The mathematics of quantum information theory: Geometry of quantum states

An introduction to QUANTUM ENTANGLEMENT

Master's Thesis submitted to the
Faculty of Informatics of the *Università della Svizzera Italiana*
in partial fulfillment of the requirements for the degree of
Master of Science in Informatics

presented by
Anita Buckley

under the supervision of
Prof. Stefan Wolf
co-supervised by
Charles Alexandre Bédard

June 2021

I certify that except where due acknowledgement has been given, the work presented in this thesis is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; and the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program.

Anita Buckley
Lugano, 24. June 2021

To my family

Abstract

This master's thesis is in the area of quantum information theory (QIT) and may be considered as an introduction to quantum entanglement. Entanglement is the key non-classical feature of quantum mechanics, and a resource for several modern applications including quantum cryptography, quantum computing and quantum communication. The thesis explores the strong links of QIT with geometry, in particular convex sets, and with functional analysis of Euclidean and Hilbert spaces and operators on them. The basic definitions and concepts are introduced in the mathematical framework and then related to the field-specific notations and concepts in quantum information theory and in quantum mechanics.

At the start the following conventions and concepts and are reviewed: the bra-ket notation, Hilbert spaces, tensor products, operator or (after specifying bases) matrix algebras and, the key concept of the thesis, the concept of states (i.e., positive self-adjoint operators of trace one) or density matrices. There are two fundamental dichotomies on the set of states. The first dichotomy is between pure states, represented by unit vectors in a complex Hilbert space, and mixed states that are statistical ensambles of pure states. The notions of multipartite states on tensor products of Hilbert spaces and the partial trace are introduced. The second dichotomy, concerning bipartite states, is between the set of separable states (i.e., convex combinations of product states) and its complement, the entangled states. Often it is convenient to drop the trace condition and consider the cone of positive semidefinite matrices instead of the convex set of states.

The Choi isomorphism plays a central role in the thesis by relating (super)operators acting on matrix or operator algebras with the Choi matrices acting on bipartite Hilbert spaces. In specified bases the Choi isomorphism is equal to

$$\begin{array}{ccc} B\left(\mathrm{M}_n, \mathrm{M}_m\right) & \xrightarrow{C} & B\left(\mathbb{C}^m \otimes \mathbb{C}^n\right) \\ \Phi\colon\ \mathrm{M}_n \to M_m & \mapsto & C(\Phi)\colon\ \mathbb{C}^m \otimes \mathbb{C}^n \to \mathbb{C}^m \otimes \mathbb{C}^n, \\ & & \| \\ & & \displaystyle\sum_{i,j} \Phi(E_{ij}) \otimes E_{ij} \end{array}$$

where B stands for bounded linear maps and M_n denotes the space of $n \times n$ matrices. This induces an isomorphism between the real vector spaces of self-adjointness-preserving linear maps $\left\{\Phi\colon\ \mathrm{M}_n^{\mathrm{sa}} \to \mathrm{M}_m^{\mathrm{sa}}\right\}$ and self-adjoint matrices in $\mathrm{M}_{m\cdot n}^{\mathrm{sa}}$. Consequently, there exist one-to-one correspondences between the cones of positivity preserving / decomposable / completely positive / PPT-inducing / entanglement breaking maps and the cones of block positive / decomposable / positive semidefinite / PPT /separable matrices, respectively. The most important of them are the two self-dual cones related by Choi's theorem, the cone of completely positive maps and

the cone of positive semidefinite matrices. In QIT, completely positive maps relate to quantum channels.

The goal of the thesis is to construct entanglement witnesses, maps that certify entanglement in bipartite states. The transposition is arguably the most powerful but certainly the most famous entanglement witness. By the Størmer-Woronowicz theorem, every state with positive partial transpose (PPT) on $\mathbb{C}^2 \otimes \mathbb{C}^2$ or $\mathbb{C}^2 \otimes \mathbb{C}^3$ is separable. The PPT criterion or Peres-Horodecki criterion is a special case of Horodecki's entanglement witness theorem. Any positivity preserving map Φ which is not completely positive (transposition being the most known one) defines an entanglement witness, i.e., $\langle C(\Phi), \cdot \rangle_{\text{HS}}$ certifies entanglement in any state ρ for which $\langle C(\Phi), \rho \rangle_{\text{HS}} < 0$.

The construction of entanglement witnesses which can detect entangled PPT states (that are not detectable by the transposition entanglement witness) is phrased as a convex optimization problem in the form of a semidefinite program (SDP).

Acknowledgements

I had been learning various topics within this thesis for many years. Klemen Šivic from University of Ljubljana first introduced me to positive maps, and by studying these together we became aware of their fundamental role in quantum information theory.

I am grateful to Università della Svizzera Italiana, to the teachers of the many great courses and the staff for their support and hospitality. I enjoyed my two years master's degree and I learnt a lot. Special thanks to Professor Stefan Wolf and Xavier Coiteux-Roy for the elegant introduction into the interplay between quantum physics, informatics and mathematics.

I benefited from the Masterclass on Tensors: Geometry and Quantum Information at QMATH Copenhagen [VLOW18], in particular from conversations with Alexander Müller-Hermes and Matthias Christandl. I learned the theoretical minimum in physics from the entertaining books of Susskind [SF15; SF18; Sus20].

I thank William Schober and Charles Alexandre Bédard for sharing their insight into physics. I am especially grateful to Will for asking questions, helping me to ask questions and never getting tired of searching for answers.

I couldn't have wished for better supervisors. Stefan and Charles gave me a free hand to explore entanglement and write the thesis, and at the same time they supported me and believed in me.

Finally, I would like to thank my family for letting me be me - my parents for making me, Dave for supporting me, and my kids for challenging me.

Contents

Figures

Tables

Chapter 1

Introduction

1.1 Preface

Many (scientists) believe that building a quantum computer is the major scientific and technological challenge of this century. Progress in the evolution of quantum computation and quantum information draws upon the perspectives and insights of computer science, mathematics, physics and even philosophy. Quantum information theory (QIT) provides the mathematical framework for this interdisciplinary field. QIT is strongly linked to geometry, in particular convex sets, and to functional analysis of Euclidean and Hilbert spaces and operators on them.

This master's thesis is in the area of QIT and may be considered as an introduction to quantum entanglement. Entanglement is the key non-classical feature of quantum mechanics, and a resource for several modern applications including quantum cryptography, quantum computing and quantum communication.

Outline of the thesis is the following. We start with the basic definitions and concepts that will be used in the thesis as a reference. We expect the reader to have the basic understanding of (linear) algebra, in particular of finite dimensional real and complex vector spaces and maps acting between them. We assume the knowledge of classical theorems, e.g., singular value decomposition or Riesz representation theorem. We introduce mathematical concepts that are field-specific to quantum information theory, like Hilbert spaces, operator algebras or (after specifying bases) matrix algebras, and relate them to the analogous concepts that are specific to quantum mechanics. This way we review the notations and conventions of the bra-ket notation, Hilbert-Schmidt inner product, tensor products and the key concept of states. Chapter 2 introduces two fundamental dichotomies on states: pure states versus mixed states and separable states versus entangled states. In Chapter 3 we define the Choi isomorphism that relates (super)operators acting on matrix or operator algebras with the Choi matrices acting on bipartite Hilbert spaces. This establishes a one-to-one correspondence between the cone of completely positive maps and the cone of positive semidefinite matrices. We explain how completely positive maps relate to quantum channels. In parallel we discuss how these concepts appear and are relevant in quantum theory; we hope this can help the reader in understanding physicist's literature on the subject. The aim of the last section is to develop entanglement witnesses, maps that certify entanglement in bipartite states.

Most of the concepts in the thesis are developed "from scratch" from the definitions and illustrated by many examples. We include the proofs of all relevant statements (or else indicate the relevant section in our main reference [AS17]). We believe that the figures in the thesis convey the adage "a picture is worth a thousand words".

Bibliography contains both, modern references that capture the latest developments in quantum information theory, and classical results (often discovered independently in mathematics and physics) serving as theoretical foundations enabling the rapid progress in the field. They may be considered as references to everyone that is interested in QIT and its mathematical background.

1.2 Notation and basic concepts

Throughout the thesis we will use the standard notation of quantum information theory as introduced in [AHW20], [NC10] or any other textbook. We start by connecting concepts of (linear) algebra and functional analysis to the Dirac bra-ket notation and states.

A vector space $\mathcal{H}$ over the field $\mathbb{K}$ (of complex numbers $\mathbb{C}$ or real numbers $\mathbb{R}$) is a *Hilbert space* if it is equipped with an inner product and is also a complete metric space with respect to the norm induced by the inner product. An *inner product* or a *scalar product* is a mapping $\langle \cdot, \cdot \rangle \colon \mathcal{H} \times \mathcal{H} \to \mathbb{K}$ with the following properties:

- $\langle \psi, \psi \rangle \geq 0$ for all $\psi \in \mathcal{H}$ and $\langle \psi, \psi \rangle = 0$ implies $\psi = 0$;
- $\langle \psi, \chi + \zeta \rangle = \langle \psi, \chi \rangle + \langle \psi, \zeta \rangle$ for all $\psi, \chi, \zeta \in \mathcal{H}$;
- $\langle \psi, \lambda \chi \rangle = \lambda \langle \psi, \chi \rangle$ for all $\psi, \chi \in \mathcal{H}$ and all $\lambda \in \mathbb{K}$;
- $\langle \psi, \chi \rangle = \overline{\langle \chi, \psi \rangle}$ for all $\psi, \chi \in \mathcal{H}$.

Note that, following the above convention, the inner product is conjugate linear in the first argument and linear in the second argument. Hilbert spaces are by definition *complete normed spaces*, in the sense that every Cauchy sequence of vectors in $\mathcal{H}$ converges in $\mathcal{H}$, in the norm acting on vectors as $||\psi|| = \sqrt{\langle \psi, \psi \rangle}$.

The above definitions allow us to generalize important concepts of finite dimensional Euclidean spaces to Hilbert spaces, such as length of a vector, orthogonality of two vectors, orthonormal basis, identification of a Hilbert space with its topological dual space etc. Combining the three fundamental structures - linear structure (vectors), metric structure (length of vectors) and geometric structure (angle between two vectors) - gives Hilbert spaces such an important role in quantum physics and functional analysis, and in particular in quantum information theory.

The space of *bounded operators* (i.e., bounded linear maps) from $\mathcal{H}'$ to $\mathcal{H}$ will be denoted by $B(\mathcal{H}', \mathcal{H})$. In particular we write $B(\mathcal{H}) = B(\mathcal{H}, \mathcal{H})$. A linear map $L \colon \mathcal{H}' \to \mathcal{H}$ is *bounded* if there exists some $c \geq 0$ such that for all $\psi \in \mathcal{H}'$,

$$||L\psi||_{\mathcal{H}} \leq c||\psi||_{\mathcal{H}'}.$$

The smallest such c is by definition the *operator norm* of L. A linear operator between normed spaces is bounded if and only if it is continuous. It holds that any operator between two finite-dimensional Hilbert spaces is bounded, which is what we will assume throughout the thesis. To each operator $A \in B(\mathcal{H}', \mathcal{H})$ we can assign its unique *adjoint* operator $A^* \in B(\mathcal{H}, \mathcal{H}')$ satisfying the property

$$\langle \psi, A\psi' \rangle = \langle A^*\psi, \psi' \rangle \text{ for all } \psi \in \mathcal{H}, \psi' \in \mathcal{H}'.$$

Operator $A \in B(\mathcal{H})$ is *self-adjoint* if $A^* = A$. Note that the space of self-adjoint operators $B^{\mathrm{sa}}(\mathcal{H})$ is a real (but not complex) vector subspace in $B(\mathcal{H})$. We call operator $S \in B(\mathcal{H})$ *positive* (or *positive semidefinite*) if it satisfies one of the equivalent properties:

- For all $\psi \in \mathcal{H}$ it holds $\langle \psi, S\psi \rangle \geq 0$;
- S is self-adjoint and $\langle \psi, S\psi \rangle \geq 0$ for all $\psi \in \mathcal{H}$;
- S is self-adjoint and its spectrum consists of non-negative real numbers;
- $S = A^*A$ for some operator $A \in B(\mathcal{H})$.

Another important family of operators are projections. $P \in B(\mathcal{H})$ is a *projection* if $P^2 = P$; this splits the Hilbert space $\mathcal{H} = \mathcal{V} \oplus \mathcal{V}^\perp$, where P acts on $\mathcal{V}$ as identity and $\mathcal{V}^\perp$ is its kernel. The operator $2P - I$ is then a *reflection* with respect to $\mathcal{V}$.

Example 1.1. If we identify vector $\psi \in \mathcal{H}$ with the operator $A_\psi \colon \alpha \mapsto \alpha\psi$ in $B(\mathbb{C}, \mathcal{H})$, its adjoint operator $\langle \psi, \cdot \rangle \colon \chi \mapsto \langle \psi, \chi \rangle$ is in the dual Hilbert space $B(\mathcal{H}, \mathbb{C}) = \mathcal{H}^*$ of linear functionals. Indeed, for $\alpha \in \mathbb{C}$ and $\chi \in \mathcal{H}$ it holds

$$\begin{array}{ccccc} \langle \chi, A_\psi \alpha \rangle & = & \langle \chi, \alpha\psi \rangle & = & \alpha \langle \chi, \psi \rangle \\ \| & & & & \\ \langle A_\psi^* \chi, \alpha \rangle & = & \langle \langle \psi, \chi \rangle, \alpha \rangle & = & \overline{\langle \psi, \chi \rangle} \alpha, \end{array}$$

where the inner products in the bottom line are in $\mathbb{C}$. The canonical norm and the canonical inner product on $\mathcal{H}^*$ are obtained by the Riesz representation theorem. In particular it holds $\|\langle \psi, \cdot \rangle\|_{\mathcal{H}^*} := \sup_{\chi \in \mathcal{H}} \frac{|\langle \psi, \chi \rangle|}{\|\chi\|_{\mathcal{H}}} = \|\psi\|_{\mathcal{H}}$.

The above example shows that $\mathcal{H}^*$ identifies canonically with $\overline{\mathcal{H}} = \overline{B(\mathbb{C}, \mathcal{H})}$. This identification is elegantly captured in the Dirac *bra-ket notation*, where a standard vector $\psi \in \mathcal{H}$ is written as $|\psi\rangle$ *ket vector*, and $\langle \psi|$ *bra vector* is the corresponding vector in $\overline{\mathcal{H}} \equiv \mathcal{H}^*$. Bra-ket notation generalizes well to standard operations on Hilbert spaces. The inner product $\langle \psi, \chi \rangle$ corresponds to the action of linear functional $\langle \psi|$ on vector $|\chi\rangle$, denoted as $\langle \psi|\chi \rangle$. Moreover, for $A \in B(\mathcal{H})$ and $\psi, \chi \in \mathcal{H}$ we have $A|\psi\rangle = |A\psi\rangle$ and $\langle \psi|A^* = \langle \psi A|$, and consequently $\langle \psi, A\chi \rangle = \langle A^*\psi, \chi \rangle$ is written as $\langle \psi|A|\chi \rangle$. We refer to the standard basis $e_1, e_2, \ldots, e_d$ of $\mathbb{C}^d$ as the *computational basis* $|0\rangle, |1\rangle, \ldots, |d-1\rangle$.

Any n-dimensional complex Hilbert space is isomorphic to $\mathbb{C}^n$. This allows us to identify the space of complex $m \times n$ matrices $\mathrm{M}_{m,n}$ with the space of operators $B(\mathbb{C}^n, \mathbb{C}^m)$ and, more generally after specifying bases, with operators between any complex Hilbert spaces of appropriate dimensions. Similarly we write $\mathrm{M}_n = B(\mathbb{C}^n)$ and $\mathrm{M}_n^{\mathrm{sa}} = B^{\mathrm{sa}}(\mathbb{C}^n)$; note that M_n is an n^2-dimensional complex vector space and $\mathrm{M}_n^{\mathrm{sa}}$ is a real vector space of dimension $n + 2\frac{n(n-1)}{2} = n^2$. These identifications ensure that the conjugate transposition of a matrix is consistent with the notion of the adjoint operator, a composition of operators corresponds to matrix multiplication and moreover, the trace duality induces an inner product on $\mathrm{M}_{m,n}$ defined as the *Hilbert–Schmidt inner product*

$$\langle M, N \rangle_{\mathrm{HS}} = \mathrm{Tr}\, M^*N \text{ for } M, N \in \mathrm{M}_{m,n}\,. \tag{1.1}$$

The corresponding norm $\|M\|_{\mathrm{HS}} = \sqrt{\mathrm{Tr}\, M^*M}$ is called the *Hilbert-Schmidt norm*, in mathematics it is usually called the *Frobenius norm*. We remark that the definition is independent of the choice of the orthonormal basis, therefore the Hilbert–Schmidt inner product and norm on $B(\mathcal{H})$

are well defined and make $B(\mathcal{H})$ into a Hilbert space. Similar interplay between operators and their matrix representations will be relevant in all the chapters. Therefore it is important to introduce the intrinsic definitions and properties (i.e., independent of the basis) in a canonical way.

The central concept of this thesis is that of quantum states. On a Hilbert space $\mathcal{H}$, a *quantum state* is a positive self-adjoint operator of trace one. Following the above identifications on finite-dimensional spaces, alternative names for states are *density matrices* or *density operators*, thus the set of states on $\mathcal{H}$ is denoted by $\mathrm{D}(\mathcal{H})$.

Remark 1.2. This definition of states is consistent with the definition of states in functional analysis, where a *state on a C^*-algebra* is a positive linear functional that maps unit element to 1. Indeed, $B(\mathbb{C}^n) = \mathrm{M}_n$ is an example of a C^*-algebra (i.e., a Banach algebra over $\mathbb{C}$ together with an involution $*$ satisfying $(\alpha M + \beta N)^* = \bar{\alpha} M^* + \bar{\beta} N^*$, $(MN)^* = N^* M^*$ and $\|MM^*\| = \|M\|^2$, the so-called adjoint properties). A state on $B(\mathbb{C}^n)$ is by definition a linear functional $\Phi\colon B(\mathbb{C}^n) \to \mathbb{C}$ such that $\Phi(I) = 1$ and $\Phi(XX^*) \geq 0$ for all $X \in B(\mathbb{C}^n)$. Since $\Phi \in B(\mathbb{C}^n)^*$, the Reisz representation theorem yields a matrix $M_\Phi \in B(\mathbb{C}^n) = \mathrm{M}_n$ for which it holds

$$\Phi = \langle M_\Phi, \cdot \rangle_{\mathrm{HS}} : \begin{array}{ccc} B(\mathcal{H}) & \to & \mathbb{C} \\ N & \mapsto & \langle M_\Phi, N \rangle_{\mathrm{HS}} = \mathrm{Tr}\, M_\Phi^* N. \end{array}$$

This implies that M_Φ is a density matrix. Indeed, its trace is $\mathrm{Tr}\, M_\Phi = \Phi(I) = 1$ and, by considering $\Phi(XX^*) = \mathrm{Tr}\, M_\Phi^* XX^* = \mathrm{Tr} X^* M_\Phi^* X \geq 0$ for suitable matrices X, we can prove that M_Φ is positive semi-definite.

In quantum mechanics the self-adjoint elements in $B^{sa}(\mathcal{H})$ are called *observables*, the measurable quantities of the physical system. As explained in Remark 1.2, a state Φ of the system is a positive functional on $B(\mathcal{H})$ or equivalently, its dual positive operator $M_\Phi \in B(\mathcal{H})$ of trace one. When measuring a system in state Φ with observable $L \in B^{\mathrm{sa}}(\mathcal{H})$, the possible results are the real eigenvalues of L. In Section 2.1 we will compute the probabilities of measuring a particular eigenvalue. Moreover, if the system is in state Φ, then the expected value of observable L is $\Phi(L) = \langle M_\Phi, L \rangle = \mathrm{Tr}\, M_\Phi^* L$.

Tensors describe states of quantum mechanical systems. If a system has k particles, its state is an operator on a *multipartite* Hilbert space

$$\mathcal{H} = \bigotimes_{j=1}^{k} \mathcal{H}_j = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_k,$$

where $\mathcal{H}_j$ is a Hilbert space associated to the j-th particle. We will mostly work with *bipartite* Hilbert spaces for $k = 2$. The *tensor product* $\mathcal{H}_1 \otimes \mathcal{H}_2$ can be defined as the vector space of linear maps $\mathcal{H}_1^* \to \mathcal{H}_2$, or equivalently, as the space of bilinear functions $\mathcal{H}_1^* \times \mathcal{H}_2^* \to \mathbb{K}$. We can turn $\mathcal{H}_1 \otimes \mathcal{H}_2$ into a Hilbert space by defining the inner product of product vectors by

$$\langle \psi_1 \otimes \psi_2, \chi_1 \otimes \chi_2 \rangle = \langle \psi_1, \chi_1 \rangle \langle \psi_2, \chi_2 \rangle \text{ for } \psi_1, \chi_1 \in \mathcal{H}_1,\ \psi_2, \chi_2 \in \mathcal{H}_2,$$

and extending by linearity. This is in fact the Hilbert-Schmidt inner product of operators which can be verified by using the bra-ket notation: $\psi_1 \otimes \psi_2 \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is by definition the operator

$$|\psi_1\rangle \otimes |\psi_2\rangle : \begin{array}{ccc} \mathcal{H}_1^* & \to & \mathcal{H}_2 \\ \langle \xi_1 | & \mapsto & \langle \xi_1 | \psi_1 \rangle \, |\psi_2\rangle \end{array} \text{ with adjoint } \langle \psi_1 | \otimes \langle \psi_2 | : \begin{array}{ccc} \mathcal{H}_2 & \to & \mathcal{H}_1^* \\ |\xi_2\rangle & \mapsto & \langle \psi_2 | \xi_2 \rangle \, \langle \psi_1 | \end{array},$$

where we canonically identified $(\mathcal{H}_1 \otimes \mathcal{H}_2)^*$ with $\mathcal{H}_1^* \otimes \mathcal{H}_2^*$, therefore

$$\langle \psi_1 \otimes \psi_2, \chi_1 \otimes \chi_2 \rangle_{\mathrm{HS}} = \mathrm{Tr}\left(\langle \psi_1| \otimes \langle \psi_2| \, |\chi_1\rangle \otimes |\chi_2\rangle\right) = \langle \psi_1, \chi_1\rangle \, \langle \psi_2, \chi_2\rangle.$$

As an immediate consequence we get that, if $\{\varphi_i\}$ and $\{\xi_j\}$ are orthonormal bases of $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, then $\{\varphi_i \otimes \xi_j\}$ is an orthonormal basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$. We will mostly work with concrete bipartite spaces $\mathbb{C}^m \otimes \mathbb{C}^n$ and use the standard basis $\{e_i \otimes e_j\}$ for $i = 1, \dots, m$ and $j = 1, \dots, n$. In the computational basis it is convenient to drop the tensor product sign, for example the four vectors $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ form the computational basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$.

It is also convenient to identify the space of operators $B(\mathbb{C}^m \otimes \mathbb{C}^n)$ with $mn \times mn$ matrices M_{mn}. More precisely, to each operator $A \in B(\mathbb{C}^m \otimes \mathbb{C}^n)$ we assign the $m \times m$ block matrix whose elements are $n \times n$ matrices defined as

$$M = \left[M_{ij}\right]_{i,j=1}^{m}, \text{ where each } M_{ij} = \left[\, \left\langle e_i \otimes e_k \middle| A \middle| e_j \otimes e_l \right\rangle\right]_{k,l=1}^{n}. \tag{1.2}$$

By applying canonical identifications, we can find an isomorphisms between

$$B\left(\mathcal{H}_1 \otimes \mathcal{H}_2\right) \longleftrightarrow B(\mathcal{H}_1) \otimes B(\mathcal{H}_2),$$

where the tensor products are over the same field, either $\mathbb{R}$ or $\mathbb{C}$. We will frequently use the following equalities for $A_1, A_1' \in B(\mathcal{H}_1)$ and $A_2, A_2' \in B(\mathcal{H}_2)$:

- $(A_1 \otimes A_2)(A_1' \otimes A_2') = A_1 A_1' \otimes A_2 A_2'$,
- $(A_1 \otimes A_2)(A_1^{-1} \otimes A_2^{-1}) = I_{\mathcal{H}_1} \otimes I_{\mathcal{H}_2} = I_{\mathcal{H}_1 \otimes \mathcal{H}_2}$,
- $(A_1 \otimes A_2) = (A_1 \otimes I_{\mathcal{H}_2})(I_{\mathcal{H}_1} \otimes A_2) = (I_{\mathcal{H}_1} \otimes A_2)(A_1 \otimes I_{\mathcal{H}_2})$,
- $(A_1 \otimes A_2)^* = A_1^* \otimes A_2^*$,
- $\mathrm{Tr}(A_1 \otimes A_2) = \mathrm{Tr} A_1 \cdot \mathrm{Tr} A_2$.

On the other hand, canonical identification between self-adjoint operators is possible only for complex Hilbert spaces,

$$B^{\mathrm{sa}}\left(\mathcal{H}_1 \otimes \mathcal{H}_2\right) \longleftrightarrow B^{\mathrm{sa}}(\mathcal{H}_1) \otimes B^{\mathrm{sa}}(\mathcal{H}_2), \tag{1.3}$$

where the left-hand side tensor product is over $\mathbb{C}$, whereas the right-hand side tensor product is over $\mathbb{R}$. This subtlety is demonstrated in the following exercise.

Example 1.3. Consider complex Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, and vectors $\psi_1, \chi_1 \in \mathcal{H}_1$ and $\psi_2, \chi_2 \in \mathcal{H}_2$. The operator

$$|\psi_1 \otimes \psi_2 + \chi_1 \otimes \chi_2\rangle\langle \psi_1 \otimes \psi_2 + \chi_1 \otimes \chi_2| \in B^{\mathrm{sa}}\left(\mathcal{H}_1 \otimes \mathcal{H}_2\right)$$

can be explicitly written in $B^{\mathrm{sa}}(\mathcal{H}_1) \otimes B^{\mathrm{sa}}(\mathcal{H}_2)$ as

$$\begin{aligned} &|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2| + |\chi_1\rangle\langle\chi_1| \otimes |\chi_2\rangle\langle\chi_2| \\ &\qquad + \frac{1}{4}\sum_{k=1}^{4}(-1)^k \left|\psi_1 + i^k \chi_1\middle\rangle\middle\langle \psi_1 + i^k \chi_1\right| \otimes \left|\psi_2 + i^k \chi_2\middle\rangle\middle\langle \psi_2 + i^k \chi_2\right|. \end{aligned}$$

We now introduce the Schmidt decomposition of vectors in bipartite Hilbert spaces, which is nothing but the *singular value decomposition* (SVD) for matrices translated into the language of tensors. By "translation" we mean the canonical identification

$$\begin{array}{ccc} \mathcal{H}_1^* \otimes \mathcal{H}_2 & \to & B(\mathcal{H}_1, \mathcal{H}_2) \\ u \otimes v & \mapsto & |v\rangle\langle u| \end{array} .$$

The use of complex conjugacy in the canonical identification $\mathcal{H}^* \longleftrightarrow \overline{\mathcal{H}}$ can be avoided if we work in specified bases. For fixed bases $\{\varphi_i\}$ of $\mathcal{H}_1$ and $\{\vartheta_j\}$ of $\mathcal{H}_2$ we can define a $\mathbb{C}$-linear map as follows:

$$\begin{array}{rcl} \mathrm{vec}\colon B(\mathcal{H}_1, \mathcal{H}_2) & \longrightarrow & \mathcal{H}_2 \otimes \mathcal{H}_1 \\ \left|\vartheta_j\right\rangle\!\left\langle\varphi_i\right| & \mapsto & \vartheta_j \otimes \varphi_i \end{array} \tag{1.4}$$

and extend by $\mathbb{C}$-linearity. This is the same as the linear map $\mathrm{vec}\,|\psi_2\rangle\langle\psi_1| = \psi_2 \otimes \overline{\psi_1}$ where $\psi_1 \in \mathcal{H}_1$, $\psi_2 \in \mathcal{H}_2$ and conjugacy is taken with respect to the basis $\{\varphi_i\}$ in $\mathcal{H}_1$. In particular we have

$$\mathbb{C}^m \otimes \mathbb{C}^n \longleftrightarrow \mathrm{M}_{m,n} . \tag{1.5}$$

We recall SVD: any matrix $A \in \mathrm{M}_{m,n}$ can be decomposed as $A = U\Sigma V^*$ for some unitary matrices $U \in \mathrm{U}(m)$, $V \in \mathrm{U}(n)$ and nonnegative diagonal matrix $\Sigma \in \mathrm{M}_{m,n}$ (i.e., $\Sigma_{ij} = 0$ whenever $i \neq j$ and the singular values are $\Sigma_{ii} \geq 0$). Up to permutation, the nonzero singular values of A coincide with the nonzero eigenvalues of $(AA^*)^{1/2}$ or $(A^*A)^{1/2}$. In fact, the singular value decomposition for A is constructed from the spectral theorem for the positive semi-definite AA^* or A^*A. An equivalent presentation of $A = U\Sigma V^*$ (in a unique way) is

$$A = \sum_{j=1}^{\min(m,n)} \sigma_j \left|u_j\right\rangle\!\left\langle v_j\right| ,$$

for non-increasing singular values $\sigma_j \geq 0$ and orthonormal vectors $u_j \in \mathbb{C}^m$ and $v_j \in \mathbb{C}^n$. When applied to a bipartite Hilbert space, this translates into the *Schmidt decomposition*.

Corollary 1.4. *Let ψ be a vector in a bipartite Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$. Then there exist scalars $\sigma_j \geq 0$ and orthonormal vectors $\varphi_j \in \mathcal{H}_1$ and $\vartheta_j \in \mathcal{H}_2$ for $j = 1, \ldots, \min(\dim \mathcal{H}_1, \dim \mathcal{H}_2)$, such that*

$$\psi = \sum_j \sigma_j \, \varphi_j \otimes \vartheta_j .$$

In (1.1) we explained that $B(\mathcal{H})$ and $\mathrm{M}_{m,n}$, equipped with the Hilbert-Schmidt inner product, are Hilbert spaces. Therefore, it is natural to consider linear maps between the large Hilbert spaces of operators. In quantum information theory, operators between spaces of operators have a distinct name, *superoperators*. Accordingly, we denote by $I_{\mathcal{H}}$ the identity operator on a Hilbert space $\mathcal{H}$ and by $\mathrm{Id}_{B(\mathcal{H})}$ the identity superoperator on $B(\mathcal{H})$. A superoperator is *positive* or *positivity preserving* if it maps positive operators into positive operators.

Chapter 2

The geometry of quantum states

This chapter formalizes the mathematical approach to quantum information theory. In parallel we discuss the physical perspective of the same basic concepts, that serves as a motivation for studying the geometry of the set of quantum states and the dichotomy between separability and entanglement.

2.1 Pure and mixed states

The set of quantum states on a complex Hilbert space $\mathcal{H}$ (see the definition and Remark 1.2 on pg. 4) is the set

$$\mathrm{D}(\mathcal{H}) := \{\rho \in B^{\mathrm{sa}}(\mathcal{H})\colon \rho \text{ is positive and } \operatorname{Tr}\rho = 1\},$$

which is clearly a convex set. A state $\rho \in \mathrm{D}(\mathcal{H})$ is *pure* if it has rank 1. In this case there exists a unit vector $|\psi\rangle \in \mathcal{H}$, called a *state vector*, such that

$$\rho = |\psi\rangle\langle\psi|.$$

Note that $|\psi\rangle$ is uniquely determined up to a number $\lambda \in \mathbb{C}$ with $|\lambda| = 1$. This identifies the set of pure states with the projective space $\mathrm{P}(\mathcal{H})$. It is a common abuse of notation to say "pure state $|\psi\rangle$" instead of state vector $|\psi\rangle$ representing the pure state $|\psi\rangle\langle\psi|$. As an operator, $|\psi\rangle\langle\psi|$ is the orthogonal projection onto the one-dimensional subspace of $\mathcal{H}$ spanned by $|\psi\rangle$.

It can be shown that pure states are exactly the extreme points of the convex set $\mathrm{D}(\mathcal{H})$. A point in a convex set is *extreme* if it cannot be written as convex combination of other points in the set. Krein-Milman theorem [AS17, Thm 1.3] asserts that any convex set is the convex hull of its extreme points, i.e., the extreme points determine the entire set.

Definition 2.1. We call a state in $\mathrm{D}(\mathcal{H})$ that is not pure a *mixed state*, thus every mixed state is a convex combination of pure states.

Remark 2.2. This definition is equivalent to the definition of mixed states in quantum mechanics, where a mixed state can be viewed as a quantum system that is a statistical ensamble of pure states. This means that every mixed state is of the form

$$\sum_j p_j \left|\psi_j\right\rangle\!\left\langle\psi_j\right|$$

for some state vectors $\left|\psi_j\right\rangle$ and some classical probabilities p_j that sum to 1.

In Chapter 3 we will extensively use a consequence of this fact, namely that the extremum of any convex or concave function over the set $\mathrm{D}(\mathcal{H})$ is achieved on a pure state. Moreover, the spectral theorem implies the following proposition, which significantly reduces the dimension of the problem.

Proposition 2.3. *Any state in* $\mathrm{D}(\mathcal{H})$ *is a convex combination of at most* $\dim \mathcal{H}$ *pure states of the form* $|\psi_j\rangle\langle\psi_j|$, *where* $\psi_j \in \mathcal{H}$ *are pairwise orthogonal unit vectors.*

Example 2.4. In quantum computing, a *qubit* (short for *quantum bit*) is the basic unit of quantum information. Qubits describe the simplest, two-state quantum mechanical systems (e.g., the spin of the electron or the polarization of a single photon). Unlike the classic binary bit corresponding to one of the two states of a classical system, the quantum bit is allowed to be in a coherent superposition of both states simultaneously. This means, the state vectors in $\mathcal{H} = \mathbb{C}^2$ are of the form

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

for some $\alpha, \beta \in \mathbb{C}$ constrained by the equation $|\alpha|^2 + |\beta|^2 = 1$.

2.1.1 Observables

Physicists observe a mechanical system by designing an experiment and making measurements. An experiment thus involves a system together with an apparatus that makes measurements and records the results of the measurements. The mathematical abstraction of apparatus are observables - their eigenvalues represent possible outcomes of measurements. Recall our definition of observables, elements in $B^{\mathrm{sa}}(\mathcal{H})$ corresponding to measurable entities in the quantum mechanical system, and their expectations on pg. 4. We now use the spectral theorem to relate the definitions to the actual measurement results.

Suppose observable $L \in B^{\mathrm{sa}}(\mathcal{H})$ has eigenvalues λ_j and eigenvectors φ_j, forming an orthonormal basis of $\mathcal{H}$. The corresponding spectral decomposition of L is

$$L = \sum_j \lambda_j \,|\varphi_j\rangle\langle\varphi_j|\,.$$

When measuring a system in a pure state $\psi \in \mathcal{H}$ with observable L, we get the outcome value λ_j with probability $|\langle\varphi_j|\psi\rangle|^2$. This can be seen by expanding ψ in the basis of eigenvectors of observable L,

$$|\psi\rangle = \sum_j \langle\varphi_j|\psi\rangle\,|\varphi_j\rangle\,.$$

Note that, since $\langle\psi|\psi\rangle = 1$, the probabilities add up to 1. We will interchangeably use the phrases "measure with observable L" and "measure in the basis $\{\varphi_j\}$".

Moreover, the expected value of the measurement is by definition the scalar product of λ_j with the corresponding probabilities,

$$\sum_j \lambda_j\,|\langle\varphi_j|\psi\rangle|^2 = \sum_j \langle\psi|\varphi_j\rangle\,\lambda_j\,\langle\varphi_j|\psi\rangle = \langle\psi|L|\psi\rangle = \mathrm{Tr}\,(|\psi\rangle\langle\psi|\,L) = \langle|\psi\rangle\langle\psi|\,, L\rangle_{\mathrm{HS}}.$$

This calculation extends to the expected value of the measurement of mixed states. Indeed, since any state $\rho \in \mathrm{D}(\mathcal{H})$ is a convex combination of pure states, we can by linearity compute the expected value of the measurement of a system in state ρ as

$$\langle\rho, L\rangle_{\mathrm{HS}} = \mathrm{Tr}\,\rho L.$$

This expected value is called the *expectation of observable* L and denoted by $\langle L\rangle$ or $\langle L\rangle_\rho$ (or $\langle L\rangle_\psi = \langle\psi|L|\psi\rangle$ for a pure state ψ).

Remark 2.5 (Collapse of the wave function)**.** The collapse of the wave function is commonly perceived as an important postulate in the Copenhagen interpretation of quantum mechanics. It states that during an experiment the state vector of a system jumps unpredictably to an eigenstate of the observable that was measured. In our case, the system just before the measurement is in state $|\psi\rangle$, and after the measurement with observable L, the system will be in state $\left|\varphi_j\right\rangle$ with probability $|\left\langle\varphi_j\middle|\psi\right\rangle|^2$. Because of this, experimental physics is about "measuring" observables and not the state vectors. An experiment to measure L will have an unpredictable outcome, but after the measurement is made, the system will be left in an eigenstate of L corresponding to the eigenvalue that is the outcome of the measurement. On the other hand, the collapse is considered a redundant postulate in some other interpretations of quantum mechanics, most notably in Everett's many-worlds interpretation.

We say that pure states are *distinguishable* if and only if their state vectors are orthogonal. The above link between observables and measurements in the corresponding orthonormal bases implies that states are distinguishable if there is an experiment that can tell them apart.

Example 2.6. The standard choices of the measurement bases for $\mathcal{H} = \mathbb{C}^2$ are

$$\begin{aligned} |z_+\rangle &= |0\rangle \quad &\text{and}\quad |z_-\rangle &= |1\rangle\,, \\ |x_+\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad &\text{and}\quad |x_-\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\,, \\ |y_+\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle \quad &\text{and}\quad |y_-\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle\,, \end{aligned}$$

which are referred to as up-down, right-left, in-out bases in [SF15]. They correspond to the eigenvectors of the famous observables (named after their discoverer), the *Pauli matrices*

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{2.1}$$

Remark 2.7 (POVM)**.** Observables are not the most general way to describe a measurement in quantum theory. The most general quantum measurement consists of a set of operators $\{M_j\}$ that are complete in the following way,

$$\sum_j M_j^* M_j = I.$$

The set of positive operators $\{M_j^* M_j\}$ is called a *positive operator-valued measure* (POVM).

It is easy to see why POVMs are a generalization of observables: given an observable L, its spectral decomposition yields an orthonormal basis $\{\varphi_j\}$ with the property

$$\sum_j |\varphi_j\rangle\langle\varphi_j| = I,$$

therefore $\left\{\left|\varphi_j\right\rangle\left\langle\varphi_j\right|\right\}$ is a POVM. In general, each $M_j^* M_j$ can be decomposed as a sum of pure states (with orthogonal state vectors), and each state vector corresponds to a possible measurement outcome. In Example 2.26 we will show that the famous Bell states (2.13) are a POVM.

For more on how to specify measurements with POVMs and on POVM formalism see [Wil17].

2.1.2 Unitary

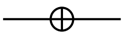
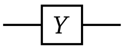
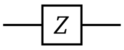
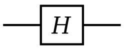
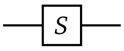
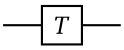
Unitary operators play a crucial role in quantum computing and quantum mechanics, representing all kinds of transformations on the set of states. In fact, unitaries are the only affine maps preserving $\mathrm{D}(\mathbb{C}^n)$.

Theorem 2.8 (Kadison's theorem, [AS17]: Thm. 2.4). *Any affine map preserving* $\mathrm{D}(\mathbb{C}^n)$ *is of the form* $\rho \mapsto U\rho U^*$ *or* $\rho \mapsto U\rho^T U^*$ *for some unitary* $U \in \mathrm{U}(n)$. *These maps are isometries with respect to the distance induced by the Hilbert-Schmidt norm on* M_n.

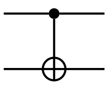
In quantum computing, unitary operators are called *quantum gates*, and they are usually written in the computational basis. Quantum gates act on states representing systems comprised of finite numbers of qubits, i.e., for $\mathcal{H} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{k\text{-times}}$ the action of $U \in \mathrm{U}(2^k)$ is

$$\begin{array}{ccc} \mathrm{D}(\mathcal{H}) & \longrightarrow & \mathrm{D}(\mathcal{H}) \\ \rho & \mapsto & U\rho U^* \end{array} \quad \text{or} \quad \begin{array}{ccc} \mathcal{H} & \longrightarrow & \mathcal{H} \\ |\psi\rangle & \mapsto & U\,|\psi\rangle \end{array},$$

by the standard abuse of notation for pure states $\rho = |\psi\rangle\langle\psi|$. A unitary operator on a single qubit is a *unary*. Some of the most famous unaries are:

Pauli-X		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$
Pauli-Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$
Pauli-Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$
Hadamard		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$
Phase		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},$
$\pi/8$		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix},$

and the most famous two-qubit unitary (i.e., acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$) is the *Controlled Not* gate

CNOT  $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$

In fact, any k-qubit quantum gate U (i.e., acting on state vectors in $\mathbb{C}^{2^k}$) can be implemented by using only the CNOT gate and unaries. Moreover, as explained in [NC10, Section 4.5], the Hadamard, phase, CNOT and $\pi/8$ gates are universal for the quantum computation in the sense that it is possible to simulate the circuit U to good accuracy using only this discrete set of gates. The Solovay-Kitaev theorem [NC10, Appendix 3] ensures that the simulation can be performed efficiently.

In the next paragraph we will briefly describe *time evolution*, arguably the most famous example of unitaries in quantum mechanics, and connect it to self-adjoint operators representing observables. For a practical introduction and more details see [SF15].

Example 2.9 (Time evolution)**.** Let us consider a closed system that at time t is in the pure quantum state $|\psi(t)\rangle$. We assume that $|\psi(t)\rangle$ is given by some operation $U(t)$ acting on the state vector $|\psi(0)\rangle$. Conventional quantum mechanics requires $U(t)$ to be linear, and moreover, that it *conserves distinctions* - recall that states $|\psi(0)\rangle$ and $|\chi(0)\rangle$ are distinguishable if and only if they are orthogonal. In other words, conservation of distinctions implies that when $\langle\psi(0)|\chi(0)\rangle = 0$, then $\langle\psi(t)|\chi(t)\rangle = 0$ for all t. If we take $|\psi(0)\rangle, |\chi(0)\rangle$ to be vectors $|j\rangle, |k\rangle$ in the computational basis, we get

$$\langle\psi(t)|\chi(t)\rangle = \langle j|U^*(t)\,U(t)|k\rangle = \delta_{jk},$$

which proves that time evolution $U(t)$ is unitary. Another natural requirement is that the state vector changes smoothly, which means that $U(t)$ is continious, therefore $U(0) = I$ and for very small ϵ, $U(\epsilon)$ differs from the identity by something of order ϵ,

$$U(\epsilon) = I - \frac{i}{\hbar}\epsilon H. \tag{2.2}$$

The factor $-\frac{i}{\hbar}$ in front of H seems arbitrary at this stage, but the Planck's constant $\hbar$ gives the equation a meaning as H will become the quantum Hamiltonian representing the energy of a system. By expanding

$$\begin{aligned} U^*(\epsilon)U(\epsilon) &= I \\ \left(I + \frac{i}{\hbar}\epsilon H^*\right)\left(I - \frac{i}{\hbar}\epsilon H\right) &= I \end{aligned}$$

in ϵ, we find $H^* = H$. This says that H is a self-adjoint operator, or a *Hermitian operator* in the physics literature, thus H is an observable with a complete set of orthonormal eigenvectors and eigenvalues. We can easily turn (2.2) into a differential equation:

$$\begin{aligned} |\psi(\epsilon)\rangle \;=\; U(\epsilon)\,|\psi(0)\rangle &= |\psi(0)\rangle - \frac{i}{\hbar}\epsilon H\,|\psi(0)\rangle \\ \frac{|\psi(\epsilon)\rangle - |\psi(0)\rangle}{\epsilon} &= -\frac{i}{\hbar}H\,|\psi(0)\rangle \\ \hbar\frac{\partial\,|\psi\rangle}{\partial t} &= -iH\,|\psi\rangle, \end{aligned} \tag{2.3}$$

the famous *time-dependent Schrödinger equation*, where the Hamiltonian operator H represents energy. More precisely, the observable values of energy are the eigenvalues of H, which we denote by E_j, and we denote the corresponding eigenvectors by $|\vartheta_j\rangle$. By definition, this yields the *time-independent Schrödinger equation*

$$H\,|\vartheta_j\rangle = E_j\,|\vartheta_j\rangle. \tag{2.4}$$

We can now solve the time-dependent Schrödinger equation (2.3) by expanding the state vector $|\psi(t)\rangle$ in the orthonormal basis of eigenvectors of H, and then solving the differential equation for an exponential function of time on each component. The solution is

$$|\psi(t)\rangle = \sum_j |\vartheta_j\rangle\langle\vartheta_j|\psi(0)\rangle\, e^{-\frac{i}{\hbar}E_j t},$$

or in the matrix form, again represented in the eigenbasis of H,

$$|\psi(t)\rangle = U(t)\,|\psi(0)\rangle = \begin{bmatrix} \ddots & & \\ & e^{-\frac{i}{\hbar}E_j t} & \\ & & \ddots \end{bmatrix} |\psi(0)\rangle\,.$$

We can now predict the probabilities for each possible outcome of an experiment as a function of time. Suppose observable L has eigenvalues λ_j and eigenvectors $\left|\varphi_j\right\rangle$. Then the probability for the outcome λ_j, when measuring the system in the state $|\psi(t)\rangle$ at time t, is $\left|\left\langle\varphi_j\middle|\psi(t)\right\rangle\right|^2$.

Remark 2.10. A naive observation is that every state is a self-adjoint operator and thus it is also an observable. Let us consider a simple example, the pure state $|0\rangle\langle 0|$, and view it as an observable $H = |0\rangle\langle 0| \in \mathrm{M}_n^{\mathrm{sa}}$. The orthonormal basis of eigenvectors of H is the computational basis $\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ with the first eigenvalue 1 and all the other eigenvalues 0. Then the corresponding time evolution

$$U(t) = \begin{bmatrix} e^{-\frac{i}{\hbar}t} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

acting on the state vector $|\psi(0)\rangle = \sum_{j=0}^{n-1} \alpha_j\,|j\rangle$ results in

$$|\psi(t)\rangle = \alpha_0 e^{-\frac{i}{\hbar}t}\,|0\rangle + \sum_{j=1}^{n-1} \alpha_j\,|j\rangle\,.$$

In particular, the system at time t is in state $|\psi(t)\rangle\langle\psi(t)|$ and the expected value of observable $H = |0\rangle\langle 0|$ is

$$\mathrm{Tr}\left(|\psi(t)\rangle\langle\psi(t)|\,|0\rangle\langle 0|\right) = \alpha_0\overline{\alpha_0},$$

which is independent of time t.

2.1.3 States vs. positive semi-definite matrices

The most central element in the set of states $\mathrm{D}(\mathcal{H})$ is the state $\frac{1}{\dim\mathcal{H}} I_{\mathcal{H}}$, called *maximally mixed state* and denoted by ρ_*. In the computational basis $\rho_* \in \mathrm{D}(\mathbb{C}^n)$ equals

$$\rho_* = \frac{1}{n}\left(|0\rangle\langle 0| + \cdots + |n-1\rangle\langle n-1|\right). \tag{2.5}$$

We will show that for $n > 2$ the set $\mathrm{D}(\mathbb{C}^n)$ is not centrally symmetric, however, the maximally mixed state ρ_* plays the role of a center in the following way.

Proposition 2.11. *Maximally mixed state ρ_* is the only state in $D(\mathbb{C}^n)$ that is fixed by all the isometries of $D(\mathbb{C}^n)$ (with respect to the Hilbert-Schmidt distance).*

Proof. From the singular value decomposition (see SVD on pg. 6) it follows that a complex matrix $M \in \mathrm{M}_n$ can be written as a linear combination of two unitary matrices. Indeed, by

SVD we may assume that M is diagonal and with $\|M\| \le 1$, thus $M = \operatorname{diag}(\sigma_1, \dots, \sigma_n)$ and $0 \le \sigma_j \le 1$. Since

$$\sigma_j = \frac{1}{2}(z_j + \overline{z_j}), \text{ where } z_j = \sigma_j + i\sqrt{1-\sigma_j^2},$$

it follows from $z_j\overline{z_j} = 1$ that M is the average of two unitary matrices.

Next, let $\rho \in D(\mathbb{C}^n)$ be a state that is fixed by all unitary matrices, $U\rho U^* = \rho$ (which are isometries by Theorem 2.8). We proved that unitary matrices span the entire M_n as a complex vector space, so ρ must commute with any matrix. Therefore $\rho = \alpha I$ for some $\alpha \in \mathbb{C}$, and from $\operatorname{Tr}\rho = 1$ we get $\alpha = \frac{1}{n}$. □

In the definition of the set of states

$$\mathrm{D}(\mathbb{C}^n) := \left\{\rho \in \mathrm{M}_n^{\mathrm{sa}} : \rho \text{ is positive semi-definite and } \operatorname{Tr}\rho = 1\right\},$$

it is often convenient to drop the trace restriction in $\mathrm{D}(\mathbb{C}^n)$ and instead consider the entire cone of positive semi-definite matrices in $\mathrm{M}_n^{\mathrm{sa}}$. A nontrivial closed convex set $\mathcal{C} \subset \mathbb{R}^n$ is called a *cone* if $\mathrm{x} \in \mathcal{C}$ and $t \ge 0$ implies $t\,\mathrm{x} \in \mathcal{C}$. The *dual cone* is defined as

$$\mathcal{C}^* := \left\{\mathrm{x} \in \mathbb{R}^n : \langle \mathrm{x}, \mathrm{y}\rangle \ge 0 \text{ for all } \mathrm{y} \in \mathcal{C}\right\}. \tag{2.6}$$

For a given point $\mathsf{e} \in \mathcal{C}^* \backslash \mathcal{C}^\perp$, the intersection of the affine hyperplane

$$H_{\mathsf{e}} = \left\{\mathrm{x} \in \mathbb{R}^n : \langle \mathrm{x}, \mathsf{e}\rangle = |\,\mathsf{e}\,|^2\right\} \tag{2.7}$$

with $\mathcal{C}$ is a nonempty closed convex set $\mathcal{C}^{\mathrm{b}} := \mathcal{C} \cap H_{\mathsf{e}}$, called a *base*. Note that e is the point in H_{e} that is the closest to the origin.

Example 2.12. We will extensively avail the following examples of cones:

- The *Positive orthant* $\mathbb{R}_+^n$, i.e., the elements of $\mathbb{R}^n$ with positive coordinates.
- The *Lorentz cone* $\mathcal{L}_n = \left\{(x_0, x_1, \dots, x_{n-1}) : x_0 \ge 0,\ \sum_{k=1}^{n-1} x_k^2 \le x_0^2\right\} \subset \mathbb{R}^n$.
- $\mathcal{PSD}(\mathbb{C}^n)$ cone of complex positive semi-definite matrices in the real vector space $\mathrm{M}_n^{\mathrm{sa}}$.

It is easy to check that the three cones are *self-dual*, i.e., they satisfy $\mathcal{C}^* = \mathcal{C}$.

Using the cone notation, we can say that $\mathrm{D}(\mathbb{C}^n)$ is the base of the positive semi-definite cone $\mathcal{PSD}(\mathbb{C}^n)$ defined in the hyperplane of trace one matrices; in short,

$$\mathcal{PSD}^{\mathrm{b}} = \mathrm{D}\,.$$

Note that the hyperplane of trace one matrices is H_{ρ_*}, with $\rho_* = \frac{1}{n}I$ being the maximally mixed state. Indeed,

$$H_{\rho_*} = \left\{X \in \mathrm{M}_n^{\mathrm{sa}} : \langle X, \rho_*\rangle_{\mathrm{HS}} = \frac{1}{n}\operatorname{Tr}X = \|\rho_*\|_{\mathrm{HS}}^2 = \frac{1}{n}\right\}.$$

On page 3 we computed that the real dimension of the cone $\mathcal{PSD}(\mathbb{C}^n) \subset \mathrm{M}_n^{\mathrm{sa}}$ is n^2, and the set of density matrices $\mathrm{D}(\mathbb{C}^n)$ is n^2-1 dimensional. Their geometry is shown on Figure 2.1.

Next we will describe the geometry of cones $\mathcal{PSD}(\mathbb{C}^n)$ and their bases $\mathrm{D}(\mathbb{C}^n)$ for $n \ge 2$.

Lemma 2.13. *Matrix $\rho \in \mathrm{M}_2^{sa}$ with trace 1 is a state if and only if $\|\rho - \rho_*\|_{HS} \le \frac{1}{\sqrt{2}}$.*

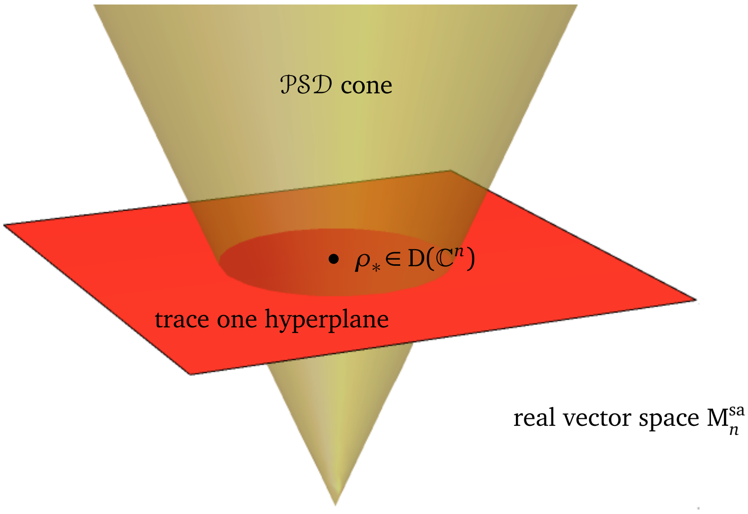

$\mathcal{PSD}$ cone
$\bullet\ \rho_* \in \mathrm{D}(\mathbb{C}^n)$
trace one hyperplane
real vector space $\mathrm{M}_n^{\mathrm{sa}}$

Figure 2.1. Cone $\mathcal{PSD}(\mathbb{C}^n)$ and its base $\mathrm{D}(\mathbb{C}^n)$.

Proof. The eigenvalues of $\rho \in \mathrm{M}_2^{\mathrm{sa}}$ with $\operatorname{Tr} \rho = 1$ are of the form $\frac{1}{2} - \lambda$ and $\frac{1}{2} + \lambda$ for some $\lambda \in \mathbb{R}$. This implies that ρ is a state if and only if $-\frac{1}{2} \le \lambda \le \frac{1}{2}$, from which we conclude

$$\|\rho - \rho_*\|_{\mathrm{HS}} = \sqrt{2}|\lambda| \le \frac{1}{\sqrt{2}}.$$

□

We have proved that, in the affine space of trace one operators in $\mathrm{M}_2^{\mathrm{sa}}$, the set of states $\mathrm{D}(\mathbb{C}^2)$ is an Euclidean ball with center ρ_* and radius $\frac{1}{\sqrt{2}}$. This ball is the *Bloch ball* and its boundary, consisting of pure states, is called the *Bloch sphere*. Classically, the Bloch ball is defined using the trace zero Pauli matrices (2.1)

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

in the following way. Since

$$\frac{1}{\sqrt{2}} I, \quad \frac{1}{\sqrt{2}} \sigma_x, \quad \frac{1}{\sqrt{2}} \sigma_y, \quad \frac{1}{\sqrt{2}} \sigma_z \tag{2.8}$$

form an orthonormal basis in $\mathrm{M}_2^{\mathrm{sa}}$ (with respect to the Hilbert-Schmidt inner product), any $\rho \in \mathrm{M}_2^{\mathrm{sa}}$ with $\operatorname{Tr} \rho = 1$ can be written as

$$\rho = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} I + a_x \cdot \frac{1}{\sqrt{2}} \sigma_x + a_y \cdot \frac{1}{\sqrt{2}} \sigma_y + a_z \cdot \frac{1}{\sqrt{2}} \sigma_z.$$

By Lemma 2.13, ρ is a state if and only if

$$\|\rho - \rho_*\|_{\mathrm{HS}}^2 = a_x^2 + a_y^2 + a_z^2 \le \frac{1}{2}.$$

On the other hand, when we consider the $\mathcal{PSD}(\mathbb{C}^2)$ cone, it is convenient to use the *spinor map* defined as

$$\mathbb{R}^4 \ni (t,x,y,z) \;\mapsto \begin{bmatrix} t+z & x-iy \\ x+iy & t-z \end{bmatrix} = X \in \mathrm{M}_2^{\mathrm{sa}}.$$

The spinor map yields an explicit isomorphism between the Lorentz cone

$$\mathcal{L}_4 = \left\{(t,x,y,z) \in \mathbb{R}^4 \colon t \geq 0 \text{ and } x^2+y^2+z^2 \leq t^2\right\}$$

and positive semi-definite matrices in $\mathrm{M}_2^{\mathrm{sa}}$. Indeed, $X = tI + x\sigma_x + y\sigma_y + z\sigma_z$ is positive semi-definite if and only if

$$\mathrm{Tr}X = 2t \geq 0 \text{ and } \det X = t^2 - x^2 - y^2 - z^2 \geq 0.$$

For $n \geq 3$ the set of states $\mathrm{D}(\mathbb{C}^n)$ is no longer a ball. However, we can compute the radius of its inscribed and circumscribed Hilbert-Schmidt balls.

Lemma 2.14. *It holds that*

$$B\left(\rho_*, \frac{1}{\sqrt{n(n-1)}}\right) \subset \mathrm{D}(\mathbb{C}^n) \subset B\left(\rho_*, \sqrt{\frac{n-1}{n}}\right),$$

where $B(\rho_*, r)$ denotes the ball with center ρ_* and radius r in the Hilbert-Schmidt norm inside the affine hyperplane $\left\{\rho \in \mathrm{M}_n^{sa} \colon \mathrm{Tr}(\rho) = 1\right\}$.

Proof. Consider $\rho \in \mathrm{M}_n^{\mathrm{sa}}$ with $\mathrm{Tr}\,\rho = 1$. The n eigenvalues of ρ can be written as

$$\frac{1}{n} + \lambda_1,\ \frac{1}{n} + \lambda_2,\ \ldots,\ \frac{1}{n} + \lambda_{n-1},\ \frac{1}{n} - \sum_{j=1}^{n-1} \lambda_j,$$

which means that ρ is positive semi-definite if and only if $\lambda_j \geq -\frac{1}{n}$ and $\sum_{j=1}^{n-1} \lambda_j \leq \frac{1}{n}$. From $\|\rho - \rho_*\|_{\mathrm{HS}}^2 = \sum_{j=1}^{n-1} \lambda_j^2 + \left(\sum_{j=1}^{n-1} \lambda_j\right)^2$ we conclude that:

- if ρ is positive semi-definite, it must hold $\|\rho - \rho_*\|_{\mathrm{HS}} \leq \sqrt{\frac{n-1}{n}}$,
- if the inequality $\|\rho - \rho_*\|_{\mathrm{HS}} \leq \frac{1}{\sqrt{n(n-1)}}$ holds, ρ must be positive semi-definite.

□

In the sequel we visualize how $\mathrm{D}(\mathbb{C}^n)$ differs from a ball for $n = 3$. In the proof of Lemma 2.14 we wrote the necessary and sufficient conditions for $\rho \in \mathrm{M}_3^{\mathrm{sa}}$ to be in $\mathrm{D}(\mathbb{C}^3)$. Concretely, $\rho \in \mathrm{M}_3^{\mathrm{sa}}$ with eigenvalues $\frac{1}{3} + \lambda_1,\ \frac{1}{3} + \lambda_2,\ \frac{1}{3} - \lambda_1 - \lambda_2$ is a state if and only if

$$(\lambda_1, \lambda_2) \in \text{ simplex } \left\{\lambda_1, \lambda_2 \geq -\frac{1}{3},\ \lambda_1 + \lambda_2 \leq \frac{1}{3}\right\},$$

which has inscribed circle with radius $\frac{1}{\sqrt{6}}$ and circumscribed circle with radius $\sqrt{\frac{2}{3}}$. Figure 2.2 shows the points $(\lambda_1, \lambda_2, z) \in \mathbb{R}^3$, where (λ_1, λ_2) are inside the simplex parametrizing $\mathrm{D}(\mathbb{C}^3)$, and

$$z(\lambda_1, \lambda_2) = \|\rho - \rho_*\|_{\mathrm{HS}}^2 = \lambda_1^2 + \lambda_2^2 + (\lambda_1 + \lambda_2)^2$$

is restricted to the interval $\frac{1}{6} \leq z \leq \frac{2}{3}$.

The 3-dimensional analogue of Pauli matrices for qutrits are the 8 *Gell-Mann matrices*:

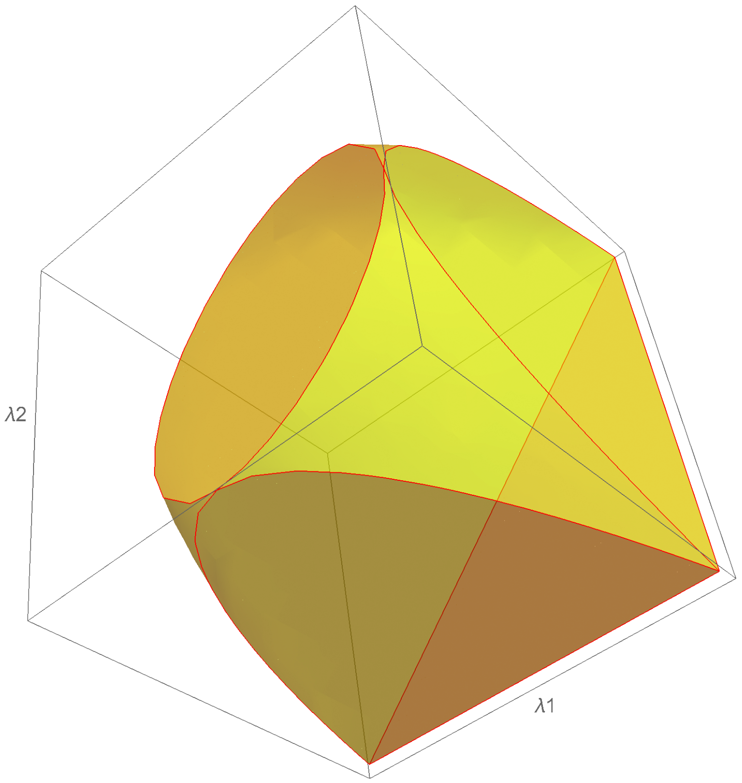


Figure 2.2. Surface $z = \|\rho - \rho_*\|_{\mathrm{HS}}$ defined on the simplex that is parametrizing $\rho \in \mathrm{D}(\mathbb{C}^3)$.

- symmetric: $\sigma_{s_{12}} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\sigma_{s_{13}} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$, $\sigma_{s_{23}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$,
- antisymmetric: $\sigma_{a_{12}} = \begin{bmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\sigma_{a_{13}} = \begin{bmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{bmatrix}$, $\sigma_{a_{23}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{bmatrix}$,
- and diagonal: $\sigma_{d_1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $\sigma_{d_2} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{bmatrix}$.

It is straightforward to check that

$$\frac{1}{\sqrt{3}}I,\ \frac{1}{\sqrt{2}}\sigma_{s_{12}},\ \frac{1}{\sqrt{2}}\sigma_{s_{13}},\ \frac{1}{\sqrt{2}}\sigma_{s_{23}},\ \frac{1}{\sqrt{2}}\sigma_{a_{12}},\ \frac{1}{\sqrt{2}}\sigma_{a_{13}},\ \frac{1}{\sqrt{2}}\sigma_{a_{23}},\ \frac{1}{\sqrt{2}}\sigma_{d_1},\ \frac{1}{\sqrt{2}}\sigma_{d_2}$$

form an orthonormal basis in $\mathrm{M}_3^{\mathrm{sa}}$ with respect to the Hilbert-Schmidt inner product. In this basis, any $\rho \in \mathrm{M}_3^{\mathrm{sa}}$ with $\mathrm{Tr}\,\rho = 1$ can be written as

$$\rho = \left(\frac{1}{\sqrt{3}},\ a_{s_{12}},\ a_{s_{13}},\ a_{s_{23}},\ a_{a_{12}},\ a_{a_{13}},\ a_{a_{23}},\ a_{d_1},\ a_{d_2}\right),$$

and $\rho - \rho_* = \left(0,\ a_{s_{12}},\ a_{s_{13}},\ a_{s_{23}},\ a_{a_{12}},\ a_{a_{13}},\ a_{a_{23}},\ a_{d_1},\ a_{d_2}\right)$ can be represented as a vector in $\mathbb{R}^8$. Moreover, by Lemma 2.14, for every state ρ it holds

$$a_{s_{12}}^2 + a_{s_{13}}^2 + a_{s_{23}}^2 + a_{a_{12}}^2 + a_{a_{13}}^2 + a_{a_{23}}^2 + a_{d_1}^2 + a_{d_2}^2 \leq \frac{2}{3}.$$

States in $\mathrm{D}(\mathbb{C}^3) \subset B\left(\rho_*, \sqrt{\frac{2}{3}}\right)$ can be thus visualised inside the Euclidean ball $B\left(0, \sqrt{\frac{2}{3}}\right) \subset \mathbb{R}^8$. Bellow we present some illustrative cases obtained as projections of $\mathrm{D}(\mathbb{C}^3)$ onto 2-dimensional subspaces of $\mathbb{R}^8$.

Case 1. A diagonal $\rho \in \mathrm{M}_3^{\mathrm{sa}}$ with $\operatorname{Tr}\rho = 1$ corresponds to $\left(0,\ 0,\ 0,\ 0,\ 0,\ 0,\ a_{d_1},\ a_{d_2}\right) \in \mathbb{R}^8$. Then

$$\rho = \rho_* + a_{d_1}\frac{1}{\sqrt{2}}\sigma_{d_1} + a_{d_2}\frac{1}{\sqrt{2}}\sigma_{d_2} = \begin{bmatrix} \frac{1}{3} + \frac{a_{d_1}}{\sqrt{2}} + \frac{a_{d_2}}{\sqrt{6}} & 0 & 0 \\ 0 & \frac{1}{3} - \frac{a_{d_1}}{\sqrt{2}} + \frac{a_{d_2}}{\sqrt{6}} & 0 \\ 0 & 0 & \frac{1}{3} - 2\frac{a_{d_2}}{\sqrt{6}} \end{bmatrix}$$

has nonnegative eigenvalues

$$\frac{1}{3} \pm \frac{a_{d_1}}{\sqrt{2}} + \frac{a_{d_2}}{\sqrt{6}} \geq 0, \text{ and } \frac{1}{3} - 2\frac{a_{d_2}}{\sqrt{6}} \geq 0,$$

which cut a triangle out of the disk $a_{d_1}^2 + a_{d_2}^2 \leq \frac{2}{3}$ as shown in Figure 2.3.

We remark that the three states corresponding to the vertices of the triangle, where $\left(a_{d_1}, a_{d_2}\right)$ are $\left(0, -\sqrt{\frac{2}{3}}\right)$, $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{6}}\right)$, $\left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{6}}\right)$ respectively, are the pure states

$$\rho_* - \frac{1}{\sqrt{3}}\sigma_{d_2} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \rho_* \pm \frac{1}{2}\sigma_{d_1} + \frac{1}{2\sqrt{3}}\sigma_{d_2} = \begin{bmatrix} \frac{1}{2} \pm \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} \mp \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

or $|2\rangle\langle 2|$, $|0\rangle\langle 0|$, $|1\rangle\langle 1|$ in the computational basis. If we act on $|0\rangle\langle 0|$ with the unitary

$$U(t) = \begin{bmatrix} \cos t & -\sin t & 0 \\ \sin t & \cos t & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

we get

$$U\,|0\rangle\,\langle 0|\,U^* = U \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} U^* = \begin{bmatrix} \cos^2 t & \sin t \cos t & 0 \\ \sin t \cos t & \sin^2 t & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Note that this pure state is not diagonal unless $t = \frac{\pi}{2}$. In other words, $U(t)$ is the time evolution of state $|0\rangle$ and $U\left(\frac{\pi}{2}\right)|0\rangle = |1\rangle$.

Case 2. A symmetric $\rho \in \mathrm{M}_3^{\mathrm{sa}}$ with $\operatorname{Tr}\rho = 1$ corresponding to $\left(a_{s_{12}},\ a_{s_{13}},\ 0,\ 0,\ 0,\ 0,\ 0,\ 0\right) \in \mathbb{R}^8$ is equal to

$$\rho = \rho_* + a_{s_{12}}\frac{1}{\sqrt{2}}\sigma_{s_{12}} + a_{s_{13}}\frac{1}{\sqrt{2}}\sigma_{s_{13}} = \begin{bmatrix} \frac{1}{3} & \frac{a_{s_{12}}}{\sqrt{2}} & \frac{a_{s_{13}}}{\sqrt{2}} \\ \frac{a_{s_{12}}}{\sqrt{2}} & \frac{1}{3} & 0 \\ \frac{a_{s_{13}}}{\sqrt{2}} & 0 & \frac{1}{3} \end{bmatrix}.$$

Its eigenvalues

$$\frac{1}{6}\left(2 \pm 3\sqrt{2a_{s_{12}}^2 + 2a_{s_{13}}^2}\right) \text{ and } \frac{1}{3}$$

are nonnegative inside the circle with radius $\frac{\sqrt{2}}{3}$ shown in Figure 2.3 (see the red disk inside the pink disk $a_{s_{12}}^2 + a_{s_{13}}^2 \leq \frac{2}{3}$ in the second image).

Case 3. Next consider a trace one $\rho \in \mathrm{M}_3^{\mathrm{sa}}$ corresponding to $\left(0,\, 0,\, 0,\, 0,\, a_{a_{13}},\, 0,\, a_{d_1},\, 0\right) \in \mathbb{R}^8$. Then

$$\rho = \rho_* + a_{d_1}\frac{1}{\sqrt{2}}\sigma_{d_1} + a_{a_{13}}\frac{1}{\sqrt{2}}\sigma_{a_{13}} = \begin{bmatrix} \frac{1}{3} + \frac{a_{d_1}}{\sqrt{2}} & 0 & -i\frac{a_{a_{13}}}{\sqrt{2}} \\ 0 & \frac{1}{3} - \frac{a_{d_1}}{\sqrt{2}} & 0 \\ i\frac{a_{a_{13}}}{\sqrt{2}} & 0 & \frac{1}{3} \end{bmatrix}$$

has eigenvalues

$$\frac{1}{6}\left(2 - 3\sqrt{2}a_{d_1}\right) \text{ and } \frac{1}{12}\left(4 + 3\sqrt{2}a_{d_1} \pm 3\sqrt{8a_{a_{13}}^2 + 2a_{d_1}^2}\right).$$

The positive eigenvalues cut a parabolic region out of the disk $a_{d_1}^2 + a_{a_{13}}^2 \leq \frac{2}{3}$, as shown in the third image in Figure 2.3.

We remark that the vertex of the parabola corresponds to $(a_{d_1}, a_{a_{13}}) = \left(-\frac{\sqrt{2}}{3}, 0\right)$ and its intersections with the vertical line have coordinates $\left(\frac{\sqrt{2}}{3}, \pm\frac{2}{3}\right)$. These three points define the states

$$\rho_* - \frac{1}{3}\sigma_{d_1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & \frac{2}{3} & 0 \\ 0 & 0 & \frac{1}{3} \end{bmatrix} \text{ and } \rho_* + \frac{1}{3}\sigma_{d_1} \pm \frac{\sqrt{2}}{3}\sigma_{a_{13}} = \begin{bmatrix} \frac{2}{3} & 0 & \mp i\frac{\sqrt{2}}{3} \\ 0 & 0 & 0 \\ \pm i\frac{\sqrt{2}}{3} & 0 & \frac{1}{3} \end{bmatrix},$$

where the first state $\frac{2}{3}\,|1\rangle\langle 1| + \frac{1}{3}\,|2\rangle\langle 2|$ is mixed with rank 2, while the next two are pure states of the form $|\varphi\rangle\langle\varphi|$ for $|\varphi\rangle = \sqrt{\frac{2}{3}}\,|0\rangle \pm \frac{i}{\sqrt{3}}\,|2\rangle$.

Case 4. Finally, consider $\rho \in \mathrm{M}_3^{\mathrm{sa}}$ with $\mathrm{Tr}\,\rho = 1$ corresponding to $\left(0,0,0,0,a_{a_{13}},0,0,a_{d_2}\right) \in \mathbb{R}^8$. Then

$$\rho = \rho_* + a_{a_{13}}\frac{1}{\sqrt{2}}\sigma_{a_{13}} + a_{d_2}\frac{1}{\sqrt{2}}\sigma_{d_2} = \begin{bmatrix} \frac{1}{3} + \frac{a_{d_2}}{\sqrt{6}} & 0 & -i\frac{a_{a_{13}}}{\sqrt{2}} \\ 0 & \frac{1}{3} + \frac{a_{d_2}}{\sqrt{6}} & 0 \\ i\frac{a_{a_{13}}}{\sqrt{2}} & 0 & \frac{1}{3} - 2\frac{a_{d_2}}{\sqrt{6}} \end{bmatrix}$$

and its eigenvalues are

$$\frac{1}{3} + \frac{1}{\sqrt{6}}a_{d_2} \text{ and } \frac{1}{12}\left(4 - \sqrt{6}a_{d_2} \pm 3\sqrt{8a_{a_{13}}^2 + 6a_{d_2}^2}\right).$$

The ellipse inside the disk $a_{d_2}^2 + a_{a_{13}}^2 \leq \frac{2}{3}$, representing the positive eigenvalues, is shown on Figure 2.3. Their intersection $\left(a_{d_2}, a_{a_{13}}\right) = \left(-\sqrt{\frac{2}{3}}, 0\right)$ corresponds to the pure state

$$\rho_* - \frac{1}{\sqrt{3}}\sigma_{d_2} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = |2\rangle\langle 2|\,.$$

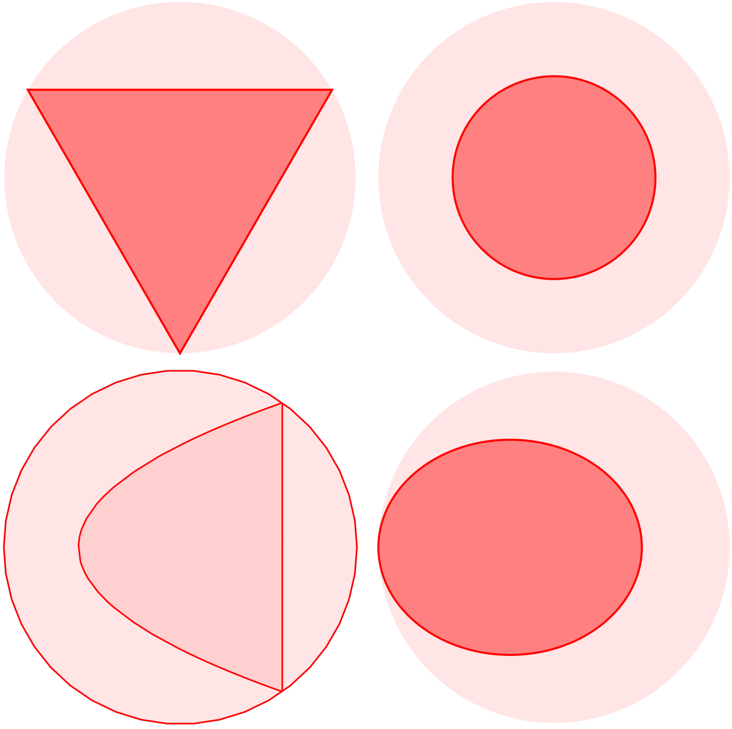


Figure 2.3. States in $B\left(0,\sqrt{\frac{2}{3}}\right) \subset \mathbb{R}^8$ projected to 2-dimensional planes a_{d_1}, a_{d_2}; $a_{s_{12}}, a_{s_{13}}$; $a_{d_1}, a_{a_{13}}$ and $a_{d_2}, a_{a_{13}}$ respectively.

2.2 Bipartite states: separability vs. entanglement

In this section we introduce a fundamental concept, the dichotomy between separability and entanglement, which is the key non-classical feature of quantum mechanics. The phenomenon of entanglement only happens in composite systems.

For a classical system consisting of multiple components, the space of states is the Cartesian product of the corresponding state spaces. If the state spaces (more precisely, the spaces of state vectors) of the components are Hilbert spaces $\mathcal{H}_1, \ldots, \mathcal{H}_k$ (e.g., particles, subsystems, ... in the quantum setting), then the state space of the composite system is the tensor product $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k$. We may assume that all the factors are at least 2-dimensional, as $\mathcal{H} \otimes \mathbb{K}$ is always identified with $\mathcal{H}$.

Definition 2.15. On a complex multipartite Hilbert space $\mathcal{H}$, a pure state $\rho = |\psi\rangle\langle\psi| \in \mathrm{D}(\mathcal{H})$ is *pure separable* if the state vector is a product vector, i.e., it can be written as $\psi = \psi_1 \otimes \cdots \otimes \psi_k$ for some unit vectors $\psi_j \in \mathcal{H}_j$. Following the canonical identification (1.3), we have

$$\rho = |\psi\rangle\langle\psi| = |\psi_1\rangle\langle\psi_1| \otimes \cdots \otimes |\psi_k\rangle\langle\psi_k|.$$

For this reason, pure separable states are often called *pure product states*.

Definition 2.16. A mixed state on $\mathcal{H}$ is *separable* if it is a convex combination of pure separable states. We denote the set of separable states by

$$\textsc{Sep}(\mathcal{H}) = \operatorname{conv}\left\{|\psi_1 \otimes \cdots \otimes \psi_k\rangle\langle\psi_1 \otimes \cdots \otimes \psi_k| : \psi_j \in \mathcal{H}_j \text{ for } j = 1,\ldots,k\right\}.$$

States that are not separable are *entangled*.

By definition, the extreme points of the convex set $\textsc{Sep}(\mathcal{H})$ are exactly the pure separable states. On the other hand, not all pure states (i.e., the extreme points of $\mathrm{D}(\mathcal{H})$) are pure separable states - or in other words - not all state vectors in $\mathcal{H}$ are product vectors. Therefore,

$$\textsc{Sep}(\mathcal{H}) \subsetneq \mathrm{D}(\mathcal{H}).$$

Alternatively, the set $\textsc{Sep}(\mathcal{H})$ can be presented as the convex hull of product states

$$\textsc{Sep}(\mathcal{H}) = \operatorname{conv}\left\{\rho_1 \otimes \cdots \otimes \rho_k : \rho_j \in \mathrm{D}(\mathcal{H}_j) \text{ for } j = 1,\ldots,k\right\}. \tag{2.9}$$

In particular this shows that in $\mathbb{R}$,

$$\dim \textsc{Sep}(\mathcal{H}) = \dim \mathrm{D}(\mathcal{H}) = (\dim \mathcal{H})^2 - 1.$$

For bipartite Hilbert spaces an even deeper result holds, namely, that the sets $\textsc{Sep}$ and D have the same inradius.

Theorem 2.17 (Gurvits-Barnum theorem, [AS17] Thm. 9.15)**.** *Let $\mathcal{H} = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, $n = d_1 d_2$ and ρ be a state on $\mathcal{H}$. If the inequality*

$$||\rho - \rho_*||_{HS} \leq \frac{1}{\sqrt{n(n-1)}}$$

holds, ρ must be separable.

In the general setting the problem whether a state is separable is NP-hard [Gha10]. This explains why there is no known simple description of the facial structure of $\textsc{Sep}$ (unlike the geometry of D which we considered in Subsection 2.1.3). The next Lemma illustrates that, despite having the same dimension and inradius, D is a larger set than $\textsc{Sep}$.

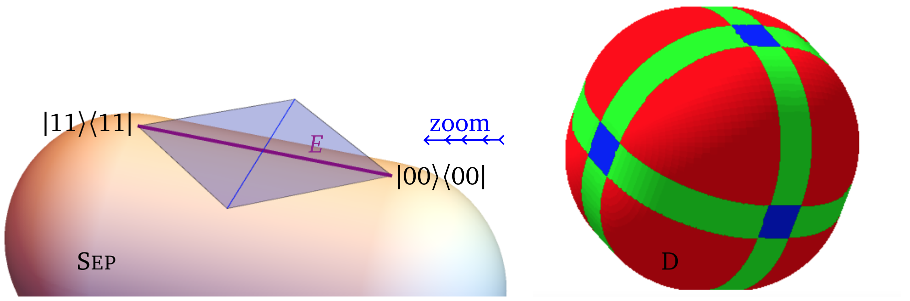


Figure 2.4. One-dimensional face of Sep.

Lemma 2.18. *The convex set $\textsc{Sep}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ has a one-dimensional face (which lies in a higher dimensional face of $\mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$).*

Proof. Consider the plane

$$\mathcal{E} = \operatorname{span}\{|00\rangle, |11\rangle\} \subset \mathbb{C}^2 \otimes \mathbb{C}^2 .$$

Note that $|00\rangle$ and $|11\rangle$ are the only product vectors in $\mathcal{E}$, so the intersection of $\textsc{Sep}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ with the hyperplane

$$\Big\{A \in B(\mathbb{C}^2 \otimes \mathbb{C}^2) : A = \sum \alpha_{ij} |ij\rangle\langle ij| ,\ \mathrm{Tr} A = 1\Big\}$$

is the 1-dimensional face

$$E = \{\alpha |00\rangle\langle 00| + (1-\alpha) |11\rangle\langle 11| : 0 \leq \alpha \leq 1\} \subset \textsc{Sep}(\mathbb{C}^2 \otimes \mathbb{C}^2)$$

shown on Figure 2.4[1]. On the other hand, E is not a 1-dimensional face in $\mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, as it lies in a 2-dimensional face of $\mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. For example, for

$$|\psi\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \text{ and } |\chi\rangle = \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle$$

the states $\{\beta |\psi\rangle\langle\psi| + (1-\beta) |\chi\rangle\langle\chi| : 0 \leq \beta \leq 1\} \subset \mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ are colored blue on the figure.

We remark that a similar proof constructs one-dimensional faces of $\textsc{Sep}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$. □

By analogy with the $\mathcal{PSD}$ cone, it is often convenient to consider the cone of separable operators

$$\mathcal{SEP}(\mathcal{H}) = \{\alpha\rho : \alpha \geq 0,\ \rho \in \textsc{Sep}(\mathcal{H})\} . \tag{2.10}$$

In some texts the cone of separable operators is defined as

$$\mathcal{SEP}(\mathbb{C}^m \otimes \mathbb{C}^n) = \operatorname{conv}\{\mathcal{PSD}(\mathbb{C}^m) \otimes \mathcal{PSD}(\mathbb{C}^n)\} , \tag{2.11}$$

which is the same as (2.9) written in the language of cones.

We now present some families of classical states on $\mathbb{C}^d \otimes \mathbb{C}^d$ that are regularly used in quantum information theory. We use the computational basis $\{|jk\rangle\}_{j,k=0,\dots,d-1}$ of $\mathbb{C}^d \otimes \mathbb{C}^d$ (recall that $\mathbb{C}^{d^2}$, M_d and $\mathbb{C}^d \otimes \mathbb{C}^d$ are isomorphic vector spaces) and avail the identifications in (1.3), (1.4) and (1.5):

$$\begin{tikzcd}
B^{\mathrm{sa}}(\mathbb{C}^d \otimes \mathbb{C}^d) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & B^{\mathrm{sa}}(\mathbb{C}^d) \otimes B^{\mathrm{sa}}(\mathbb{C}^d) \arrow[d, equal] & \\
\mathrm{M}_{d^2} & \mathrm{M}_d \otimes \mathrm{M}_d \arrow[r, leftrightarrow] & \mathrm{M}_{d^2} .
\end{tikzcd}$$

Example 2.19 (Maximally entangled states)**.** A pure state

$$|\psi\rangle\langle\psi| \in \mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d) \subset B^{\mathrm{sa}}(\mathbb{C}^d \otimes \mathbb{C}^d)$$

is *maximally entangled* if the state vector $\psi \in \mathbb{C}^d \otimes \mathbb{C}^d$ is of the form

$$\psi = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} u_j \otimes v_j \tag{2.12}$$

for some orthonormal bases $\{u_j\}$ and $\{v_j\}$ of $\mathbb{C}^d$. A unit vector ψ of such form is called a *maximally entangled vector*.

[1] The image of the Minkowski sum of a ball and a cube is from [SPJ05].

The case $d = 2$ represents bipartite systems of two qubits. The maximally entangled states, called *Bell states*, are used in the majority of quantum information protocols. Written in the computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ of $\mathbb{C}^2 \otimes \mathbb{C}^2$, the four Bell state vectors are

$$\begin{aligned} \left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle, \\ \left|\Phi^-\right\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle, \\ \left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle, \\ \left|\Psi^-\right\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle. \end{aligned} \tag{2.13}$$

Example 2.20. A simple calculation shows that Bell states are indeed entangled. Consider for example

$$\rho = \left|\Phi^+\middle\rangle\middle\langle\Phi^+\right| = \begin{bmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{bmatrix},$$

which is entangled since it is not a pure separable state. In other words, $|\Phi^+\rangle$ is not a product vector since it cannot be written as $(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$ for some $\alpha_0, \alpha_1, \beta_0, \beta_1$.

On the other hand, the mixed state

$$\rho = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11| = \begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \end{bmatrix}$$

is separable. Indeed, it is a convex (statistical) combination of pure separable states

$$\rho = \frac{1}{2}|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \otimes |1\rangle\langle 1|.$$

Example 2.21 (Isotropic states)**.** *Isotropic states* on $\mathbb{C}^d \otimes \mathbb{C}^d$ are affine combinations of the maximally mixed state (2.5) and a maximally entangled state (2.12). They are of the form

$$\rho_\beta = \beta\,|\psi\rangle\langle\psi| + (1-\beta)\frac{1}{d^2}I,$$

where ψ is a maximally entangled state vector and $-\frac{1}{d^2-1} \leq \beta \leq 1$.

Example 2.22 (Werner states)**.** We define the*flip operator* $F \in B^{\mathrm{sa}}(\mathbb{C}^d \otimes \mathbb{C}^d)$ on product vectors by $F(x \otimes y) = y \otimes x$ and extend it by linearity. For $\lambda \in [0,1]$ we define the *Werner state* as

$$\omega_\lambda = \frac{1}{d^2 - d\alpha}(I - \alpha F),$$

where $\alpha = \frac{1+d(1-2\lambda)}{1+d-2\lambda} \in [-1,1]$.

2.2.1 Mixed states

In Definition 2.1 we defined mixed quantum states as convex combinations of pure states. In this subsection we give a meaning to the definition; broadly speaking, using mixed states we will be able to predict the behaviour of parts of a multipartite system.

Assume now that we have a bipartite system $\mathcal{H} \otimes \mathcal{K}$ and that we can only access the subsystem $\mathcal{H}$. We ask the following question. When our system is in a pure state $\psi \in \mathcal{H} \otimes \mathcal{K}$, what can we tell about the $\mathcal{H}$-*marginal* of ψ, i.e., the state describing $\mathcal{H}$ whose measurements are consistent with measurements (if we were able to make them) of ψ. Recall Subsection 2.1.1 that connects observables (i.e., self-adjoint operators) with actual measurements. The eigenvectors of an observable determine the orthonormal basis in which we measure.

Suppose that the state vector $\psi = \xi \otimes \eta$ is a product vector. If we measure ξ in some basis $\{\varphi_j\}$ of $\mathcal{H}$, we obtain the j-th outcome with probability $|\langle \varphi_j, \xi \rangle|^2$. Hypothetically, if we had access to the entire system $\mathcal{H} \otimes \mathcal{K}$ we could perform a measurement in the basis $\{\varphi_j \otimes \vartheta_k\}$, where $\{\vartheta_k\}$ is some basis of $\mathcal{K}$. Then we would obtain the (j,k)-th outcome with probability

$$|\langle \varphi_j \otimes \vartheta_k, \xi \otimes \eta \rangle|^2 = |\langle \varphi_j, \xi \rangle|^2 \cdot |\langle \vartheta_k, \eta \rangle|^2.$$

Summing over k verifies that the probability of the j-th outcome on $\mathcal{H}$ is $|\langle \varphi_j, \xi \rangle|^2$.

This approach doesn't work when ψ is not a product vector. Instead, for a given $\varphi \in \mathcal{H}$, we define the operator

$$P_\varphi = |\varphi\rangle\langle\varphi| \otimes I_{\mathcal{K}} \in B^{\mathrm{sa}}(\mathcal{H} \otimes \mathcal{K}),$$

which is the orthogonal projection onto the subspace $\{\varphi\} \otimes \mathcal{K} \subset \mathcal{H} \otimes \mathcal{K}$. Observe that for $\psi = \xi \otimes \eta$ it holds

$$|\langle \varphi_j, \xi \rangle|^2 = \mathrm{Tr}\Big(|\psi\rangle\langle\psi| P_{\varphi_j}\Big),$$

which is independent of the basis of $\mathcal{K}$ and is well defined also if ψ is not a product vector. Next we take the Schmidt decomposition of $\psi \in \mathcal{H} \otimes \mathcal{K}$ defined in Corollary 1.4,

$$\psi = \sum_{i=1}^{r} a_i \, \xi_i \otimes \eta_i,$$

where, assuming that ψ is not a product vector, the Schmidt rank $r \geq 2$. Then we can express the marginal probability of j-th outcome as

$$\begin{aligned}
\mathrm{Tr}\Big(|\psi\rangle\langle\psi| P_{\varphi_j}\Big) &= \mathrm{Tr}\left(\left(\sum_{i,l=1}^{r} a_i \overline{a}_l \, |\xi_i\rangle\langle\xi_l| \otimes |\eta_i\rangle\langle\eta_l|\right)\Big(\big|\varphi_j\big\rangle\big\langle\varphi_j\big| \otimes I_{\mathcal{K}}\Big)\right) \\
&= \sum_{i,l=1}^{r} a_i \overline{a}_l \, \mathrm{Tr}\Big((|\xi_i\rangle\langle\xi_l|)\big(\big|\varphi_j\big\rangle\big\langle\varphi_j\big|\big)\Big) \, \mathrm{Tr}\left(|\eta_i\rangle\langle\eta_l|\right) \\
&= \mathrm{Tr}\left(\left(\sum_{i=1}^{r} |a_i|^2 \, |\xi_i\rangle\langle\xi_i|\right)\big|\varphi_j\big\rangle\big\langle\varphi_j\big|\right) \\
&= \Big\langle\varphi_j\Big| \sum_{i=1}^{r} |a_i|^2 \, |\xi_i\rangle\langle\xi_i| \, \Big|\varphi_j\Big\rangle.
\end{aligned}$$

This lengthy calculation says that the probability of j-th outcome, when measurement is performed in a basis $\{\varphi_j\}$ of $\mathcal{H}$, is $\big\langle\varphi_j\big| \rho_{\mathcal{H}} \big|\varphi_j\big\rangle = \mathrm{Tr}\big(\rho_{\mathcal{H}} \big|\varphi_j\big\rangle\big\langle\varphi_j\big|\big)$, where

$$\rho_{\mathcal{H}} = \sum_{i=1}^{r} |a_i|^2 \, |\xi_i\rangle\langle\xi_i|. \tag{2.14}$$

In other words, given a pure state $\rho = |\psi\rangle\langle\psi|$ on $\mathcal{H} \otimes \mathcal{K}$, its $\mathcal{H}$-marginal is the mixed state $\rho_{\mathcal{H}}$. The "strength" of $\rho_{\mathcal{H}}$ is that

- it does not depend on the basis of $\mathcal{H}$ in which we measure, and
- it contains all the information that can be obtained about the global state ρ on $\mathcal{H} \otimes \mathcal{K}$ while being restricted to the measurements inside $\mathcal{H}$.

Remark 2.23. Note that for $\psi \in \mathcal{H} \otimes \mathcal{K}$ and complex numbers ω_i with $|\omega_i| = 1$,

$$\psi = \sum_{i=1}^{r} a_i\, \xi_i \otimes \eta_i \text{ and } \psi = \sum_{i=1}^{r} a_i \omega_i\, \xi_i \otimes \eta_i$$

are two different decompositions of ψ that yield the same $\mathcal{H}$-marginal $\rho_{\mathcal{H}} = \sum_{i=1}^{r} |a_i|^2\, |\xi_i\rangle\langle\xi_i|$. Therefore, in the Schmidt decomposition in Corollary 1.4, we do not need to fulfil the requirement that all the coefficients are nonnegative. In practice, in quantum computing, ψ is decomposed in the computational bases of $\mathcal{H}$ and $\mathcal{K}$.

Remark 2.24. On the other hand, in a quantum superposition of pure states

$$\sum_j \alpha_j \psi_j,$$

represented by some unit vectors $\psi_j \in \mathcal{H}$, the probability amplitudes $\alpha_j \in \mathbb{C}$ (such that $\sum_j \alpha_j \overline{\alpha_j} = 1$) encode more information than just the probabilities of the measurement outcomes. For example, quantum interference in the two-slit experiment happens because of the relative phase of α and β in a single qubit $\alpha\,|0\rangle + \beta\,|1\rangle$ considered in Example 2.4.

In reality we can never perform measurement in a global basis of the entire multipartite system. And, even though the state of a quantum system is described by a vector (i.e., a state vector representing a pure state or a wave function, or equivalently a rank one projection), we showed that we can only model such a system by using mixed states.

Example 2.25. Suppose $\rho = |\psi\rangle\langle\psi|$ is a pure state on $\mathbb{C}^2 \otimes \mathbb{C}^2$ where ψ is one of the four Bell vectors defined in Example 2.19. In each of the four cases, the $\mathbb{C}^2$-marginal on either factor is

$$\rho_{\mathbb{C}^2} = \frac{1}{2}\,|0\rangle\langle 0| + \frac{1}{2}\,|1\rangle\langle 1| = \frac{1}{2} I = \rho_*.$$

This can be interpreted in the following way. Assume we measure in a basis $\{u_1, u_2\}$ of the first $\mathbb{C}^2$ factor. Then each of the two outcomes occurs with the probability $\frac{1}{2}$. Additionally, these measurements can not distinguish between the four Bell states, even though a global measurement of ρ in the basis of the Bell vectors would distinguish them perfectly.

We conclude this subsection with an example that illustrates how mixed states are able to behave classically in some respects, but quantum mechanically in others.

Example 2.26. Consider the statistical combination of Bell states,

$$\rho = \frac{1}{4}\left|\Phi^+\middle\rangle\middle\langle\Phi^+\right| + \frac{1}{4}\left|\Phi^-\middle\rangle\middle\langle\Phi^-\right| + \frac{1}{4}\left|\Psi^+\middle\rangle\middle\langle\Psi^+\right| + \frac{1}{4}\left|\Psi^-\middle\rangle\middle\langle\Psi^-\right|.$$

After expanding ρ in the computational basis we get $\rho = \frac{1}{4} I = \rho_*$, the maximally mixed state in $\mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$.

2.2.2 Partial trace

In the previous subsection we learned that operators representing mixed states (rather than state vectors) are a natural way of modeling quantum systems, in particular when modeling a subsystem of a quantum system.

On a bipartite Hilbert space $\mathcal{H} \otimes \mathcal{K}$, the $\mathcal{H}$-marginals can be elegantly expressed by *partial trace*, which is defined as

$$\mathrm{Tr}_{\mathcal{K}} = \mathrm{Id}_{B(\mathcal{H})} \otimes \mathrm{Tr} \colon B(\mathcal{H}) \otimes B(\mathcal{K}) \to B(\mathcal{H}).$$

This means that

$$\mathrm{Tr}_{\mathcal{K}}(\sigma \otimes \tau) = \mathrm{Tr}(\tau)\,\sigma$$

for $\sigma \in B(\mathcal{H})$ and $\tau \in B(\mathcal{K})$, and the map extends by linearity on the entire $B(\mathcal{H}) \otimes B(\mathcal{K})$.

We now show that the partial trace of $\rho = |\psi\rangle\langle\psi| \in B(\mathcal{H} \otimes \mathcal{K}) \equiv B(\mathcal{H}) \otimes B(\mathcal{K})$ with respect to $\mathcal{K}$ is exactly the $\mathcal{H}$-marginal $\rho_{\mathcal{H}}$ obtained in (2.14) in Subsection 2.2.1. Indeed, if $\psi = \xi \otimes \eta \in \mathcal{H} \otimes \mathcal{K}$ is a product vector, then

$$\mathrm{Tr}_{\mathcal{K}}\left(|\xi \otimes \eta\rangle\langle\xi \otimes \eta|\right) = \mathrm{Tr}_{\mathcal{K}}\left(|\xi\rangle\langle\xi| \otimes |\eta\rangle\langle\eta|\right) = |\xi\rangle\langle\xi|,$$

and if $\psi = \sum_{i=1}^{r} a_i\, \xi_i \otimes \eta_i$ is a Schmidt decomposition, then

$$\mathrm{Tr}_{\mathcal{K}}\left(|\psi\rangle\langle\psi|\right) = \sum_{i=1}^{r} |a_i|^2\, |\xi_i\rangle\langle\xi_i| = \rho_{\mathcal{H}}. \tag{2.15}$$

Example 2.27. The identification (1.5) between tensor products of vectors and matrices, i.e., $\psi \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is identified with $M \in \mathrm{M}_{d_1,d_2}$, yields the following equality,

$$\mathrm{Tr}_{\mathbb{C}^{d_2}} |\psi\rangle\langle\psi| = MM^*.$$

The next Lemma shows that $\mathcal{H}$-marginals of pure states on $\mathcal{H} \otimes \mathcal{K}$ yield the entire set of quantum states $D(\mathcal{H})$, as long as $\dim \mathcal{K} \geq \dim \mathcal{H}$.

Lemma 2.28 (Purification). *On a bipartite system $\mathcal{H} \otimes \mathcal{K}$ with $\dim \mathcal{K} \geq \dim \mathcal{H}$, the set of quantum states on $\mathcal{H}$ (i.e., $\mathrm{D}(\mathcal{H})$) can be obtained as $\mathcal{H}$-marginals of pure states.*

Proof. For $\rho \in \mathrm{D}(\mathcal{H}) \subset B^{\mathrm{sa}}(\mathcal{H})$ with spectral decomposition $\rho = \sum_{i=1}^{r} \lambda_i\, |\xi_i\rangle\langle\xi_i|$, we choose an orthonormal basis $\{\eta_i\}$ of $\mathcal{K}$ and define

$$\psi = \sum_{i=1}^{r} \sqrt{\lambda_i}\xi_i \otimes \eta_i \in \mathcal{H} \otimes \mathcal{K}.$$

Then $\mathrm{Tr}_{\mathcal{K}}\left(|\psi\rangle\langle\psi|\right) = \rho$. We call $|\psi\rangle\langle\psi|$ (or simply ψ) a *purification* of ρ. □

2.3 PPT states: First attempts at detecting entanglement

As explained in Section 2.2, in the general setting, the problem whether a state is separable is NP-hard. The aim of this section is to construct a map (a superoperator, acting between spaces of operators, as defined in the last paragraph of Section 1.2) that will be able to detect some entangled states.

In Section 1.2 we introduced canonical notions like duality, adjoint, trace, inner product, etc., that are independent on the choice of a basis in the Hilbert space $\mathcal{H}$. On the other hand, transposition in linear algebra is usually defined with respect to the standard basis and is not canonical. Now we give a definition of *transposition* with respect to an orthonormal basis $\{\varphi_j\}$ of $\mathcal{H}$. Once the basis is fixed, we can identify the set of operators with the set of matrices

$$\begin{array}{ccc} B(\mathcal{H}) & \longleftrightarrow & \mathrm{M}_n \\ \sum_{i,j=1}^{n} a_{ij} \left|\varphi_i\middle\rangle\!\middle\langle\varphi_j\right| & \longleftrightarrow & [a_{ij}] \end{array} ,$$

and define the transposition as

$$\begin{array}{cccc} T: & B(\mathcal{H}) & \longrightarrow & B(\mathcal{H}) \\ & \sum_{i,j} a_{ij} \left|\varphi_i\middle\rangle\!\middle\langle\varphi_j\right| & \mapsto & \sum_{i,j} a_{ij} \left|\varphi_j\middle\rangle\!\middle\langle\varphi_i\right| \end{array} ,$$

which equals $T([a_{ij}]) = [a_{ji}]$ in the matrix representation. Sometimes we will write $A^T = T(A)$. This allows us to define the partial transposition on bipartite systems as follows.

Definition 2.29. Let $\mathcal{H} \otimes \mathcal{K}$ be a bipartite Hilbert space. Denote by T the transposition on $B(\mathcal{H})$ with respect to a specified basis. The *partial transposition* (or *partial transpose*) with respect to the first factor $\mathcal{H}$ is

$$\Gamma := T \otimes \mathrm{Id}_{B(\mathcal{K})} : B(\mathcal{H} \otimes \mathcal{K}) \longrightarrow B(\mathcal{H} \otimes \mathcal{K}) \ .$$

The partial transposition with respect to the second factor is defined by switching the roles of $\mathcal{H}$ and $\mathcal{K}$. The partial transposition of a state $\rho \in \mathrm{D}(\mathcal{H} \otimes \mathcal{K})$ with respect to the first factor will be denoted by $\rho^\Gamma = \Gamma(\rho)$.

A convenient way to compute the partial transposition is by using the block matrix representation (1.2). If $\rho \in \mathrm{D}(\mathcal{H} \otimes \mathcal{K})$ is represented by a block operator $\left[M_{ij}\right]_{i,j=1}^{\dim \mathcal{H}}$, where each $M_{ij} \in B(\mathcal{K})$, then ρ^Γ corresponds to the block operator $\left[M_{ji}\right]_{i,j=1}^{\dim \mathcal{H}}$. Analogously, the partial transposition of ρ with respect to the second factor is represented by $\left[M_{ij}^T\right]_{i,j=1}^{\dim \mathcal{H}}$

Example 2.30. For the Bell state $\rho = |\Phi^+\rangle\langle\Phi^+|$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ we have

$$\rho = \frac{1}{2}\left[\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right] \quad \text{and} \quad \rho^\Gamma = \frac{1}{2}\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] .$$

Another way to represent the partial transposition is to write Γ as a reflection over a subspace in $B^{\mathrm{sa}}(\mathcal{H} \otimes \mathcal{K})$: since $\Gamma^2 = \mathrm{Id}$, we can write $\Gamma = 2P_E - \mathrm{Id}$, where P_E is the projection onto the subspace

$$E = \left\{A \in B^{\mathrm{sa}}(\mathcal{H} \otimes \mathcal{K}) : A^\Gamma = A\right\} .$$

The following proposition shows that, even though the partial transposition depends on the choice of a basis, the eigenvalues of a partially transposed operator are the same regardless of the basis with respect to which the state is transposed.

Proposition 2.31. *The eigenvalues of the partial transposition of an operator in $B(\mathcal{H} \otimes \mathcal{K})$ do not depend on on a choice of basis.*

Proof. Denote by T and T' the transpositions with respect to the orthonormal bases $\{\varphi_j\}$ and $\{\varphi'_j\}$ of $\mathcal{H}$. Let U be the unitary transformation on $\mathcal{H}$ such that $U(\varphi_j) = \varphi'_j$. We will prove that for $X \in B(\mathcal{H})$ it holds

$$T(X) = (UT(U))^* \, T'(X) \, UT(U), \tag{2.16}$$

which shows that the partial transpositions $\Gamma = T \otimes \mathrm{Id}_{B(\mathcal{K})}$ and $\Gamma' = T' \otimes \mathrm{Id}_{B(\mathcal{K})}$ are conjugates of each other via the unitary transformation $(UT(U)) \otimes I_{\mathcal{K}}$; and since eigenvalues are preserved under unitary conjugation this will conclude the proof. By linearity it is enough to verify (2.16) for $X = \left|\varphi'_i\middle\rangle\middle\langle\varphi'_j\right|$. Then $T'(X) = \left|\varphi'_j\middle\rangle\middle\langle\varphi'_i\right|$, and since $X = \left|U\varphi_i\middle\rangle\middle\langle U\varphi_j\right| = U\left|\varphi_i\middle\rangle\middle\langle\varphi_j\right|U^*$, we have

$$T(X) = T(U^*)\left|\varphi_j\middle\rangle\middle\langle\varphi_i\right|T(U) = T(U^*)U^*\left|\varphi'_j\middle\rangle\middle\langle\varphi'_i\right|UT(U) = T(U)^*U^*\left|\varphi'_j\middle\rangle\middle\langle\varphi'_i\right|UT(U),$$

as claimed. □

It is important to note that the partial transposition (unlike transposition) does not necessarily preserve the spectrum, as we demonstrate in the next example.

Example 2.32 (Eigenvalues of the partial transpose of a pure state.)**.** For a given state vector $\psi \in \mathcal{H} \otimes \mathcal{K}$, let $\psi = \sum_j \sigma_j \, \varphi_j \otimes \vartheta_j$ be its Schmidt decomposition from Corollary 1.4. Then, $|\psi\rangle\langle\psi|$ is the projection onto ψ with the only nonzero eigenvalue 1 and its corresponding eigenvector ψ. In the basis $\{\varphi_i \otimes \vartheta_j\}$ of $\mathcal{H} \otimes \mathcal{K}$ we can write

$$|\psi\rangle\langle\psi| = \sum_{i,j} \sigma_i \sigma_j \left|\varphi_i \otimes \vartheta_i\middle\rangle\middle\langle\varphi_j \otimes \vartheta_j\right| = \sum_{i,j} \sigma_i \sigma_j \left|\varphi_i\middle\rangle\middle\langle\varphi_j\right| \otimes \left|\vartheta_i\middle\rangle\middle\langle\vartheta_j\right|.$$

Then,

$$|\psi\rangle\langle\psi|^\Gamma = \sum_{i,j} \sigma_i \sigma_j \left|\varphi_j\middle\rangle\middle\langle\varphi_i\right| \otimes \left|\vartheta_i\middle\rangle\middle\langle\vartheta_j\right| = \sum_{i,j} \sigma_i \sigma_j \left|\varphi_j \otimes \vartheta_i\middle\rangle\middle\langle\varphi_i \otimes \vartheta_j\right|$$

has the following spectrum:

- eigenvalues σ_i^2 with eigenvectors $\varphi_i \otimes \vartheta_i$,
- eigenvalues $\sigma_i \sigma_j$ with eigenvectors $\varphi_i \otimes \vartheta_j + \varphi_j \otimes \vartheta_i$,
- eigenvalues $-\sigma_i \sigma_j$ with eigenvectors $\varphi_i \otimes \vartheta_j - \varphi_j \otimes \vartheta_i$.

A state whose partial transpose has nonnegative eigenvalues deserves a special name, it is called a state with positive partial transpose (or simply a PPT state).

Definition 2.33. We say that a state $\rho \in \mathrm{D}(\mathcal{H} \otimes \mathcal{K})$ has a *positive partial transpose* if the operator $\rho^\Gamma \in B^{\mathrm{sa}}(\mathcal{H} \otimes \mathcal{K})$ is positive. We denote by $\mathrm{PPT}(\mathcal{H} \otimes \mathcal{K})$, or shortly PPT, the convex set of PPT states.

Proposition 2.31 implies that PPT states are well defined since the spectrum is independent on the choice of a basis. Moreover, it is not necessary to specify whether we apply the partial transpose on the first or the second factor. Indeed, switching the roles of $\mathcal{H}$ and $\mathcal{K}$ is the same as applying the full transposition, which preserves the spectrum.

Since the partial transposition preserves the trace, we observe that ρ is a PPT state if and only if ρ^Γ is a state. In other words, the set of PPT states is the intersection

$$\mathrm{PPT} = \mathrm{D} \cap \Gamma(\mathrm{D}).$$

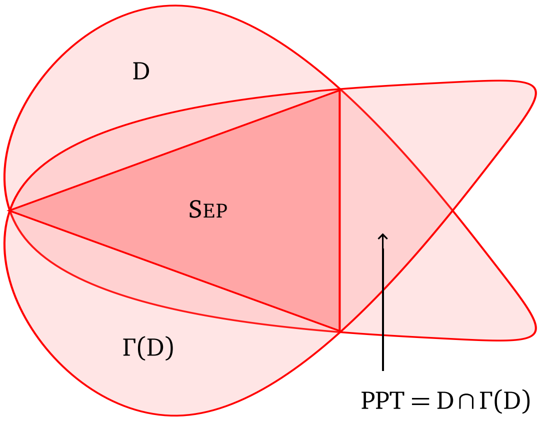


Figure 2.5. For $\dim\mathcal{H}\dim\mathcal{K} > 6$ the inclusion $\mathrm{Sep} \subset \mathrm{PPT} = \mathrm{D} \cap \Gamma(\mathrm{D})$ is strict.

The partial transposition is a linear map that preserves the Hilbert-Schmidt norm, therefore $\Gamma\colon \mathrm{D} \to \Gamma(\mathrm{D})$ is an isometry as illustrated on Figure 2.5. Note that, even though Γ depends on the chosen basis and is thus not a canonical map, the intersection $\mathrm{PPT} = \mathrm{D} \cap \Gamma(\mathrm{D})$ is basis-independent.

PPT states have attracted much attention in the literature because, as we will deduce from the PPT criterion, they can be seen as rough approximations to separable states.

Proposition 2.34 (PPT criterion (or Peres-Horodecki criterion due to [HHH96] and [Per96])**.** *The following inclusion holds*

$$\mathrm{Sep}(\mathcal{H}\otimes\mathcal{K}) \subset \mathrm{PPT}(\mathcal{H}\otimes\mathcal{K}).$$

In other words, if $\rho \in \mathrm{D}(\mathcal{H}\otimes\mathcal{K})$ is a separable state, then ρ is a PPT state.

Proof. The sets $\mathrm{Sep}(\mathcal{H}\otimes\mathcal{K})$ and $\mathrm{PPT}(\mathcal{H}\otimes\mathcal{K})$ are both convex, therefore it suffices to show that the extreme points of Sep (i.e., pure separable states by Definition 2.15 and Definition 2.16) are PPT. Pure separable states are pure product states of the form

$$\rho = |\xi\otimes\eta\rangle\langle\xi\otimes\eta| = |\xi\rangle\langle\xi| \otimes |\eta\rangle\langle\eta|$$

for some unit vectors $\xi \in \mathcal{H}, \eta \in \mathcal{K}$. The partial transpose is then

$$\rho^\Gamma = |\xi\rangle\langle\xi|^\Gamma \otimes |\eta\rangle\langle\eta| = \left|\overline{\xi}\right\rangle\left\langle\overline{\xi}\right| \otimes |\eta\rangle\langle\eta| = \left|\overline{\xi}\otimes\eta\right\rangle\left\langle\overline{\xi}\otimes\eta\right|,$$

where $\overline{\xi}$ is the coordinate-wise complex conjugate of ξ. This shows that ρ^Γ is positive and hence ρ has PPT. □

The strength of the Peres-Horodecki criterion is in detecting entanglement: if the partial transpose of a state is not positive, the state itself must be non-separable, i.e., entangled.

Example 2.35. The pure Bell state $|\Phi^+\rangle\langle\Phi^+|$ from Example 2.30 is entangled since $|\Phi^+\rangle\langle\Phi^+|^\Gamma$ has eigenvalues ± 1 (this can be verified by calculating the spectrum directly or by using Example 2.32) and is thus not positive semidefinite.

However, the PPT criterion is (in general, as shown on Figure 2.5) only a necessary condition for separability. In small dimensions the next lemma and theorem show when the PPT criterion is also a sufficient condition for separability.

Lemma 2.36. *A pure state has a positive partial transpose if and only if it is separable.*

Proof. In Example 2.32 we computed the eigenvalues of the partial transpose of a pure state $\Psi \in \mathcal{H} \otimes \mathcal{K}$: $|\psi\rangle\langle\psi|^\Gamma$ has a negative eigenvalue $\iff$ the Schmidt decomposition of ψ has at least two nonzero Schmidt coefficients $\iff$ Ψ is entangled.

It follows that $|\psi\rangle\langle\psi|$ is a PPT state if and only if ψ has exactly one nonzero Schmidt coefficient, which means that ψ is a product vector and therefore $|\psi\rangle\langle\psi|$ is separable. □

Theorem 2.37 (Størmer-Woronowitz theorem, [AS17]:Thm 2.15)**.** *On the Hilbert spaces*

$$\mathbb{C}^2 \otimes \mathbb{C}^2, \textit{ and } \mathbb{C}^2 \otimes \mathbb{C}^3,\ \mathbb{C}^3 \otimes \mathbb{C}^2,$$

representing bipartite systems of qubits and qutrits, every PPT state is separable. In other words, $\textsc{Sep}\left(\mathbb{C}^2 \otimes \mathbb{C}^2\right) = \mathrm{PPT}\left(\mathbb{C}^2 \otimes \mathbb{C}^2\right)$ *and* $\textsc{Sep}\left(\mathbb{C}^2 \otimes \mathbb{C}^3\right) = \mathrm{PPT}\left(\mathbb{C}^2 \otimes \mathbb{C}^3\right)$.

It was observed by the Horodecki group [HHH96] that the $2 \otimes 2$ case of Theorem 2.37 follows from the work of Størmer [Stø63], and the $2 \otimes 3$ case follows from the results by Woronowitz [Wor76]. For a new proof in the language of quantum information theory see [AS17, Theorem 2.36]. In fact, $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$ are the only bipartite spaces for which the inclusion $\textsc{Sep} \subset \mathrm{PPT} = \mathrm{D} \cap \Gamma(\mathrm{D})$ is not strict.

PPT states were introduced by Peres [Per96], a physicist and pioneer in quantum information theory. Within a short period of time P. Horodecki [Hor97], another physicist working in the field of quantum information theory, published an example of a PPT state in $\mathrm{D}\left(\mathbb{C}^3 \otimes \mathbb{C}^3\right)$ which is not separable. Actually, analogous examples had been constructed much earlier by mathematicians studying C^*-algebras (see Remark 1.2) and matrix algebras: examples of [Stø82], [TT88], [Osa91], [KK94] are all generalizations of the famous Choi map [Cho75b], which is an indecomposable map in the least possible dimension, 3×3 matrices (check forward Section 3.2 and Example 3.47). These examples translated to the language of states correspond to non-separable PPT states in $\mathrm{D}\left(\mathbb{C}^3 \otimes \mathbb{C}^3\right)$. Examples of entangled PPT states are known in $\mathrm{D}\left(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}\right)$ for all dimensions $d_1 \geq 3, d_2 \geq 3$. A modern discussion of PPT states can be found in [BŻ17].

Remark 2.38. Besides pure states and states on $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$, the Werner states in Example 2.22 are another family of states for which separability and PPT property are equivalent. A proof can be found in [AS17, Proposition 2.16], where it is shown that a Werner state $\omega_\lambda \in \mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is separable $\iff$ ω_λ is PPT $\iff$ $\lambda \geq \frac{1}{2}$.

Example 2.39. Using the above classification of separable Werner states, we will show that an isotropic state (defined in Example 2.21)

$$\rho_\beta = \beta\, |\psi\rangle\langle\psi| + (1-\beta)\frac{1}{d^2} I \in \mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d),$$

where $\psi = \frac{1}{\sqrt{d}} \sum_{j=1}^d u_j \otimes v_j$, is separable if and only if $\beta \le \frac{1}{d+1}$. From Example 2.32 (in which we computed the eigenvalues of the partial transposition of a pure state) we conclude that ρ_β^Γ has eigenvalues $\pm\frac{\beta}{d} + \frac{1-\beta}{d^2}$. Therefore, ρ_β has PPT if and only if $\beta \le \frac{1}{d+1}$, which implies that ρ_β is entangled for $\beta > \frac{1}{d+1}$. Next observe that

$$\rho_\beta^\Gamma = \frac{\beta}{d} F + (1-\beta)\frac{1}{d^2} I,$$

(where F is the flip operator in Example 2.22) and that $\rho_\beta = \omega_\lambda^\Gamma$ for $\lambda = (\beta(d^2-1)+d+1)/2d$. Our claim then follows since ω_λ is separable for $\lambda \ge \frac{1}{2}$.

We conclude the section with another superoperator that is able to detect entanglement.

Definition 2.40. The *realignment* of an operator in $B\left(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}\right)$ is the map

$$\begin{array}{rcccl} R\colon & B\left(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}\right) & \longrightarrow & B\left(\mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}, \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_1}\right) & \\ & |ij\rangle\langle kl| & \mapsto & |ik\rangle\langle jl|\,, & \left(\text{for } |i\rangle, |k\rangle \in \mathbb{C}^{d_1},\ |j\rangle, |l\rangle \in \mathbb{C}^{d_2}\right), \\ & \| & & \| & \\ & |i\rangle\langle k| \otimes |j\rangle\langle l| & & |i\rangle\langle j| \otimes |k\rangle\langle l| & \end{array}$$

defined on the computational basis and extended by linearity.

Proposition 2.41 (The realignment criterion)**.** *The trace norm of an operator is defined as* $\|M\|_1 = \operatorname{Tr}|M|$*, where* $|M| = (M^*M)^{1/2}$*.*
(i) A separable state $\rho \in \mathrm{D}\left(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}\right)$ *has* $\|\rho^R\|_1 \le 1$.
(ii) A pure entangled state $\rho \in \mathrm{D}\left(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}\right)$ *has* $\|\rho^R\|_1 > 1$.

Proof. (i) For unit vectors $\xi \in \mathbb{C}^{d_1}, \eta \in \mathbb{C}^{d_2}$ we have

$$|\xi \otimes \eta\rangle\langle\xi \otimes \eta|^R = \left|\xi \otimes \overline{\xi}\right\rangle\!\left\langle\overline{\eta} \otimes \eta\right|.$$

Then $\|\, |\xi \otimes \eta\rangle\langle\xi \otimes \eta|^R \,\|_1 = 1$, and from the triangle inequality for $\|\cdot\|_1$ it follows that any separable state (which is a convex combination of pure product states) has $\|\rho^R\|_1 \le 1$.

(ii) Consider a pure state $\rho = |\psi\rangle\langle\psi|$, where $\psi \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ and $\psi = \sum_j \sigma_j\, \varphi_j \otimes \vartheta_j$ is its Schmidt decomposition from Corollary 1.4. Then,

$$\rho^R = \sum_{i,j} \sigma_i \sigma_j \left|\varphi_i \otimes \overline{\varphi_j}\right\rangle\!\left\langle\overline{\vartheta_i} \otimes \vartheta_j\right|.$$

The sets $\left\{\varphi_i \otimes \overline{\varphi_j}\right\}$ and $\left\{\overline{\vartheta_i} \otimes \vartheta_j\right\}$ are orthonormal in $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$ respectively, therefore $\|\rho^R\|_1 = \sum_{i,j} \sigma_i \sigma_j = \left(\sum_i \sigma_i\right)^2$. Then $1 = \langle\psi|\psi\rangle = \sum_i \sigma_i^2$ implies that $\|\rho^R\|_1 > 1$ unless ρ is separable. □

Example 2.42. For the Bell state $\rho = |\Phi^+\rangle\langle\Phi^+|$ with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ we get

$$\rho^R = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|10\rangle\langle 10| + \frac{1}{2}|11\rangle\langle 11|\,.$$

Its norm $\|\rho^R\|_1 = 2$ certifies that the Bell state is entangled.

The realignment criterion is neither weaker nor stronger than the Peres-Horodecki criterion. Other separability criteria can be found in [HHHH09].

Chapter 3

Superoperators and quantum maps

This chapter is devoted to the study of linear maps acting between spaces of operators, hence the name *superoperators*. In the Introduction we explained that operator algebras equipped with the Hilbert-Schmidt inner product are also Hilbert spaces. Any superoperator is thus just a usual operator acting on a larger Hilbert space.

Like in Chapter 2, we merge the mathematical and physical notions (as it is done in quantum information theory for the last 20 years), and we associate superoperators between spaces of operators with *quantum maps* or *quantum operations* acting on states. We introduce completely positive maps and the associated quantum channels, we construct entanglement witnesses and derive criteria for detecting entangled states.

3.1 Positive and completely positive maps

Definition 3.1. The linear map $\Phi\colon B(\mathcal{H}) \to B(\mathcal{K})$ is *positive* or *positivity preserving* if it maps positive operators into positive operators. In other words, the image of every positive semidefinite operator on $\mathcal{H}$ is a positive semidefinite operator on $\mathcal{K}$. The map Φ is said to be *n-positive* if its n-th ampliation

$$\Phi^{(n)} := \Phi \otimes \mathrm{Id}\colon B(\mathcal{H} \otimes \mathbb{C}^n) \to B(\mathcal{K} \otimes \mathbb{C}^n) \tag{3.1}$$

is positive. (Note that if Φ is n-positive, then Φ is automatically k-positive for any $k < n$.) When Φ is n-positive for all $n \in \mathbb{N}$, it is said to be *completely-positive*. The set of completely positive maps from $B(\mathcal{H})$ to $B(\mathcal{K})$, which is clearly a convex cone in $B\left(B(\mathcal{H}), B(\mathcal{K})\right)$, will be denoted by $\boldsymbol{CP}(\mathcal{H}, \mathcal{K})$.

Example 3.2. Transposition T is an example of a positive map which is not 2-positive (since the partial transposition in Definition 2.29 is the 2-nd ampliation of the transposition) and thus it is not completely positive. For the proof see Example 2.35, where we showed that the partial transposition of the pure Bell state has a negative eigenvalue.

3.1.1 The Choi and Jamiołkowski isomorphisms

Before we give a structure theorem for completely positive maps, we introduce the (basis-independent) Jamiołkowski isomorphism and the (basis-dependent, but often more useful)

Choi isomorphism. Choi's and Jamiołkowski's isomorphisms are rarely distinguished in the literature; we will explain their relation in Remark 3.3.

Recall the canonical isomorphisms between tensor products defined in the Introduction:

$$(\mathcal{H}_1 \otimes \mathcal{H}_2)^* \longleftrightarrow \mathcal{H}_1^* \otimes \mathcal{H}_2^* \quad \text{and} \quad \mathcal{H}_1^* \otimes \mathcal{H}_2 \longleftrightarrow B(\mathcal{H}_1, \mathcal{H}_2),$$

where $\mathcal{H}^* = B(\mathcal{H}, \mathbb{C})$ is the dual Hilbert space of linear functionals. This induces another canonical isomorphism, which can be written concretely via the trace duality,

$$\begin{array}{rcl} B(\mathcal{H}_2, \mathcal{H}_1) & \longleftrightarrow & B(\mathcal{H}_1, \mathcal{H}_2)^* \\ S & \longmapsto & T \mapsto \operatorname{Tr} ST. \end{array}$$

A straightforward iteration of the above yields that $B(B(\mathcal{H}_1), B(\mathcal{H}_2))$ and $B(\mathcal{H}_2 \otimes \mathcal{H}_1)$ are both canonically isomorphic to $\mathcal{H}_1 \otimes \mathcal{H}_1^* \otimes \mathcal{H}_2 \otimes \mathcal{H}_2^*$, which defines the *Jamiołkowski isomorphism*

$$J : B(B(\mathcal{H}_1), B(\mathcal{H}_2)) \longrightarrow B(\mathcal{H}_2 \otimes \mathcal{H}_1).$$

If we select any basis $\{e_i\}$ in $\mathcal{H}_1$ and denote the corresponding operators by $E_{ij} = |e_i\rangle\langle e_j| \in B(\mathcal{H}_1)$, then the explicit representation of J is

$$\begin{array}{rcl} J : B(B(\mathcal{H}_1), B(\mathcal{H}_2)) & \longrightarrow & B(\mathcal{H}_2 \otimes \mathcal{H}_1) \\ \Phi & \longmapsto & \sum_{i,j} \Phi(E_{ij}) \otimes E_{ji}. \end{array}$$

Once a basis of $\mathcal{H}_1$ is fixed, we can define the *Choi isomorphism* as the $\mathbb{C}$-linear isomorphism

$$\begin{array}{rcl} C : B(B(\mathcal{H}_1), B(\mathcal{H}_2)) & \longrightarrow & B(\mathcal{H}_2 \otimes \mathcal{H}_1) \\ \Phi & \longmapsto & \sum_{i,j} \Phi(E_{ij}) \otimes E_{ij}. \end{array}$$

We name the matrix $C_\Phi := C(\Phi)$ the *Choi matrix* of Φ.

Remark 3.3. The Choi isomorphism C and the Jamiołkowski isomorphism J are related via the partial transposition in Definition 2.29. Indeed, let Γ denote the partial transposition on $\mathcal{H}_2 \otimes \mathcal{H}_1$ with respect to the second factor $\mathcal{H}_1$, then $C = \Gamma \circ J$. This relation is consistent with the fact that C and Γ are both basis-dependent, whereas the Jamiołkowski isomorphism is not.

In is often useful to know which superoperators in $B(B(\mathcal{H}_1), B(\mathcal{H}_2))$ correspond to rank one operators in $B(\mathcal{H}_2 \otimes \mathcal{H}_1)$ under the Choi isomorphism. In particular, by applying Choi's theorem 3.9, we will be able to construct superoperators that the Choi isomorphism maps to pure states.

Lemma 3.4. *For given $A, B \in B(\mathcal{H}_1, \mathcal{H}_2)$ consider the map*

$$\begin{array}{rcl} \Phi : B(\mathcal{H}_1) & \longrightarrow & B(\mathcal{H}_2) \\ X & \longmapsto & AXB^*. \end{array}$$

The Choi matrix of Φ is $C(\Phi) = |a\rangle\langle b|$, where $a = \operatorname{vec} A$ and $b = \operatorname{vec} B$ are vectors in $\mathcal{H}_2 \otimes \mathcal{H}_1$ defined in (1.4). *Recall that operators A, B have rank 1 if and only if the corresponding vectors a, b are product vectors.*

Proof. By $\mathbb{C}$-linearity it is enough to prove the lemma for $A = |\psi\rangle\langle e_i|$ and $B = \left|\chi\middle\rangle\middle\langle e_j\right|$ for some $\psi, \chi \in \mathcal{H}_2$ and basis vectors $e_i, e_j \in \mathcal{H}_1$. By definition we have $a = \mathrm{vec}A = \psi \otimes e_i$ and $b = \mathrm{vec}B = \chi \otimes e_j$, then

$$|a\rangle\langle b| = \left|\psi \otimes e_i\middle\rangle\middle\langle\chi \otimes e_j\right| = |\psi\rangle\langle\chi| \otimes \left|e_i\middle\rangle\middle\langle e_j\right| = |\psi\rangle\langle\chi| \otimes E_{ij}$$

and

$$C(\Phi) = \sum_{i,j} AE_{ij}B^* \otimes E_{ij} = |\psi\rangle \langle e_i|e_i\rangle \left\langle e_j\middle|e_j\right\rangle \langle\chi| \otimes E_{ij} = |\psi\rangle\langle\chi| \otimes E_{ij}.$$

□

The proof of the next Lemma shows how a superoperator is connected to its Choi matrix in the computational basis.

Lemma 3.5. *The matrix of a superoperator $\Phi\colon B(\mathbb{C}^{d_1}) \to B(\mathbb{C}^{d_2})$ with respect to the standard bases $\{E_{ij}\}_{1\le i,j\le d_1}$ and $\{E_{kl}\}_{1\le k,l\le d_2}$ is equal to $C(\Phi)^R$, where R is the realignment of operators from $B(\mathbb{C}^{d_2} \otimes \mathbb{C}^{d_1})$ in Definition 2.40.*

Proof. Recall the identification (1.2) of the space of operators $B(\mathbb{C}^m \otimes \mathbb{C}^n)$ with $mn \times mn$ block matrices. We can represent $C(\Phi) \in B(\mathbb{C}^{d_2} \otimes \mathbb{C}^{d_1})$ as a $d_2 \times d_2$ block matrix whose elements are $d_1 \times d_1$ matrices defined as

$$C(\Phi) = [C(\Phi)_{kl}]_{k,l=1}^{d_2},$$

where each

$$\begin{aligned} C(\Phi)_{kl} &= \left[\left\langle e_k \otimes e_i\middle| C(\Phi) \middle|e_l \otimes e_j\right\rangle\right]_{i,j=1}^{d_1} \\ &= \left[\left\langle e_k \otimes e_i\middle| \Phi(E_{ij}) \otimes E_{ij} \middle|e_l \otimes e_j\right\rangle\right]_{i,j=1}^{d_1} \\ &= \left[\langle e_k| \Phi(E_{ij}) |e_l\rangle\right]_{i,j=1}^{d_1}. \end{aligned} \tag{3.2}$$

This shows that the Choi matrix has the following entries: the ij-th entry of the kl-th block is the kl-th entry of $\Phi(E_{ij})$. Then $C(\Phi)^R \in B\left(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_1}, \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}\right)$ is the matrix representing Φ by the definition of R. □

Example 3.6. In Section 3.3 we will need to compute the Choi matrix of a superoperator Φ acting on $\mathrm{M}_3 = B(\mathbb{C}^3)$. The explicit formula follows from (3.2). Let $\Phi(E_{ij})_{kl}$ denote the kl-th entry of the matrix $\Phi(E_{ij})$ (we keep the indices consistent with the computational basis, i.e., $i, j, k, l \in \{0, 1, 2\}$). Then $C(\Phi)$ is equal to

$$\left[\begin{array}{ccc|ccc|ccc}
\Phi(E_{00})_{00} & \Phi(E_{01})_{00} & \Phi(E_{02})_{00} & \Phi(E_{00})_{01} & \Phi(E_{01})_{01} & \Phi(E_{02})_{01} & \Phi(E_{00})_{02} & \Phi(E_{01})_{02} & \Phi(E_{02})_{02} \\
\Phi(E_{10})_{00} & \Phi(E_{11})_{00} & \Phi(E_{12})_{00} & \Phi(E_{10})_{01} & \Phi(E_{11})_{01} & \Phi(E_{12})_{01} & \Phi(E_{10})_{02} & \Phi(E_{11})_{02} & \Phi(E_{12})_{02} \\
\Phi(E_{20})_{00} & \Phi(E_{21})_{00} & \Phi(E_{22})_{00} & \Phi(E_{20})_{01} & \Phi(E_{21})_{01} & \Phi(E_{22})_{01} & \Phi(E_{20})_{02} & \Phi(E_{21})_{02} & \Phi(E_{22})_{02} \\
\hline
\Phi(E_{00})_{10} & \Phi(E_{01})_{10} & \Phi(E_{02})_{10} & \Phi(E_{00})_{11} & \Phi(E_{01})_{11} & \Phi(E_{02})_{11} & \Phi(E_{00})_{12} & \Phi(E_{01})_{12} & \Phi(E_{02})_{12} \\
\Phi(E_{10})_{10} & \Phi(E_{11})_{10} & \Phi(E_{12})_{10} & \Phi(E_{10})_{11} & \Phi(E_{11})_{11} & \Phi(E_{12})_{11} & \Phi(E_{10})_{12} & \Phi(E_{11})_{12} & \Phi(E_{12})_{12} \\
\Phi(E_{20})_{10} & \Phi(E_{21})_{10} & \Phi(E_{22})_{10} & \Phi(E_{20})_{11} & \Phi(E_{21})_{11} & \Phi(E_{22})_{11} & \Phi(E_{20})_{12} & \Phi(E_{21})_{12} & \Phi(E_{22})_{12} \\
\hline
\Phi(E_{00})_{20} & \Phi(E_{01})_{20} & \Phi(E_{02})_{20} & \Phi(E_{00})_{21} & \Phi(E_{01})_{21} & \Phi(E_{02})_{21} & \Phi(E_{00})_{22} & \Phi(E_{01})_{22} & \Phi(E_{02})_{22} \\
\Phi(E_{10})_{20} & \Phi(E_{11})_{20} & \Phi(E_{12})_{20} & \Phi(E_{10})_{21} & \Phi(E_{11})_{21} & \Phi(E_{12})_{21} & \Phi(E_{10})_{22} & \Phi(E_{11})_{22} & \Phi(E_{12})_{22} \\
\Phi(E_{20})_{20} & \Phi(E_{21})_{20} & \Phi(E_{22})_{20} & \Phi(E_{20})_{21} & \Phi(E_{21})_{21} & \Phi(E_{22})_{21} & \Phi(E_{20})_{22} & \Phi(E_{21})_{22} & \Phi(E_{22})_{22}
\end{array}\right].$$

In the literature the Choi isomorphism is often defined as

$$\begin{array}{rcl} \tilde{C}: B\,(B(\mathcal{H}_1), B(\mathcal{H}_2)) & \longrightarrow & B(\mathcal{H}_1 \otimes \mathcal{H}_2) \\ \Phi & \mapsto & \sum_{i,j} E_{ij} \otimes \Phi(E_{ij}). \end{array}$$

In this representation, the Choi matrix $\tilde{C}(\Phi)$ has a simpler block form. For $\Phi\colon B(\mathbb{C}^{d_1}) \to B(\mathbb{C}^{d_2})$,

$$\tilde{C}(\Phi) = \left[\Phi(E_{ij})\right]_{i,j=1}^{d_1}. \tag{3.3}$$

In Example 3.6, the alternative Choi matrix of $\Phi\colon \mathrm{M}_3 \to \mathrm{M}_3$ is

$$\tilde{C}(\Phi) = \begin{bmatrix} \Phi(E_{00}) & \Phi(E_{01}) & \Phi(E_{02}) \\ \Phi(E_{10}) & \Phi(E_{11}) & \Phi(E_{12}) \\ \Phi(E_{20}) & \Phi(E_{21}) & \Phi(E_{22}) \end{bmatrix}.$$

The two different definitions of the Choi matrix do not change the theory succeeding Choi's therem 3.9 because of the following lemma.

Lemma 3.7. *Let $\Phi\colon B(\mathbb{C}^{d_1}) \to B(\mathbb{C}^{d_2})$ be a superoperator. The Choi matrix $C(\Phi)$ is positive semidefinite if and only if $\tilde{C}(\Phi)$ is positive semidefinite.*

Proof. Consider $\psi = \sum_k \beta_k\, \xi_k \otimes \eta_k \in \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_1}$. The lemma follows from the following equalities

$$\begin{array}{rl} \langle \psi | C(\Phi) | \psi \rangle & = \\ \left\langle \sum_k \beta_k\, \xi_k \otimes \eta_k \middle| \sum_{i,j} \Phi(E_{ij}) \otimes E_{ij} \middle| \sum_l \beta_l\, \xi_l \otimes \eta_l \right\rangle & = \\ \sum_{k,l} \overline{\beta_k} \beta_l \sum_{i,j} \langle \xi_k | \Phi(E_{ij}) | \xi_l \rangle\, \langle \eta_k | E_{ij} | \eta_l \rangle & = \\ \left\langle \sum_k \beta_k\, \eta_k \otimes \xi_k \middle| \sum_{i,j} E_{ij} \otimes \Phi(E_{ij}) \middle| \sum_l \beta_l\, \eta_l \otimes \xi_l \right\rangle & = \\ \langle \tilde{\psi} | \tilde{C}(\Phi) | \tilde{\psi} \rangle, & \end{array}$$

for $\tilde{\psi} = \sum_k \beta_k\, \eta_k \otimes \xi_k \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$. □

3.1.2 Choi's theorem

Recall that in the definition of the Choi isomorphism on page 34 we fixed a basis $\{e_i\}$ in $\mathcal{H}_1$. Then the corresponding Choi matrix can be rewritten in an elegant way (by repeating the proof of Lemma 3.5) as follows:

$$C(\Phi) = \left(\Phi \otimes \mathrm{Id}_{B(\mathcal{H}_1)}\right)(|\chi\rangle\langle\chi|), \tag{3.4}$$

where $\chi = \sum_i e_i \otimes e_i \in \mathcal{H}_1 \otimes \mathcal{H}_1$. (Note that $1/\sqrt{\dim \mathcal{H}_1}\,\chi$ is a maximally entangled state vector (2.12).) Maps of the form

$$\Phi \otimes \mathrm{Id}_{B(\mathcal{H}_1)}$$

are called *extensions* of Φ; for example, the partial transposition Γ (from Definition 2.29) is an extension of the transposition T.

Throughout this section we will consider *self-adjointness-preserving* superoperators, defined as linear maps

$$\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2) \text{ such that } \Phi\left(B^{\mathrm{sa}}(\mathcal{H}_1)\right) \subset B^{\mathrm{sa}}(\mathcal{H}_2).$$

If we restrict a self-adjointness-preserving $\mathbb{C}$-linear map $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$, we obtain an $\mathbb{R}$-linear map $\Psi\colon B^{\mathrm{sa}}(\mathcal{H}_1) \to B^{\mathrm{sa}}(\mathcal{H}_2)$. This is in actually a one-to-one correspondence, as Φ can be obtained from Ψ by complexification. Indeed, if we write $X \in B(\mathcal{H}_1)$ as a sum of self-adjoint operators

$$X = \frac{X+X^*}{2} + i\,\frac{X-X^*}{2i}, \text{ this implies } \Phi(X) = \Psi\left(\frac{X+X^*}{2}\right) + i\,\Psi\left(\frac{X-X^*}{2i}\right).$$

Lemma 3.8. *The following properties of a map $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ are equivalent:*

1. *Φ is self-adjointness-preserving,*
2. *$\Phi(X^*) = (\Phi(X))^*$ for any $X \in B(\mathcal{H}_1)$,*
3. *$J(\Phi) \in B^{sa}(\mathcal{H}_2 \otimes \mathcal{H}_1)$,*
4. *$C(\Phi) \in B^{sa}(\mathcal{H}_2 \otimes \mathcal{H}_1)$.*

Proof. It is straightforward to check the implications 2. $\Longrightarrow$ 3. $\Longrightarrow$ 4. $\Longrightarrow$ 1. The implication 1. $\Longrightarrow$ 2. follows by $\mathbb{C}$-linearity of Φ. Indeed, the equality $\Phi(E_{kl}) = \Phi(E_{lk})^*$ follows from the linear equations:

$$\begin{aligned}
\Phi(E_{kl}) + \Phi(E_{lk}) &= \Phi(E_{kl} + E_{lk}) = (\Phi(E_{kl} + E_{lk}))^* = \Phi(E_{kl})^* + \Phi(E_{lk})^*, \\
i\Phi(E_{kl}) - i\Phi(E_{lk}) &= \Phi(iE_{kl} - iE_{lk}) = (\Phi(iE_{kl} - iE_{lk}))^* = -i\Phi(E_{kl})^* + i\Phi(E_{lk})^*.
\end{aligned}$$

□

The *adjoint* of a self-adjointness-preserving Φ is the unique adjoint superoperator $\Phi^*\colon B(\mathcal{H}_2) \to B(\mathcal{H}_1)$ with respect to the Hilbert-Schmidt inner product, thus

$$\begin{aligned}
\langle X, \Phi(Y)\rangle_{\mathrm{HS}} &= \langle \Phi^*(X), Y\rangle_{\mathrm{HS}} \\
\mathrm{Tr}\,(X^*\Phi(Y)) &= \mathrm{Tr}\,(\Phi^*(X^*)Y),
\end{aligned}$$

where $X \in B(\mathcal{H}_2)$ and $Y \in B(\mathcal{H}_1)$. Note that since Φ is self-adjointness-preserving, also Φ^* is self-adjointness-preserving.

We have now prepared all the notions to state an important and useful structure theorem for completely positive maps.

Theorem 3.9 (Choi's theorem)**.** *For a self-adjointness-preserving map $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ the following statements are equivalent:*

1. *The map Φ is completely positive.*
2. *The Choi matrix $C(\Phi) \in B^{sa}(\mathcal{H}_2 \otimes \mathcal{H}_1)$ is positive semidefinite.*
3. *There exist operators $A_1, \ldots, A_N \in B(\mathcal{H}_1, \mathcal{H}_2)$ such that, for any $X \in B(\mathcal{H}_1)$, it holds*

$$\Phi(X) = \sum_{n=1}^{N} A_n X A_n^*. \tag{3.5}$$

Proof. We first prove the implication 3. $\Longrightarrow$ 1.. By Definition 3.1, Φ is completely positive if every m-ampliation $\Phi^{(m)} = \Phi \otimes \mathrm{Id}\colon B(\mathcal{H}_1 \otimes \mathbb{C}^m) \to B(\mathcal{H}_2 \otimes \mathbb{C}^m)$ is positive. By the spectral theorem and by linearity it is enough to verify positivity on rank one operators $|v\rangle\langle v| \in B(\mathcal{H}_1 \otimes \mathbb{C}^m)$, where $v = \sum_{i,j} \lambda_{ij}\, e_i \otimes |j\rangle$. Then

$$\Phi^{(m)}(|v\rangle\langle v|) = \sum_{i,j,k,l} \lambda_{ij}\overline{\lambda_{kl}}\,\Phi^{(m)}(|e_i\rangle\langle e_k| \otimes |j\rangle\langle l|) = \sum_{i,j,k,l} \lambda_{ij}\overline{\lambda_{kl}}\,\Phi(|e_i\rangle\langle e_k|) \otimes |j\rangle\langle l| =$$
$$\sum_{n=1}^{N}\sum_{i,j,k,l} \lambda_{ij}\overline{\lambda_{kl}}\,(|A_n e_i\rangle\langle A_n e_k|) \otimes |j\rangle\langle l| =$$
$$\sum_{n=1}^{N} |w_n\rangle\langle w_n|,$$

where $w_n = \sum_{i,j} \lambda_{ij}\,(A_n e_i) \otimes |j\rangle$, which is clearly positive.
The implication 1. $\Longrightarrow$ 2. follows from the Choi matrix representation (3.4).
Finally we prove 2. $\Longrightarrow$ 3. Since $C(\Phi)$ is positive semi-definite, the spectral theorem yields vectors $a_n \in \mathcal{H}_2 \otimes \mathcal{H}_1$ such that

$$C(\Phi) = \sum_n |a_n\rangle\langle a_n|.$$

By Lemma 3.4, each $|a_n\rangle\langle a_n|$ equals the Choi matrix of the map $X \mapsto A_n X A_n^*$, where $a_n = \mathrm{vec} A_n$ and $A_n \in B(\mathcal{H}_1, \mathcal{H}_2)$. This together with the linearity of the Choi isomorphism proves (3.5). □

Definition 3.10 (Kraus decomposition)**.** A decomposition of the form (3.5) is called a *Kraus decomposition* of Φ. As seen in the proof of Theorem 3.9, the smallest possible N for which a Kraus decomposition exists is equal to the rank of $C(\Phi)$, hence it is referred to as the *Kraus rank* of Φ. In particular, this means that the Kraus rank of a completely positive map $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is at most $\dim \mathcal{H}_1 \dim \mathcal{H}_2$.

A simple check shows that a self-adjointness-preserving superoperator $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is positivity preserving if and only if its adjoint $\Phi^*\colon B(\mathcal{H}_2) \to B(\mathcal{H}_1)$ is positivity preserving. By the spectral theorem it suffices to verify the semi-definiteness on rank one operators, and by Lemma 3.8, 2. we get,

$$\begin{array}{rcl} \langle\psi_2|\,\Phi(|\psi_1\rangle\langle\psi_1|)\,|\psi_2\rangle &=& \mathrm{Tr}(|\psi_2\rangle\langle\psi_2|\,\Phi(|\psi_1\rangle\langle\psi_1|)) = \langle|\psi_2\rangle\langle\psi_2|, \Phi(|\psi_1\rangle\langle\psi_1|)\rangle_{\mathrm{HS}} \\ && \hspace{8em} \| \\ \langle\psi_1|\,\Phi^*(|\psi_2\rangle\langle\psi_2|)\,|\psi_1\rangle &=& \mathrm{Tr}(\Phi^*(|\psi_2\rangle\langle\psi_2|)\,|\psi_1\rangle\langle\psi_1|) = \langle\Phi^*(|\psi_2\rangle\langle\psi_2|), |\psi_1\rangle\langle\psi_1|\rangle_{\mathrm{HS}} \end{array}$$

and therefore the following are equivalent:

- Φ is positivity preserving,
- $\Phi(|\psi_1\rangle\langle\psi_1|)$ is positive semidefinite for all $\psi_1 \in \mathcal{H}_1$,
- $\langle\psi_2|\,\Phi(|\psi_1\rangle\langle\psi_1|)\,|\psi_2\rangle \geq 0$ for all $\psi_1 \in \mathcal{H}_1$ and $\psi_2 \in \mathcal{H}_2$,
- $\Phi^*(|\psi_2\rangle\langle\psi_2|)$ is positive semidefinite for all $\psi_2 \in \mathcal{H}_1$,
- Φ^* is positivity preserving.

An analogous proof shows that for a given $n \in \mathbb{N}$, Φ is n-positive if and only if Φ^* is n-positive. Moreover, Φ is completely positive if and only if its adjoint Φ^* is completely positive. This can be seen also from the Kraus decomposition (3.5) of Φ, which is related to the Kraus decomposition of Φ^* in the following way,

$$\Phi^*(Y) = \sum_{n=1}^{N} A_n^* Y A_n \quad \text{for all} \quad Y \in B(\mathcal{H}_2).$$

Corollary 3.11. *The statements of Choi's theorem 3.9 are equivalent to the fact that Φ is n-positive, where $n = \min\{\dim \mathcal{H}_1, \dim \mathcal{H}_2\}$.*

Proof. Without loss of generality we can assume that $\dim \mathcal{H}_1 \leq \dim \mathcal{H}_2$, otherwise we switch the roles of $\mathcal{H}_1$ and $\mathcal{H}_2$ by considering Φ^*. Then the corollary follows from the proof of 3. $\Longrightarrow$ 1. in Theorem 3.9. □

Corollary 3.12. *Any self-adjointness-preserving map $\Phi \colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is a difference of two completely positive maps.*

Proof. We will write the Choi matrix $C(\Phi) \in B^{\mathrm{sa}}(\mathcal{H}_2 \otimes \mathcal{H}_1)$ as a difference of two positive operators and then apply Choi's theorem 3.9. By the spectral theorem, $C(\Phi) = UDU^*$ for some unitary U and a real diagonal matrix D. In D we can separate the nonnegative and negative eigenvalues. In other words, $D = D_{\geq 0} - D_{<0}$ where $D_{\geq 0}$ and $D_{<0}$ are diagonal with nonegative entries, therefore $C(\Phi) = UD_{\geq 0}U^* - UD_{<0}U^*$. □

In the next examples we explore some further properties of positive and completely positive maps.

Example 3.13. We will show that $\Phi \colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ and $\Psi \colon B(\mathcal{K}_1) \to B(\mathcal{K}_2)$ being completely positive maps implies that $\Phi \otimes \Psi$ and $\Phi \circ \Psi$ are completely positive.

Note that the composition is defined only when $\mathcal{K}_2 = \mathcal{H}_1$. Then $\Phi \circ \Psi \colon B(\mathcal{K}_1) \to B(\mathcal{H}_2)$ has the following Kraus decomposition

$$(\Phi \circ \Psi)(X) = \Phi\left(\sum_{m=1}^{M} B_m X B_m^*\right) = \sum_{m,n} A_n B_m X (A_n B_m)^*,$$

where $\Psi(X) = \sum_{m=1}^{M} B_m X B_m^*$ for $X \in B(\mathcal{K}_1)$, $B_m \in B(\mathcal{K}_1, \mathcal{K}_2)$ and $\Phi(Z) = \sum_{n=1}^{N} A_n Z A_n^*$ for $Z \in B(\mathcal{H}_1)$, $A_n \in B(\mathcal{H}_1, \mathcal{H}_2)$ are Kraus decompositions of Ψ and Φ respectively.

Furthermore, $\Phi \otimes \Psi \colon B(\mathcal{H}_1 \otimes \mathcal{K}_1) \to B(\mathcal{H}_2 \otimes \mathcal{K}_2)$ is completely positive since

$$\Phi \otimes \Psi = \left(\Phi \otimes \mathrm{Id}_{B(\mathcal{K}_2)}\right) \circ \left(\mathrm{Id}_{B(\mathcal{H}_1)} \otimes \Psi\right).$$

Example 3.14. For integers $k < n$, the map

$$\begin{aligned} \Phi \colon \mathrm{M}_n &\longrightarrow \mathrm{M}_n \\ X &\longmapsto k\,\mathrm{Tr}(X)I - X \end{aligned}$$

is k-positive but not $(k+1)$-positive.

First we show that Φ is not $(k+1)$-positive by evaluating $\Phi \otimes \mathrm{Id}\colon \mathrm{M}_n \otimes \mathrm{M}_{k+1} \to \mathrm{M}_n \otimes \mathrm{M}_{k+1}$ on $|\psi\rangle\langle\psi|$ for $\psi = \sum_{i=1}^{k+1} |i\rangle \otimes |i\rangle \in \mathbb{C}^n \otimes \mathbb{C}^{k+1}$. We compute

$$\begin{aligned}
\left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_{k+1}}\right)(|\psi\rangle\langle\psi|) &= \\
(\Phi \otimes \mathrm{Id})\left(\sum_{i,j=1}^{k+1} |i\rangle\langle j| \otimes |i\rangle\langle j|\right) &= \\
\sum_{i,j=1}^{k+1} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j| &= \\
\sum_{i=1}^{k+1} \Phi(|i\rangle\langle i|) \otimes |i\rangle\langle i| + \sum_{i\neq j} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j| &= \\
\sum_{i=1}^{k+1} (kI_n - |i\rangle\langle i|) \otimes |i\rangle\langle i| - \sum_{i\neq j} |i\rangle\langle j| \otimes |i\rangle\langle j| &=: \Theta \in \mathrm{M}_n \otimes \mathrm{M}_{k+1},
\end{aligned}$$

which is not positive semidefinite since $\left\langle \sum_{i=1}^{k+1} i \otimes i \middle| \Theta \middle| \sum_{i=1}^{k+1} i \otimes i \right\rangle = (k-(k+1))(k+1) < 0$.

On the other hand, the spectral theorem implies that Φ is k-positive if and only if the matrix $\left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_k}\right)(|\psi\rangle\langle\psi|)$ is positive semidefinite for all $\psi \in \mathbb{C}^n \otimes \mathbb{C}^k$. We can write any ψ in the form $\psi = \sum_{i=1}^{k} \chi_i \otimes \varphi_i$, where $\{\varphi_i\}$ is an orthonormal basis of $\mathbb{C}^k$. Then,

$$\left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_k}\right)(|\psi\rangle\langle\psi|) \geq \sum_{i<j} \left|\chi_i \otimes \varphi_i - \chi_j \otimes \varphi_j\right\rangle\!\left\langle \chi_i \otimes \varphi_i - \chi_j \otimes \varphi_j\right| \geq 0.$$

3.1.3 Quantum channels

In this subsection we introduce quantum channels, a fundamental family of superoperators in quantum information theory.

We say that a self-adjointness-preserving map $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is *unital* if $\Phi(I_{\mathcal{H}_1}) = I_{\mathcal{H}_2}$; and it is *trace preserving* if $\operatorname{Tr}\Phi(X) = \operatorname{Tr}X$ for all $X \in B(\mathcal{H}_1)$.

Lemma 3.15. *A self-adjointness-preserving map $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is unital if and only if $\Phi^*\colon B(\mathcal{H}_2) \to B(\mathcal{H}_1)$ is trace preserving.*

Proof. If Φ is unital and $Y \in B(\mathcal{H}_2)$, we have

$$\operatorname{Tr} Y = \langle Y^*, I_{\mathcal{H}_2}\rangle_{\mathrm{HS}} = \langle Y^*, \Phi(I_{\mathcal{H}_1})\rangle_{\mathrm{HS}} = \langle \Phi^*(Y^*), I_{\mathcal{H}_1}\rangle_{\mathrm{HS}} = \operatorname{Tr}\Phi^*(Y),$$

where the last equality follows from Lemma 3.8, 2. On the other hand, if Φ^* is trace preserving, it holds

$$\langle Y^*, I_{\mathcal{H}_2}\rangle_{\mathrm{HS}} = \operatorname{Tr} Y = \operatorname{Tr}\Phi^*(Y) = \langle Y^*, \Phi(I_{\mathcal{H}_1})\rangle_{\mathrm{HS}}$$

for each $Y \in B(\mathcal{H}_2)$, which implies $\Phi(I_{\mathcal{H}_1}) = I_{\mathcal{H}_2}$. □

Definition 3.16. A *quantum channel* $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ is a completely positive and trace preserving map; thus a quantum channel is also called a CPTP map. A unital quantum channel is called *doubly stochastic* or *bistochastic*.

In quantum information theory Φ is representing some physical process where it is natural to expect that states are mapped to states. This is the reason why quantum channels are by definition positivity preserving and trace preserving. The reason for the "complete" positivity assumption is slightly more subtle and will be addressed in Remark 3.20. Note that if a quantum channel Φ is additionally unital (i.e., bistochastic), then both Φ and Φ^* are quantum channels, in which case it must hold $\dim \mathcal{H}_1 = \dim \mathcal{H}_2$.

Lemma 3.17. *For a map $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ with Kraus decomposition* (3.5)*, the following equivalences hold:*

1. *The condition $\sum_{n=1}^N A_n A_n^* = I_{\mathcal{H}_2}$ is equivalent to Φ being unital.*
2. *The condition $\sum_{n=1}^N A_n^* A_n = I_{\mathcal{H}_1}$ is equivalent to Φ being trace preserving.*

Proof. The first equivalence is obtained directly from the Kraus decomposition of Φ:

$$\Phi(I_{\mathcal{H}_1}) = \sum_{n=1}^N A_n I_{\mathcal{H}_1} A_n^* = \sum_{n=1}^N A_n A_n^* = I_{\mathcal{H}_2}.$$

By linearity of Φ and the spectral theorem it is enough to show that the second condition is equivalent to $\operatorname{Tr}\Phi(X) = \operatorname{Tr} X$ for $X = |\xi\rangle\langle\xi|$. This is true, since the argument

$$\operatorname{Tr}(|\xi\rangle\langle\xi|) = \operatorname{Tr}\left(\sum_{n=1}^N A_n^* A_n |\xi\rangle\langle\xi|\right) = \operatorname{Tr}\left(\sum_{n=1}^N A_n |\xi\rangle\langle\xi| A_n^*\right)$$

holds both ways for any $\xi \in \mathcal{H}_1$. □

Now we state another fundamental representation theorem describing the structure of quantum maps.

Theorem 3.18 (Stinespring theorem). *For a completely positive map $\Phi\colon B(\mathcal{H}_1) \to B(\mathcal{H}_2)$ there exists a Hilbert space $\mathcal{E}$ of $\dim \mathcal{E} \leq \dim \mathcal{H}_1 \dim \mathcal{H}_2$ and an embedding $V\colon \mathcal{H}_1 \to \mathcal{H}_2 \otimes \mathcal{E}$ for which it holds,*

$$\Phi(X) = \operatorname{Tr}_{\mathcal{E}} VXV^* \quad \textit{for any} \quad X \in B(\mathcal{H}_1).$$

Moreover, if Φ is a quantum channel, then the embedding V is an isometry. Conversely, an isometric embedding V induces the map $X \mapsto \operatorname{Tr}_{\mathcal{E}} VXV^*$ that is a quantum channel.

Proof. By Choi's theorem 3.9, we can assign to Φ a Kraus decomposition with the Kraus rank $N \leq \dim \mathcal{H}_1 \dim \mathcal{H}_2$. Define $\mathcal{E} = \mathbb{C}^N$ and

$$\begin{aligned} V\colon \mathcal{H}_1 &\longrightarrow \mathcal{H}_2 \otimes \mathcal{E} \\ |\xi\rangle &\mapsto \sum_{i=1}^N A_i |\xi\rangle \otimes |i\rangle \quad \text{for} \quad \xi \in \mathcal{H}_1 . \end{aligned}$$

Then, for any $X \in B(\mathcal{H}_1)$, it holds

$$VXV^* = \sum_{i,j=1}^N A_i X A_j \otimes |i\rangle\langle j| ,$$

which proves the first statement of the theorem. (This follows by linearity from operators of the form $X = |\xi\rangle\langle\xi|$, like in the proof of Lemma 3.17). From evaluating V on an orthonormal basis we get $V^*V = \sum_{i=1}^N A_i^* A_i$. Then by Lemma 3.17 it holds $V^*V = I_{\mathcal{H}_1}$ if and only if Φ is a quantum channel; this means that V is an isometry. On the other hand, the map $X \mapsto \operatorname{Tr}_{\mathcal{E}} VXV^*$ induced by an isometric embedding V is a quantum channel. Indeed, it is completely positive by Choi's theorem 3.9 (repeat the easy step 3. $\Longrightarrow$ 1. in the proof) and it is trace preserving since V is an isometry (i.e., $V^*V = I_{\mathcal{H}_1}$). □

When $\mathcal{H}_1 = \mathcal{H}_2$, the Stinespring theorem is even more descriptive: any quantum channel can be "lifted" to a unitary transformation acting on a larger composite system (by using some auxiliary Hilbert space).

Corollary 3.19. *For a quantum channel $\Phi\colon B(\mathcal{H}) \to B(\mathcal{H})$ there exists a finite-dimensional Hilbert space $\mathcal{E}$, a unit vector $\eta \in \mathcal{E}$ and a unitary transformation U on $\mathcal{H} \otimes \mathcal{E}$ such that for any $X \in B(\mathcal{H})$ it holds,*

$$\Phi(X) = \operatorname{Tr}_{\mathcal{E}} U(X \otimes |\eta\rangle\langle\eta|)U^*. \tag{3.6}$$

Proof. Let $\mathcal{E}$ be the finite dimensional space and $V\colon \mathcal{H} \to \mathcal{H} \otimes \mathcal{E}$ the isomorphism given by the Stinespring theorem 3.18. Select any unit vector $\eta \in \mathcal{E}$ and on the subspace $\mathcal{H} \otimes \eta \subset \mathcal{H} \otimes \mathcal{E}$ define the following isometry

$$\begin{aligned} U_\eta\colon \mathcal{H} \otimes \eta &\longrightarrow \mathcal{H} \otimes \mathcal{E} \\ \xi \otimes \eta &\mapsto V(\xi). \end{aligned}$$

Then U_η can be extended to a unitary on $\mathcal{H} \otimes \mathcal{E}$. As before, by linearity it suffices to check (3.6) for $X = |\xi\rangle\langle\xi|$,

$$\Phi(X) = \operatorname{Tr}_{\mathcal{E}} V\,|\xi\rangle\langle\xi|\,V^* = \operatorname{Tr}_{\mathcal{E}} U\,|\xi \otimes \eta\rangle\langle\xi \otimes \eta|\,U^* = \operatorname{Tr}_{\mathcal{E}} U(X \otimes |\eta\rangle\langle\eta|)U^*.$$

□

Remark 3.20 (Complete positivity of quantum channels)**.** First we give a mathematical motivation of complete positivity that will follow from Proposition 3.39 in the next Section 3.2. Namely, completely positive maps characterise automorphisms of the $\mathcal{PSD}$ cone. Consequently, completely positive maps can be seen as generalizations of unitaries in Kadison's theorem 2.8.

Next we give the motivation behind complete positivity that is usually found in physics textbooks. A quantum evolution map (or a quantum operation) $\Phi\colon B(\mathcal{H}) \to B(\mathcal{H})$ maps density matrices to density matrices. When Φ is linear, this assumption is equivalent to the map being positive and trace preserving. When Φ is extended with an identity on the environment $\mathcal{E}$, then $\Phi \otimes \mathrm{Id}_{B(\mathcal{E})}\colon B(\mathcal{H} \otimes \mathcal{E}) \to B(\mathcal{H} \otimes \mathcal{E})$ is also required to be a quantum operation, thus it should be positive. If $\dim \mathcal{H} \le \dim \mathcal{E}$, this is equivalent to complete positivity of Φ by Choi's theorem 3.9 and Corollary 3.11.

Finally we present a more elaborate motivation for complete positivity that is phisically more natural, since it relates to unitary (time) evolutions (see Subsection 2.1.2) of a composite system $\mathcal{H} \otimes \mathcal{E}$. Our aim is to describe the evolution of an initial $\mathcal{H}$-marginal $\sigma \mapsto \Phi(\sigma)$ (i.e., σ is the initial state of subsystem $\mathcal{H}$ and $\Phi(\sigma)$ is its terminal state) in terms of a CPTP map Φ acting on $B(\mathcal{H})$. Assume first that a unitary U is acting on the global space $\mathcal{H} \otimes \mathcal{E}$ and it is of the form $U = V \otimes W$, where V and W are unitary operators on $\mathcal{H}$ and $\mathcal{E}$ respectively. Moreover, assume that $\psi = \xi \otimes \eta$ is a product state vector. Then, the evolution of the subsystem $\mathcal{H}$ is the action $\sigma \mapsto V\sigma V^*$, where $\sigma = \operatorname{Tr}_{\mathcal{E}}(|\psi\rangle\langle\psi|) = |\xi\rangle\langle\xi|$ and $V\sigma V^* = \operatorname{Tr}_{\mathcal{E}}(U\,|\psi\rangle\langle\psi|\,U^*)$ (see Subsection 2.2.2 for the definition of the partial trace). In the language of state vectors this evolution of the subsystem $\mathcal{H}$ is given by $\xi \mapsto V\xi$. On the other hand, when U is not a product of two unitaries, the terminal $\mathcal{H}$-marginal of an initial pure separable state may be a mixed state, as discussed in (2.15). Therefore, we need to generalize the above product unitary evolution $\xi \otimes \eta \mapsto U(\xi \otimes \eta)$ of $\mathcal{H} \otimes \mathcal{E}$ and its "shadow" evolution $\xi \mapsto V\xi$ of $\mathcal{H}$. In order to achieve this, for a given unitary U acting on $\mathcal{H} \otimes \mathcal{E}$, we fix an $\eta \in \mathcal{E}$ and define the isometry

$$\begin{aligned} V\colon \mathcal{H} &\longrightarrow \mathcal{H} \otimes \mathcal{E} \\ \xi &\mapsto U(\xi \otimes \eta). \end{aligned}$$

Then the evolution of the $\mathcal{H}$-marginal is by Stinespring's theorem 3.18 equal to

$$\sigma = |\xi\rangle\langle\xi| \mapsto \operatorname{Tr}_{\mathcal{E}} V\sigma V^*.$$

In a specified orthonormal basis $\{\vartheta_i\}$ of $\mathcal{E}$, there exist operators $A_i \in B(\mathcal{H})$ such that V can be represented as $V\xi = \sum_i (A_i\xi) \otimes \vartheta_i$. This implies

$$V\sigma V^* = \sum_{i,j} \left(A_i |\xi\rangle\langle\xi| A_j^*\right) \otimes \left|\vartheta_i\middle\rangle\middle\langle\vartheta_j\right|,$$

and moreover

$$\operatorname{Tr}_{\mathcal{E}} V\sigma V^* = \sum_{i,j} \left(A_i |\xi\rangle\langle\xi| A_j^*\right) \operatorname{Tr} \left|\vartheta_i\middle\rangle\middle\langle\vartheta_j\right| = \sum_i A_i |\xi\rangle\langle\xi| A_i^*.$$

Thus we found a description of the evolution of the subsystem $\mathcal{H}$ which is intrinsic to $\mathcal{H}$,

$$\Phi\colon \sigma \mapsto \sum_i A_i \sigma A_i^*,$$

and by Choi's theorem 3.9 it corresponds to a completely positive map on $B(\mathcal{H})$. Furthermore, since $\xi \mapsto V\xi = \sum_i (A_i\xi) \otimes \vartheta_i$ is an isometry, it holds

$$\langle\xi|\xi\rangle = \langle V\xi|V\xi\rangle = \sum_{i,j} \left\langle A_i\xi\middle|A_j\xi\right\rangle \left\langle\vartheta_i\middle|\vartheta_j\right\rangle = \sum_i \langle A_i\xi|A_i\xi\rangle = \langle\xi|\sum_i A_i^* A_i|\xi\rangle$$

for all $\xi \in \mathcal{H}$. This proves that V is an isometry if and only if $\sum_i A_i^* A_i = I_{\mathcal{H}}$, which is by Lemma 3.17 equivalent to Φ being trace preserving.

In the next examples we list the most common and important families of quantum channels and superoperators. We explain their properties and their relevance in quantum information theory. (If convenient, we will omit the trace preserving condition.)

Example 3.21 (Unitary channels). *Unitary channels* are the completely positive isometries of the set of states $\mathrm{D}(\mathbb{C}^d) \subset B(\mathbb{C}^d)$ of the form $\rho \mapsto U\rho U^*$ for some unitary $U \in \mathrm{U}(d)$. Recall that we identified these maps in Kadison's theorem 2.8, they are the affine maps that globally preserve $\mathrm{D}(\mathbb{C}^d)$.

Example 3.22 (Mixed-unitary channels). A quantum channel $\Phi\colon B(\mathbb{C}^d) \to B(\mathbb{C}^d)$ which is a convex combination of unitary channels is a *mixed-unitary channel*. In other words, Φ is of the form

$$\Phi(\rho) = \sum_{i=1}^{N} \lambda_i U_i \rho U_i^*,$$

where $U_i \in \mathrm{U}(d)$ and $\lambda_i \geq 0$ such that $\sum_{i=1}^N \lambda_i = 1$. It follows directly from the definition that mixed-unitary channels are unital. For $d = 2$ the converse implication is also true.

Proposition 3.23. *A unital quantum channel $\Phi\colon B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ is a mixed-unitary channel.*

Proof. We break the proof into three parts. (i) We claim that it is enough to prove the proposition for channels that are diagonal with respect to the basis of Pauly matrices (2.1). As explained on page 14, $\rho \in \mathrm{M}_2^{\mathrm{sa}}$ is a state if and only if it is of the form

$$\rho = \frac{1}{2} I + a_x \cdot \frac{1}{\sqrt{2}} \sigma_x + a_y \cdot \frac{1}{\sqrt{2}} \sigma_y + a_z \cdot \frac{1}{\sqrt{2}} \sigma_z \text{ with } a_x^2 + a_y^2 + a_z^2 \leq \frac{1}{2}.$$

Since Φ is unital, it preserves the center of the Bloch ball. Then $\Phi(\rho)$ is the state

$$\Phi(\rho) = \frac{1}{2} I + a_x \cdot \frac{1}{\sqrt{2}} \Phi(\sigma_x) + a_y \cdot \frac{1}{\sqrt{2}} \Phi(\sigma_y) + a_z \cdot \frac{1}{\sqrt{2}} \Phi(\sigma_z)$$

with

$$\begin{aligned} \Phi(\sigma_x) &= \varphi_{xx}\sigma_x + \varphi_{yx}\sigma_y + \varphi_{zx}\sigma_z \\ \Phi(\sigma_y) &= \varphi_{xy}\sigma_x + \varphi_{yy}\sigma_y + \varphi_{zy}\sigma_z \\ \Phi(\sigma_z) &= \varphi_{xz}\sigma_x + \varphi_{yz}\sigma_y + \varphi_{zz}\sigma_z \end{aligned}$$

defining a contraction in the basis of Pauli matrices

$$\begin{bmatrix} \varphi_{xx} & \varphi_{xy} & \varphi_{xz} \\ \varphi_{yx} & \varphi_{yy} & \varphi_{yz} \\ \varphi_{zx} & \varphi_{zy} & \varphi_{zz} \end{bmatrix}, \tag{3.7}$$

or equivalently, a contraction of the Bloch ball. Therefore we can diagonalize Φ (i.e., $\Phi(I) = I$, $\Phi(\sigma_x) = a\sigma_x$, $\Phi(\sigma_y) = b\sigma_y$, $\Phi(\sigma_z) = c\sigma_z$ for some $a, b, c \in \mathbb{R}$) by composing it with the map $X \mapsto UXU^*$ for $U \in \mathrm{U}(2)$, where U corresponds to the rotation of the Bloch sphere, which is induced by the contraction in (3.7) with eigenvalues a, b, c.

(ii) Next we define a superoperator on $B(\mathbb{C}^2)$ that is unital and acts diagonally on Pauli matrices. For

$$\Phi = \frac{1}{2}\left(|I\rangle\langle I| + a\,|\sigma_x\rangle\langle\sigma_x| + b\,\big|\sigma_y\big\rangle\big\langle\sigma_y\big| + c\,|\sigma_z\rangle\langle\sigma_z|\right)$$

we can show that it is completely positive if and only if $(a+b)^2 \leq (1+c)^2$ and $(a-b)^2 \leq (1-c)^2$. Indeed, we explicitly write the Choi matrix (3.2) and use Choi's theorem 3.9. It is straightforward to verify that

$$C(\Phi) = \frac{1}{2}\begin{bmatrix} 1+c & 0 & 0 & a+b \\ 0 & 1-c & a-b & 0 \\ 0 & a-b & 1-c & 0 \\ a+b & 0 & 0 & 1+c \end{bmatrix}$$

is positive semi-definite if and only a, b, c satisfy the above inequalities.

(iii) Finally, observe that

$$\begin{aligned} \left\{(a,b,c) \in \mathbb{R}^3 : (a+b)^2 \leq (1+c)^2 \text{ and } (a-b)^2 \leq (1-c)^2\right\} &= \\ \operatorname{conv}\{(1,1,1),(1,-1,-1),(-1,1,-1),(-1,-1,1)\} &= \\ \left\{\lambda_1(1,1,1) + \lambda_2(1,-1,-1) + \lambda_3(-1,1,-1) + \lambda_4(-1,-1,1) : \lambda_i \geq 0 \text{ and } \sum \lambda_i = 1\right\}. \end{aligned}$$

This implies that Φ acts on $X = h_I I + h_x\sigma_x + h_y\sigma_y + h_z\sigma_z$ as

$$\begin{array}{rcc}
\Phi(X) & = & h_I I + h_x a\,\sigma_x + h_y b\,\sigma_y + h_z c\,\sigma_z \\
& = & h_I I + h_x(\lambda_1{+}\lambda_2{-}\lambda_3{-}\lambda_4)\sigma_x + h_y(\lambda_1{-}\lambda_2{+}\lambda_3{-}\lambda_4)\sigma_y + h_z(\lambda_1{-}\lambda_2{-}\lambda_3{+}\lambda_4)\sigma_z \\
& = & \lambda_1 X + \lambda_2(h_I I{+}h_x\sigma_x{-}h_y\sigma_y{-}h_z\sigma_z) \\
& & +\,\lambda_3(h_I I{-}h_x\sigma_x{+}h_y\sigma_y{-}h_z\sigma_z) + \lambda_4(h_I I{-}h_x\sigma_x{-}h_y\sigma_y{+}h_z\sigma_z) \\
& = & \lambda_1 X + \lambda_2\,\sigma_x X\sigma_x + \lambda_3\,\sigma_y X\sigma_y + \lambda_4\,\sigma_z X\sigma_z,
\end{array}$$

which concludes the proof that Φ is mixed-unitary with $U_1 = I$, $U_2 = \sigma_x$, $U_3 = \sigma_y$, $U_4 = \sigma_z$. □

Example 3.24 (Depolarizing and dephasing channels)**.** The *completely depolarizing channel* is by definition

$$\begin{array}{rcl}
R\colon B(\mathbb{C}^d) & \longrightarrow & B(\mathbb{C}^d) \\
X & \mapsto & \frac{1}{d}\operatorname{Tr} X\, I.
\end{array}$$

Since R maps every state to a maximally mixed state, it is also called the *completely randomizing channel*. A *depolarizing channel* is a quantum channel in the family $R_\lambda = \lambda I + (1-\lambda)R$ for $-\frac{1}{d^2-1} \le \lambda \le 1$. The *completely dephasing channel* $D\colon B(\mathbb{C}^d) \to B(\mathbb{C}^d)$ maps any operator (in a specified basis) into its diagonal part.

The following lemma connects depolarizing channels with the isotropic states defined in Example 2.21.

Lemma 3.25. *The Choi matrix of the depolarizing channel R_λ is $d\rho_\lambda$, where ρ_λ is the isotropic state.*

Proof. The proof will follow from the Choi matrix written in the form (3.4). We get $C(R_\lambda) = \big(R_\lambda \otimes \mathrm{Id}_{B(\mathbb{C}^d)}\big)\,(|\chi\rangle\langle\chi|)$, where $|\chi\rangle = \sum_i |ii\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$. Then,

$$\begin{array}{rcc}
C(R_\lambda) & = & \big(R_\lambda \otimes \mathrm{Id}_{B(\mathbb{C}^d)}\big)\left(\sum_{i,j} |i\rangle\langle j| \otimes |i\rangle\langle j|\right) \\
& = & \lambda \sum_{i,j} |i\rangle\langle j| \otimes |i\rangle\langle j| + \frac{1-\lambda}{d}\sum_i I_2 \otimes |i\rangle\langle i| \\
& = & \lambda\,|\chi\rangle\langle\chi| + (1-\lambda)\frac{1}{d}\sum_i I_4,
\end{array}$$

which is an isotropic state (defined in Example 2.21) on $\mathbb{C}^d \otimes \mathbb{C}^d$ multiplied by d. □

Example 3.26 (Quantum-classical and classical-quantum channels)**.** Recall the definition of POVMs (positive operator-valued measures) in Remark 2.7. A POVM on $\mathcal{H}$ is a finite family of positive semidefinite operators $\{M_i\}$ with the property $\sum_{i=1}^N M_i = I_{\mathcal{H}}$. For a given POVM we define its *quantum-classical channel* (or q-c channel) by

$$\begin{array}{rcl}
\Phi\colon B(\mathcal{H}) & \longrightarrow & B(\mathbb{C}^N) \\
\rho & \mapsto & \sum_{i=1}^N \operatorname{Tr}(M_i\rho)\,|i\rangle\langle i|.
\end{array}$$

Its dual concept is a *classical-quantum channel* (or c-q channel), defined for a finite family of states ρ_i on $\mathcal{H}$,

$$\begin{aligned} \Psi\colon B(\mathbb{C}^N) &\longrightarrow \quad B(\mathcal{H}) \\ \rho \quad &\mapsto \sum_{i=1}^{N} \rho_i \langle i|\rho|i\rangle \,. \end{aligned}$$

The next lemma explicitly assigns a c-q channel to a unital q-c channel.

Lemma 3.27. *Let Φ be a q-c channel associated to a POVM $\{M_i\}$. When $\operatorname{Tr} M_i = 1$ for all i, the q-c channel Φ is unital. The dual of a unital q-c channel is a c-q channel.*

Proof. The condition $\operatorname{Tr} M_i = 1$ implies $\Phi(I_{\mathcal{H}}) = \sum_{i=1}^{N} \operatorname{Tr}(M_i)\,|i\rangle\langle i| = I_N$, and in particular $\dim \mathcal{H} = N$. From the definition of the dual superoperator Φ^*,

$$\langle \rho_{\mathbb{C}^N}, \Phi(\rho_{\mathcal{H}})\rangle_{\mathrm{HS}} = \langle \Phi^*(\rho_{\mathbb{C}^N}), \rho_{\mathcal{H}}\rangle_{\mathrm{HS}},$$

for $\rho_{\mathbb{C}^N} \in B(\mathbb{C}^N)$ and $\rho_{\mathcal{H}} \in B(\mathcal{H})$, we can directly compute $\Phi^*(\rho_{\mathbb{C}^N}) = \sum_{i=1}^{N} M_i \langle i|\rho_{\mathbb{C}^N}|i\rangle$. □

Example 3.28 (Entanglement breaking maps)**.** A completely positive map $\Phi \in \boldsymbol{CP}(\mathcal{H}^{\mathrm{in}}, \mathcal{H}^{\mathrm{out}})$ is *entanglement breaking* if, for any $d \in \mathbb{N}$ and any positive operator $X \in B^{\mathrm{sa}}(\mathcal{H}^{\mathrm{in}} \otimes \mathbb{C}^d)$, the operator

$$\left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_d}\right)(X) \in \mathcal{SEP}(\mathcal{H}^{\mathrm{out}} \otimes \mathbb{C}^d)$$

is in the cone of separable operators (2.10). In review, the definition involves the following operators:

$$\begin{aligned} \text{completely positive } \Phi\colon \quad B(\mathcal{H}^{\mathrm{in}}) &\longrightarrow B(\mathcal{H}^{\mathrm{out}}), \\ \text{positive } X\colon \quad \mathcal{H}^{\mathrm{in}} \otimes \mathbb{C}^d &\longrightarrow \mathcal{H}^{\mathrm{in}} \otimes \mathbb{C}^d, \\ \text{separable } \left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_d}\right)(X)\colon \mathcal{H}^{\mathrm{out}} \otimes \mathbb{C}^d &\longrightarrow \mathcal{H}^{\mathrm{out}} \otimes \mathbb{C}^d \,. \end{aligned}$$

The following lemma characterizes entanglement breaking maps.

Lemma 3.29. *For a completely positive map $\Phi\colon B(\mathcal{H}^{in}) \to B(\mathcal{H}^{out})$ the following descriptions are equivalent:*

1. *Φ is an entanglement breaking map.*

2. *The Choi matrix $C(\Phi)$ is a separable operator on $\mathcal{H}^{out} \otimes \mathcal{H}^{in}$.*

3. *All the operators in the Kraus decomposition of Φ have rank 1.*

Proof. The implication 1. $\Longrightarrow$ 2. follows from the form (3.4) of the Choi matrix. In a fixed basis $\{e_i\}$ of $\mathcal{H}^{\mathrm{in}}$ it holds $C(\Phi) = \left(\Phi \otimes \mathrm{Id}_{B(\mathcal{H}^{\mathrm{in}})}\right)(|\chi\rangle\langle\chi|)$, where $\chi = \sum_i e_i \otimes e_i \in \mathcal{H}^{\mathrm{in}} \otimes \mathcal{H}^{\mathrm{in}}$. If we identify $\mathcal{H}^{\mathrm{in}}$ with $\mathbb{C}^d$ in the definition of an entanglement breaking map, it follows immediately that $C(\Phi)$ lies in the separable cone $\mathcal{SEP}\left(\mathcal{H}^{\mathrm{out}} \otimes \mathcal{H}^{\mathrm{in}}\right)$. For the implication 2. $\Longrightarrow$ 3. we write $C(\Phi) = \sum |x_i \otimes y_i\rangle\langle x_i \otimes y_i|$ for some $x_i \in \mathcal{H}^{\mathrm{out}}$ and $y_i \in \mathcal{H}^{\mathrm{in}}$; then we repeat the proof of the analogous implication in Choi's theorem 3.9. The final implication 3. $\Longrightarrow$ 1. is obtained from the following fact: for a rank one operator $G_i = \left|g^{\mathrm{out}}\right\rangle\!\left\langle g^{\mathrm{in}}\right| \in B\left(\mathcal{H}^{\mathrm{in}}, \mathcal{H}^{\mathrm{out}}\right)$, we define

$$B_i = \left|g^{\mathrm{in}}\right\rangle\!\left\langle g^{\mathrm{in}}\right| \in B\left(\mathcal{H}^{\mathrm{in}}\right) \text{ and } A_i = \left|g^{\mathrm{out}}\right\rangle\!\left\langle g^{\mathrm{out}}\right| \in B\left(\mathcal{H}^{\mathrm{out}}\right),$$

and verify that for any $Y \in B(\mathcal{H}^{\text{in}})$,

$$G_i Y G_i^* = \left|g^{\text{out}}\middle\rangle\!\middle\langle g^{\text{in}}\right| Y \left|g^{\text{in}}\middle\rangle\!\middle\langle g^{\text{out}}\right| = \operatorname{Tr}\left(\left|g^{\text{in}}\middle\rangle\!\middle\langle g^{\text{in}}\right| Y\right) \left|g^{\text{out}}\middle\rangle\!\middle\langle g^{\text{out}}\right| = \operatorname{Tr}(B_i Y) A_i.$$

Consequently, for any positive operator $X \in B^{\text{sa}}(\mathcal{H}^{\text{in}} \otimes \mathbb{C}^d)$ it holds that

$$\left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_d}\right)(X) = \sum_i A_i \otimes \operatorname{Tr}_{\mathcal{H}^{\text{in}}}\left[\left(B_i^{1/2} \otimes I\right) X \left(B_i^{1/2} \otimes I\right)\right]$$

is a separable operator in the separable cone $\mathcal{SEP}(\mathcal{H}^{\text{out}} \otimes \mathbb{C}^d)$. □

Entanglement breaking quantum channels are sometimes called *super-positive maps*. The proofs in Lemma 3.27 and Lemma 3.29 show that a quantum channel is entanglement breaking if and only if it can be written as the composition of a q-c channel with a c-q channel. For this reason, entanglement breaking quantum channels are also called *q-c-q channels*.

Let Φ, Ψ be completely positive maps and let Φ be entanglement breaking. We can write $\Phi \otimes \Psi = (\mathrm{Id} \otimes \Psi) \circ (\Phi \otimes \mathrm{Id})$, and use the fact that the product superoperator $\mathrm{Id} \otimes \Psi$ maps the separable cone to the separable cone. This proves the next corollary.

Corollary 3.30 (Once broken, always broken). *If one of the two completely positive maps Φ, Ψ is entanglement breaking, then $(\Phi \otimes \Psi)(X) \in \mathcal{SEP}$ for any positive operator X.*

We conclude the survey of entanglement breaking maps with an open problem.

Conjecture 3.31 (Christandl's conjecture). A superoperator $\Phi\colon \mathrm{M}_d \to \mathrm{M}_d$ is by definition *co-completely positive* (or co-cp) if Φ composed with the transposition T is completely positive. In 2012 Matthias Christandl conjectured that Φ being completely positive and co-completely positive implies that $\Phi \circ \Phi$ is entanglement breaking. Only recently some progress has been made in proving the conjecture [CMHW19], in particular the conjecture holds for $d = 3$.

Example 3.32 (PPT-inducing maps). A completely positive map $\Phi \in \boldsymbol{CP}(\mathcal{H}^{\text{in}}, \mathcal{H}^{\text{out}})$ is called *PPT-inducing* if, for any $d \in \mathbb{N}$ and any positive operator $X \in B^{\text{sa}}(\mathcal{H}^{\text{in}} \otimes \mathbb{C}^d)$, the operator

$$\left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_d}\right)(X) \text{ has positive partial transpose.}$$

In the next lemma we give a characterization of PPT-inducing maps in terms of the Choi matrix. Recall Definition 2.29 of the partial transposition Γ and Remark 3.3, stating the relation between the Choi and the Jamiołkowski isomorphisms, $C = \Gamma \circ J$.

Lemma 3.33. *A completely positive map Φ is PPT-inducing if and only if $J(\Phi) = C(\Phi)^\Gamma$ is positive semidefinite.*

Proof. If Φ is PPT-inducing, the positive semidefiniteness of $C(\Phi)^\Gamma$ follows directly from (3.4). Conversely, if $C(\Phi)^\Gamma$ is positive semidefinite, it is by the spectral theorem enough to verify that $\left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_d}\right)(|\psi\rangle\langle\psi|)$ has a positive partial transpose for every $\psi \in \mathcal{H}^{\text{in}} \otimes \mathbb{C}^d$. We connect ψ to the basis of the Choi matrix as follows: there exists $B \in B(\mathcal{H}^{\text{in}}, \mathbb{C}^d)$ such that $\psi = (I \otimes B)\chi$, where $\chi = \sum e_i \otimes e_i \in \mathcal{H}^{\text{in}} \otimes \mathcal{H}^{\text{in}}$. This implies that

$$\left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_d}\right)(|\psi\rangle\langle\psi|) = \left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_d}\right)((I \otimes B)\,|\chi\rangle\langle\chi|\,(I \otimes B^*)) = (I \otimes B) C(\Phi)(I \otimes B^*)$$

has a positive partial transpose (in the last equality we used (3.4) to obtain the Choi matrix $C(\Phi)$). □

The next families of quantum channels are characterized by their particular Kraus decompositions.

Example 3.34 (Schur channels). The *Schur product* $A \odot B$ of two same-dimensional matrices $A = \left[A_{ij}\right]_{i,j=1}^{d}$, $B = \left[B_{ij}\right]_{i,j=1}^{d} \in \mathrm{M}_d$ is defined by componentwise multiplication $(A \odot B)_{ij} = A_{ij}B_{ij}$. Then, for any given matrix $A \in \mathrm{M}_d$, the induced map

$$\begin{aligned} \Theta_A \colon \mathrm{M}_d &\longrightarrow \mathrm{M}_d \\ X &\mapsto A \odot X \end{aligned}$$

is called a *Schur multiplier*. When A is positive semidefinite and $A_{ii} = 1$ for $i = 1, \ldots, d$, the corresponding Schur multiplier Θ_A is a quantum channel called a *Schur channel*.

We remark that $A \odot B$ can be seen as a submatrix in $A \otimes B$. From this it can be shown that if A and B are being positive semidefinite, then also $A \odot B$ is positive semidefinite. Additionally, we can write $\Theta_A \otimes \mathrm{Id}_{\mathrm{M}_k} = \Theta_{A \otimes J}$, where J is the $k \times k$ matrix of ones. This shows that the following statements are equivalent (and consequently Schur channels are well defined):

1. A is a positive semidefinite matrix,
2. Θ_A is positive,
3. Θ_A is completely positive.

Alternatively, Schur channels can be defined as quantum channels with diagonal operators in their Kraus decomposition (3.5).

Lemma 3.35. *A quantum channel $\Phi \colon \mathrm{M}_d \to \mathrm{M}_d$ is a Schur operator if and only if it admits a Kraus decomposition with diagonal operators.*

Proof. The lemma follows from the next observations. Given an $a \in \mathbb{C}^d$, define the diagonal matrix D_a with a's entries along the diagonal. Then $A = |a\rangle\langle a|$ defines a completely positive Θ_A. Moreover, for all $X \in \mathrm{M}_d$ the following equality holds $D_a X D_a^* = \Theta_{|a\rangle\langle a|}(X)$. □

Example 3.36 (Separable superoperators). Let now $\mathcal{H}^{\mathrm{in}} = \mathcal{H}_1^{\mathrm{in}} \otimes \mathcal{H}_2^{\mathrm{in}}$ and $\mathcal{H}^{\mathrm{out}} = \mathcal{H}_1^{\mathrm{out}} \otimes \mathcal{H}_2^{\mathrm{out}}$ be bipartite Hilbert spaces. A map $\Phi \in \boldsymbol{CP}(\mathcal{H}^{\mathrm{in}}, \mathcal{H}^{\mathrm{out}})$ is said to be *separable* if it admits a Kraus decomposition consisting of product operators. This means, there exist $A_{1,i} \colon \mathcal{H}_1^{\mathrm{in}} \to \mathcal{H}_1^{\mathrm{out}}$ and $A_{2,i} \colon \mathcal{H}_2^{\mathrm{in}} \to \mathcal{H}_2^{\mathrm{out}}$ such that for all $X \in B(\mathcal{H}^{\mathrm{in}})$,

$$\Phi(X) = \sum_{i=1}^{N} \left(A_{1,i} \otimes A_{2,i}\right) X \left(A_{1,i} \otimes A_{2,i}\right)^* .$$

For the sake of completeness we name another important class of separable operators called the LOCC channels (Local Operations and Classical Communication). We will not define the LOCC channels in this thesis, we only mention that they are placed between the separable and product channels:

$$\operatorname{conv}\{\text{product channels}\} \subset \{\text{LOCC channels}\} \subset \{\text{separable channels}\}.$$

The LOCC channels are connected to the famous distillability problem, one of the most important open problems connected to entanglement. For more on the distillability problem and other properties of the LOCC family see [AS17, Section 12.2].

Example 3.37 (Direct sums)**.** It is also possible to construct quantum channels on direct sums of Hilbert spaces. Let $\Phi_1 \colon B(\mathcal{H}_1^{\text{in}}) \to B(\mathcal{H}_1^{\text{out}})$ and $\Phi_2 \colon B(\mathcal{H}_2^{\text{in}}) \to B(\mathcal{H}_2^{\text{out}})$ be two quantum channels. Their *direct sum* is the quantum channel defined on the block operators as

$$\begin{aligned} \Phi_1 \oplus \Phi_2 \colon B(\mathcal{H}_1^{\text{in}} \oplus \mathcal{H}_2^{\text{in}}) &\longrightarrow \quad B(\mathcal{H}_1^{\text{out}} \oplus \mathcal{H}_2^{\text{out}}) \\ \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix} &\mapsto \begin{bmatrix} \Phi_1(X_{11}) & 0 \\ 0 & \Phi_2(X_{22}) \end{bmatrix}. \end{aligned}$$

A straightforward calculation shows that, if $\left\{A_{1,i}\right\}$ and $\left\{A_{2,i}\right\}$ are the Kraus operators corresponding to the Kraus decompositions of Φ_1 and Φ_2 respectively, then

$$\left\{A_{1,i} \otimes I\right\} \cup \left\{I \otimes A_{2,i}\right\}$$

are the Kraus operators for $\Phi_1 \oplus \Phi_2$.

3.2 Cones of QIT

In this section we give a summary of the cones and their bases considered in Chapters 2 and 3. Moreover, we construct an inclusion hierarchy of the relevant cones. We will denote a generic cone of operators by $\mathcal{C}$ and a generic cone of superoperators by $\boldsymbol{C}$. To each cone of superoperators $\boldsymbol{C}$ we will associate the cone of operators $\mathcal{C}$, which consists of the Choi matrices of maps in $\boldsymbol{C}$.

3.2.1 Cones of operators

Given a Hilbert space $\mathcal{H}$, a cone of operators $\mathcal{C}$ lies in the real vector space $B^{\text{sa}}(\mathcal{H})$ of self-adjoint operators. For the vector defining the base of $\mathcal{C}$ in (2.7) we always select $\mathsf{e} = \rho^* = \frac{1}{\dim \mathcal{H}} I$, the maximally mixed state (2.5). Recall that the notion of separability and the PPT property (considered in Section 2.2 and Section 2.3 respectively) are defined on bipartite spaces with respect to a fixed partition $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$.

The fundamental cone in this thesis is the $\mathcal{PSD}$ cone of positive semidefinite matrices, where its associated base D is the convex set of states (see Subsection 2.1.3 and Figure 2.1). We define the cone of co-PSD states by

$$\text{co-}\mathcal{PSD} := \Gamma(\mathcal{PSD}) = \left\{\rho \in B^{\text{sa}}(\mathcal{H}) \colon \rho^\Gamma \in \mathcal{PSD}\right\}, \tag{3.8}$$

where Γ is the partial transposition from Definition 2.29. By the the PPT criterion in Proposition 2.34 we have,

$$\text{Sep} \subset \text{PPT} = \text{D} \cap \Gamma(\text{D}),$$

as illustrated on Figure 2.5. The convex set of separable states Sep gives rise to (after dropping the trace one constraint) the separable cone $\mathcal{SEP}$. Analogously, the convex set of states with positive partial transpose PPT is the base of the $\mathcal{PPT}$ cone. Then, on the level of cones, we can write

$$\mathcal{SEP} \subset \mathcal{PPT} = \text{co-}\mathcal{PSD} \cap \mathcal{PSD}\,. \tag{3.9}$$

In quantum computation it is standard to take $\mathcal{H} = \mathbb{C}^m \otimes \mathbb{C}^n$ with the computational basis $\{|ij\rangle\}$, and represent the operators in $B^{\text{sa}}(\mathcal{H})$ as block matrices of the form $M = \left[M_{ij}\right]_{i,j=1}^m$, where $\mathrm{M}_{ij} \in \mathrm{M}_n$ (as explained in (1.2)).

For the sake of completeness we define the cone of block-positive matrices $\mathcal{BP}$. We say that a block matrix $M = \left[M_{ij}\right]_{i,j=1}^{m}$ is *block-positive* if

$$\sum_{i,j=1}^{m} \overline{\xi_i}\xi_j M_{ij} \in \mathcal{PSD}(\mathbb{C}^n) \tag{3.10}$$

for all $\xi = (\xi_1, \ldots, \xi_m) \in \mathbb{C}^m$. The extreme points of the convex set Sep are generated by pure separable states $|\xi \otimes \eta\rangle\langle\xi \otimes \eta|$ (see the discussion after Definition 2.16). After dropping the trace constraint, we can view $|\xi \otimes \eta\rangle\langle\xi \otimes \eta|$ as the extreme rays of the $\mathcal{SEP}$ cone. This implies that,

$$\begin{gathered} M \in \mathcal{SEP}^* \\ \Longleftrightarrow \\ \operatorname{Tr}(M\,|\xi \otimes \eta\rangle\langle\xi \otimes \eta|) \geq 0 \text{ for all } \xi \in \mathbb{C}^m \text{ and all } \eta \in \mathbb{C}^n \\ \Longleftrightarrow \\ \text{the block matrix } M \text{ is block-positive,} \end{gathered} \tag{3.11}$$

where * stands for the dual cone (2.6) and the last equivalence follows from

$$\langle\xi \otimes \eta|M|\xi \otimes \eta\rangle = \langle\eta|\sum_{i,j=1}^{m} \overline{\xi_i}\xi_j M_{ij}|\eta\rangle\,.$$

Thus we proved $\mathcal{SEP}^* = \mathcal{BP}$. Since $\mathcal{PSD}$ and co-$\mathcal{PSD}$ are both self-dual cones, inclusion (3.9) can be rephrased as

$$\mathcal{PPT}^* = \text{co-}\mathcal{PSD} + \mathcal{PSD} \subset \mathcal{BP}. \tag{3.12}$$

We summarize the relations among the cones in $B^{\mathrm{sa}}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ in Table 3.1. (A bird's-eye view of the inclusions $\mathcal{SEP}(\mathbb{C}^m \otimes \mathbb{C}^n) \subset \mathcal{PSD}(\mathbb{C}^m \otimes \mathbb{C}^n) \subset \mathcal{BP}(\mathbb{C}^m \otimes \mathbb{C}^n)$ in $B^{\mathrm{sa}}(\mathbb{C}^m \otimes \mathbb{C}^n)$ is illustrated in Figure 3.1.)

	cone $\mathcal{C}$	base $\mathcal{C}^{\mathrm{b}}$	dual cone $\mathcal{C}^*$
block positive	$\mathcal{BP}$	BP	$\mathcal{SEP}$
decomposable	co-$\mathcal{PSD}+\mathcal{PSD}$	$\mathrm{conv}(\mathrm{D} \cup \Gamma(\mathrm{D}))$	$\mathcal{PPT}$
positive	$\mathcal{PSD}$	D	$\mathcal{PSD}$
PPT	$\mathcal{PPT}$	PPT	co-$\mathcal{PSD}+\mathcal{PSD}$
separable	$\mathcal{SEP}$	Sep	$\mathcal{BP}$

Table 3.1. The cones of operators: each cone is included in the cones above it, and each dual cone is included in the dual cones below it.

3.2.2 Cones of superoperators

On the level of superoperators, we consider self-adjointness-preserving maps in Subsection 3.1.3 acting from $B^{\mathrm{sa}}(\mathcal{H})$ to $B^{\mathrm{sa}}(\mathcal{K})$. The corresponding cones $\boldsymbol{C}(\mathcal{H}, \mathcal{K})$ lie in the real vector space $B(B^{\mathrm{sa}}(\mathcal{H}), B^{\mathrm{sa}}(\mathcal{K}))$; we denote the cones as $\boldsymbol{C}(\mathcal{H})$ when $\mathcal{H} = \mathcal{K}$, or simply by $\boldsymbol{C}$ when there is no ambiguity about the underlying Hilbert spaces.

Recall Definition 3.1 of a positive or positivity preserving linear map $\Phi\colon B(\mathcal{H}) \to B(\mathcal{K})$. In the language of operator cones, Φ is positivity preserving if $\Phi(\mathcal{PSD}(\mathcal{H})) \subset \mathcal{PSD}(\mathcal{K})$. Obviously, the set of positivity preserving linear maps is a cone in $B\left(B(\mathcal{H}), B(\mathcal{K})\right)$, which we denote by $\boldsymbol{P}(\mathcal{H},\mathcal{K})$. On page 38 we showed that $\Phi\colon B(\mathcal{H}) \to B(\mathcal{K})$ is positivity preserving if and only if its adjoint $\Phi^*\colon B(\mathcal{K}) \to B(\mathcal{H})$ is positivity preserving. In the language of superoperator cones, $\Phi \in \boldsymbol{P}(\mathcal{H},\mathcal{K})$ if and only if $\Phi^* \in \boldsymbol{P}(\mathcal{K},\mathcal{H})$. However, from this it would be wrong to conclude that $\boldsymbol{P}$ is a self-dual cone.

The most fundamental cone of superoperators in quantum information theory is the $\boldsymbol{CP}$ cone of completely positive maps, giving rise to quantum channels (see Definition 3.1 and Definition 3.16). In Choi's theorem 3.9 we proved that $\Phi\colon \mathrm{M}_m^{\mathrm{sa}} \to \mathrm{M}_n^{\mathrm{sa}}$ is completely positive if and only if its Choi Matrix $C(\Phi)\colon \mathbb{C}^n \otimes \mathbb{C}^m \to \mathbb{C}^n \otimes \mathbb{C}^m$ is positive semidefinite. In the language of cones, $\Phi \in \boldsymbol{CP}(\mathbb{C}^m, \mathbb{C}^n)$ if and only if $C(\Phi) \in \mathcal{PSD}(\mathbb{C}^n \otimes \mathbb{C}^m)$. This leads to the following lemma.

Lemma 3.38. *The completely positive cone $\boldsymbol{CP}$ is self-dual.*

Proof. Self-duality of the $\boldsymbol{CP}$ cone will follow from

$$\boldsymbol{CP}(\mathbb{C}^n, \mathbb{C}^m) = \left\{\Psi \in B\left(\mathrm{M}_n^{\mathrm{sa}}, \mathrm{M}_m^{\mathrm{sa}}\right) : \mathbf{Tr}\left(\Phi \circ \Psi\right) \geq 0 \text{ for all } \Phi \in \boldsymbol{CP}(\mathbb{C}^m, \mathbb{C}^n)\right\},$$

where $\mathbf{Tr}$ denotes the trace on $B\left(\mathrm{M}_n^{\mathrm{sa}}\right)$. By Lemma 3.5, the matrix representations of superoperators $\Phi \in B\left(\mathrm{M}_m^{\mathrm{sa}}, \mathrm{M}_n^{\mathrm{sa}}\right), \Psi \in B\left(\mathrm{M}_n^{\mathrm{sa}}, \mathrm{M}_m^{\mathrm{sa}}\right)$ with respect to the standard bases are equal to $C(\Phi)^R, C(\Psi)^R$ respectively, where R is the realignment. This implies that

$$\mathbf{Tr}\left(\Phi \circ \Psi\right) = \mathrm{Tr}\left(C(\Phi)\, F\, C(\Psi) F^*\right),$$

where $F\colon \mathbb{C}^m \otimes \mathbb{C}^n \to \mathbb{C}^n \otimes \mathbb{C}^m$ is the flip operator from Example 2.22. The statement follows from the self-duality of the $\mathcal{PSD}$ cone. □

Recall the ntanglement breaking maps from Example 3.28. The Choi isomorphism $\Phi \mapsto C(\Phi)$ and Lemma 3.29 induce the association between the cone of entanglement breaking maps,

$$\boldsymbol{EB}\left(\mathbb{C}^m, \mathbb{C}^n\right) = \left\{\Phi \in B\left(\mathrm{M}_m^{\mathrm{sa}}, \mathrm{M}_n^{\mathrm{sa}}\right) : \Phi \text{ is entanglement breaking}\right\}$$

and the separable cone $\mathcal{SEP}(\mathbb{C}^n \otimes \mathbb{C}^m)$.

Similarly, it follows from Lemma 3.33 that the Choi isomorphism relates

$$\boldsymbol{PPT}\left(\mathbb{C}^m, \mathbb{C}^n\right) = \left\{\Phi \in B\left(\mathrm{M}_m^{\mathrm{sa}}, \mathrm{M}_n^{\mathrm{sa}}\right) : \Phi \text{ is PPT-inducing}\right\},$$

the cone of PPT-inducing maps in Example 3.32, to the $\mathcal{PPT}(\mathbb{C}^n \otimes \mathbb{C}^m)$ cone.

For the sake of completeness we relate the cone of decomposable maps $\boldsymbol{DEC}\left(\mathbb{C}^m, \mathbb{C}^n\right)$ to the cone of decomposable matrices in the following way. As stated in Conjecture 3.31, a map $\Phi\colon \mathrm{M}_m^{\mathrm{sa}} \to \mathrm{M}_n^{\mathrm{sa}}$ is by definition *co-completely positive* if $T \circ \Phi \in \boldsymbol{CP}\left(\mathbb{C}^m, \mathbb{C}^n\right)$. Moreover, Φ is said to be *decomposable* if it can be written as a sum of a completely positive and a co-completely positive map. It follows that the correspondence $\Phi \mapsto C(\Phi)$ associates the cone $\boldsymbol{DEC}\left(\mathbb{C}^m, \mathbb{C}^n\right)$ of decomposable maps with the co-$\mathcal{PSD}+\mathcal{PSD}$ cone considered in (3.9) and (3.12). In other words, the Choi matrix of a decomposable map can be written as a sum of a positive semidefinite and a co-positive semidefinite matrix. This follows from Choi's theorem 3.9 and from Remark 3.3,

$$C(T \circ \Phi) = C(\Phi)^{\Gamma}.$$

Finally, we use the Choi isomorphism $\Phi \mapsto C(\Phi)$ to identify the cone of positivity preserving maps $\boldsymbol{P}(\mathbb{C}^m, \mathbb{C}^n)$ with $\mathcal{SEP}^*(\mathbb{C}^n \otimes \mathbb{C}^m) = \mathcal{BP}(\mathbb{C}^n \otimes \mathbb{C}^m)$. This follows from the equivalences in (3.10) and (3.11). Indeed, by (3.3), the alternative Choi matrix is $\tilde{C}(\Phi) = \left[M_{ij}\right]$ for $M_{ij} = \Phi(\left|e_i\middle\rangle\middle\langle e_j\right|)$; furthermore for any $\xi = (\xi_1, \dots, \xi_m) \in \mathbb{C}^m$ it holds $\Phi(|\xi\rangle\langle\xi|) = \sum_{i,j=1}^m \xi_i \overline{\xi_j} M_{ij}$. Consequently,

$$\begin{gathered}\tilde{C}(\Phi) \in \mathcal{SEP}^*(\mathbb{C}^m \otimes \mathbb{C}^n) \\ \Longleftrightarrow \\ \Phi\left(|\xi\rangle\langle\xi|\right) \in \mathcal{PSD}(\mathbb{C}^n) \text{ for all } \xi \in \mathbb{C}^m \\ \Longleftrightarrow \\ \Phi \in \boldsymbol{P}(\mathbb{C}^m, \mathbb{C}^n).\end{gathered} \tag{3.13}$$

In Table 3.2 we summarize the above relations between a cone of superoperators $\boldsymbol{C}$ and the associated cone of operators $\mathcal{C}$, consisting of the Choi matrices of elements in $\boldsymbol{C}$.

	cone $\boldsymbol{C}$	cone $\mathcal{C}$
positivity preserving	$\boldsymbol{P}$	$\mathcal{BP}$
decomposable	$\boldsymbol{DEC}$	co-$\mathcal{PSD} + \mathcal{PSD}$
completely positive	$\boldsymbol{CP}$	$\mathcal{PSD}$
PPT-inducing	$\boldsymbol{PPT}$	$\mathcal{PPT}$
entanglement breaking	$\boldsymbol{EB}$	$\mathcal{SEP}$

Table 3.2. The cones of superoperators: $\Phi \in \boldsymbol{C} \Longleftrightarrow C(\Phi) \in \mathcal{C}$.

We conclude the study of the positive semidefinite cone $\mathcal{PSD}(\mathcal{H}) \subset B^{\mathrm{sa}}(\mathcal{H})$ with a "cone version" of Kadison's theorem 2.8 (stating that unitaries are the only affine maps preserving the set of states $\mathrm{D}(\mathcal{H}) = \mathcal{PSD}^{\mathrm{b}}(\mathcal{H})$). A fundamental consequence is that automorphisms of the $\mathcal{PSD}$ cone must be either completely positive or co-completely positive.

Proposition 3.39 (Characterization of automorphisms of the $\mathcal{PSD}$ cone, [AS17]: Prop. 2.29). *Let $\Phi\colon \mathrm{M}_n^{sa} \to \mathrm{M}_n^{sa}$ be an affine map which satisfies $\Phi(\mathcal{PSD}(\mathbb{C}^n)) = \mathcal{PSD}(\mathbb{C}^n)$. Then Φ is a linear automorphisms of $\mathcal{PSD}(\mathbb{C}^n)$ and is of one of the two possible forms: $\Phi(\rho) = V\rho V^*$ or $\Phi(\rho) = V\rho^T V^*$ for some $V \in \mathrm{GL}(n, \mathbb{C})$. In the first case Φ is completely positive, whereas in the second case Φ is co-completely positive.*

Without proof (for which we would need to use Brouwer's fixed-point theorem) we give a generalization of Proposition 3.39, when Φ is not assumed to be an automorphism of the $\mathcal{PSD}$ cone but is only positivity preserving. Proposition 3.40 characterizes how close a positivity preserving map is to being both unital and trace preserving (see Subsection 3.1.3 for its relation with quantum channels).

Proposition 3.40 (Sinkhorn's normal form for positive maps, [AS17]: Prop. 2.32). *Consider a linear map $\Phi\colon \mathrm{M}_m^{sa} \to \mathrm{M}_n^{sa}$ which is in the interior of the cone of positivity preserving maps $\boldsymbol{P}$. Then there exist positive operators $A \in \mathcal{PSD}(\mathbb{C}^n)$ and $B \in \mathcal{PSD}(\mathbb{C}^m)$ such that the map*

$$\tilde{\Phi}(\rho) = A\Phi(B\rho B)A$$

is trace preserving and maps the maximally mixed state to maximally mixed state (i.e., is unital).

3.3 Entanglement witnesses

This section is devoted to detecting entanglement. We will introduce the concept of entanglement witnesses which detect states that are not separable.

In order to do this, we employ the relations between the cones of operators and superoperators considered in Subsections 3.2.1 and 3.2.2. Equivalence (3.11) yields the identification between the dual cone $\mathcal{SEP}^*$ and $\mathcal{BP}$. Furthermore, equivalence (3.13) identifies $\mathcal{SEP}^*$ with the corresponding cone of superoperators $\boldsymbol{P}$ (via the Choi isomorphism). This can be reformulated as follows.

Proposition 3.41 (Entanglement witnesses). *For $\mathcal{H} = \mathbb{C}^m \otimes \mathbb{C}^n$ and $\rho \in \mathrm{D}(\mathcal{H})$ the following conditions are equivalent:*

1. *state ρ is entangled,*
2. *there exists $\sigma \in \mathcal{SEP}^*(\mathcal{H}) = \mathcal{BP}$ such that $\langle \sigma, \rho \rangle_{HS} = \mathrm{Tr}(\sigma\rho) < 0$,*
3. *there exists a positivity preserving linear map $\Psi\colon \mathrm{M}_n^{sa} \to \mathrm{M}_m^{sa}$ such that $\mathrm{Tr}(C(\Psi)\rho) < 0$.*

Proof. It holds that: ρ is entangled $\iff \rho \notin \mathcal{SEP} \iff$

$$\text{there exists } \sigma \in \mathcal{SEP}^* := \{\sigma_s\colon \langle \sigma_s, \rho_s \rangle_{\mathrm{HS}} \geq 0,\ \forall \rho_s \in \mathcal{SEP}\} \text{ such that } \langle \sigma, \rho \rangle_{\mathrm{HS}} < 0,$$

where the first equivalence is the definition of an entangled state and the second equivalence is the definition of the dual cone. In order to prove 3., we represent σ as the Choi matrix of some positive superoperator which comes from Choi's isomorphism. □

Corollary 3.42 (Horodecki's entanglement witness theorem). *Consider $\mathcal{H} = \mathbb{C}^m \otimes \mathbb{C}^n$. A state ρ on $\mathcal{H}$ is entangled if and only if there exists a positivity preserving map $\Phi\colon \mathrm{M}_m^{sa} \to \mathrm{M}_n^{sa}$ such that the operator $\left(\Phi \otimes Id_{\mathrm{M}_n^{sa}}\right)\rho$ is not positive semidefinite.*

Proof. First we prove the sufficiency implication ($\neg \implies \neg$). Since a separable state ρ is a convex combination of product states by (2.9), it suffices to take $\rho = \tau_m \otimes \tau_n \in \mathrm{M}_m \otimes \mathrm{M}_n$ and observe that $\left(\Phi \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}\right)\rho = \Phi(\tau_m) \otimes \tau_n$ is positive (since Φ is positive). Conversely, for showing the necessity implication ($\implies$), we take the positivity preserving linear map $\Psi\colon \mathrm{M}_n^{\mathrm{sa}} \to \mathrm{M}_m^{\mathrm{sa}}$ from Proposition 3.41. Then, for $\chi = \sum_i |ii\rangle \in \mathbb{C}^m \otimes \mathbb{C}^n$ we use the Choi matrix representation (3.4), which implies

$$\begin{aligned} 0 \ > \ & \mathrm{Tr}(C(\Psi)\rho) = \langle C(\Psi), \rho \rangle_{\mathrm{HS}} = \left\langle \left(\Psi \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}\right)(|\chi\rangle\langle\chi|),\, \rho \right\rangle_{\mathrm{HS}} \\ = \ & \left\langle |\chi\rangle\langle\chi|,\, \left(\Psi^* \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}\right)\rho \right\rangle_{\mathrm{HS}} = \langle\chi| \left(\Psi^* \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}\right)\rho\, |\chi\rangle\,. \end{aligned}$$

This shows that $\left(\Psi^* \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}\right)\rho$ is not positive semidefinite. On page 38 we showed that Ψ^* is positivity preserving if and only if Ψ is, therefore choosing $\Phi = \Psi^*$ concludes the proof. □

Using the above notation, we say that the positivity preserving map Φ in Corollary 3.42 (or equivalently, σ or the linear functional $\langle \sigma, \cdot \rangle_{\mathrm{HS}}$ in Proposition 3.41) is an *entanglement witness* certifying entanglement of the state ρ.

The most fundamental entanglement witness in quantum information theory is the transposition $T\colon \mathrm{M}_n^{\mathrm{sa}} \to \mathrm{M}_n^{\mathrm{sa}}$ considered in Section 2.3, where we developed the the famous PPT criterion (or Peres-Horodecki criterion, see Proposition 2.34) for certifying entanglement. Actually, the PPT criterion is the Horodecki's entanglement witness theorem 3.42 applied to $\Gamma = T \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}$. Indeed, by Definition 2.33, state $\rho \in \mathrm{D}(\mathbb{C}^n \otimes \mathbb{C}^n)$ is a PPT state if it has positive partial transpose, i.e., if $\rho^\Gamma = \Gamma(\rho) = \left(T \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}\right)\rho$ is positive semidefinite.

It is natural to restrict the set of entanglement witnesses to the ones in an affine hyperplane, e.g., $\mathrm{Tr}\,\sigma = 1$ or $\mathrm{Tr}\,\Phi(I) = 1$. This reduces the search of a witness to a convex compact set. Moreover, by Krein-Milman theorem on page 7, it suffices to consider entanglement witnesses σ or Φ that are extreme points (or belong to extreme rays of the respective cones). In the next examples we will explore what additional properties can we assign to entanglement witnesses.

Example 3.43 (Unital witnesses suffice)**.** Corollary 3.42 remains valid if we require that Φ is unital. Indeed, if ρ and Φ are as in Corollary 3.42, then the map $\hat{\Phi}(X) := \Phi(X) + \epsilon(\mathrm{Tr}X)I$ also fulfils corollary's conclusions for small enough $\epsilon > 0$. Consequently, the map

$$\Psi(X) := \hat{\Phi}(I)^{-1/2}\,\hat{\Phi}(X)\,\hat{\Phi}(I)^{-1/2}$$

is unital and satisfies the properties of Corollary 3.42.

Example 3.44 (Trace preserving witnesses suffice)**.** In Corollary 3.42 we can achieve that Φ is trace preserving, by extending its range to be $\mathrm{M}_{m+n}^{\mathrm{sa}}$.

For $A = \Phi^*(I)$ and any $\rho \in \mathrm{M}_m^{\mathrm{sa}}$ it holds $\mathrm{Tr}\,\Phi(\rho) = \langle I, \Phi(\rho)\rangle_{\mathrm{HS}} = \mathrm{Tr}(A\rho)$. We may assume that A is positive definite and $I - A$ is positive semidefinite. Then it is easy to verify that for $B = (I-A)^{1/2}$,

$$\begin{aligned} \tilde{\Phi}\colon\ \mathrm{M}_m^{\mathrm{sa}} &\longrightarrow \quad \mathrm{M}_{m+n}^{\mathrm{sa}} \\ \rho \quad &\mapsto \ B\rho B \oplus \Phi(\rho) \end{aligned}$$

is trace preserving. Indeed, $\mathrm{Tr}\,\tilde{\Phi}(\rho) = \mathrm{Tr}(\rho(I-A)) + \mathrm{Tr}\,\Phi(\rho) = \mathrm{Tr}\,\rho - \mathrm{Tr}(\rho\Phi^*(I)) + \mathrm{Tr}\,\Phi(\rho) = \mathrm{Tr}\,\rho$. Moreover, $\tilde{\Phi}(\rho)$ is positive semidefinite if and only if $\Phi(\rho)$ is positive semidefinite, and the same holds for any extensions $\tilde{\Phi} \otimes \mathrm{Id}$ and $\Phi \otimes \mathrm{Id}$. This proves that $\tilde{\Phi}$ preserves positivity and detects entanglement of ρ in Corollary 3.42 if and only if Φ does.

Example 3.45 (Optimal entanglement witnesses)**.** Consider the bipartite Hilbert space $\mathcal{H} = \mathbb{C}^m \otimes \mathbb{C}^n$. For $\sigma \in \mathcal{BP}$, let

$$\mathrm{E}(\sigma) = \{\rho \in \mathrm{D}(\mathcal{H})\colon\ \mathrm{Tr}(\rho\sigma) = \langle \sigma, \rho\rangle_{\mathrm{HS}} < 0\},$$

be the set of entangled states detected by the entanglement witness σ. We define σ to be an *optimal entanglement witness* if $\mathrm{E}(\sigma)$ is maximal (i.e., if $\mathrm{E}(\sigma) \subset \mathrm{E}(\tau)$ for $\tau \in \mathcal{BP}$, then $\mathrm{E}(\sigma) = \mathrm{E}(\tau)$). From the S-lemma (a well-known fact from control theory and semi-definite programming stated in Appendix) it follows that if σ lies on an extreme ray of $\mathcal{BP}$ and $\sigma \notin \mathcal{PSD}$, then σ is an optimal entanglement witness.

3.3.1 Construction of entanglement witnesses

In this subsection we explain how entanglement witnesses arise from positivity preserving maps that are not completely positive. This will be done by explicitly constructing the identifications in Proposition 3.41. Consider a positive map $\Psi\colon\ \mathrm{M}_n^{\mathrm{sa}} \to \mathrm{M}_m^{\mathrm{sa}}$ that is not completely positive, i.e., $\Psi \in \boldsymbol{P} \setminus \boldsymbol{CP}$. Then, the Choi matrix $C(\Psi) \in B^{\mathrm{sa}}(\mathbb{C}^m \otimes \mathbb{C}^n)$ is not positive semidefinite by Choi's theorem 3.9. More precisely, in the language of cones (see (3.13) and Tables 3.1, 3.2), this means

$$\text{(i) } C(\Psi) \in \mathcal{SEP}^* = \mathcal{BP} \quad \text{and} \quad \text{(ii) } C(\Psi) \notin \mathcal{PSD} = \mathcal{PSD}^* .$$

In other words, in the language of the dual cones (2.6), the the first condition says

(I) $\langle C(\Psi), \rho \rangle_{\mathrm{HS}} = \mathrm{Tr}\,(C(\Psi)\rho) \geq 0$ for any separable operator $\rho \in \mathcal{SEP}(\mathbb{C}^m \otimes \mathbb{C}^n)$,

and consequently, together with the second condition we get:

(II) there exists an entangled positive semidefinite $\rho_{\mathrm{E}} \in \mathcal{PSD}(\mathbb{C}^m \otimes \mathbb{C}^n) \backslash \mathcal{SEP}(\mathbb{C}^m \otimes \mathbb{C}^n)$ such that $\langle C(\Psi),\, \rho_{\mathrm{E}} \rangle_{\mathrm{HS}} = \mathrm{Tr}\,(C(\Psi)\,\rho_{\mathrm{E}}) < 0$.

Then Proposition 3.41 asserts that $C(\Psi)$ is an entanglement witness, namely, $C(\Psi)$ certifies the entanglement present in ρ_{E}. This is equivalent to saying that $\Psi^* \colon \mathrm{M}_m^{\mathrm{sa}} \to \mathrm{M}_n^{\mathrm{sa}}$ is an entanglement witness since $\left(\Psi^* \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}\right)\rho_{\mathrm{E}}$ is not positive semidefinite by Corollary 3.42.

In Figure 3.1 we illustrate the above points (I) and (II): the hyperplane $\langle C(\Psi), \cdot \rangle_{\mathrm{HS}} = 0$ in $B^{\mathrm{sa}}(\mathbb{C}^m \otimes \mathbb{C}^n)$ separates the $\mathcal{SEP}(\mathbb{C}^m \otimes \mathbb{C}^n)$ cone (which lies in the $\langle C(\Psi), \cdot \rangle_{\mathrm{HS}} \geq 0$ halfplane) from the entangled operator ρ_E. (which lies in the $\langle C(\Psi), \cdot \rangle_{\mathrm{HS}} < 0$ halfplane). As shown in the figure, the optimal entanglement witness Ψ certifies entanglement of all operators in the set $\mathrm{E}(C(\Psi)) = \{\rho \colon \langle C(\Psi), \rho \rangle_{\mathrm{HS}} < 0\}$. Observe also that the set of $\mathrm{E}(C(\Psi'))$ is smaller for an entanglement witness Ψ' which is not optimal (in the sense of Example 3.45).

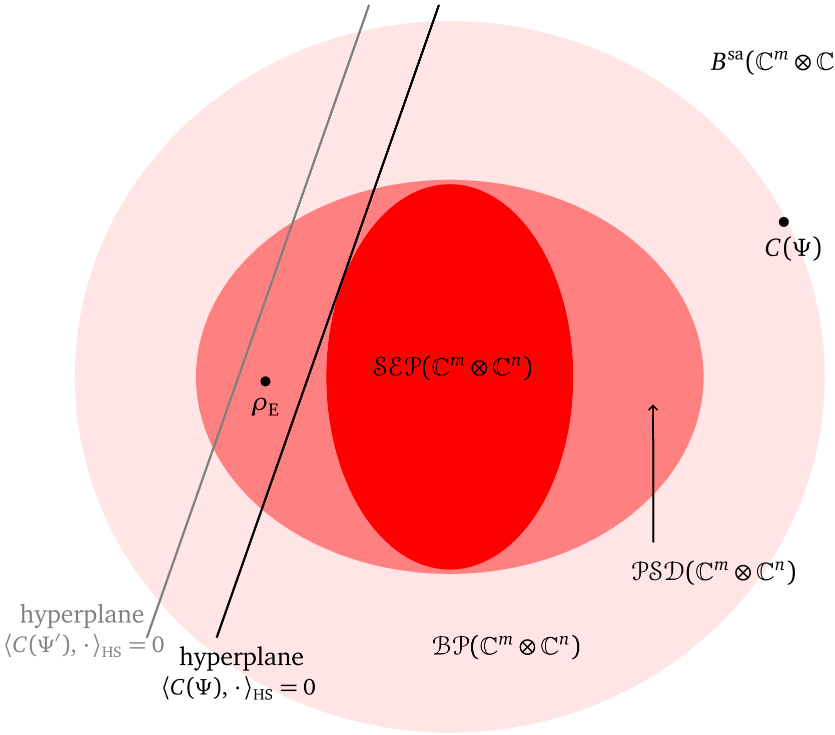

$B^{\mathrm{sa}}(\mathbb{C}^m \otimes \mathbb{C}^n)$
$C(\Psi)$
$\mathcal{SEP}(\mathbb{C}^m \otimes \mathbb{C}^n)$
ρ_{E}
$\mathcal{PSD}(\mathbb{C}^m \otimes \mathbb{C}^n)$
hyperplane
$\langle C(\Psi'), \cdot \rangle_{\mathrm{HS}} = 0$
hyperplane
$\langle C(\Psi), \cdot \rangle_{\mathrm{HS}} = 0$
$\mathcal{BP}(\mathbb{C}^m \otimes \mathbb{C}^n)$

Figure 3.1. Linear functional $\langle C(\Psi), \cdot \rangle_{\mathrm{HS}}$ of an optimal entanglement witness Ψ.

Remark 3.46 (Construction of completely positive maps that are not entanglement breaking)**.** We describe another use of positivity preserving maps that are not completely positive. Namely, the above entangled positive semidefinite $\rho_{\mathrm{E}} \in \mathcal{PSD}$ can be represented as the Choi matrix of some completely positive map $\boldsymbol{CP} \ni \Theta\colon \mathrm{M}_n^{\mathrm{sa}} \to \mathrm{M}_m^{\mathrm{sa}}$, i.e., $\rho_{\mathrm{E}} = C(\Theta)$. Then such Θ is not an entanglement breaking map by Lemma 3.29.

Entanglement witnesses are linear by definition. They are extensively used in quantum information theory and quantum physics. In [ASLB13] the authors experimentally implemented a nonlinear entanglement witness (which fits closer to the $\mathcal{SEP}$ cone than linear witnesses); see also modern work from Otfried Gühne and co-workers at Universität Siegen.

3.3.2 Examples of entanglement witnesses

In Subsection 3.3.1 we explained that having an entanglement witness is equivalent to having a positivity preserving map that is not completely positive. Moreover, in Example 3.45 we showed that $C(\Psi)$ is an optimal entanglement witness if and only if Ψ belongs to an extreme ray in the positive cone $\boldsymbol{P}$ (for this reason, $C(\Psi) \in \mathcal{BP}$ in Figure 3.1 is drawn as an extreme point). In summary, we gave an explicit construction of the equivalences

$$\begin{gathered}\Psi \in \boldsymbol{P}(\mathbb{C}^n, \mathbb{C}^m) \setminus \boldsymbol{CP}(\mathbb{C}^n, \mathbb{C}^m) \\ \Longleftrightarrow \\ C(\Psi) \in \mathcal{BP}(\mathbb{C}^m \otimes \mathbb{C}^n) \text{ is an entanglement witness} \\ \Longleftrightarrow \\ \Psi(|\mathrm{x}\rangle\langle\mathrm{x}|) \in \mathcal{PSD}(\mathbb{C}^m) \text{ for all } \mathrm{x} \in \mathbb{C}^n \quad \text{and} \quad C(\Psi) \notin \mathcal{PSD}(\mathbb{C}^m \otimes \mathbb{C}^n). \end{gathered} \tag{3.14}$$

Recall the Størmer-Woronowitz theorem 2.37, stating that $\mathrm{SEP}\left(\mathbb{C}^2 \otimes \mathbb{C}^2\right) = \mathrm{PPT}\left(\mathbb{C}^2 \otimes \mathbb{C}^2\right)$ and $\mathrm{SEP}\left(\mathbb{C}^2 \otimes \mathbb{C}^3\right) = \mathrm{PPT}\left(\mathbb{C}^2 \otimes \mathbb{C}^3\right)$. This implies that the transposition entanglement witness detects every entangled state on $\mathbb{C}^2 \otimes \mathbb{C}^2$ or $\mathbb{C}^2 \otimes \mathbb{C}^3$. Thus, in order to construct new entanglement witnesses we need to consider the Hilbert spaces $\mathbb{C}^m \otimes \mathbb{C}^n$ with $m, n \geq 3$.

Example 3.47 (The Choi map)**.** The first example of a positive map that is not completely positive is due to Choi [Cho75b]. The Choi map $\Phi_C\colon \mathrm{M}_3 \to \mathrm{M}_3$ is defined as

$$\Phi_C\left(\begin{bmatrix} z_{00} & z_{01} & z_{02} \\ z_{10} & z_{11} & z_{12} \\ z_{20} & z_{21} & z_{22} \end{bmatrix}\right) = \begin{bmatrix} z_{00} + z_{11} & -z_{01} & -z_{02} \\ -z_{10} & z_{11} + z_{22} & -z_{12} \\ -z_{20} & -z_{21} & z_{00} + z_{22} \end{bmatrix}.$$

Choi studied positive maps on real symmetric matrices whereas, as we noted in the historical overview on page 29, the extensions of positive maps to Hermitian matrices became relevant much later with the work of the Horodecki group. Choi identified linear maps $\Phi\colon \mathrm{SYM}_n \to \mathrm{SYM}_m$ with biquadratic forms p_Φ in $n+m$ variables via the isomorphism

$$\Phi \;\longleftrightarrow\; p_\Phi(\mathrm{x}, \mathrm{y}) = \left\langle \mathrm{y} \middle| \Phi(|\mathrm{x}\rangle\langle\mathrm{x}|) \middle| \mathrm{y} \right\rangle,$$

where $\mathrm{x} \in \mathbb{R}^n$ and $\mathrm{y} \in \mathbb{R}^m$. Then Φ is positivity preserving if and only if the polynomial p_Φ is nonnegative on $\mathbb{R}^n \times \mathbb{R}^m$, and Φ is completely positive if and only if p_Φ is a sum of squares (SOS) of bilinear forms [Cho75a]. Nonnegative polynomials p_Φ representing positive but not completely positive maps $\Phi\colon \mathrm{SYM}_3 \to \mathrm{SYM}_3$ attain value zero in 7, 8, 9 or 10 points (this is a known fact from real algebraic geometry [Qua15]). In particular, p_Φ representing the Choi map has 7 zeros.

We will use the equivalences in (3.14) to show that the Choi map Φ_C is positive but not completely positive. First we verify that Φ_C is positivity preserving by checking that $\Phi_C(|\mathrm{x}\rangle\langle\mathrm{x}|)$ is positive semidefinite for all $\mathrm{x} = (x_0, x_1, x_2) \in \mathbb{C}^3$. It suffices to verify that the principal minors of $\Phi_C(|\mathrm{x}\rangle\langle\mathrm{x}|)$ are nonnegative:

$$\begin{aligned}\det\Phi_C(|\mathrm{x}\rangle\langle\mathrm{x}|) &= \begin{vmatrix} |x_0|^2+|x_1|^2 & -x_0\overline{x_1} & -x_0\overline{x_2} \\ -x_1\overline{x_0} & |x_1|^2+|x_2|^2 & -x_1\overline{x_2} \\ -x_2\overline{x_0} & -x_2\overline{x_1} & |x_2|^2+|x_0|^2 \end{vmatrix} \\ &= |x_0|^2|x_1|^4+|x_1|^2|x_2|^4+|x_2|^2|x_0|^4-3|x_0|^2|x_1|^2|x_2|^2.\end{aligned}$$

The first 2×2 principal minor is

$$\begin{vmatrix} |x_0|^2+|x_1|^2 & -x_0\overline{x_1} \\ -x_1\overline{x_0} & |x_1|^2+|x_2|^2 \end{vmatrix} = |x_2|^2|x_0|^2+|x_1|^4+|x_1|^2|x_2|^2 \geq 0$$

(the other 2×2 principal minors are the same, up to a permutation of indices) and the 1×1 minors are clearly nonnegative. In order to show that $\det\Phi_C(|\mathrm{x}\rangle\langle\mathrm{x}|) \geq 0$, we solve the equivalent optimization problem

$$\begin{aligned}\text{minimize:}\ & ab^2+bc^2+ca^2-3abc \\ \text{subject to:}\ & a,b,c \geq 0 \\ & a+b+c=1.\end{aligned}$$

where we set $a = |x_0|^2,\ b = |x_1|^2,\ c = |x_2|^2$. Alternatively, deploy `Wolfram Mathematica` and draw some contour plots like we show on Figure 3.2. We find that $\det\Phi_C(|\mathrm{x}\rangle\langle\mathrm{x}|)$ attains minimal value 0 in 7 real points $(1,1,1)$, $(-1,1,1)$, $(1,-1,1)$, $(1,1,-1)$, $(1,0,0)$, $(0,1,0)$, $(0,0,1)$. This configuration of 7 points is called *the Choi set of zeros*.

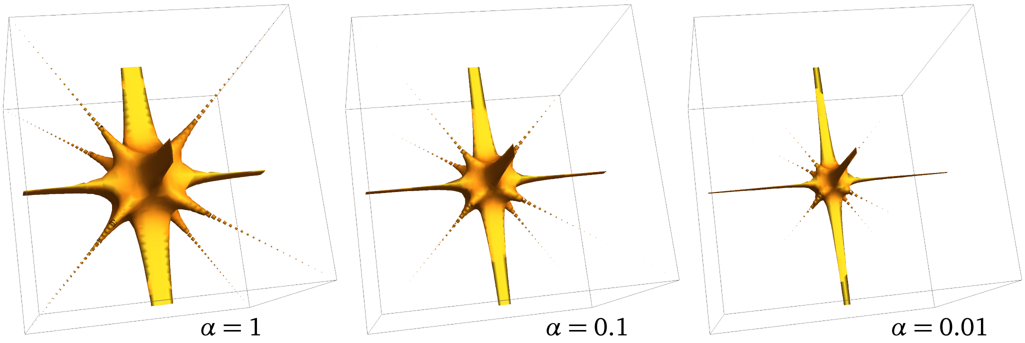


Figure 3.2. Contour plots of $y_0^2y_1^4+y_1^2y_2^4+y_2^2y_0^4-3y_0^2y_1^2y_2^2=\alpha$.

Next we calculate the Choi matrix of the Choi map $C(\Phi_C)$ and show that it is not positive semidefinite. In Example 3.6 we calculated (for clarity purposes we write only the nonzero entries),

$$C(\Phi) = \left[\begin{array}{ccc|ccc|ccc} 1 & \cdot & \cdot & \cdot & -1 & \cdot & \cdot & \cdot & -1 \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & -1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot & -1 & \cdot & \cdot & \cdot & 1 \end{array}\right].$$

For $\mathrm{c} = (1,0,0,0,1,0,0,0,1) \in \mathbb{C}^3 \otimes \mathbb{C}^3$ we get $\langle \mathrm{c}|\, C(\Phi_C)\, |\mathrm{c}\rangle = -3$, which proves that $C(\Phi_C)$ is not positive semidefinite, thus Φ_C is not completely positive.

Remark 3.48. The equality $\langle \mathrm{c}|\, C(\Phi_C)\, |\mathrm{c}\rangle = \mathrm{Tr}(C(\Phi_C)\, |\mathrm{c}\rangle\langle \mathrm{c}|) = \langle C(\Phi_C), |\mathrm{c}\rangle\langle \mathrm{c}|\rangle_{\mathrm{HS}} < 0$ shows that $C(\Phi_C)$ is an entanglement witness certifying entanglement in the pure state

$$\rho = \left|\frac{1}{\sqrt{3}}\mathrm{c}\right\rangle\!\left\langle\frac{1}{\sqrt{3}}\mathrm{c}\right| \in \mathrm{D}(\mathbb{C}^3 \otimes \mathbb{C}^3).$$

However, entanglement of c is already detected by the partial transposition. Indeed, in the computational basis $\mathrm{c} = (1,0,0,0,1,0,0,0,1) = |00\rangle + |11\rangle + |22\rangle \in \mathbb{C}^3 \otimes \mathbb{C}^3$, thus ρ is the maximally entangled state (2.12). Actually, by Lemma 2.36 the partial transposition detects entanglement in every pure state. In Subsection 3.3.3 we will present an algorithm how the Choi map can be used to certify entanglement also in the states which cannot be detected by the partial transposition.

In 2013 (nearly 30 years after Choi), K.-C. Ha [Ha13] proved that the Choi map Φ_C on the Hermitian matrices $\mathrm{M}_3^{\mathrm{sa}}$ is an extremal positive map (i.e., Φ_C belongs to an extreme ray in the cone $\boldsymbol{P}(\mathbb{C}^3, \mathbb{C}^3)$), and thus it defines an optimal entanglement witness from Example 3.45.

Example 3.49 (Buckley-Šivic maps)**.** In [BŠ20] we extend Choi's approach from symmetric matrices to Hermitian matrices and construct new families of positivity preserving maps which are not completely positive. The basic idea is as follows. We identify positive maps $\Psi\colon \mathrm{M}_3^{\mathrm{sa}} \to \mathrm{M}_3^{\mathrm{sa}}$ with biquadratic forms p_Ψ via the isomorphism

$$\Psi \;\longleftrightarrow\; p_\Psi(\mathrm{x},\mathrm{y}) = \big\langle \mathrm{y}\big|\, \Psi(|\mathrm{x}\rangle\langle \mathrm{x}|)\, \big|\mathrm{y}\big\rangle,$$

where $\mathrm{x} = (x_0, x_1, x_2) \in \mathbb{C}^3$ and $\mathrm{y} = (y_0, y_1, y_2) \in \mathbb{C}^3$. We find new families of nonnegative polynomials p_Ψ, which (when restricted to $\mathbb{R}$) have 8, 9 or 10 zeros. This ensures that the corresponding positive maps $\Psi\colon \mathrm{M}_3^{\mathrm{sa}} \to \mathrm{M}_3^{\mathrm{sa}}$ are significantly different from the Choi map in Example 3.47 and its generalizations found in the literature. Our examples of positive maps are not completely positive maps and moreover, they belong to extreme rays in the cone of positive maps $\boldsymbol{P}$. Therefore, as explained in Subsection 3.3.1, the associated entanglement witnesses are optimal.

Here we present the most symmetric example from [BŠ20], corresponding to p_Ψ with 10 zeros.

Theorem 3.50. *Superoperators $\Psi_t\colon \mathrm{M}_3^{sa} \to \mathrm{M}_3^{sa}$ of the form*

$$\begin{bmatrix} z_{00} & z_{01} & z_{02} \\ z_{10} & z_{11} & z_{12} \\ z_{20} & z_{21} & z_{22} \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} (t^2-1)^2 z_{00} + z_{11} + t^4 z_{22} & -(t^4-t^2+1)\,z_{10} & -(t^4-t^2+1)\,z_{20} \\ -(t^4-t^2+1)\,z_{01} & t^4 z_{00} + (t^2-1)^2 z_{11} + z_{22} & -(t^4-t^2+1)\,z_{21} \\ -(t^4-t^2+1)\,z_{02} & -(t^4-t^2+1)\,z_{12} & z_{00} + t^4 z_{11} + (t^2-1)^2 z_{22} \end{bmatrix}$$

are positive for $t \in \mathbb{R}$. Apart from $t = \pm 1$, these positive maps are not completely positive. Moreover, Ψ_t define extreme rays in the convex cone of positive maps $\boldsymbol{P}(\mathbb{C}^3, \mathbb{C}^3)$.

Proof. We will use (3.14) to show that the Ψ_t are positive but not completely positive (by repeating the steps in Example 3.47 of the Choi map). First we verify that Ψ_t are positivity preserving. Matrix $\Psi_t\left(|\mathrm{x}\rangle\langle \mathrm{x}|\right)$ is positive semidefinite for all $\mathrm{x} = (x_0, x_1, x_2) \in \mathbb{C}^3$ if its principal minors are nonnegative for all x. This is equivalent to showing that, for all $\mathrm{x} \in \mathbb{C}^3$,

1. $\operatorname{Tr}\Psi_t\left(|\mathrm{x}\rangle\langle \mathrm{x}|\right) = 2\left(1-t^2+t^4\right)\left(|x_0|^2+|x_1|^2+|x_2|^2\right) \geq 0$,
2. the sum of the principal 2×2 minors $= \left(1-t^2+t^4\right)^2\left(|x_0|^2+|x_1|^2+|x_2|^2\right)^2 \geq 0$,
3. $\det\Psi_t\left(|\mathrm{x}\rangle\langle \mathrm{x}|\right) \geq 0$,

where $\det\Psi_t\left(|\mathrm{x}\rangle\langle \mathrm{x}|\right) =$

$$\begin{aligned}&(1-t^2)^2 \times \\ &\left[t^4\left(|x_0|^6+|x_1|^6+|x_2|^6\right) + (t^8-2t^2)\left(|x_0|^4|x_1|^2+|x_0|^2|x_2|^4+|x_1|^4|x_2|^2\right) + \right. \\ &\left.(1-2t^6)\left(|x_0|^2|x_1|^4+|x_0|^4|x_2|^2+|x_1|^2|x_2|^4\right) - 3(1-2t^2+t^4-2t^6+t^8)|x_0|^2|x_1|^2|x_2|^2\right].\end{aligned}$$

Polynomials in 1. and 2. are clearly nonnegative. And the determinant (considered as a real polynomial in $|x_0|, |x_1|, |x_2|$) is the *generalized Robinson polynomial*, which is known to be positive everywhere except at the 10 zeros

$$(1,1,1), (1,1,-1), (1,-1,1), (-1,1,1), (1,t,0), (0,1,t), (t,0,1), (1,-t,0), (0,1,-t), (-t,0,1).$$

Next we calculate the Choi matrix $C(\Psi_t)$,

$$\left[\begin{array}{ccc|ccc|ccc} (t^2-1)^2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & -1+t^2-t^4 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & t^4 & \cdot & \cdot & \cdot & -1+t^2-t^4 & \cdot & \cdot \\ \hline \cdot & -1+t^2-t^4 & \cdot & t^4 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & (t^2-1)^2 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & -1+t^2-t^4 & \cdot \\ \hline \cdot & \cdot & -1+t^2-t^4 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -1+t^2-t^4 & \cdot & t^4 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & (t^2-1)^2 \end{array}\right].$$

For $\mathrm{v} = (0,0,1,0,0,0,1,0,0) = |02\rangle + |20\rangle \in \mathbb{C}^3 \otimes \mathbb{C}^3$ we get $\langle \mathrm{v}|C(\Psi_t)|\mathrm{v}\rangle = -(t^2-1)^2$, which proves that $C(\Psi_t)$ is not positive semidefinite for all t except ± 1, thus Ψ_t is not completely positive for $t \in \mathbb{R} \setminus \{\pm 1\}$.

Finally, Ψ_t is an extremal map (i.e., $\Psi_t \in \boldsymbol{P}(\mathbb{C}^3, \mathbb{C}^3)$ is an extreme ray) since it is, up to a positive factor, the only positive linear map for which p_Ψ has the prescribed set of zeros. For computational purposes it is convenient to represented p_Ψ as a nonnegative polynomial in real variables

$$\frac{1}{2}(x_k + \overline{x_k}),\ \frac{1}{2i}(x_k - \overline{x_k}),\ \frac{1}{2}(y_k + \overline{y_k}),\ \frac{1}{2i}(y_k - \overline{y_k}),\quad \text{for } k = 0,1,2.$$

□

Remark 3.51. For $t = 0$, the map Ψ_0 is equal to the Choi map Φ_C in Example 3.47.

Remark 3.52. For $t = 1$ or $t = -1$ the Choi matrix $C(\Psi_t)$ is positive semidefinite. Thus, by Choi's theorem 3.9, the completely positive $\Psi_{\pm 1}$ has a Kraus decomposition. For $Z = |\mathrm{x}\rangle\langle \mathrm{x}| \in \mathrm{M}_3$ we compute

$$\begin{aligned}
\Psi_{\pm 1}(|\mathrm{x}\rangle\langle \mathrm{x}|) &= \begin{bmatrix} |x_1|^2 + |x_2|^2 & -x_1\overline{x_0} & -x_2\overline{x_0} \\ -x_0\overline{x_1} & |x_0|^2 + |x_2|^2 & -x_2\overline{x_1} \\ -x_0\overline{x_2} & -x_1\overline{x_2} & |x_0|^2 + |x_1|^2 \end{bmatrix} \\
&= |(x_1, -x_0, 0)\rangle\langle (x_1, -x_0, 0)| + \\
&\quad\ |(-x_2, 0, x_0)\rangle\langle(-x_2, 0, x_0)| + \\
&\quad\ |(0, x_2, -x_1)\rangle\langle(0, x_2, -x_1)| \\
&= A_1 |\mathrm{x}\rangle\langle \mathrm{x}| A_1^* + A_2 |\mathrm{x}\rangle\langle \mathrm{x}| A_2^* + A_3 |\mathrm{x}\rangle\langle \mathrm{x}| A_3^*,
\end{aligned}$$

where

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},\ A_2 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix},\ A_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}.$$

This implies that, for all $Z \in \mathrm{M}_3$,

$$\Psi_{\pm 1}(Z) = A_1 Z A_1^* + A_2 Z A_2^* + A_3 Z A_3^*$$

is a Kraus decomposition of $\Psi_{\pm 1}$. All operators A_1, A_2, A_3 have rank 2, thus $\Psi_{\pm 1}$ is not entanglement breaking by Lemma 3.29. Since $\Psi_{\pm 1}(I) = 2I$,

$$\frac{1}{2}\Psi_{\pm 1} : \begin{bmatrix} z_{00} & z_{01} & z_{02} \\ z_{10} & z_{11} & z_{12} \\ z_{20} & z_{21} & z_{22} \end{bmatrix} \mapsto \frac{1}{2} \begin{bmatrix} z_{11} + z_{22} & -z_{10} & -z_{20} \\ -z_{01} & z_{00} + z_{22} & -z_{21} \\ -z_{02} & -z_{12} & z_{00} + z_{11} \end{bmatrix}$$

is a unital entanglement witness considered in Example 3.43. Moreover, $\frac{1}{2}\Psi_{\pm 1}$ is trace preserving by definition. In Definition 3.16 we called a completely positive, trace preserving and unital map a bistochastic quantum channel.

3.3.3 Semidefinite programming

Semidefinite programming is a class of conic programming (in the theory of convex optimization) with respect to the $\mathcal{PSD}$ cone. In Appendix we overview the conic programming for the fundamental cones in Example 2.12: the nonnegative orthant, the Lorentz cone and the $\mathcal{PSD}$ cone.

Definition 3.53. Let $\Phi\colon \mathrm{M}_m \to \mathrm{M}_n$ be a self-adjointness-preserving map. A *semidefinite program* (SDP), associated with Φ and two fixed operators $A \in \mathrm{M}_m$ and $B \in \mathrm{M}_n$, is the following optimization problem:

$$\begin{aligned} \text{minimize:} \quad & \mathrm{Tr}(AX) \\ \text{subject to:} \quad & \Phi(X) - B \succeq 0 \\ & X \succeq 0 \end{aligned}$$

In the above SDP we optimize over the positive semidefinite matrices $X \in \mathcal{PSD}$ (the constraint $\succeq 0$ denotes that the matrices on the left are positive semidefinite).

The aim of this subsection is to construct entanglement witnesses that can detect entanglement in some PPT states, which are by definition states ρ for which ρ^Γ is positive semidefinite. PPT states are exactly the states that the transposition (arguably the most famous, but not the strongest entanglement witness) cannot detect. This follows from the PPT criterion 2.34, which is the same as the Horodecki's entanglement witness theorem 3.42 applied to the transposition (as explained on page 53). By Lemma 2.36 we know that the partial transposition certifies entanglement in all pure states.

Here is an example of a mixed entangled PPT state.

Example 3.54. It is straightforward to check that the following state $\rho \in \mathrm{D}\big(\mathbb{C}^3 \otimes \mathbb{C}^3\big)$ has positive partial transpose,

$$\rho = \frac{1}{21}\left[\begin{array}{ccc|ccc|ccc} 2 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & 2 \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & 4 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 2 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & 2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 4 & \cdot \\ 2 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & 2 \end{array}\right].$$

However, the Choi entanglement witness (i.e., the Choi map Φ_C in Example 3.47) certifies entanglement in ρ. Indeed, $C(\Phi_C)\rho$ has an eigenvalue equal to $-\frac{2}{7}$, thus ρ is entangled by Corollary 3.42. We can apply the same argument to certify entanglement in ρ, by using the maps $\Psi_t \in \boldsymbol{P} \setminus \boldsymbol{CP}$ from Theorem 3.50 instead of the Choi map Φ_C, since $C(\Psi_t)\rho$ is not positive semidefinite for any $t \in \mathbb{R} \setminus \{\pm 1\}$.

The following example shows that, there is no reason to believe that the Choi map can detect entanglement in any state.

Example 3.55 (Unextendible product bases (UPB)). Consider vectors in $\mathbb{C}^3 \otimes \mathbb{C}^3$,

$$\begin{aligned} |v_1\rangle &= \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle), \\ |v_2\rangle &= \frac{1}{\sqrt{2}}|2\rangle \otimes (|1\rangle - |2\rangle), \\ |v_3\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |2\rangle, \\ \left|v_4\right\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \otimes |0\rangle, \\ |v_5\rangle &= \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle) \otimes (|0\rangle + |1\rangle + |2\rangle). \end{aligned}$$

These vectors are called a UPB or *tiles* because they satisfy the two properties,

1. $\left\langle v_i \middle| v_j \right\rangle = 0$ for all $i \neq j$, and
2. no product vector $z \in \mathbb{C}^3 \otimes \mathbb{C}^3$ exists such that $\langle v_i | z \rangle = 0$ for $1 \leq i \leq 5$.

Then the state

$$\rho_{\text{tiles}} = \frac{1}{4}\left(I - \sum_{i=1}^{5} |v_i\rangle\langle v_i|\right)$$

is entangled, which follows directly from the UPB properties. However, ρ_{tiles} is a PPT state and moreover, it is not detectable by the Choi map Φ_C. In order to check this we write ρ_{tiles} in the computational basis. Observe that $9\,|v_5\rangle\langle v_5| = J$, the 9×9 matrix of ones. Then,

$$\rho_{\text{tiles}} = \frac{1}{8}\left[\begin{array}{ccc|ccc|ccc} 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 \end{array}\right] - \frac{1}{36}J$$

remains unchanged under the partial transposition. Moreover, in `Wolfram Mathematica` we can check that the matrix $C(\Phi_C)\,\rho_{\text{tiles}}$ has eigenvalues

$$\{0.4281, 0.3069, 0.125, 0.0148, 0, 0, 0, 0, 0\}$$

and is thus positive semidefinite. Analogous calculation shows that neither the positive maps Ψ_t from Theorem 3.50 are able to detect entanglement in ρ_{tiles}, since $C(\Psi_t)\,\rho_{\text{tiles}}$ is positive semidefinite for all $t \in \mathbb{R}$. We are optimistic that other examples of positive maps in [BŠ20] will prove to detect entanglement in ρ_{tiles}, however this is beyond the scope of this thesis.

In Subsection 3.3.1 we constructed entanglement witnesses from positive maps that are not completely positive. Now we put additional assumptions on $\Psi \in \boldsymbol{P} \setminus \boldsymbol{CP}$, so that it will detect entanglement also in the states with positive partial transpose. For this purpose we revisit Table 3.2 and Table 3.1 and their association via the Choi isomorphism $\Psi \mapsto C(\Psi)$.

Assume that $\Psi \in \boldsymbol{DEC}(\mathbb{C}^n, \mathbb{C}^m) \setminus \boldsymbol{CP}(\mathbb{C}^n, \mathbb{C}^m)$. By the definition of decomposable maps on page 51, this means that $\Psi = \Psi_{\mathrm{cp}_1} + T \circ \Psi_{\mathrm{cp}_2}$, where $\Psi_{\mathrm{cp}_1}, \Psi_{\mathrm{cp}_2}$ are completely positive maps. By Corollary 3.42 there exists a state ρ on $\mathbb{C}^m \otimes \mathbb{C}^n$ such that $\left(\Psi \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}\right)\rho$ is not positive semidefinite. However, the entanglemnt of this ρ is already detected by the partial transposition $\Gamma = T \otimes \mathrm{Id}_{\mathrm{M}_n^{\mathrm{sa}}}$. Indeed, this follows from the cone duality,

$$C(\Psi) \in \text{co-}\mathcal{PSD} + \mathcal{PSD} = \mathcal{PPT}^* := \{\tau \colon \langle \tau, \rho \rangle_{\mathrm{HS}} \geq 0, \forall \rho \in \mathcal{PPT}\}.$$

Therefore, in order to obtain new entanglement witnesses, we need to consider

$$\begin{gathered} \Psi \in \boldsymbol{P}(\mathbb{C}^n, \mathbb{C}^m) \setminus \boldsymbol{DEC}(\mathbb{C}^n, \mathbb{C}^m) \\ \Longleftrightarrow \\ C(\Psi) \in \mathcal{BP}(\mathbb{C}^m \otimes \mathbb{C}^n) \setminus (\text{co-}\mathcal{PSD} + \mathcal{PSD}) \\ \Longleftrightarrow \\ \Psi(|\mathrm{x}\rangle\langle\mathrm{x}|) \in \mathcal{PSD}(\mathbb{C}^m) \text{ for all } \mathrm{x} \in \mathbb{C}^n \quad \text{and} \quad C(\Psi) \notin \mathcal{PPT}^*. \end{gathered} \tag{3.15}$$

The last equivalence follows from (3.13) and the duality co-$\mathcal{PSD} + \mathcal{PSD} = \mathcal{PPT}^*$. In particular,

$$C(\Psi) \notin \mathcal{PPT}^* \Longleftrightarrow \text{ there exists } \rho \in \mathcal{PPT} \text{ such that } \langle C(\Psi), \rho \rangle_{\mathrm{HS}} < 0.$$

Such an entanglement witness $C(\Psi)$ induces a linear functional $\langle C(\Psi), \cdot \rangle_{\mathrm{HS}}$. We summarize the above considerations as an optimization problem.

Proposition 3.56. *Let* $\Psi \colon \mathrm{M}_n \to \mathrm{M}_m$ *be a positivity preserving map that is not decomposable. The solution of the semidefinite program*

$$\begin{aligned} \textit{minimize}\colon &\ \mathrm{Tr}(C(\Psi)\rho) \\ \textit{subject to}\colon &\ \rho^{\Gamma} \succeq 0 \\ &\ \rho \succeq 0 \end{aligned}$$

is an entangled PPT state on $\mathbb{C}^m \otimes \mathbb{C}^n$.

This way we can use the positive and not completely positive maps in Example 3.47 and Example 3.49 to produce new entangled states on $\mathbb{C}^3 \otimes \mathbb{C}^3$, which cannot be detected by the partial transposition. Furthermore, as explained in Remark 3.46, from new entangled states in $\mathrm{D}\left(\mathbb{C}^3 \otimes \mathbb{C}^3\right)$ we can construct new completely positive maps on $\mathrm{M}_3^{\mathrm{sa}}$ that are not entanglement breaking.

For further links between semidefinite programming and entanglement detection we refer to [HNW17]. For various forms of semi-definite programming in quantum information theory see [Wat18].

Appendix A

Conic programming

A.1 Semidefinite programming

Semidefinite programming is a class of conic programming and conic programming is a class of mathematical programming. Appendix A is an introduction to this hierarchy.

Definition A.1 (Mathematical programming)**.** Mathematical programming is about solving optimization programs of the form

$$\mathrm{Opt} = \min_{x\in\mathbb{R}^n}\{f_0(x)\colon f_i(x) \leq 0,\, i = 1,\ldots,m\},$$

where the *objective* $f_0\colon \mathbb{R}^n \to \mathbb{R}$ and the *constraints* $f_i\colon \mathbb{R}^n \to \mathbb{R}$ are functions at least in $\mathrm{C}^1(\mathbb{R}^n)$.

Mathematical programming is a generalization of *linear programming* (LP), where the objective and constraints are linear functions. Linear program has an elegant formulation in the matrix form.

Definition A.2 (Linear programming)**.** Given $c \in \mathbb{R}^n$, $A \in \mathrm{M}_{m,n}$, $b \in \mathbb{R}^m$, solve the following optimization program:

$$\mathrm{Opt} = \min_{x\in\mathbb{R}^n}\{\langle c|x\rangle : Ax \leq b\}\,.$$

The corresponding objective and constraints are then indeed linear functions,

- objective $f_0 = \langle c|x\rangle = \sum_{j=1}^n c_j x_j$,
- constraints $f_i = (Ax)_i - b_i = \sum_{j=1}^n a_{ij}x_j - b_i$, for $i = 1\ldots,m$.

Usually we assume $m >> n$, i.e., more constraints than variables.

Next we present an alternative way to introduce nonlinearity (in terms of extending the linear programming). Note that in Definition A.2, $\geq$ denotes the standard coordinate-wise vector inequality

$$a \geq b \Leftrightarrow a - b \geq 0 \Leftrightarrow a - b \in \mathbb{R}^m_+,$$

where $\mathbb{R}^m_+$ is the *positive orthant* cone defined in Example 2.12. The concept of convex cones (the fundamental geometrical objects of this thesis) gives rise to another "reasonable" definition of vector inequality induced by a regular cone $\mathcal{K} \subset \mathbb{R}^m$,

$$a \geq_{\mathcal{K}} b \Leftrightarrow a - b \geq_{\mathcal{K}} 0 \Leftrightarrow a - b \in \mathcal{K}.$$

Then we can define a conic program as an extension of a linear program in the following way.

Definition A.3 (Conic program)**.** A conic program on a regular cone $\mathcal{K}$ is the optimization program

$$\min_x\{\langle c|x\rangle : Ax \leq_{\mathcal{K}} b\} = \min_x\{\langle c|x\rangle : Ax - b \in \mathcal{K}\}.$$

There are two main benefits of conic representation:

- it is easy to distinguish between the structure (given by the cone $\mathcal{K}$) and the data c, A, b;
- independently of the data, we are optimizing a linear objective over a convex set (i.e., convexity of the cone is built into the problem).

The three families of cones, the positive orthants, the Lorentz cones and the $\mathcal{PSD}$ cones of complex positive semidefinite matrices (defined in in Example 2.12), allow to represent an extremely wide spectrum of convex optimization problems. Specifically,

1. nonnegative orthants $\mathbb{R}^m_+$ give rise to *linear programs* (LP);
2. finite direct products of Lorentz cones give rise to *conic quadratic programs* (CQPs)

   $$\min_x\{c^T x : \|A_i x - b_i\|_2 \leq c_i^T x - d_i,\ i = 1, \dots, m\},$$

   where A_i, b_i, c_i, d_i are matrices and vectors of appropriate dimensions;
3. Direct products of semidefinite cones give rise to *semidefinite programs* (SDPs)

   $$\min_X\{\langle C, X\rangle_{\mathrm{HS}} : \Phi_i(X) - B_i \succeq 0,\ i = 1, \dots, m\},$$

   were we minimize over $X \in \mathrm{M}^{\mathrm{sa}}_{d_1}$ for given $\Phi_i : \mathrm{M}^{\mathrm{sa}}_{d_1} \to \mathrm{M}^{\mathrm{sa}}_{d_2}$ and $C \in \mathrm{M}^{\mathrm{sa}}_{d_1}$, $B_i \in \mathrm{M}^{\mathrm{sa}}_{d_2}$.

Here we view the $\mathcal{PSD}$ cones in the real vector space of Hermitian matrices $\mathrm{M}^{\mathrm{sa}}_d = B^{\mathrm{sa}}(\mathbb{C}^d)$.

We refer the interested reader to the survey on conic programming and its relation to convex optimization [Nem07], and to the book on convex optimization [BV04].

The S-lemma

We present a well-known and useful fact from control theory and semidefinite programming.

Lemma A.4 (S-lemma, [AS17]: C.3)**.** *Let M, N be real symmetric matrices of size $n \times n$. The following two statements are equivalent:*

1. $\{x \in \mathbb{R}^n : \langle x|M|x\rangle \geq 0\} \cup \{x \in \mathbb{R}^n : \langle x|N|x\rangle \geq 0\} = \mathbb{R}^n$,
2. *there exists $t \in [0, 1]$ such that the matrix $(1 - t)M + tN$ is positive semidefinite.*

We use the following reformulation of the S-lemma (for $M = F$ and $N = -G$).

Corollary A.5. *Let F, G be real symmetric matrices of size $n \times n$ for which there exists a $y \in \mathbb{R}^n$ such that $\langle y|G|y\rangle > 0$. Then the following two statements are equivalent:*

1. *if $x \in \mathbb{R}^n$ verifies $\langle x|G|x\rangle \geq 0$, then $\langle x|F|x\rangle \geq 0$,*
2. *there exists $\mu \geq 0$ such that $F - \mu G$ is positive semidefinite.*

Bibliography

[AHW20] Ulla Aeschbacher, Arne Hansen, and Stefan Wolf. *Invitation to Quantum Informatics*. vdf Hochschulverlag, ETH Zürich, 2020.

[AS17] Guillaume Aubrun and Stanislav J. Szarek. *Alice and Bob Meet Banach: The interface of asymptotic geometric analysis and quantum information theory*, volume 223 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, Rhode Island, 2017.

[ASLB13] M. Agnew, J. Z. Salvail, J. Leach, and R. W. Boyd. Generation of orbital angular momentum bell states and their verification via accessible nonlinear witnesses. *Phys. Rev. Lett.*, 111, 2013.

[BŠ20] A. Buckley and K. Šivic. New examples of extremal positive linear maps. *Linear Algebra Appl.*, 598:110–144, 2020.

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge University Press, 2004.

[BŻ17] Ingemar Bengtsson and Karol Życzkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, 2017.

[Cho75a] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra Appl.*, 10:285–290, 1975.

[Cho75b] M.-D. Choi. Positive semidefinite biquadratic forms. *Linear Algebra Appl.*, 12:95–100, 1975.

[CMHW19] M. Christandl, A. Müller-Hermes, and M. M. Wolf. When do composed maps become entanglement breaking? *Annales Henri Poincare*, 20:2295–2322, 2019.

[Gha10] S. Gharibian. Strong np-hardness of the quantum separability problem. *Quantum Information and Computation*, 10:343–360, 2010.

[Ha13] K.-C. Ha. Notes on extremality of the choi map. *Linear Algebra Appl.*, 439:3156–3165, 2013.

[HH99] Michał Horodecki and Paweł Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Phys. Rev. A*, 59(6):4206–4216, 1999.

[HHH96] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223(1-2):1–8, 1996.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Modern Phys.*, 81(2):865–942, 2009.

[HNW17] A. W. Harrow, A. Natarajan, and X. Wu. An improved semidefinite programming hierarchy for testing entanglement. *Comm. Math. Phys.*, 352(3):881–904, 2017.

[Hor97] Paweł Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232(5):333–339, 1997.

[KK94] H.-J. Kim and S.-H. Kye. Indecomposable positive linear maps in matrix algebras. *Bull. Lond. Math. Soc.*, 26:575–581, 1994.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum Information*. Cambridge University Press, Cambridge, United Kingdom, 10th anniversary edition edition, 2010.

[Nem07] A. Nemirovski. Advances in convex optimization: Conic programming. *Proc. of the International Congress of Math, Eur. Math. Soc., Zürich*, 1:413–444, 2007.

[Osa91] H. Osaka. Indecomposable positive maps in low-dimensional matrix algebras. *Linear Algebra Appl.*, 153:73–83, 1991.

[Per96] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77(8):1413–1415, 1996.

[Qua15] R. Quarez. On the real zeros of positive semidefinite biquadratic forms. *Commun. Algebra*, 43:1317–1353, 2015.

[SF15] Leonard Susskind and Art Friedman. *Quantum Mechanics: The Theoretical Minimum*. Penguin, 2015.

[SF18] Leonard Susskind and Art Friedman. *Special Relativity and Classical Field Theory: The Theoretical Minimum*. Penguin, 2018.

[SPJ05] M. Sampoli, M. Peternell, and B. Jüttler. Exact parameterization of convolution surfaces and rational surfaces with linear normals. *accessed March 2021, <https://dmg.tuwien.ac.at/peternell/lnsurf.pdf>*, 2005.

[Stø63] Erling Størmer. Positive linear maps of operator algebras. *Acta Math.*, 110:233–278, 1963.

[Stø82] Erling Størmer. Decomposable positive maps on c^*-algebras. *Proc. Am. Math. Soc.*, 86(3):402–404, 1982.

[Stø13] Erling Størmer. *Positive Linear Maps of Operator Algebras*. Springer Monographs in Mathematics. Springer-Verlag, Berlin Heidelberg, 2013.

[Sus20] Leonard Susskind. *Three Lectures on Complexity and Black Holes*. SpringerBriefs in Physics. Springer, 2020.

[TT88] K. Tanahashi and J. Tomiyama. Indecomposable positive maps in matrix algebras. *Can. Math. Bull.*, 31(3):308–317, 1988.

[VLOW18] P. Vrana, J.M. Landsberg, G. Ottaviani, and M. Walter. Masterclass on tensors: Geometry and quantum information. Centre for the Mathematics of Quantum Theory, University of Copenhagen, June 2018.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[Wil17] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2nd edition edition, 2017.

[Wor76] S.L. Woronowicz. Positive maps of low dimensional matrix algebras. *Rep. Math. Phys.*, 10(2):165–183, 1976.