redhead. *Incompleteness, Nonlocality, and Realism: A Prolegomenon to the Philosophy of Quantum Mechanics*. Clarendon Press, Oxford, 1990.

[45] André Tanus Cesário de Souza. *An Essay on the Foundations of Classical and Quantum Information Theory*. MSc. thesis. Universidade Federal de Minas Gerais, 2011.

[46] A. Peres. 'Separability Criterion for Density Matrices'. *Phys. Rev. Lett.* **77** (1996), pp. 1413–1415. arXiv:quant-ph/9604005.

[47] M. Horodecki, P. Horodecki and R. Horodecki. 'Separability of mixed states: necessary and sufficient conditions'. *Phys. Lett. A* **223** (1996), pp. 1–8. arXiv:quant-ph/9605038.

[48] L. Gurvits. 'Quantum Matching Theory (with new complexity theoretic, combinatorial and topological insights on the nature of the Quantum Entanglement)' (2002). arXiv:quant-ph/0201022.

[49] Fernando G.S.L. Brandão, Matthias Christandl and Jon Yard. 'A quasipolynomial-time algorithm for the quantum separability problem'. *Proceedings of the 43rd annual ACM symposium on Theory of computing*. STOC '11. 2011, pp. 343–352. arXiv:1011.2751.

[50] Fernando G.S.L. Brandão, Matthias Christandl and Jon Yard. 'Detection of Multipartite Entanglement: Quantifying the Search for Symmetric Extensions' (2011). arXiv:1105.5720.

[51] F. G. S. L. Brandão and R. O. Vianna. 'Separable Multipartite Mixed States: Operational Asymptotically Necessary and Sufficient Conditions'. *Phys. Rev. Lett.* **93**, 22 (2004). arXiv:quant-ph/0405063.

[52] F. G. S. L. Brandão. 'Quantifying entanglement with witness operators'. *Phys. Rev. A* **72**, 2 (2005). arXiv:quant-ph/0503152.

[53] F. G. S. L. Brandao and R. O. Vianna. 'Witnessed Entanglement'. *Int. J. Quantum Inf.* **4** (2006), p. 331. arXiv:quant-ph/0405096v5.

[54] Dagmar Bruß. 'Characterizing entanglement'. *J. Math. Phys.* **43**, 9 (2002), pp. 4237–4251. arXiv:quant-ph/0110078.

[55] Dagmar Bruß, J. Ignacio Cirac, Pawel Horodecki, Florian Hulpke, Barbara Kraus, Maciej Lewenstein and Anna Sanpera. 'Reflections upon separability and distillability'. *Journal of Modern Optics* **49**, 8 (2002), pp. 1399–1418. arXiv:quant-ph/0110081.

[56] K. Eckert, O. Gühne, F. Hulpke, P. Hyllus, J. Korbicz, J. Mompart, D. Bruß, M. Lewenstein and A. Sanpera. 'Entanglement Properties of Composite Quantum Systems'. *Quantum Information Processing*. Wiley-VCH Verlag, 2005, pp. 79–95.

[57] M. Lewenstein, D. Bruß, J. I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera and R. Tarrach. 'Separability and distillability in composite quantum systems-a primer'. *Journal of Modern Optics* **47**, 14-15 (2000), pp. 2481–2499. arXiv:quant-ph/0006064.

[58] A. Sen De, U. Sen, M. Lewenstein and A. Sanpera. *Lectures on quantum information. The separability versus entanglement problem*. 2005. arXiv:quant-ph/0508032.

[59] Barbara M. Terhal. 'Bell inequalities and the separability criterion'. *Physics Letters A* **271**, 5-6 (2000), pp. 319 –326. arXiv:quant-ph/9911057.

[60] Barbara M. Terhal. 'Detecting Quantum Entanglement'. *Journal of Theoretical Computer Science* **287**, 1 (2002), pp. 313–335. arXiv:quant-ph/0101032.

[61] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki and Karol Horodecki. 'Quantum entanglement'. *Rev. Mod. Phys.* **81**, 2 (2009), pp. 865–942. arXiv:quant-ph/0702225.

[62] N. Gisin. 'Bell's inequality holds for all non-product states'. *Physics Letters A* **154**, 5-6 (1991), pp. 201 –202.

[63] Sandu Popescu and Daniel Rohrlich. 'Generic quantum nonlocality'. *Physics Letters A* **166**, 5-6 (1992), pp. 293 –297. issn: 0375-9601.

[64] Ryszard Horodecki, Michal Horodecki and Pawel Horodecki. 'Teleportation, Bell's inequalities and inseparability'. *Physics Letters A* **222**, 1-2 (1996), pp. 21 –25. arXiv:quant-ph/9606027.

[65] Sandu Popescu. 'Bell's inequalities versus teleportation: What is nonlocality?' *Phys. Rev. Lett.* **72**, 6 (1994), pp. 797–799.

[66] N. Gisin. 'Hidden quantum nonlocality revealed by local filters'. *Physics Letters A* **210**, 3 (1996), pp. 151 –156.

[67] Sandu Popescu. 'Bell's Inequalities and Density Matrices: Revealing "Hidden" Nonlocality'. *Phys. Rev. Lett.* **74**, 14 (1995), pp. 2619–2622. arXiv:quant-ph/9502005.

[68] Asher Peres. 'Collective tests for quantum nonlocality'. *Phys. Rev. A* **54**, 4 (1996), pp. 2685–2689. arXiv:quant-ph/9603023.

[69] Artur Ekert and Peter L. Knight. 'Entangled quantum systems and the Schmidt decomposition'. *Am. J. Phys.* **63**, 5 (1995), pp. 415–423.

[70] E. Schrödinger. 'Discussion of probability distributions between separated systems'. *Proceedings of the Cambridge Philosophical Society*. Vol. 31. 1935, pp. 555–563.

[71] Erhard Schmidt. 'Zur Theorie der linearen und nichtlinearen Integralgleichungen. 1. Entwicklung willküriger Funktionen nach Systemevorgeschriebener'. *Mathematische Annalen* **63** (4 1907), pp. 433–476.

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

[73] P.D. Lax. *Functional analysis*. Pure and applied mathematics. Wiley, 2002.

[74] R.T. Rockafellar. *Convex analysis*. Princeton Mathematical Series. Princeton University Press, 1997. ISBN: 9780691015866.

[75] Philipp Hyllus, Otfried Gühne, Dagmar Bruß and Maciej Lewenstein. 'Relations between entanglement witnesses and Bell inequalities'. *Phys. Rev. A* **72**, 1 (2005), p. 012321. arXiv:quant-ph/0504079.

[76] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello and A. Sanpera. 'Detection of entanglement with few local measurements'. *Phys. Rev. A* **66**, 6 (2002), p. 062305. arXiv:quant-ph/0205089.

[77] O. Gühne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello and A. Sanpera. 'Experimental detection of entanglement via witness operators and local measurements'. *Journal of Modern Optics* **50**, 6-7 (2003), pp. 1079–1102. arXiv:quant-ph/0210134.

[78] Martin B. Plenio and S. Virmani. 'An introduction to entanglement measures'. *Quant. Inf. Comp.* **7** (2007), p. 1. arXiv:quant-ph/0504163.

[79] Timothy F. Havel. 'Robust procedures for converting among Lindblad, Kraus and matrix representations of quantum dynamical semigroups'. *J. Math. Phys.* **44**, 2 (2003), pp. 534–557.

[80] Michal Horodecki, Pawel Horodecki and Ryszard Horodecki. 'Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps'. *Physics Letters A* **283**, 1-2 (2001), pp. 1 –7. arXiv:quant-ph/0006071.

[81] N. J. Cerf and C. Adami. 'Quantum extension of conditional probability'. *Phys. Rev. A* **60**, 2 (1999), pp. 893–897. arXiv:quant-ph/9710001.

[82] Michał Horodecki and Paweł Horodecki. 'Reduction criterion of separability and limits for a class of distillation protocols'. *Phys. Rev. A* **59**, 6 (1999), pp. 4206–4216. arXiv:quant-ph/9708015.

[83] Paweł Horodecki, Maciej Lewenstein, Guifré Vidal and Ignacio Cirac. 'Operational criterion and constructive checks for the separability of low-rank density matrices'. *Phys. Rev. A* **62**, 3 (2000), p. 032310. arXiv:quant-ph/0002089.

[84] Pawel Horodecki, John A. Smolin, Barbara M. Terhal and Ashish V. Thapliyal. 'Rank two bipartite bound entangled states do not exist'. *Theoretical Computer Science* **292**, 3 (2003), pp. 589 –596. arXiv:quant-ph/9910122.

[85] M. Horodecki, P. Horodecki and R. Horodecki. 'Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?' *Phys. Rev. Lett.* **80** (1998), pp. 5239–5242. arXiv:quant-ph/9801069.

[86] E. C. G. Sudarshan and Anil Shaji. 'Structure and parametrization of stochastic maps of density matrices'. *Journal of Physics A* **36**, 18 (2003), p. 5073. arXiv:quant-ph/0109158.

[87] Erling Størmer. 'Positive linear maps of operator algebras'. *Acta Math.* **110** (1963), pp. 233–278.

[88] Man-Duen Choi. 'Completely Positive linear maps on complex matrices'. *Linear Algebra Appl.* **10**, 3 (1975), pp. 285–290.

[89] S. L. Woronowicz. 'Positive maps of low dimensional matrix algebras'. *Rep. Math. Phys* **10**, 2 (1976), pp. 165–183.

[90] Man-Duen Choi and Tsit-Yuen Lam. 'Extremal positive semidefinite forms'. *Mathematische Annalen* **231** (1 1977), pp. 1–18.

[91] Paweł Horodecki, Michał Horodecki and Ryszard Horodecki. 'Bound Entanglement Can Be Activated'. *Phys. Rev. Lett.* **82**, 5 (1999), pp. 1056–1059.

[92] Mohamed Bourennane, Manfred Eibl, Christian Kurtsiefer, Sascha Gaertner, Harald Weinfurter, Otfried Gühne, Philipp Hyllus, Dagmar Bruß, Maciej Lewenstein and Anna Sanpera. 'Experimental Detection of Multipartite Entanglement using Witness Operators'. *Phys. Rev. Lett.* **92**, 8 (2004), p. 087902. arXiv:quant-ph/0309043.

[93] A. C. Doherty, Pablo A. Parrilo and Federico M. Spedalieri. 'Distinguishing Separable and Entangled States'. *Phys. Rev. Lett.* **88**, 18 (2002), p. 187904. arXiv:quant-ph/0112007.

[94] Andrew C. Doherty, Pablo A. Parrilo and Federico M. Spedalieri. 'Complete family of separability criteria'. *Phys. Rev. A* **69**, 2 (2004), p. 022308. arXiv:quant-ph/0308032.

[95] Andrew C. Doherty, Pablo A. Parrilo and Federico M. Spedalieri. 'Detecting multipartite entanglement'. *Phys. Rev. A* **71**, 3 (2005), p. 032333. arXiv:quant-ph/0407143.

[96] F Hulpke and D BruÃŸ. 'A two-way algorithm for the entanglement problem'. *Journal of Physics A: Mathematical and General* **38**, 24 (2005), p. 5573. arXiv:quant-ph/0407179.

[97] Hugo J. Woerdeman. 'Checking $2 \times M$ quantum separability via semidefinite programming'. *Phys. Rev. A* **67**, 1 (2003), p. 010303. arXiv:quant-ph/0301058.

[98] Jens Eisert, Philipp Hyllus, Otfried Gühne and Marcos Curty. 'Complete hierarchies of efficient approximations to problems in entanglement theory'. *Phys. Rev. A* **70**, 6 (2004), p. 062317. arXiv:quant-ph/0407135.

[99] Maciej Lewenstein and Anna Sanpera. 'Separability and Entanglement of Composite Quantum Systems'. *Phys. Rev. Lett.* **80**, 11 (1998), pp. 2261–2264. arXiv:quant-ph/9707043.

[100] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004. URL: http://www.stanford.edu/~boyd/cvxbook/.

[101] Jos F. Sturm. *Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones*. 1998.

[102] V. Vedral, M. B. Plenio, M. A. Rippin and P. L. Knight. 'Quantifying Entanglement'. *Phys. Rev. Lett.* **78**, 12 (1997), pp. 2275–2279. arXiv:quant-ph/9702027.

[103] M. Horodecki. 'Entanglement easures'. *Quant. Inf. Comp.* **1** (2001), p. 3.

[104] Guifré Vidal. 'Entanglement monotones'. *Journal of Modern Optics* **47**, 2-3 (2000), pp. 355–376. arXiv:quant-ph/9807077.

[105] Guifré Vidal and Rolf Tarrach. 'Robustness of entanglement'. *Phys. Rev. A* **59**, 1 (1999), pp. 141–155.

[106] Michael Steiner. 'Generalized robustness of entanglement'. *Phys. Rev. A* **67**, 5 (2003), p. 054305.

[107] S. P. Walborn, P. H. Souto Ribeiro, L. Davidovich, F. Mintert and A. Buchleitner. 'Experimental determination of entanglement with a single measurement'. *Nature* **440**, 1022 (2006).

[108] Florian Mintert, Marek Ku ś and Andreas Buchleitner. 'Concurrence of Mixed Multipartite Quantum States'. *Phys. Rev. Lett.* **95**, 26 (2005).

[109] Christian Schmid, Nikolai Kiesel, Witlef Wieczorek, Harald Weinfurter, Florian Mintert and Andreas Buchleitner. 'Experimental Direct Observation of Mixed State Entanglement'. *Phys. Rev. Lett.* **101**, 26 (2008).

[110] Florian Mintert and Andreas Buchleitner. 'Observable Entanglement Measure for Mixed Quantum States'. *Phys. Rev. Lett.* **98**, 14 (2007).

[111] Chang-shui Yu, C. Li and He-shan Song. 'Measurable concurrence of mixed states'. *Phys. Rev. A* **77**, 1 (2008), p. 012305.

[112] J Eisert, F G S L Brandão and K M R Audenaert. 'Quantitative entanglement witnesses'. *New Journal of Physics* **9**, 3 (2007), p. 46.

[113] O. Gühne, M. Reimpell and R. F. Werner. 'Estimating Entanglement Measures in Experiments'. *Phys. Rev. Lett.* **98**, 11 (2007), p. 110502.

[114] Piotr Badzia ̧g, Časlav Brukner, Wiesław Laskowski, Tomasz Paterek and Marek Żukowski. 'Experimentally Friendly Geometrical Criteria for Entanglement'. *Phys. Rev. Lett.* **100**, 14 (2008), p. 140403.

[115] Ali Saif M. Hassan and Pramod S. Joag. 'Experimentally accessible geometric measure for entanglement in N -qubit pure states'. *Phys. Rev. A* **77**, 6 (2008), p. 062334.

[116] Marcos Curty, Maciej Lewenstein and Norbert Lütkenhaus. 'Entanglement as a Precondition for Secure Quantum Key Distribution'. *Phys. Rev. Lett.* **92**, 21 (2004), p. 217903.

[117] Jianming Cai and Wei Song. 'Novel Schemes for Directly Measuring Entanglement of General States'. *Phys. Rev. Lett.* **101**, 19 (2008), p. 190503.

[118] J. Löfberg. 'YALMIP : A Toolbox for Modeling and Optimization in MATLAB'. *Proceedings of the CACSD Conference*. Taipei, Taiwan, 2004. URL: http://control.ee.ethz.ch/\~{}joloef/yalmip.php.

[119] Michel Planat, Anne-Céline Baboin and Metod Saniga. 'Multi-Line Geometry of Qubit–Qutrit and Higher-Order Pauli Operators'. *International Journal of Theoretical Physics* **47** (4 2008), pp. 1127–1135.

[120] Bandyopadhyay, Boykin, Roychowdhury and Vatan. 'A New Proof for the Existence of Mutually Unbiased Bases'. *Algorithmica* **34** (4 2008), pp. 512–528.

[121] Jay Lawrence. 'Mutually unbiased bases and trinary operator sets for N qutrits'. *Phys. Rev. A* **70**, 1 (2004), p. 012302.

[122] P.K. Aravind. 'Solution to the King's Problem in prime power dimensions'. *Z.Naturforsch* **58a** (2003), p. 2212. arXiv:quant-ph/0210007.

[123] I D Ivonovic. 'Geometrical description of quantal state determination'. *Journal of Physics A: Mathematical and General* **14**, 12 (1981), p. 3241.

[124] William K Wootters and Brian D Fields. 'Optimal state-determination by mutually unbiased measurements'. *Annals of Physics* **191**, 2 (1989), pp. 363 –381.

[125] R.F. Werner. *See, for example, the quantum information open problem #13 in Prof. Werner's homepage*. URL: http://www.imaph.tu-bs.de/qi/problems/13.html.

[126] Berthold-Georg Englert and Yakir Aharonov. 'The mean king's problem: prime degrees of freedom'. *Physics Letters A* **284**, 1 (2001), pp. 1 –5.

[127] A. Klappenecher and M. Rotteler. 'Constructions of Mutually Unbiased Bases'. *Finite Fields and Applications* **2948**, 137 (2004), 262–266.

[128] M. Grassl. 'On SIC-POVMs and MUBs in dimension 6' (2009). arXiv:quant-ph/0406175.

[129] Clinton J. Oxenrider and Richard D. Hill. 'On the matrix reorderings Γ and ψ'. *Linear Algebra and its Applications* **69** (1985), pp. 205 –212.

[130] David A. Yopp and Richard D. Hill. 'On completely copositive and decomposable linear transformations'. *Linear Algebra and its Applications* **312**, 1-3 (2000), pp. 1 –12.