Quantum State Local Distinguishability via Convex Optimization

by

Alessandro Cosentino

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Computer Science

Waterloo, Ontario, Canada, 2015

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Entanglement and nonlocality play a fundamental role in quantum computing. To understand the interplay between these phenomena, researchers have considered the model of local operations and classical communication, or LOCC for short, which is a restricted subset of all possible operations that can be performed on a multipartite quantum system. The task of distinguishing states from a set that is known a priori to all parties is one of the most basic problems among those used to test the power of LOCC protocols, and it has direct applications to quantum data hiding, secret sharing and quantum channel capacity.

The focus of this thesis is on state distinguishability problems for classes of quantum operations that are more powerful than LOCC, yet more restricted than global operations, namely the classes of separable and positive-partial-transpose (PPT) measurements. We build a framework based on convex optimization (on cone programming, in particular) to study such problems. Compared to previous approaches to the problem, the method described in this thesis provides precise numerical bounds and quantitative analytic results. By combining the duality theory of cone programming with the channel-state duality, we also establish a novel connection between the state distinguishability problem and the study of positive linear maps, which is a topic of independent interest in quantum information theory.

We apply our framework to several questions that were left open in previous works regarding the distinguishability of maximally entangled states and unextendable product sets. First, we exhibit sets of $k < n$ orthogonal maximally entangled states in $\mathbb{C}^n \otimes \mathbb{C}^n$ that are not perfectly distinguishable by LOCC. As a consequence of this, we show a gap between the power of PPT and separable measurements for the task of distinguishing sets consisting only of maximally entangled states. Furthermore, we prove tight bounds on the entanglement cost that is necessary to distinguish any sets of Bell states, thus showing that quantum teleportation is optimal for this task. Finally, we provide an easily checkable characterization of when an unextendable product set is perfectly discriminated by separable measurements, along with the first known example of an unextendable product set that cannot be perfectly discriminated by separable measurements.

Acknowledgements

First and foremost, I would like to thank my advisor John Watrous for his guidance over my PhD years. His meticulous style of writing has been and always will be an inspiration for me. I also thank him for teaching two terrific courses on quantum information theory and semidefinite programming. From his lectures I learned almost all the mathematical tools I needed for writing this thesis.

Next, I am grateful to professors Richard Cleve, Runyao Duan, Debbie Leung, and Ashwin Nayak for agreeing to be in my defense committee, and to professor Andrew Childs for being in my comprehensive exam committee.

Most of the questions addressed in this thesis were explained to me by Som Bandyopadhyay, Nengkun Yu, and Michael Nathanson. I thank them for a lot of insightful discussions on the problem. The "state distinguishability" research community is small, but has welcomed me warmly.

I owe some of the ideas presented in this work to my colleagues and co-authors Vincent Russo and Nathaniel Johnston. I must thank them also for helping me with coding in MATLAB the optimization problems presented in this thesis.

From my great nerdy friends Robin and Vinayak, I learned too much: lots of theoretical computer science, many research skills and, more importantly, rationality.

I wish to thank grad school fellows Stacey, Adam, Ansis, Jamie, Laura, and Abel, for making my life at IQC more enjoyable, and for being the coolest bunch of quantum kids in the world. I hope our paths will cross many times in the years to come.

Thanks to my roommate Daniele for bringing a piece of Italy into my everyday life. (And I am not talking *only* about Baricelle olive oil!)

To all my soccer team-mates, I'm very sad that I will no longer be playing for Hopeless Experts. Every game, every defeat, every win with you guys has been fantastic. I wish the team every success in the future seasons.

Throughout the past years, my *classical* friend Diego has been reminding me of the joy of computer hacking and of how damn interesting every branch of computer science can be. Thanks for that and for keeping me updated on your favorite musical discoveries.

I have to save my last thanks to my family for their love and support. I missed you!

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

A central subject of study in quantum information theory is the interplay between entanglement and nonlocality. An important tool to study this relationship is the paradigm of local quantum operations and classical communication (LOCC, for short). This is a subset of all global quantum operations, with a fairly intuitive physical description. In a two-party LOCC protocol, Alice and Bob can perform quantum operations only on their local subsystems and the communication must be classical. This restricted paradigm has played a crucial role in the understanding of the role of entanglement in quantum information. It has also provided a framework for the description of basic quantum tasks such as quantum key distribution and entanglement distillation. Furthermore, LOCC protocols are operationally well-motivated, in the sense that classical communication is easy to implement.

The LOCC paradigm does not have a proper classical counterpart. It is worth noticing that its definition does not impose any restriction on the amount of classical communication that is allowed between the parties, and therefore it should not be confused with other setups studied in theoretical computer science where such constraints are instead imposed, such as communication complexity, or information complexity.

A fundamental problem that has been studied to understand the limitations of LOCC protocols is the problem of distinguishing quantum states. The setup of the problem is pretty simple in the bipartite case. The two parties are given a single copy of a quantum state chosen with some probability from a collection of states and their goal is to identify

which state was given, with the assumption that the parties have full a priori knowledge of the collection.

When restricted to classical states, this is an easy task, different strings of bits are always completely distinguishable. In the quantum case, if the states are orthogonal and global operations are permitted, then it is always possible to determine the state with certainty. On the contrary, when the states are not orthogonal, quantum mechanics does not allow perfect discrimination [NC11]. The problem of distinguishing quantum states by global operations dates back to the '70s [Hel69], and since then it has been given different names: *quantum state distinguishability*, *quantum state discrimination*, *quantum detection*, *quantum hypothesis testing*.

Even when the states are orthogonal, things get interesting in the quantum setting once we impose restrictions on the measurements that can be performed on the unknown state. Say the two parties to whom the state is given, Alice and Bob, have their quantum labs very far apart from each other's and, say, their research budget pays only for an infrastructure to communicate with each other on a classical network. In other words, say that only LOCC measurements are allowed on the state. Then Alice and Bob cannot in general discover the state they have been given, even if the states are orthogonal.

The problem of distinguishing among a known set of orthogonal quantum states by LOCC protocols has been studied by several researchers in the last 15 years[1] [BDM+99, WSHV00, GKR+01, HSSH03, Fan04, GKRS04, Nat05, Wat05, YDY11, YDY12]. It is referred to as the *local state distinguishability problem* (or *local state discrimination*) and it has some direct applications to other problems in quantum information theory, such as secret sharing [CGL99, Got00], data hiding [TDL01, DLT02], and the study of quantum channel capacity (see [Wat05, YDY11] and references therein).

Local state distinguishability problems offer insights into how useful entanglement is in quantum information processing tasks. The reason why investigating these problems is helpful comes from the fact that the role of entanglement in such tasks is twofold. On the one hand, many LOCC protocols, such as the ones based on teleportation, are fueled by entanglement shared by the parties, and therefore entanglement turns out to be a helpful resource for distinguishability. On the other hand, if the states to be distinguished are themselves entangled, local measurements on only a part of the states do not always suffice to reveal all the information hidden in the remaining part. The dual role of entanglement has led us towards the choice of the sets to analyze in this work, which ended up belonging to two antipodal categories: sets consisting only of orthogonal maximally entangled states and sets consisting only of product states.

[1] The reader may want to browse through the References section of this thesis for a more complete list.

The set of measurements that can be implemented through LOCC has an apparently complex mathematical structure—no tractable characterization of this set is known, representing a clear obstacle to a better understanding of the limitations of LOCC measurements. For example, given a collection of operators describing a measurement on a bipartite system, the problem of determining whether or not this collection describes an LOCC measurement, or is closely approximated by an LOCC measurement, is not known to be a computationally decidable problem. For this reason, the state discrimination problem described above is sometimes considered for more tractable classes of measurements that approximate, in some sense, the set of LOCC measurements, and that are mathematically and computationally more tractable than the LOCC set. Among these classes, the set of separable and positive-partial-transpose (PPT) measurements are the subject of study of this thesis. Since these classes contain LOCC, any bound on their power is reflected into a bound on the power of LOCC.

The key observation of this dissertation is that the set of PPT operators and the set of separable operators both form closed convex cones and many problems concerning them, including state distinguishability, can be phrased in terms of cone programming, which is a convex optimization framework that generalizes semidefinite programming. In general, we do not have a classical polynomial-time algorithm to solve cone programs and, in fact, optimizing over separable operators is an NP-hard task. Nevertheless, cone programming, like semidefinite programming, comes with a rich duality theory, which can be exploited in order to derive analytical bounds for the problems we are seeking to solve. From the numerical point of view, we exploit the fact that the particular cone programs we are interested in can be approximated by efficiently solvable hierarchies of semidefinite programs [DPS02].

1.2 Summary of the results

We prove the following specific results:

- We obtain an exact formula for the optimal probability of correctly discriminating any set of either three or four Bell states via separable measurements, when the parties are given a partially entangled pair of qubits as a resource. In particular, it is proved that this ancillary pair of qubits must be maximally entangled in order for three Bell states to be perfectly discriminated by separable (or LOCC) measurements, which answers an open question of [YDY14].

- We build up on a construction by Yu, Duan, and Ying [YDY12], and we show the first example of a set with less than n orthogonal maximally entangled states in $\mathbb{C}^n \otimes \mathbb{C}^n$ that are not perfectly distinguishable by LOCC. One takeaway from this is that the dimension of the local subsystems does not play any special role in the nonlocality exhibited by LOCC-indistinguishable sets of maximally entangled states. The same example serves to exhibit a gap between the power of separable and PPT measurements for the task of distinguishing maximally entangled states.

- We provide an easily checkable characterization of when an unextendable product set is perfectly discriminated by separable measurements, and we use this characterization to present an example of an unextendable product set in $\mathbb{C}^4 \otimes \mathbb{C}^4$ that is not perfectly discriminated by separable measurements. This resolves an open question raised in [DFXY09].

- We show that every unextendable product set together with one extra pure state orthogonal to every member of the unextendable product set is not perfectly discriminated by separable measurements.

1.3 Overview

We assume that the reader is familiar with basic concepts of quantum computation and the main target is a researcher in quantum information or a graduate student who has taken an introductory course to quantum based on Nielsen and Chuang [NC11]. Familiarity with more advanced concepts of quantum information theory (based on [Wat15], for example) would certainly help, but it is not necessary. The same can be said about notions of convex optimization, the syllabus of an introductory graduate-level course in convex optimization covers more than is necessary to grasp the material of this thesis. In Chapter 2 basic notions of quantum information and convex optimization are reviewed.

Chapter 3 reviews background material on bipartite state discrimination, including a comparison between previous approaches to the problem and ours.

In Chapter 4, we lay out a general cone programming framework for bipartite state discrimination and we instantiate it for the particular cases of separable and PPT measurement.

In Chapters 5 and 6, we apply the framework described in Chapter 4 to study the distinguishability of sets of maximally entangled states, and unextendable product sets,

respectively. These two chapters are independent from each other and they can be read in any order.

In the last chapter we draw conclusions and ask some open questions that may be of interest for future work.

The thesis is based on the following papers:

- A. Cosentino. **PPT-indistinguishable states via semidefinite programming**. *Physical Review A*, 2013. [Cos13]
- A. Cosentino and V. Russo. **Small sets of locally indistinguishable orthogonal maximally entangled states**. *Quantum Information & Computation*, 2014. [CR14]
- S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu. **Limitations on separable measurements by convex optimization**. *IEEE Transactions on Information Theory*, 2015. [BCJ+15]

Chapter 2

Preliminaries

In this chapter we summarize basic concepts of quantum information theory that will be used in the rest of the thesis. Along the way, we will also pin down the notation that we use throughout this thesis, although for most part, we use notation that is standard in quantum information theory. In particular, we will follow the same terminology and conventions adopted in [Wat15]. This should not serve as in introduction to quantum information. For such an introduction we refer the reader to a standard textbook [NC11].

The last section introduces the basic concepts of convex optimization that are necessary for analyzing problems in quantum information theory. For a more extended treatment of semidefinite programming and cone programming, we refer the reader to [WSV00, TW12] and the references therein.

Contents

2.1 Basic notions of quantum information theory

2.1.1 Vector spaces, linear operators, and linear mappings

All vector spaces considered here are assumed to be complex Euclidean spaces (or, equivalently, finite-dimensional complex Hilbert spaces) and are denoted by scripted capital letters from the end of the English alphabet, such as $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$. Elements of a complex Euclidean space are denoted by lower-case letters from the end of the English alphabet, such as u, v, w, z. For a complex Euclidean spaces of dimension n, elements of the space can be represented as vectors in $\mathbb{C}^n$. The standard basis of such a space is denoted using the Dirac notation as $\{|0\rangle, \ldots, |n-1\rangle\}$.

The inner product of two vectors $u, v \in \mathbb{C}^n$ is defined as

$$\langle u, v \rangle = \sum_{i \in \{1,\ldots,n\}} \overline{u(i)} v(i). \tag{2.1}$$

We write $\mathrm{L}(\mathcal{X}, \mathcal{Y})$ to denote the space of linear operators from a space $\mathcal{X}$ to a space $\mathcal{Y}$, and we write $\mathrm{L}(\mathcal{X})$ as shorthand for $\mathrm{L}(\mathcal{X}, \mathcal{X})$. Throughout the thesis, linear operators will be denoted with capital letters from the beginning and the end of the English alphabet, such as A, B, C, X, Y, Z.

For every operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$, the operator $A^* \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ denotes the adjoint of A, that is, the unique operator that satisfies the equation

$$\langle v, Au \rangle = \langle A^* v, u \rangle, \tag{2.2}$$

for all $u \in \mathcal{X}$ and $v \in \mathcal{Y}$. In the matrix representation of linear operators, A^* is the conjugate transpose of the matrix corresponding to A.

For any space $\mathcal{X}$, we consider the following important sets of operators acting on $\mathcal{X}$:

Hermitian operators – $\mathrm{Herm}(\mathcal{X})$: operators $X \in \mathrm{L}(\mathcal{X})$ such that $X^* = X$.

Positive semidefinite operators – $\mathrm{Pos}(\mathcal{X})$: operators $X \in \mathrm{L}(\mathcal{X})$ for which it holds that $X = Y^* Y$ for some operator $Y \in \mathrm{L}(\mathcal{X})$.

Density operators – $\mathrm{D}(\mathcal{X})$: positive semidefinite operators having trace equal to 1. To denote density operators, we will use letters from the Greek alphabet, such as ρ, σ, ξ.

The eigenvalues of an Hermitian operator are all real numbers. Positive semidefinite operators are Hermitian by definition, and they can be described as those Hermitian operators that have only nonnegative eigenvalues. To recap, we have the following chain of containments:

$$\mathrm{D}(\mathcal{X}) \subset \mathrm{Pos}(\mathcal{X}) \subset \mathrm{Herm}(\mathcal{X}) \subset \mathrm{L}(\mathcal{X}). \tag{2.3}$$

The identity operator acting on a given space $\mathcal{X}$ is denoted by $\mathbb{1}_{\mathcal{X}}$, or just as $\mathbb{1}$ when $\mathcal{X}$ is implicit. For Hermitian operators $A, B \in \mathrm{Herm}(\mathcal{X})$ the notations $A \geq B$ and $B \leq A$ indicate that $A - B$ is positive semidefinite.

Other important operators are *linear isometries*, which are all operators $X \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ such that $X^*X = \mathbb{1}_{\mathcal{X}}$. The set of linear isometries from $\mathcal{X}$ to $\mathcal{Y}$ is denoted by $\mathrm{U}(\mathcal{X}, \mathcal{Y})$. Linear isometries in $\mathrm{L}(\mathcal{X})$ are called *unitary operators* and their set is denoted by $\mathrm{U}(\mathcal{X})$.

We denote the standard Hilbert-Schmidt inner product of two operators X and Y as

$$\langle X, Y \rangle = \mathrm{Tr}(X^*Y). \tag{2.4}$$

The trace norm of an operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is defined as

$$\|A\|_1 = \mathrm{Tr}(\sqrt{A^*A}), \tag{2.5}$$

where $\sqrt{X}$ denotes the square root of a positive semidefinite operator X, that is, the unique positive semidefinite operator Y such that $Y^2 = X$.

A quantum state is represented by a density operator $\rho \in \mathrm{D}(\mathcal{X})$, for some complex Euclidean space $\mathcal{X}$. A state $\rho \in \mathrm{D}(\mathcal{X})$ is said to be *pure* if and only if it has rank equal to 1, or equivalently, if there exists a unit vector $u \in \mathcal{X}$ such that

$$\rho = uu^*.$$

Along with linear operators, we will consider linear mappings of the form

$$\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y}),$$

for complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$. The *adjoint* of a mapping Φ is defined to be the unique mapping

$$\Phi^* : \mathrm{L}(\mathcal{Y}) \to \mathrm{L}(\mathcal{X}),$$

which satisfies the equation

$$\langle \Phi(X), Y \rangle = \langle X, \Phi^*(Y) \rangle, \tag{2.6}$$

for every $X \in \mathrm{L}(\mathcal{X})$ and $Y \in \mathrm{L}(\mathcal{Y})$. Some important sets of linear mappings that we will consider in this thesis are the following:

Hermiticity preserving – mappings of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ such that

$$\Phi(X) \in \mathrm{Herm}(\mathcal{Y}),$$

for any $X \in \mathrm{Herm}(\mathcal{X})$.

Positive – mappings of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ such that $\Phi(X) \in \mathrm{Pos}(\mathcal{Y})$, for any $X \in \mathrm{Pos}(\mathcal{X})$.

Completely positive – mappings of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$, such that

$$\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})}(X) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z}),$$

for every complex Euclidean space $\mathcal{Z}$, and any $X \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Z})$.

Trace-preserving – mappings of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ such that

$$\mathrm{Tr}(\Phi(X)) = \mathrm{Tr}(X),$$

for all $X \in \mathrm{L}(\mathcal{X})$.

Transformations of a quantum system from one state to another are described by *quantum channel*, which are completely positive, trace-preserving linear mappings.

Given the tensor product $\mathcal{X}_1 \otimes \ldots \otimes \mathcal{X}_n$ of n complex Euclidean spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$, and a partition

$$(k_1, \ldots, k_i : k_{i+1}, \ldots, k_n)$$

of the set $\{1, \ldots, n\}$, we use the notation

$$(\mathcal{X}_{k_1} \otimes \ldots \otimes \mathcal{X}_{k_i} : \mathcal{X}_{k_{i+1}} \otimes \ldots \otimes \mathcal{X}_{k_n})$$

to denote a bipartition of the entire space.

It is convenient for the analysis of states in a bipartition $(\mathcal{X} : \mathcal{Y})$ to make use of the correspondence between operators and vectors given by the linear function

$$\mathrm{vec} : \mathrm{L}(\mathcal{Y}, \mathcal{X}) \to \mathcal{X} \otimes \mathcal{Y} \tag{2.7}$$

defined by the action

$$\mathrm{vec}(|k\rangle\langle j|) = |k\rangle|j\rangle \tag{2.8}$$

on standard basis vectors, and by linearity to all $\mathrm{L}(\mathcal{Y}, \mathcal{X})$.

Definition 2.1. Suppose that $\mathcal{X}$ and $\mathcal{Y}$ are complex Euclidean spaces with $n = \dim(\mathcal{X})$ and $m = \dim(\mathcal{Y})$, and assume $n \geq m$. A unit vector $u \in \mathcal{X} \otimes \mathcal{Y}$, representing a pure state, is said to be *maximally entangled* provided that

$$\mathrm{Tr}_{\mathcal{X}}(uu^*) = \frac{\mathbb{1}_{\mathcal{Y}}}{m}. \tag{2.9}$$

This condition is equivalent to

$$u = \frac{1}{\sqrt{m}} \mathrm{vec}(A) \tag{2.10}$$

for $A \in \mathrm{U}(\mathcal{Y}, \mathcal{X})$ being a linear isometry.

2.1.2 Pauli operators and Bell states

One particularly important set of linear operators in $\mathrm{L}(\mathbb{C}^2)$ is the set of Pauli operators

$$\sigma_0 = \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.11}$$

The operators $\sigma_1, \sigma_2, \sigma_3$ are often referred as Pauli-X, -Y, -Z, respectively. The Pauli operators are Hermitian, unitary operators, and moreover, they are orthogonal under the inner product, thus forming an orthogonal basis for $\mathrm{L}(\mathbb{C}^2)$.

Through the vector-operator correspondence of Eq. 2.7, the Pauli operators define an important class of maximally entangled states, famously known as *Bell states*:

$$\psi_k = \frac{1}{2} \mathrm{vec}(\sigma_k) \mathrm{vec}(\sigma_k)^*, \tag{2.12}$$

for $k \in \{0, 1, 2, 3\}$. More explicitly, the Bell states can be written down as follows:

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle, \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}}|0\rangle|1\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle, \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle, \\ |\psi_3\rangle &= \frac{1}{\sqrt{2}}|0\rangle|0\rangle - \frac{1}{\sqrt{2}}|1\rangle|1\rangle. \end{aligned} \tag{2.13}$$

In higher dimensions, one can consider a generalization of the Pauli operators. For any positive integer n, let us the define an n-th primitive root of unity as

$$\omega_n = \exp(2\pi i/n). \tag{2.14}$$

The generalizations of Pauli-X and Pauli-Z in $\mathrm{U}(\mathbb{C}^n)$ are defined as follows:

$$X_n = \sum_{j \in \mathbb{Z}_n} |j+1\rangle\langle j|, \tag{2.15}$$

and

$$Z_n = \sum_{j \in \mathbb{Z}_n} \omega_n^j |j\rangle\langle j|. \tag{2.16}$$

Now we can define the set of *generalized Pauli operators* in $\mathrm{U}(\mathbb{C}^n)$ as the set

$$\left\{ W_{a,b}^{(n)} = X_n^a Z_n^b : a, b \in \mathbb{Z}_n \right\}. \tag{2.17}$$

Starting from these operators we define the *generalized Bell basis* through the vector-operator bijection:

$$\left\{ \psi_{a,b}^{(n)} = \frac{1}{\sqrt{n}} \operatorname{vec}\left(W_{a,b}^{(n)}\right) \operatorname{vec}\left(W_{a,b}^{(n)}\right)^* : a, b \in \mathbb{Z}_n \right\}. \tag{2.18}$$

2.1.3 The Choi isomorphism

To a quantum mapping $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$, we associate an operator $J(\Phi) \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$ defined as follows:

$$J(\Phi) = (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\operatorname{vec}(\mathbb{1}_{\mathcal{X}}) \operatorname{vec}(\mathbb{1}_{\mathcal{X}})^*). \tag{2.19}$$

If we assume that $\mathcal{X}$ has dimension n, we can alternatively write this as

$$J(\Phi) = \sum_{1 \le i,j \le n} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j|. \tag{2.20}$$

The operator $J(\Phi)$ is called the *Choi representation* of Φ. It is often the case that properties of the Choi representation reveal useful information on the mapping. For instance, positive semidefinite operators correspond to Choi representations of completely positive mappings.

2.2 Quantum measurements

When we analyze state distinguishability problems, all the physical operations performed by the involved parties can be formally phrased in terms of quantum measurements. A *quantum measurement* is defined as a function

$$\mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X}), \tag{2.21}$$

for some choice of a positive integer $N > 0$ and a complex Euclidean space $\mathcal{X}$, satisfying the constraint

$$\sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}}. \tag{2.22}$$

The values $\{1, \ldots, N\}$ are the *measurement outcomes* of μ, and the operator $\mu(k)$ is the *measurement operator* of μ associated with the outcome k. The set of all measurements over $\mathcal{X}$ with N outcomes is denoted by $\mathrm{Meas}(N, \mathcal{X})$ and it is a subset of all functions of the same kind of μ, that is,

$$\mathrm{Meas}(N, \mathcal{X}) \subset \mathrm{Pos}(\mathcal{X})^{\{1,\ldots,N\}}. \tag{2.23}$$

Given a measurement $\mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X})$, it is useful to associate a mapping $\Phi_\mu : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathbb{C}^N)$ to it, defined as follows:

$$\Phi_\mu(X) = \sum_{k=1}^{N} \langle \mu(k), X \rangle |k\rangle\langle k|, \tag{2.24}$$

for any $X \in \mathrm{L}(\mathcal{X})$. The mapping Φ_μ is a quantum channel and, in fact, it is a *quantum-to-classical* channel.

In order to capture the limitation of some physical processes, we can define more restricted classes of measurements, which will be the object of study of this thesis. In the definitions that follow it will be assumed that the measurements always act on a bipartite space $\mathcal{X} \otimes \mathcal{Y}$, where $\mathcal{X}$ and $\mathcal{Y}$ denote the complex Euclidean spaces underlying Alice's and Bob's systems, respectively. Although all the notions considered in this section could be extended to a more general scenario where more than two parties are involved in the measurement, here and in the rest of the thesis we restrict our attention to the bipartite case.

2.2.1 LOCC measurements

We refer the reader to the references [Man13, Wat15] for the precise definition of an LOCC channel. To a measurement $\mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ on a bipartite system, we associate the quantum-to-classical channel

$$\Phi_\mu(X) = \sum_{k=1}^{N} \langle \mu(k), X \rangle |k\rangle\langle k| \otimes |k\rangle\langle k|, \tag{2.25}$$

and we say that μ is an LOCC measurement if the channel Φ_μ can be implemented by an LOCC protocol between Alice and Bob.

Notice that we can define different classes of LOCC, according to the number (finite or infinite) of rounds that compose the protocols. For the scope of this thesis, the only important thing to notice is that all the LOCC variants are contained in the class of separable measurement (defined in the next section).

We denote the set of all N-outcome LOCC bipartite measurements on the bipartition $(\mathcal{X} : \mathcal{Y})$ by $\mathrm{Meas}_{\mathrm{LOCC}}(N, \mathcal{X} : \mathcal{Y})$.

2.2.2 Separable measurements

The class of *separable measurements* represents a commonly studied approximation of the set of LOCC measurements. A positive semidefinite operator $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is said to be *separable* if it is possible to write

$$P = \sum_{k=1}^{M} Q_k \otimes R_k, \tag{2.26}$$

for some choice of a positive integer M and positive semidefinite operators

$$Q_1, \ldots, Q_M \in \mathrm{Pos}(\mathcal{X}) \qquad \text{and} \qquad R_1, \ldots, R_M \in \mathrm{Pos}(\mathcal{Y}). \tag{2.27}$$

Definition 2.2. Let $\mathcal{X}^{\mathsf{A}}, \mathcal{X}^{\mathsf{B}}, \mathcal{Y}^{\mathsf{A}}$, and $\mathcal{Y}^{\mathsf{B}}$ be complex Euclidean spaces. A completely positive mapping

$$\Phi : \mathrm{L}(\mathcal{X}^{\mathsf{A}} \otimes \mathcal{X}^{\mathsf{B}}) \to \mathrm{L}(\mathcal{Y}^{\mathsf{A}} \otimes \mathcal{Y}^{\mathsf{B}})$$

is said to be a *separable channel* if it is a trace-preserving mappings and it is possible to write

$$\Phi = \sum_{k=1}^{M} \Psi_k^{\mathsf{A}} \otimes \Psi_k^{\mathsf{B}}, \tag{2.28}$$

for some choice of a positive integer M and collections of completely positive mappings

$$\Psi_1^{\mathsf{A}}, \ldots, \Psi_M^{\mathsf{A}} : \mathrm{L}(\mathcal{X}^{\mathsf{A}}) \to \mathrm{L}(\mathcal{Y}^{\mathsf{A}}) \qquad \text{and} \qquad \Psi_1^{\mathsf{B}}, \ldots, \Psi_M^{\mathsf{B}} : \mathrm{L}(\mathcal{X}^{\mathsf{B}}) \to \mathrm{L}(\mathcal{Y}^{\mathsf{B}}). \tag{2.29}$$

Definition 2.3. Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and $N > 0$ be a positive integer. A measurement

$$\mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}) \tag{2.30}$$

is said to be a *separable measurement* if the corresponding quantum-to-classical channel Φ_μ, defined as in Eq. (2.25), is a separable channel.

We denote the set of all N-outcome separable measurements on the bipartition $(\mathcal{X} : \mathcal{Y})$ by $\mathrm{Meas}_{\mathrm{Sep}}(N, \mathcal{X} : \mathcal{Y})$. Separable measurements can be alternatively characterized as those measurements whose measurement operators are separable, as it is formalized by the following proposition.

Proposition 2.4. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, and let $N > 0$. A measurement $\mu \in \mathrm{Meas}_{\mathrm{Sep}}(N, \mathcal{X} : \mathcal{Y})$ is separable if and only if each $\mu(k)$ is a separable operator, that is, $\mu(k) \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y})$, for each $k \in \{1, \ldots, N\}$.*

We refer the reader to [Wat15] for a proof of Proposition 2.4, as well as for a proof that every LOCC measurement is necessarily a separable measurement. From this latter fact it follows that any limitation proved to hold for every separable measurement must also hold for every LOCC measurement.

2.2.3 PPT measurements

Another class that represents a relaxation of the set of LOCC measurements is the class of PPT measurements. Let $\mathrm{T}_{\mathcal{X}} : \mathrm{L}(\mathcal{X} \otimes \mathcal{Y}) \to \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$ be the linear mapping representing partial transposition with respect to the standard basis $\{|0\rangle, \ldots, |n-1\rangle\}$ of $\mathcal{X}$. Equivalently,

$$\mathrm{T}_{\mathcal{X}}(X) = (\mathrm{T} \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(X), \tag{2.31}$$

for any operator $X \in \mathrm{L}(X \otimes \mathcal{Y})$, where $\mathrm{T} : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{X})$ is the transpose mapping.

When proving facts about PPT operators, we will use the fact that the transpose mapping is its own adjoint and inverse, that is,

$$\langle \mathrm{T}(X), Y \rangle = \langle X, \mathrm{T}(Y) \rangle, \qquad \text{for any } X, Y \in \mathrm{L}(\mathcal{X}), \tag{2.32}$$

and

$$\mathrm{T}(\mathrm{T}(X)) = X, \qquad \text{for any } X \in \mathrm{L}(\mathcal{X}). \tag{2.33}$$

A positive semidefinite operator $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is a *PPT* operator (short for *positive partial transpose*) if it holds that

$$\mathrm{T}_{\mathcal{X}}(P) \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}). \tag{2.34}$$

We denote the set of all PPT operators in $\mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ as

$$\mathrm{PPT}(\mathcal{X} : \mathcal{Y}) = \{P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}) \,:\, \mathrm{T}_{\mathcal{X}}(P) \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})\}. \tag{2.35}$$

Notice that transpose and partial transpose are basis dependent, but the notion of PPT is not. Also, in the definition of $\mathrm{PPT}(\mathcal{X} : \mathcal{Y})$, it is irrelevant which of the two subspaces the partial transpose acts on. In fact, since the transpose is a positive mapping, we have that

$$\mathrm{T}_{\mathcal{Y}}(P) \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}) \Rightarrow \mathrm{T}(\mathrm{T}_{\mathcal{Y}}(P)) = \mathrm{T}_{\mathcal{X}}(P) \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}). \tag{2.36}$$

A measurement is PPT if all its operators are PPT, as formally specified by the following definition.

Definition 2.5. A measurement $\mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is called *PPT* if it is represented by a collection of PPT measurement operators, that is,

$$\mu(k) \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y}), \tag{2.37}$$

for all $k \in \{1, \ldots, N\}$.

We denote the set of all N-outcome PPT measurements on the bipartition $(\mathcal{X} : \mathcal{Y})$ by $\mathrm{Meas}_{\mathrm{PPT}}(N, \mathcal{X} : \mathcal{Y})$.

Every separable operator is a PPT operator, so every separable measurement (and therefore every LOCC measurement) is a PPT measurement as well.

Proposition 2.6. *Any separable operator $P \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y})$ is also a PPT operator over the same bipartition, that is, $P \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$.*

Proof. Suppose that $P \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y})$. Then it holds that

$$P = \sum_{k=1}^{M} Q_k \otimes S_k, \tag{2.38}$$

for some choice of a positive integer $M > 0$ and collections of operators

$$Q_1, \ldots, Q_M \in \mathrm{Pos}(\mathcal{X}) \qquad \text{and} \qquad R_1, \ldots, R_M \in \mathrm{Pos}(\mathcal{Y}). \tag{2.39}$$

As the transpose mapping is positive, we have

$$(\mathrm{T} \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(S) = \sum_{k=1}^{M} \mathrm{T}(P_k) \otimes Q_k \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}), \tag{2.40}$$

and therefore $S \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$. □

For a positive semidefinite operator, the condition of remaining positive semidefinite under the operation of partial transpose is therefore a necessary condition for separability. It is also sufficient in $\mathbb{C}^2 \otimes \mathbb{C}^3$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$ [Per96, HHH96], but it is not in higher dimension, where there are entangled PPT operators.

The Choi operator of the transpose mapping $\mathrm{T} : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ is the *swap operator* $W_n \in \mathrm{U}(\mathbb{C}^n \otimes \mathbb{C}^n)$, defined on the standard basis as

$$W_n = \sum_{i,j=0}^{n-1} |i\rangle\langle j| \otimes |j\rangle\langle i|. \tag{2.41}$$

The swap operator is not positive semidefinite and therefore the transpose mapping is not completely positive.

The primary appeal of the set of PPT measurements is its mathematical simplicity. In particular, the PPT condition is represented by linear and positive semidefinite constraints, which allows for an optimization over the collection of PPT measurements to be represented by a semidefinite program.

The reader may find useful the Venn diagram of Figure 2.1, which pictures inclusion relationships between the main classes of mesaurements considered in the thesis. Notice that all inclusion in the diagram are known to be strict.

2.3 Convex optimization

All the results of this thesis are based on a mathematical framework called cone programming, which generalizes semidefinite programming. There has been an extensive range of applications of semidefinite programming to quantum information theory, but this is not

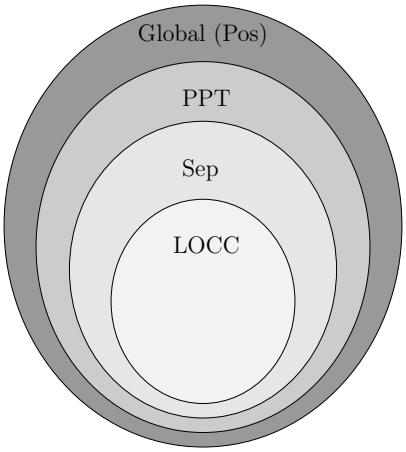

Figure 2.1: Inclusion relationships between the classes of measurements studied in the thesis.

the case for the more general cone programming framework. The success of semidefinite programming in quantum information comes from the fact that many quantum primitives (states, channels, global measurements) can be represented within the cone of positive semidefinite operators with the addition of simple linear constraints. Problems in which one optimizes over the cone of separable operators, such as the problem of discriminating states by separable measurements considered in this thesis, do not have a characterization in the framework of semidefinite programming and for such problems the full expressivity of the general cone programming framework is required. In this section we review basic definitions in convex analysis and convex optimization.

Let $\mathcal{V}$ be an arbitrary vector space over the real or complex number. A subset $\mathcal{C}$ of $\mathcal{V}$ is a *cone* if $u \in \mathcal{C}$ implies that $\lambda u \in \mathcal{C}$, for all $\lambda \geq 0$. A cone $\mathcal{C}$ is convex if $u, v \in \mathcal{C}$ implies that $u + v \in \mathcal{K}$. A cone program (also known as a *conic program*) expresses the maximization of a linear function over the intersection of an affine subspace and a closed convex cone in a finite-dimensional real inner product space [BV04].

When describing a cone program, it is sometimes convenient to compose small closed convex cones in a bigger one, and in order to do that, one can make use of the following fact.

Fact 2.7. *The direct sum $\mathcal{K} \oplus \mathcal{K}'$ of two closed convex cones $\mathcal{K}$ and K' is a closed convex cone.*

Linear programming (LP) and semidefinite programming (SDP) are special cases of

cone programming: in linear programming, the closed convex cone over which the optimization occurs is the positive orthant in $\mathbb{R}^n$, while in semidefinite programming the optimization is over the cone $\mathrm{Pos}(\mathbb{C}^n)$ of positive semidefinite operators on $\mathbb{C}^n$. In the case of semidefinite programming, the finite-dimensional real inner product space is the real vector space $\mathrm{Herm}(\mathbb{C}^n)$ of Hermitian operators on $\mathbb{C}^n$, equipped with the Hilbert-Schmidt inner product.

Linear programming

Let n, m be positive integers, $c \in \mathbb{R}^n$ and $b \in \mathbb{R}^m$ be vectors of real numbers, and $A \in \mathbb{R}^{n \times m}$ be a matrix with real entries. Then a *linear program* is defined by the triple (c, b, A) and by the following pair of optimization problems.

Primal linear program		Dual linear program	
maximize:	$\langle c, x \rangle$	minimize:	$\langle b, y \rangle$
subject to:	$Ax = b,$	subject to:	$A^{\mathsf{T}} y \geq c,$
	$x \geq 0.$		$y \in \mathbb{R}^n.$

Semidefinite programming

Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, $A \in \mathrm{Herm}(\mathcal{X})$ and $B \in \mathrm{Herm}(\mathcal{Y})$ be Hermitian operators, and $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ be a Hermiticity preserving mapping. A *semidefinite program* is defined by the triple (A, B, Φ) and by the following pair of optimization problems.

Primal semidefinite program		Dual semidefinite program	
maximize:	$\langle A, X \rangle$	minimize:	$\langle B, Y \rangle$
subject to:	$\Phi(X) = B,$	subject to:	$\Phi^*(Y) \geq A,$
	$X \in \mathrm{Pos}(\mathcal{X}).$		$Y \in \mathrm{Herm}(\mathcal{Y}).$

Cone programming

For the purposes of the present thesis, it is sufficient to consider only cone programs defined over spaces of Hermitian operators (with the Hilbert-Schmidt inner product). In particular, let $\mathcal{Z}$ and $\mathcal{W}$ be complex Euclidean spaces and let $\mathcal{K} \subseteq \mathrm{Herm}(\mathcal{Z})$ be a closed,

convex cone. For any choice of a linear map $\Phi : \mathrm{Herm}(\mathcal{Z}) \to \mathrm{Herm}(\mathcal{W})$ and Hermitian operators $A \in \mathrm{Herm}(\mathcal{Z})$ and $B \in \mathrm{Herm}(\mathcal{W})$, one has a *cone program* defined by (A, B, Φ) and represented by the following pair of optimization problems.

Primal cone program		Dual cone program	
maximize:	$\langle A, X \rangle$	minimize:	$\langle B, Y \rangle$
subject to:	$\Phi(X) = B,$	subject to:	$\Phi^*(Y) - A \in \mathcal{K}^*,$
	$X \in \mathcal{K}.$		$Y \in \mathrm{Herm}(\mathcal{W}).$

Here, $\mathcal{K}^*$ denotes the *dual cone* to $\mathcal{K}$, defined as

$$\mathcal{K}^* = \{Y \in \mathrm{Herm}(\mathcal{Z}) \,:\, \langle X, Y \rangle \geq 0 \text{ for all } X \in \mathcal{K}\}, \tag{2.42}$$

and $\Phi^* : \mathrm{Herm}(\mathcal{W}) \to \mathrm{Herm}(\mathcal{Z})$ is the adjoint mapping to Φ.

In order to see how semidefinite programming is a special case of cone programming, let us observe the following elementary fact that comes from the definition of positive semidefinite operators.

Fact 2.8. *The cone of positive semidefinite operators is self-dual, that is,*

$$\mathrm{Pos}(\mathcal{X}) = (\mathrm{Pos}(\mathcal{X}))^*, \tag{2.43}$$

for any complex Euclidean space $\mathcal{X}$.

In light of this, we have that $\mathcal{K} = \mathcal{K}^* = \mathrm{Pos}(\mathcal{X})$ and we can write the constraint from the cone programming dual problem as $\Phi^*(Y) - A \in \mathrm{Pos}(\mathcal{X})$, that is, $\Phi^*(Y) \geq A$.

Most of the definitions we introduce in the rest of the section holds for all linear, semidefinite, and more general cone programs. For a cone program defined by (A, B, Φ), one defines the *feasible sets* $\mathcal{A}$ and $\mathcal{B}$ of the primal and dual problems as

$$\mathcal{A} = \big\{X \in \mathcal{K} : \Phi(X) = B\big\} \qquad \text{and} \qquad \mathcal{B} = \big\{Y \in \mathrm{Herm}(\mathcal{W}) : \Phi^*(Y) - A \in \mathcal{K}^*\big\}. \tag{2.44}$$

One says that the associated cone program is *primal feasible* if $\mathcal{A} \neq \emptyset$, and is *dual feasible* if $\mathcal{B} \neq \emptyset$. The function $X \mapsto \langle A, X \rangle$ from $\mathrm{Herm}(\mathcal{Z})$ to $\mathbb{R}$ is called the *primal objective function*, and the function $Y \mapsto \langle B, Y \rangle$ from $\mathrm{Herm}(\mathcal{W})$ to $\mathbb{R}$ is called the *dual objective function*. The *optimal values* associated with the primal and dual problems are defined as

$$\alpha = \sup\big\{\langle A, X \rangle : X \in \mathcal{A}\big\} \qquad \text{and} \qquad \beta = \inf\big\{\langle B, Y \rangle : Y \in \mathcal{B}\big\}, \tag{2.45}$$

respectively. (It is conventional to interpret that $\alpha = -\infty$ when $\mathcal{A} = \emptyset$ and $\beta = \infty$ when $\mathcal{B} = \emptyset$.) The property of *weak duality*, which holds for all cone programs, is that the primal optimum can never exceed the dual optimum.

Proposition 2.9 (Weak duality for cone programs)**.** *For any choice of complex Euclidean spaces $\mathcal{Z}$ and $\mathcal{W}$, a closed, convex cone $\mathcal{K} \subseteq \mathrm{Herm}(\mathcal{Z})$, Hermitian operators $A \in \mathrm{Herm}(\mathcal{Z})$ and $B \in \mathrm{Herm}(\mathcal{W})$, and a linear map $\Phi : \mathrm{Herm}(\mathcal{Z}) \to \mathrm{Herm}(\mathcal{W})$, it holds that $\alpha \leq \beta$, for α and β as defined in (2.45).*

Proof. The proposition is trivial in case $\mathcal{A} = \emptyset$ (which implies that $\alpha = -\infty$) or $\mathcal{B} = \emptyset$ (which implies that $\beta = \infty$), so we will restrict our attention to the case that both $\mathcal{A}$ and $\mathcal{B}$ are nonempty. For any choice of $X \in \mathcal{A}$ and $Y \in \mathcal{B}$, one must have $X \in \mathcal{K}$ and $\Phi^*(Y) - A \in \mathcal{K}^*$, and therefore $\langle \Phi^*(Y) - A, X \rangle \geq 0$. It follows that

$$\langle A, X \rangle = \langle \Phi^*(Y), X \rangle - \langle \Phi^*(Y) - A, X \rangle \leq \langle Y, \Phi(X) \rangle = \langle B, Y \rangle. \tag{2.46}$$

Taking the supremum over all $X \in \mathcal{A}$ and the infimum over all $Y \in \mathcal{B}$ establishes that $\alpha \leq \beta$. □

Weak duality implies that every dual feasible operator $Y \in \mathcal{B}$ provides an upper bound of $\langle B, Y \rangle$ on the value $\langle A, X \rangle$ that is achievable over all choices of a primal feasible operator $X \in \mathcal{A}$, and likewise every primal feasible operator $X \in \mathcal{A}$ provides a lower bound of $\langle A, X \rangle$ on the value $\langle B, Y \rangle$ that is achievable over all choices of a dual feasible solution $Y \in \mathcal{B}$. In other words, it holds that $\langle A, X \rangle \leq \alpha \leq \beta \leq \langle B, Y \rangle$, for every $X \in \mathcal{A}$ and $Y \in \mathcal{B}$.

Some cone programs also satisfy the property of *strong duality*, which holds when the optimal values of the primal program and of the dual program are equal, and the optimal value of the dual program is attained. We abstain from a formal treatment of the conditions that guarantee strong duality. Even though all cone programs described in the following chapters satisfy strong duality, none of our results depend on that.

Chapter 3

Bipartite state discrimination

This chapter introduces the problem of discriminating quantum states from a known set. A scenario describing the problem is first presented for the case where the unknown state is given to a single individual, and then generalized to a different scenario where the unknown state is distributed to two parties. In this thesis we will focus on the bipartite case, leaving for future work an extension of the results to the multipartite case.

After the problem description, this chapter reviews relevant background work, including prior results on the local distinguishability of two classes of pure states that will be the object of study in the following chapters: maximally entangled states and product states.

Contents

3.1 Problem description

Global state discrimination

An instance of the state discrimination problem is defined by a complex Euclidean space $\mathcal{X}$, a positive integer N, and by an ensemble $\mathcal{E}$ of N states, that is,

$$\mathcal{E} = \big\{(p_1, \rho_1), \ldots, (p_N, \rho_N)\big\}, \tag{3.1}$$

where $(p_1, \ldots, p_N)$ is a probability vector and $\rho_1, \ldots, \rho_N \in \mathrm{D}(\mathcal{X})$ are density operators representing quantum states. We denote the set of all ensemble of this kind by $\mathrm{Ens}(N, \mathcal{X})$.

The problem is formally described by the following scenario, which involves two individuals, Alice and Charlie (the reader who misses Bob can be reassured that he will join us soon). Charlie picks an index

$$k \in \{1, \ldots, N\},$$

according to the probability distribution $(p_1, \ldots, p_N)$, prepares a quantum register X with the state $\rho_k \in \mathrm{D}(\mathcal{X})$, and sends it to Alice, whose task is to identify the index k by performing a measurement on the register X.

For Alice performing a measurement

$$\mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X}), \tag{3.2}$$

the probability that she correctly distinguishes $\mathcal{E}$ is given by the expression

$$\mathrm{opt}(\mathcal{E}, \mu) = \sum_{k=1}^{N} p_k \langle \mu(k), \rho_k \rangle. \tag{3.3}$$

Since μ is a measurement and $\rho_1, \ldots, \rho_N$ are density operators, it is clear that

$$0 \leq \langle \mu(k), \rho_k \rangle \leq 1, \tag{3.4}$$

for each $k \in \{1, \ldots, N\}$. Moreover, since p is a probability vector, we have that

$$0 \leq \mathrm{opt}(\mathcal{E}, \mu) \leq 1. \tag{3.5}$$

We denote by $\mathrm{opt}(\mathcal{E})$ the maximum probability of distinguishing $\mathcal{E}$ for any possible measurement, that is,

$$\mathrm{opt}(\mathcal{E}) = \max_{\mu \in \mathrm{Meas}(N,\mathcal{X})} \mathrm{opt}(\mathcal{E}, \mu). \tag{3.6}$$

We say that $\mathcal{E}$ is *distinguishable with probability at least* p if we have $\mathrm{opt}(\mathcal{E}) \geq p$. Whenever $\mathcal{E}$ is distinguishable with probability 1, we say that $\mathcal{E}$ is *perfectly distinguishable* or that Alice can distinguish $\mathcal{E}$ *with certainty*.

The probability distribution with which the states are selected is not important if we are only interested in perfect distinguishability. In fact, from the bounds in Eq. (3.4) and a standard convexity argument, for any probability vector $p = (p_1, \ldots, p_N)$, it holds that

$$\sum_{k=1}^{N} p_k \langle \mu(k), \rho_k \rangle = 1 \tag{3.7}$$

if and only if

$$\langle \mu(k), \rho_k \rangle = 1, \tag{3.8}$$

for each $k \in \mathrm{supp}(p)$. For this reason, whenever we are only interested in a qualitative result (whether perfect distinguishability holds or not), we will take p to be the uniform distribution, that is, $p = (1/N, \ldots, 1/N)$. In such cases, we will simply denote the ensemble by the list of its states, that is,

$$\mathcal{E} = \{\rho_1, \ldots, \rho_N\}. \tag{3.9}$$

We will often be interested in the distinguishability of pure-state ensembles, where each density operator is a rank-one projector, that is, for each $k \in \{1, \ldots, N\}$, $\rho_k = u_k u_k^*$, for a list of unit vectors $\{u_1, \ldots, u_N\} \in \mathcal{X}$. In such case, by a further abuse of notation, we simply denote the ensemble by a list of its vectors:

$$\mathcal{E} = \{u_1, \ldots, u_N\}. \tag{3.10}$$

If the states are mutually orthogonal, that is,

$$\langle \rho_i, \rho_j \rangle = 0, \tag{3.11}$$

for all $i, j \in \{1, \ldots, N\}$ with $i \neq j$, there is a measurement that perfectly distinguishes them. Consider the spectral decomposition of each state:

$$\rho_k = \sum_{i=1}^{r_k} \lambda_i x_{k,i} x_{k,i}^*, \tag{3.12}$$

with $\lambda_1, \ldots, \lambda_{r_k}$ being positive real numbers and $\{x_{k,1}, \ldots, x_{k,r_k}\} \subset \mathcal{X}$ being an orthonormal set. Alice can then construct the quantum measurement that perfectly distinguishes the states, by defining the following measurement operators:

$$\mu(k) = \sum_{i=1}^{r_k} x_{k,i} x_{k,i}^*, \tag{3.13}$$

for each $k = 1, \ldots, N-1$, and

$$\mu(N) = \mathbb{1}_{\mathcal{X}} - \sum_{k=1}^{N-1} \mu(k). \tag{3.14}$$

It is clear that μ is a valid measurement and that

$$\langle \mu(k), \rho_k \rangle = 1, \tag{3.15}$$

for all $k \in \{1, \ldots, N\}$.

Global distinguishability of non-orthogonal states is a prolific topic on its own and a treatment of it is outside the scope of this thesis. For an exposition of results regarding global state discrimination, the reader is referred to numerous surveys on the topic [Che00, BHH04].

Bipartite state discrimination

This dissertation focuses on a modification of the above scenario in which we have three individuals involved: Alice, Bob, and Charlie. In this new scenario, the states to be distinguished lie on the tensor product of two complex Euclidean spaces, which we label by $\mathcal{X}$ and $\mathcal{Y}$ and which are held respectively by Alice and Bob. In other words, the ensemble consists of N bipartite states represented by the density matrices $\rho_1, \ldots, \rho_N \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$.

Charlie picks an index $k \in \{1, \ldots, N\}$ and prepares the corresponding state $\rho_k \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ on a pair of quantum registers (X, Y) that belong to Alice and Bob, in the sense that the underlying space is $\mathcal{X} \otimes \mathcal{Y}$. Their task is to identify the index k chosen by Charlie, by means of an LOCC measurement on (X, Y).

We will denote by $\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E})$ the maximum success probability for Alice and Bob to distinguish an ensemble $\mathcal{E} \in \mathrm{Ens}(N, \mathcal{X} \otimes \mathcal{Y})$ by means of any LOCC measurement, that is,

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) = \max_{\mu \in \mathrm{Meas}_{\mathrm{LOCC}}(N, \mathcal{X}:\mathcal{Y})} \mathrm{opt}(\mathcal{E}, \mu). \tag{3.16}$$

As it was discussed in Section 2.2, the set of LOCC measurements has a complex mathematical structure. For this reason, the state discrimination problem has been analyzed for more tractable classes of measurements that approximate, in some sense, the LOCC measurements. Among these, the classes of separable and PPT measurements are the most studied, because of their nice mathematical and computational properties.

We denote by $\mathrm{opt}_{\mathrm{Sep}}(\mathcal{E})$ and $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E})$ the optimal probability of distinguishing an ensemble $\mathcal{E} \in \mathrm{Ens}(N, \mathcal{X} \otimes \mathcal{Y})$ by separable and PPT measurements, respectively:

$$\mathrm{opt}_{\mathrm{Sep}}(\mathcal{E}) = \max_{\mu \in \mathrm{Meas}_{\mathrm{Sep}}(N, \mathcal{X}:\mathcal{Y})} \mathrm{opt}(\mathcal{E}, \mu), \tag{3.17}$$

and

$$\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) = \max_{\mu \in \mathrm{Meas}_{\mathrm{PPT}}(N, \mathcal{X}:\mathcal{Y})} \mathrm{opt}(\mathcal{E}, \mu). \tag{3.18}$$

In lights of the containments pictured by the diagram in Figure 2.1, we have the following chain of inequalities:

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \leq \mathrm{opt}_{\mathrm{Sep}}(\mathcal{E}) \leq \mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) \leq \mathrm{opt}(\mathcal{E}), \tag{3.19}$$

for any ensemble $\mathcal{E}$.

Interestingly, for each of these inequalities, there exists a set of states that makes the inequality strict. In the rest of this chapter we will see some examples for which the separation is achieved.

In most of our examples and in most prior works on bipartite state discrimination, the states are taken to be pure and orthogonal, so that a global measurement can trivially discriminate them with certainty, that is, $\mathrm{opt}(\mathcal{E}) = 1$. In such cases, a separation between $\mathrm{opt}(\mathcal{E})$ and, say, $\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E})$ is obtained by showing that the set of states is not perfectly distinguishable by LOCC measurements.

3.2 Discriminating between pairs of states

A case of particular interest is when there are two states to be distinguished, chosen with equal probability. This is equivalent to the quantum data hiding challenge in which a secret bit $b \in \{0, 1\}$ is required to be hidden into a bipartite state $\sigma_b \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$. In the language of the previous section, we say that quantum data hiding is possible if there exists an ensemble

$$\mathcal{E} = \left\{ \left(\frac{1}{2}, \sigma_0 \right), \left(\frac{1}{2}, \sigma_1 \right) \right\} \tag{3.20}$$

such that two conditions are simultaneously satisfied:

(a) $\mathrm{opt}(\mathcal{E}) = 1$, and

(b) $\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \leq 1/2 + \varepsilon$,

for some "small" values of ε. The exact bounds on ε define the strength of the hiding scheme and, of course, depend on the dimensions of Alice's and Bob's spaces.

The condition (a) above is equivalent to requiring the two states to be orthogonal[1]. A consequence of this is that at least one of them must be a mixed, since a result by Walgate, et al. [WSHV00] shows that any two orthogonal bipartite *pure* states can be perfectly distinguished by LOCC.

The problem of discriminating between two quantum states is also interesting for its connection with operator norms. In particular, a connection between the trace norm and the optimal probability of distinguishing two states by means of global measurements is estabilished by the following theorem.

Theorem 3.1 (Holevo-Helstrom)**.** *Given a complex Euclidean space $\mathcal{X}$ and two density operators $\sigma_0, \sigma_1 \in \mathrm{D}(\mathcal{X})$, it holds that*

$$\mathrm{opt}(\{\sigma_0, \sigma_1\}) = \frac{1}{2} + \frac{1}{4}\|\sigma_0 - \sigma_1\|_1. \tag{3.21}$$

By reversing the logic direction of this theorem, one can define operator norms starting from different set of measurements. This approach was taken in [MWW09], where the so-called LOCC-norm was defined so that the following holds:

$$\mathrm{opt}_{\mathrm{LOCC}}(\{\sigma_0, \sigma_1\}) = \frac{1}{2} + \frac{1}{4}\|\sigma_0 - \sigma_1\|_{\mathrm{LOCC}}. \tag{3.22}$$

Similarly, one may define norms $\|\cdot\|_{\mathrm{PPT}}$ and $\|\cdot\|_{\mathrm{Sep}}$ that correspond to distinguishability by PPT and separable measurements, respectively. (For a recent result concerning these norms, see [AL15].)

[1] We could be more general here and define another parameter $\delta \approx 0$ so to weaken Condition (a) to be $\mathrm{opt}(\mathcal{E}) \geq 1 - \delta$. This would not affect the discussion that follows, except for making the presentation less clean.

Example 3.2 (Werner hiding pairs)**.** One typical quantum data hiding scheme [TDL01, DLT02] encodes the hidden classical bit in a *Werner hiding pair*. For any positive integer $n \geq 2$, let $W_n \in \mathrm{U}(\mathbb{C}^n \otimes \mathbb{C}^n)$ be the swap operator defined in Eq. (2.41). A Werner hiding pair in $\mathbb{C}^n \otimes \mathbb{C}^n$ is defined by two states

$$\sigma_0^{(n)} = \frac{\mathbb{1} \otimes \mathbb{1} + W_n}{n(n+1)} \qquad \text{and} \qquad \sigma_1^{(n)} = \frac{\mathbb{1} \otimes \mathbb{1} - W_n}{n(n-1)}. \tag{3.23}$$

Notice that $\sigma_0^{(n)}$ and $\sigma_1^{(n)}$ are also the normalized projections on the symmetric and anti-symmetric subspace, respectively. From the orthogonality of the two states, we have

$$\mathrm{opt}(\mathcal{E}^{(n)}) = 1, \tag{3.24}$$

for any n, or equivalently

$$\|\sigma_0^{(n)} - \sigma_1^{(n)}\|_1 = 2. \tag{3.25}$$

In the next chapter we show that

$$\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}^{(n)}) \leq \frac{1}{2} + \frac{1}{n+1}, \tag{3.26}$$

and therefore this is an example of a set of states that makes the rightmost inequality in Eq. (3.19) strict. Since there is an LOCC measurement that achieves the bound [DLT02], we also have

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}^{(n)}) = \mathrm{opt}_{\mathrm{Sep}}(\mathcal{E}^{(n)}) = \mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}^{(n)}) = \frac{1}{2} + \frac{1}{n+1}, \tag{3.27}$$

or equivalently

$$\|\sigma_0^{(n)} - \sigma_1^{(n)}\|_{\mathrm{LOCC}} = \|\sigma_0^{(n)} - \sigma_1^{(n)}\|_{\mathrm{Sep}} = \|\sigma_0^{(n)} - \sigma_1^{(n)}\|_{\mathrm{PPT}} = \frac{4}{n+1}. \tag{3.28}$$

3.3 Discrimination of maximally entangled states

When investigating any kind of problem, a typical computer science approach is to bring the operating parameters of the problem to one extreme. In order to get a better understanding of the role played by entanglement in bipartite state distinguishability problems, one can restrict their attention to the case in which the sets to be distinguished consist of orthogonal maximally entangled pure states. Considering states that are maximally entangled, as opposed to partially entangled, is useful to reduce the number of variables that need to be

taken into account, and it helps to have neater problem statements. It makes the problem easier to handle mathematically (recall that maximally entangled states are in a one-to-one correspondence with unitary operators) and, at the same time, it constitutes an edge case that is interesting from the physical point of view. The reason to consider maximally entangled states can be summarized into one question: why bother with more complicated cases when we do not even know how to deal with that?

In this section, some known results on the distinguishability of maximally entangled states by LOCC, separable, and PPT measurements are reviewed, whereas new results are presented in Chapter 5.

The simplest example of a set of LOCC-indistinguishable maximally entangled states is the standard 2-qubit Bell basis (Eq. (2.13)). It turns out that the maximum probability of distinguishing these 4 states, for any LOCC measurement, is 1/2 [GKR+01]. In fact, a similar bound holds more in general: if we are given an equally probable ensemble of N orthogonal maximally entangled states in $\mathbb{C}^n \otimes \mathbb{C}^n$, the maximum probability of distinguishing them by LOCC is n/N [GKRS04]. This bound holds even for the wider class of separable [DFXY09] and PPT measurements [YDY12]. In Chapter 5 this result is re-proved using our cone programming framework.

The assumption on the sets consisting entirely of maximally entangled states is particularly significant when we inquire the question of how the size of LOCC-indistinguishable sets relates to the local dimension of each of Alice's and Bob's subsystems. In fact, if we allow states that are not maximally entangled to be in the set, we can construct indistinguishable sets with a fixed size in any dimension we like. Indeed, whenever we find a set of indistinguishable maximally entangled states for certain local dimensions, those states remain indistinguishable when embedded in any larger local dimensions. Nonetheless they are no longer maximally entangled with respect to the new larger local dimensions.

Whereas this shows that any set of $N > n$ orthogonal maximally entangled states can never be locally distinguished with certainty, it leaves open the question whether there exist sets of $N \leq n$ indistinguishable orthogonal maximally entangled states in $\mathbb{C}^n \otimes \mathbb{C}^n$. An answer to this question for the particular case of $n = 3 = N$ was given by Nathanson [Nat05], who showed that any three orthogonal maximally entangled states in $\mathbb{C}^3 \otimes \mathbb{C}^3$ can be perfectly distinguished by LOCC. In a followup work [Nat13], Nathanson proved that 3 maximally entangled states in $\mathbb{C}^n \otimes \mathbb{C}^n$, for any $n \leq 3$, are always perfectly distinguishable by PPT.

Several results aimed at filling the landscape for the case $3 < N \leq n$. For the weaker model of *one-way* LOCC protocols, Bandyopadhyay et al. [BGK11] showed some explicit examples of indistinguishable sets of states with the size of the sets being equal to the

dimension of the subsystems, i.e., $N = n$. The states they use for those examples lie on systems whose local dimension is $n = 4, 5, 6$. Later in Chapter 5, we go back to these examples and give numerical evidence that the same sets of states cannot be distinguished with certainty even if we allow the parties to perform PPT measurements.

Recently, Yu et al. [YDY12] presented the first example of N maximally entangled states in $\mathbb{C}^N \otimes \mathbb{C}^N$ that cannot be perfectly distinguished by any PPT measurement, and therefore by any general LOCC protocols. Their particular example is composed by the following $N = 4$ states in $\mathbb{C}^4 \otimes \mathbb{C}^4$:

$$\begin{aligned}
|\phi_1\rangle &= \frac{1}{2}|0\rangle|0\rangle + \frac{1}{2}|1\rangle|1\rangle + \frac{1}{2}|2\rangle|2\rangle + \frac{1}{2}|3\rangle|3\rangle, \\
|\phi_2\rangle &= \frac{1}{2}|0\rangle|3\rangle + \frac{1}{2}|1\rangle|2\rangle + \frac{1}{2}|2\rangle|1\rangle + \frac{1}{2}|3\rangle|0\rangle, \\
|\phi_3\rangle &= \frac{1}{2}|0\rangle|3\rangle + \frac{1}{2}|1\rangle|2\rangle - \frac{1}{2}|2\rangle|1\rangle - \frac{1}{2}|3\rangle|0\rangle, \\
|\phi_4\rangle &= \frac{1}{2}|0\rangle|1\rangle + \frac{1}{2}|1\rangle|0\rangle - \frac{1}{2}|2\rangle|3\rangle - \frac{1}{2}|3\rangle|2\rangle.
\end{aligned} \tag{3.29}$$

Later in Chapter 5 we turn their result into a quantitative one, by showing that PPT measurements can only succeed with probability at most $7/8$ and that $3/4$ is a tight bound on the probability of distinguishing these states by separable (and LOCC) measurements.

Yet another tile in the landscape of maximally entangled states distinguishability is a result by Fan [Fan04], for which any N generalized Bell states in $\mathbb{C}^n \otimes \mathbb{C}^n$ can be perfectly distinguished by LOCC whenever

$$\binom{N}{2} \leq n.$$

Table 3.1 summarizes known results about the distinguishability of maximally entangled states by LOCC and PPT measurements, and compares them with the results obtained in this thesis (highlighted in gray).

3.4 Discrimination of product sets

Indistinguishability by LOCC is not a prerogative of entangled states. The famous *domino state* set of [BDM+99], for example, is a collection of orthogonal *product* states that cannot

	PPT	LOCC	References
$N = 2$	—	*all* dist.	[WSHV00]
$N = 3 = n$	—	*all* dist.	[Nat05]
$N = 4 = n$	*some* indist.	—	[YDY12]
$N = n > 4$	*some* indist.	—	[Cos13]
$4 < N < n$	*some* indist.	—	[CR14, BCJ+15]
$N > n$	*all* indist.	—	[YDY12, DFXY09, GKRS04]

Table 3.1: Distinguishability of maximally entangled states. ("*some* indist.": there exist sets of states that are indistinguishable for the dimension and the class of measurements of the corresponding cell; "*all* dist./indist.": all sets of states are distinguishable/indistinguishable; "—": the distinguishability can be inferred by the rest of the row.)

be perfectly discriminated by LOCC protocols. In this example, the local dimension of the states is 3, and one takes $N = 9$, $p_1 = \cdots = p_9 = 1/9$, and

$$\begin{aligned}
|\phi_1\rangle &= |1\rangle|1\rangle, \\
|\phi_2\rangle &= |0\rangle\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right), \quad |\phi_3\rangle = |2\rangle\left(\tfrac{|1\rangle+|2\rangle}{\sqrt{2}}\right), \\
|\phi_4\rangle &= \left(\tfrac{|1\rangle+|2\rangle}{\sqrt{2}}\right)|0\rangle, \quad |\phi_5\rangle = \left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|2\rangle, \\
|\phi_6\rangle &= |0\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right), \quad |\phi_7\rangle = |2\rangle\left(\tfrac{|1\rangle-|2\rangle}{\sqrt{2}}\right), \\
|\phi_8\rangle &= \left(\tfrac{|1\rangle-|2\rangle}{\sqrt{2}}\right)|0\rangle, \quad |\phi_9\rangle = \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|2\rangle.
\end{aligned} \tag{3.30}$$

A rather complicated argument demonstrates that this collection cannot be discriminated by LOCC with probability greater than $1 - \varepsilon$ for some choice of a positive real number ε. (A simplified proof appears in [CLMO13], where this fact is proved for $\varepsilon = 1.9 \times 10^{-8}$.)

3.5 Entanglement cost of state discrimination

As explained in the introduction, three Bell states given with uniform probabilities can be discriminated by separable measurements with success probability at most 2/3, while four

Bell states can be discriminated with success probability at most 1/2. These bounds can be obtained by a fairly trivial selection of LOCC measurements, and can be shown to hold even for PPT measurements.

On the other hand, if the parties are given a maximally entangled bit as a resource, then they can perform a teleportation protocol to send each other their respective parts of the Bell pair they have been asked to identify. The set of Bell states constitutes an example of a set that is distinguishable only if we are willing to consume some entanglement (given as an additional resource) or, in other words, we say that the entanglement cost of distinguishing the Bell states with certainty is bigger than zero.

The entanglement cost of quantum operations and measurements, within the paradigm of LOCC, has been considered previously. For instance, [Coh08] studied the entanglement cost of perfectly discriminating elements of unextendable product sets by LOCC measurements. Interestingly, his work presents some protocol where entanglement is used more efficiently than in standard teleportation protocols. In later work, [BBKW09] and [BRW10] considered the entanglement cost of measurements and established lower bounds on the amount of entanglement necessary for distinguishing complete orthonormal bases of two qubits.

Our work on the entanglement cost of Bell states was inspired by a question left open by Yu, Duan, and Ying, who considered the entanglement cost of state discrimination problems by PPT and separable measurements [YDY14].

3.6 Previous approaches

In the results roundup of the previous sections, we summarized "positive" results, in which it is shown that a certain probability of success can be obtained by some measurement, as well as "negative" results, for which an upper bound on the probability of success is shown for any measurement in a certain class.

To prove the first kind of results, one needs to show a protocol (for LOCC), or a collection of measurement operators (for PPT and separable) that achieves the given probability. Some protocols/measurements might be complicated to devise, others are based on the composition of simple primitives. For instance, when Alice and Bob are supplied with entangled bits as resource, they can a perform a teleportation protocol on a part of the states they are asked to distinguish (an example of such a protocol is shown in Chapter 5 for the task of distinguishing three and four Bell states).

To show that the states are not distinguishable, many techniques have been devised. One possible approach is the one pursued by Walgate and Hardy [WH02], which is based on a cases analysis in which all possible measurements are eliminated.

Another method, considered in [GKR+01, GKRS04], is to reduce the distinguishability problem to a question on the amount of entanglement that can be distilled from a certain mixed state. Say you want to prove that the four Bell states from Eq. (2.13) are not perfectly distinguishable by any LOCC protocols. Suppose that the unknown Bell state is shared among two parties, Alice and Bob, whose spaces are denoted by $\mathcal{X}_1$ and $\mathcal{Y}_1$. Let $\mathcal{X}_2$ and $\mathcal{Y}_2$ two other spaces of the same dimensions held by two more parties, Charlie and Dan. Consider the state

$$\rho \in \mathrm{D}\left((\mathcal{X}_1 \otimes \mathcal{Y}_1) \otimes (\mathcal{X}_2 \otimes \mathcal{Y}_2)\right) \tag{3.31}$$

defined as

$$\rho = \frac{1}{4} \sum_{i \in \{0,1,2,3\}} \psi_i \otimes \psi_i. \tag{3.32}$$

By contradiction, assume that $\{\psi_0, \ldots, \psi_3\} \subset \mathrm{D}(\mathcal{X}_1 \otimes \mathcal{Y}_1)$ are distinguishable by an LOCC protocol between Alice and Bob. Then they could communicate the outcome classically to Charlie and Dan, who would use this information to create a shared entangled bit between each other. This is not possible, since ρ can also be written (because of the symmetry among Bell states) as

$$\rho = \frac{1}{4} \sum_{i \in \{0,1,2,3\}} \psi_i \otimes \psi_i \in D\left((\mathcal{X}_1 \otimes \mathcal{X}_2) \otimes (\mathcal{Y}_1 \otimes \mathcal{Y}_2)\right), \tag{3.33}$$

and therefore it contradicts the fact that ρ is separable in the cut between Alice and Charlie on one side, and Bob and Dan on the other side, that is,

$$\rho \in \mathrm{Sep}(\mathcal{X}_1 \otimes \mathcal{X}_2 : \mathcal{Y}_1 \otimes \mathcal{Y}_2). \tag{3.34}$$

A similar argument shows that no three Bell states, and more in general, no set of $n+1$ orthogonal maximally entangled states in $\mathbb{C}^n \otimes \mathbb{C}^n$, can be perfectly distinguished by LOCC[2]. This method is referred in the literature as *GKRSS method*, by the initials of the authors of [GKR+01].

In [HSSH03], a modification of the GKRSS method is presented, called *HSSH method*. In the GKRSS method, the local distinguishability problem is reduced to analyzing the

[2]Later in Section 5.1, we will show a proof of this fact by using the convex programming framework introduced in this thesis.

entanglement contained in a mixed states constructed starting from the states that are to be distinguished. The idea is to compare the entanglement in the mixed state before and after the distinguishability protocol has run its course. In HSSH the problem is reduced to comparing the entanglement measures in *pure states* instead. For some instances of the problem, the HSSH method turns out to be more powerful, due to the fact that entanglement measures for pure states are better understood. In fact, through the HSSH method, the problem reduces to understanding entanglement transformations between pure states, for which necessary and sufficient conditions were derived by Nielsen [Nie99], and Jonathan and Plenio [JP99]. An application of the method by [HSSH03] is the discovery of the first set of n indistinguishable states in $\mathbb{C}^n \otimes \mathbb{C}^n$.

The original proof in [TDL01] that the Werner states form a hiding pair (Example 3.2 above) also exploits the theory of entanglement, but makes use of an extra observation, that is, the fact that the operators that constitute an LOCC measurement must be PPT. The mathematical properties of PPT measurements were also exploited in the recent proofs by [YDY12, YDY14], which triggered the work of this thesis.

Chapter 4

A cone programming framework for local state distinguishability

Due to the intrinsic complexity of LOCC protocols, it is hard to come up with techniques for their analysis. This is true in particular for the analysis of the local state discrimination problem. All the proof techniques that have been proposed so far for this problem have their own limitations: they are mathematically cumbersome, or they bound the power only of limited subclasses of LOCC (one-way LOCC, for instance), or they can be applied only to very specific set of states.

In this chapter we provide a more general framework based on convex optimization to prove bounds on LOCC protocols for the task of bipartite state discrimination. We build on the idea described in Chapter 2 that LOCC measurements can be approximated by more tractable classes of measurements, in particular the sets of separable and PPT measurements. It turns out that we can describe them conveniently using convex cones, and therefore, many problems in which we optimize over them can be cast into the cone programming paradigm.

Contents

4.1 General cone program

The global state discrimination problem was one of the first applications of semidefinite programming to the theory of quantum information [EMV03]. Let us recall the parameters that define an instance of the problem. We are given a complex Euclidean space $\mathcal{X}$, a positive integer N, and an ensemble $\mathcal{E}$ of N states, that is,

$$\mathcal{E} = \big\{(p_1, \rho_1), \ldots, (p_N, \rho_N)\big\}, \tag{4.1}$$

where $\rho_1, \ldots, \rho_N \in \mathrm{D}(\mathcal{X})$ and $(p_1, \ldots, p_N)$ is a probability vector. We can construct a family of semidefinite programs parametrized by $\mathcal{X}$ and N, such that one program takes $\mathcal{E} \in \mathrm{Ens}(\mathcal{X}, N)$ as input and its optimal value corresponds to the maximum probability for any measurement to distinguish $\mathcal{E}$:

$$\begin{aligned} &\underline{\text{Primal (Global measurements)}} \\ \text{maximize:} \quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\ \text{subject to:} \quad & \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}} \\ & \mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X}) \end{aligned} \tag{4.2}$$

The variables of the program form a collection of operators and the constraints impose that such collection of operators forms a valid measurements. In particular, the constraints demand that each operator belongs to the cone of semidefinite operators and that all the operators sum to identity, as in the definition of measurement from Section 2.2.

The key observation of this dissertation is that we can generalize the above semidefinite program to a family of cone programs, where the set of measurements over which we are optimizing forms a convex cone. In effect, this generalization turns out to be helpful when

the set of measurements is characterized by the further property that each measurement in the set can be represented by restricting each of its measurement operators to belong to a particular convex cone.

More formally, say we are given a complex Euclidean space $\mathcal{X}$ and consider the problem of distinguishing the ensemble $\mathcal{E}$ from Eq. (4.1) by any measurement in some class

$$\mathcal{K} \subset \text{Meas}(N, \mathcal{X}). \tag{4.3}$$

Further, suppose that the following characterization of $\mathcal{K}$ holds.

Property 4.1. A measurement $\mu : \{1, \ldots, N\} \to \text{Pos}(\mathcal{X})$ belongs to the set $\mathcal{K}$ if and only if there exists a convex cone $\mathcal{C} \subset \text{Pos}(\mathcal{X})$ such that each measurement operator belongs to $\mathcal{C}$, that is, $\mu(k) \in \mathcal{C}$, for each $k \in \{1, \ldots, N\}$.

If this property is satisfied, the optimal probability of distinguishing $\mathcal{E}$ by any measurement in $\mathcal{K}$ is thus given by the optimal solution of the following cone program:

$$\begin{array}{ll} & \underline{\text{Primal (General cone program)}} \\ \text{maximize:} & \displaystyle\sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\ \text{subject to:} & \displaystyle\sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}} \\ & \mu : \{1, \ldots, N\} \to \mathcal{C} \end{array} \tag{4.4}$$

If one is to formally specify this problem according to the general form for cone programs presented in Section 2.3, the function μ may be represented as a block matrix of the form

$$X = \begin{pmatrix} \mu(1) & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & \mu(N) \end{pmatrix} \in \text{Herm}(\mathcal{X} \oplus \cdots \oplus \mathcal{X}) \tag{4.5}$$

with the off-diagonal blocks being left unspecified. The cone denoted by $\mathcal{K}$ in Section 2.3 is taken to be the cone of operators of this form for which each $\mu(k)$ belongs to the cone $\mathcal{C}$.

The mapping Φ and operators A and B are chosen in the natural way:

$$A = \begin{pmatrix} p_1\rho_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & p_N\rho_N \end{pmatrix}, \qquad B = \mathbb{1}_{\mathcal{X}}, \tag{4.6}$$

and $\Phi : \mathrm{L}(\mathcal{X} \oplus \cdots \oplus \mathcal{X}) \to \mathrm{L}(\mathcal{X})$ is defined as

$$\Phi \begin{pmatrix} X_1 & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & X_N \end{pmatrix} \equiv X_1 + \cdots + X_N, \tag{4.7}$$

for any $X_1, \ldots, X_N \in \mathrm{L}(\mathcal{X})$.

Let $\mathcal{Y} = \mathbb{C}^N$. One can easily verify that the mapping $\Phi^* : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$, defined as

$$\Phi^*(H) \equiv \mathbb{1}_{\mathcal{Y}} \otimes H, \tag{4.8}$$

satisfies Equation (2.6) and therefore is the adjoint of Φ: for any $H \in \mathrm{L}(\mathcal{X})$. Also, let $\mathcal{C}^* \subset \mathrm{Herm}(\mathcal{X})$ denote the dual cone of $\mathcal{C}$. With these definitions in hand, one can write the dual of the Program (4.4) as follows:

Dual (General cone program)

$$\begin{aligned} \text{minimize:} \quad & \mathrm{Tr}(H) \\ \text{subject to:} \quad & H - p_k \rho_k \in \mathcal{C}^* \quad (\text{for each } k = 1, \ldots, N) \\ & H \in \mathrm{Herm}(\mathcal{X}). \end{aligned} \tag{4.9}$$

Throughout the thesis we will use the property of *weak duality* of cone programs (Proposition 2.9) to upper bound the optimal solution of the primal program (4.4). The cone programs considered in this thesis also possess the property of *strong duality*. This property depends on the specific cone $\mathcal{C}$, and we will discuss it whenever we treat a specific $\mathcal{C}$, although it should be noted that strong duality is not needed for any of our results.

In the rest of this chapter, we will see different instantiations of the general program for a variety of measurements classes. We started this section by presenting the semidefinite program (4.2) for the problem of state distinguishability by global measurement. In that case, the cone $\mathcal{C}$ of the general cone program corresponded to the cone of semidefinite operators, that is, $\mathcal{C} = \mathrm{Pos}(\mathcal{X})$ and, due to Fact 2.8, we have that $\mathcal{C}^* = \mathcal{C}$. Thus we can write the following dual program of (4.2):

Dual (Global measurements)

$$\begin{aligned} \text{minimize:} \quad & \mathrm{Tr}(H) \\ \text{subject to:} \quad & H - p_k \rho_k \in \mathrm{Pos}(\mathcal{X}) \quad (\text{for each } k = 1, \ldots, N) \\ & H \in \mathrm{Herm}(\mathcal{X}). \end{aligned} \tag{4.10}$$

4.2 Bipartite measurements

The above generalization of the optimal measurement cone program turns out to be particularly helpful for the analysis of the bipartite state discrimination problem, which is the main focus of this thesis.

Recall that, as input of the problem, we are given two complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, one for each party, a positive integer N, and an ensemble of states that are distributed among the spaces of the two parties, that is,

$$\mathcal{E} = \big\{(p_1, \rho_1), \ldots, (p_N, \rho_N)\big\}, \tag{4.11}$$

with $\rho_1, \ldots, \rho_N \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$.

Ideally, we would like to solve the following problem:

$$\begin{aligned} &\underline{\text{Primal (LOCC measurements)}} \\ \text{maximize:} \quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\ \text{subject to:} \quad & \mu \in \mathrm{Meas}_{\mathrm{LOCC}}(N, \mathcal{X} : \mathcal{Y}). \end{aligned} \tag{4.12}$$

Phrasing this problem as a cone program is not interesting as such. It is technically possible, as we can write the constraints of the program in terms of membership of the variables to a convex cone[1] along with some additional linear constraints. However we would not be able to exploit the advantages that come from such formulation, due to the fact that the set of LOCC measurements does not possess nice mathematical properties. For instance, we do not have a characterization of LOCC measurements on the same lines of Property 4.1, and consequently we cannot cast the problem in the general form of Program (4.4).

As indicated in Chapter 3, the LOCC set can be approximated by other sets of measurements that are easier to be manipulated mathematically. It turns out that both the sets of PPT and separable measurements are suitable for the cone programming framework described above. In fact, they both form closed convex cones, for both these sets it is relatively easy to characterize the dual set, and moreover, an equivalent of Property

[1] The exposition of Section 2.3 limited the definition of cone programs to optimization problems in which the underlying cone is topologically *closed*. It is known that the set of LOCC operations is not closed, but one could consider the closure of the set [CLM+14] and yet the discussion here would still apply.

4.1 holds. For example, Proposition 2.4 characterizes a separable measurement over the bipartition $(\mathcal{X} : \mathcal{Y})$ as a collection of operators belonging to the cone $\mathrm{Sep}(\mathcal{X} : \mathcal{Y})$. This property allows us to characterize the maximum probability of distinguishing the ensemble in Eq. (4.11) by any separable measurement as a cone program of the same form as the one in (4.4), where instead of $\mathcal{X}$, the underlying space of the operators is $\mathcal{X} \otimes \mathcal{Y}$, and $\mathcal{C}(\mathcal{X})$ is replaced by the cone of separable operators $\mathrm{Sep}(\mathcal{X} : \mathcal{Y})$.

In the rest of this section, we study the different programs that derive from the Program (4.4) when we instantiate $\mathcal{C}$ with some particular cones corresponding to different classes of bipartite measurements. In particular, we will mainly look at the programs derived from the cones of separable operators, PPT operators, and operators with k-symmetric extensions. For each of these programs, we will show the dual program and try to make any possible simplification. Moreover, we will point it out whenever a program can be expressed by using only semidefinite constraints, as it was the case for the Program (4.2) from above.

4.2.1 PPT measurements

We start with the cone of PPT operators and we describe a semidefinite program that computes $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E})$. Using tools of convex optimization to solve problems concerning the PPT cone is not a novel idea. Two other applications of convex programming to the realm of PPT operations are the semidefinite program shown by Rains to compute the maximum fidelity obtained by a PPT distillation protocol [Rai01] and the hierarchy of semidefinite programs proposed as separability criteria by Doherty, Parrilo, and Spedalieri [DPS02, DPS04].

Recall from Definition 2.5 that a measurement $\mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is in $\mathrm{Meas}_{\mathrm{PPT}}(N, \mathcal{X} : \mathcal{Y})$ if and only if

$$\mu(1), \ldots, \mu(N) \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y}). \tag{4.13}$$

From the definition of $\mathrm{PPT}(\mathcal{X} : \mathcal{Y})$, we can write the cone program in the following form:

Primal (PPT measurements)

$$\begin{aligned}
\text{maximize:} \quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\
\text{subject to:} \quad & \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}} \\
& \mu : \{1,\ldots,N\} \to \mathrm{Pos}(\mathcal{X}\otimes\mathcal{Y}), \\
& \mathrm{T}_{\mathcal{X}}(\mu(k)) \in \mathrm{Pos}(\mathcal{X}\otimes\mathcal{Y}) \quad (\text{for each } k = 1,\ldots,N).
\end{aligned} \tag{4.14}$$

An immediate observation is that the cone program above is in fact a semidefinite program. To see this formally, let us introduce N variables $Q_1,\ldots,Q_N \in \mathrm{Herm}(\mathcal{X}\otimes\mathcal{Y})$ and, for each $k \in \{1,\ldots,N\}$, let

$$Q_k = \mathrm{T}_{\mathcal{X}}(\mu(k)). \tag{4.15}$$

One can write the above program as a semidefinite program in the standard form of Section 2.3, where

$$X = \begin{pmatrix} \mu(1) & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & \mu(N) \end{pmatrix} \oplus \begin{pmatrix} Q_1 & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & Q_N \end{pmatrix} \tag{4.16}$$

is the variable over which we optimize,

$$A = \begin{pmatrix} p_1\rho_1 & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & p_N\rho_N \end{pmatrix} \oplus \begin{pmatrix} 0 & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & 0 \end{pmatrix}, \tag{4.17}$$

and

$$B = \begin{pmatrix} \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}} & \cdot & \cdots & \cdot \\ \cdot & 0 & \cdots & \cdot \\ \vdots & \vdots & \ddots & \vdots \\ \cdot & \cdot & \cdots & 0 \end{pmatrix}. \tag{4.18}$$

are the known inputs of the problem, and the map Φ : is defined as

$$\Phi(X) \equiv \begin{pmatrix} \mu(1) + \cdots + \mu(N) & \cdot & \cdots & \cdot \\ \cdot & \mathrm{T}_{\mathcal{X}}(\mu(1)) - Q_1 & \cdots & \cdot \\ \vdots & \vdots & \ddots & \vdots \\ \cdot & \cdot & \cdots & \mathrm{T}_{\mathcal{X}}(\mu(N)) - Q_N \end{pmatrix}, \tag{4.19}$$

for any operator X in the form of Eq. (4.16).

Once the program is in the standard form, one can easily derive its dual. The variable of the dual program is the Hermitian operator $Y \in$ defined as follows:

$$Y = \begin{pmatrix} H & \cdot & \cdots & \cdot \\ \cdot & -R_1 & \cdots & \cdot \\ \vdots & \vdots & \ddots & \vdots \\ \cdot & \cdot & \cdots & -R_N \end{pmatrix}, \tag{4.20}$$

for Hermitian operators $Y, R_1, \ldots, R_N \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y})$. The adjoint of Φ is defined as the mapping

$$\Phi^*(Y) \equiv \begin{pmatrix} H - \mathrm{T}_{\mathcal{X}}(R_1) & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & H - \mathrm{T}_{\mathcal{X}}(R_N) \end{pmatrix} \oplus \begin{pmatrix} R_1 & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & R_N \end{pmatrix}, \tag{4.21}$$

for any operator Y in the form of Eq. (4.20). It is easy to verify that the map Φ^* satisfies Eq. (2.6). From the fact the the partial transpose is its own adjoint and inverse, we have that

$$\langle A, B \rangle = \langle \mathrm{T}_{\mathcal{X}}(A), \mathrm{T}_{\mathcal{X}}(B) \rangle, \tag{4.22}$$

for any operators $A, B \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$, which implies

$$\langle \mu(k), \mathrm{T}_{\mathcal{X}}(R_k) \rangle = \langle \mathrm{T}_{\mathcal{X}}(\mu(k)), R_k \rangle, \tag{4.23}$$

for any $k \in \{1, \ldots, N\}$, and therefore

$$\langle Y, \Phi(X) \rangle = \langle \Phi^*(Y), X \rangle. \tag{4.24}$$

By rearranging everything in a more explicit form, we have the following dual program:

Dual (PPT measurements)

$$\begin{aligned} \text{minimize:} \quad & \mathrm{Tr}(H) \\ \text{subject to:} \quad & H - p_k \rho_k \geq \mathrm{T}_{\mathcal{X}}(R_k) \quad (\text{for each } k = 1, \ldots, N), \\ & R_1, \ldots, R_N \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}), \\ & H \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y}). \end{aligned} \tag{4.25}$$

Decomposable operator

An equivalent way of deriving the above dual program is by defining the cone

$$\mathrm{PPT}^*(\mathcal{X} : \mathcal{Y}) = \{S + \mathrm{T}_{\mathcal{X}}(R) \ : \ S, R \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})\}, \tag{4.26}$$

which satisfies (2.42) and therefore is the dual cone of $\mathrm{PPT}(\mathcal{X} : \mathcal{Y})$. The program above corresponds to an instance of the generic dual program (4.9), where $\mathcal{C}^*$ is replaced by $\mathrm{PPT}^*(\mathcal{X} : \mathcal{Y})$.

The operators in $\mathrm{PPT}^*(\mathcal{X} : \mathcal{Y})$ can also be characterized as representations of so-called *decomposable maps* from $\mathrm{L}(\mathcal{Y})$ to $\mathrm{L}(\mathcal{X})$, via the Choi isomorphism (see Section 2.1.3)

Definition 4.2. A decomposable map $\Phi : \mathrm{L}(\mathcal{Y}) \to \mathrm{L}(\mathcal{X})$ is a linear map that can be represented as the sum of a completely positive map and a completely co-positive map, that is, there exist two completely positive maps $\Psi, \Xi : \mathrm{L}(\mathcal{Y}) \to \mathrm{L}(\mathcal{X})$, such that, for any $Y \in \mathrm{L}(\mathcal{Y})$,

$$\Phi(Y) = \Psi(Y) + (\mathrm{T} \circ \Xi)(Y), \tag{4.27}$$

where T denotes the transpose map.

Exploiting symmetries

In cases where the ensemble of states we wish to distinguish exhibit some symmetry, we can simplify the semidefinite program ($\mathrm{P}_{\mathrm{PPT}}$) to a linear program. One particular case where this kind of symmetry emerges is when we consider so-called *lattice states*. Let

$$\psi_i = |\psi_i\rangle\langle\psi_i| \in \mathrm{D}(\mathbb{C}^2 \otimes \mathbb{C}^2),$$

for $i \in \{0, 1, 2, 3\}$, be the density operators corresponding to the standard Bell states, as defined in Eq. (2.13). Let $v \in \mathbb{Z}_4^t$ be a t-dimensional vector and let $|\psi_v\rangle \in \mathbb{C}^{2^t} \otimes \mathbb{C}^{2^t}$ be the maximally entangled state given by the tensor product of Bell states indexed by the vector $v = (v_1, \ldots, v_t)$, that is,

$$|\psi_v\rangle = |\psi_{v_1}\rangle \otimes \ldots \otimes |\psi_{v_t}\rangle.$$

In the literature, operators diagonal in the basis $\{\psi_v = |\psi_v\rangle\langle\psi_v| : v \in \mathbb{Z}_4^t\}$ are called *lattice operators*, or *lattice states* if they are also density operators [Pia06].

The following equations regarding the partial transpose of the Bell states will be used in the main proof of this section and can be proved by direct inspection.

$$\begin{aligned} \mathrm{T}_{\mathcal{X}}(\psi_0) &= \frac{1}{2}\mathbb{1} - \psi_2, \qquad & \mathrm{T}_{\mathcal{X}}(\psi_1) &= \frac{1}{2}\mathbb{1} - \psi_3, \\ \mathrm{T}_{\mathcal{X}}(\psi_2) &= \frac{1}{2}\mathbb{1} - \psi_0, \qquad & \mathrm{T}_{\mathcal{X}}(\psi_3) &= \frac{1}{2}\mathbb{1} - \psi_1. \end{aligned} \tag{4.28}$$

The following proposition is useful for the proof of the main theorem of this section and, again, it can be easily proved by direct inspection.

Proposition 4.3. *Let $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\} \subset \mathrm{Herm}(\mathbb{C}^2)$ be the set of Pauli operators in defined in Eq. (2.11). It holds that the Bell states from Eq. (2.13) are invariant under the group of local symmetries*

$$G = \big\{\sigma_i \otimes \sigma_i : i \in \{0,1,2,3\}\big\}, \tag{4.29}$$

that is, $\psi_i = U\psi_i U^*$ for any $U \in G$ and any $i \in \{0,1,2,3\}$.

It turns out that in the case the set to distinguish contains only lattice states, the semidefinite program ($\mathrm{P}_{\mathrm{PPT}}$) simplifies remarkably, as it is established by the following theorem.

Theorem 4.4. *If the set to be distinguished consists only of lattice states, then the probability of successfully distinguishing them by PPT measurements can be expressed as the optimal value of a linear program.*

Proof. We will prove that for any feasible solution of the semidefinite program ($\mathrm{P}_{\mathrm{PPT}}$), there is another feasible solution consisting only of lattice operators for which the objective function takes the same value.

Let $\Delta : \mathrm{L}(\mathbb{C}^2 \otimes \mathbb{C}^2) \to \mathrm{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be the channel defined as follows:

$$\Delta(X) = \frac{1}{|G|} \sum_{U \in G} UXU^*, \tag{4.30}$$

where G is the group of local unitaries defined in Proposition 4.3. The channel $\Delta(X)$ acts on X as a completely dephasing channel in the Bell basis. Let $\mathcal{X}^{(t)} = \mathcal{Y}^{(t)} = \mathbb{C}^{2^t}$ for some positive integer $t > 1$. Say the states we want to distinguish,

$$\rho_1, \ldots, \rho_N \in \mathrm{D}(\mathcal{X}^{(t)} \otimes \mathcal{Y}^{(t)}), \tag{4.31}$$

are lattice states. Let $\Phi = \Delta^{\otimes t}$ be the t-fold tensor product of the map Δ, that is,

$$\Phi(X_1 \otimes \cdots \otimes X_t) = \Delta(X_1) \otimes \cdots \otimes \Delta(X_t), \tag{4.32}$$

for any choice of linear operators $X_1, \ldots, X_t \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$. Assume that a measurement

$$\mu : \{1, \ldots, N\} \to \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$$

is a feasible solution of the program ($\mathrm{P}_{\mathrm{PPT}}$) for the states $\rho_1, \ldots, \rho_N$. In the rest of the proof we want to show that a new measurement μ' constructed by applying Φ to each measurement operator of μ is also a feasible solution of the program ($\mathrm{P}_{\mathrm{PPT}}$), for the same set of states. Since Φ is a dephasing channel in the lattice basis, this would imply the statement of the theorem.

First, let us observe that the value of the objective function for the solution μ' is the same as the value for the original solution μ. The channel Φ is its own adjoint and therefore we have

$$\langle \mu(k), \rho_k \rangle = \langle \mu(k), \Phi(\rho_k) \rangle = \langle \Phi(\mu(k)), \rho_k \rangle,$$

for any $k = 1, \ldots, N$.

Next, we show that μ' is a PPT measurement. From the fact that Φ is unital (in fact it is a mixed unitary channel), we have

$$\Phi(\mu(1)) + \ldots + \Phi(\mu(N)) = \mathbb{1}, \tag{4.33}$$

and from the fact that Φ is positive, we have

$$\Phi(\mu(k)) \in \mathrm{Pos}(\mathcal{X}^{(t)} \otimes \mathcal{Y}^{(t)}) \tag{4.34}$$

and

$$\Phi(\mathrm{T}_{\mathcal{X}}(\mu(k))) \in \mathrm{Pos}(\mathcal{X}^{(t)} \otimes \mathcal{Y}^{(t)}), \tag{4.35}$$

for any $k \in \{1, \ldots, N\}$. The first fact implies that μ' is indeed valid measurement. The second fact is close to what we want in order to show that μ' is a PPT measurement. To complete the proof, we wish to show that the partial transpose mapping commutes with the channel Φ. First we observe how the partial transposition modifies the action of local operators. Given linear operators $A \in \mathrm{L}(\mathcal{X})$, $B \in \mathrm{L}(\mathcal{Y})$ and $X \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$, we have

$$\mathrm{T}_{\mathcal{X}}[(A \otimes B)X(A \otimes B)^*] = (\overline{A} \otimes B)\, \mathrm{T}_{\mathcal{X}}(X)(\overline{A} \otimes B)^*. \tag{4.36}$$

Now, for the Pauli matrices, we have $\overline{\sigma_j} = \sigma_j$ for $j \in \{0, 1, 3\}$ and $\overline{\sigma_2} = -\sigma_2$. Therefore

$$\Delta(\mathrm{T}_{\mathcal{X}}(X)) = \mathrm{T}_{\mathcal{X}}(\Delta(X)), \quad \text{for any } X \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y}). \tag{4.37}$$

This property trivially extends by tensor product to Φ and therefore Eq. (4.35) implies

$$\mathrm{T}_{\mathcal{X}}(\Phi(\mu(k))) \geq 0, \tag{4.38}$$

for any $k \in \{1, \ldots, N\}$, which concludes the proof. □

The advantage of the linear programming formulation is in the computational efficiency of the algorithms that solve the program. However, for sake of uniformity, in the analytic proofs that will follow, we will always stick to the more general semidefinite programming formulation, even when we consider distinguishability of lattice states.

4.2.2 Separable measurements

We have yet to fully exploit the expressive power of the cone programming language. In this section we do so by showing a connection between convex optimization and the cone of separable operators, which would not be possible if the only tool at hand was semidefinite programming. Surprisingly, there are only few examples in the literature ([GSU13] being one of those) where this connection has been made use of.

As it is stated by Proposition 2.4, a measurement $\mu : \{1, \ldots, N\} \to \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is separable when

$$\mu(1), \ldots, \mu(N) \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y}). \tag{4.39}$$

We can write the maximum probability of distinguishing an ensemble $\mathcal{E}$ by separable measurements, $\mathrm{opt}_{\mathrm{Sep}}(\mathcal{E})$, as the optimal value of the following cone program:

$$\begin{aligned} & \underline{\text{Primal } (\mathrm{P}_{\mathrm{Sep}})} \\ \text{maximize:} \quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\ \text{subject to:} \quad & \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}}, \\ & \mu : \{1, \ldots, N\} \to \mathrm{Sep}(\mathcal{X} : \mathcal{Y}). \end{aligned} \tag{4.40}$$

An important observation about this program is that, unlike the case of the PPT program, its constraints cannot be formulated as semidefinite constraints. Later in Section 4.4 we will see how this has implications in the computational complexity of the problem.

We denote the cone dual to $\mathrm{Sep}(\mathcal{X} : \mathcal{Y})$ by $\mathrm{Sep}^*(\mathcal{X} : \mathcal{Y})$, and defer its definition to the next paragraph, after we write the dual program of (4.40):

Dual ($\mathrm{D}_{\mathrm{Sep}}$)

$$\begin{aligned} \text{minimize:} \quad & \mathrm{Tr}(H) \\ \text{subject to:} \quad & H - p_k \rho_k \in \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y}) \quad (\text{for each } k = 1, \ldots, N), \\ & H \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y}). \end{aligned} \tag{4.41}$$

Block-positive operators

The cone $\mathrm{Sep}^*(\mathcal{X} : \mathcal{Y})$, which is commonly known as the set of *block-positive operators*, is

$$\mathrm{Sep}^*(\mathcal{X} : \mathcal{Y}) = \big\{ H \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y}) \,:\, \langle P, H \rangle \geq 0 \text{ for every } P \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y}) \big\}. \tag{4.42}$$

There are several equivalent characterizations of this set. For instance, one has

$$\begin{aligned} \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y}) = \big\{ H \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y}) \,:\, \\ (\mathbb{1}_{\mathcal{X}} \otimes y^*) H (\mathbb{1}_{\mathcal{X}} \otimes y) \in \mathrm{Pos}(\mathcal{X}) \text{ for every } y \in \mathcal{Y} \big\}. \end{aligned} \tag{4.43}$$

Alternatively, block-positive operators can be characterized as Choi representations of *positive* linear maps. That is, for any linear map $\Phi : \mathrm{L}(\mathcal{Y}) \to \mathrm{L}(\mathcal{X})$ mapping arbitrary linear operators on $\mathcal{Y}$ to linear operators on $\mathcal{X}$, the following two properties are equivalent:

(a) For every positive semidefinite operator $Y \in \mathrm{Pos}(\mathcal{Y})$, it holds that $\Phi(Y) \in \mathrm{Pos}(\mathcal{X})$.

(b) The Choi operator $J(\Phi)$ of the mapping Φ, defined as in Eq. (2.19), satisfies

$$J(\Phi) \in \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y}). \tag{4.44}$$

Dual to the fact that there are positive semidefinite operators, which are not separable, is the fact that there are block-positive operators, which are not positive semidefinite. Such operators are called *entanglement witnesses* and represent (via the Choi representation) linear maps that are positive, but not completely positive.

One example of entanglement witness is the swap operator defined in (2.41), which is the Choi representation of the transpose map. We will see many other example of entanglement witnesses in later sections; for a more exhaustive review, see [CS14].

The Venn diagram in Figure 4.1 depicts the containments of sets that are dual to the sets of measurements operators we have considered (a set with one shade of gray is dual to the set with the same shade of gray from Figure 2.1).

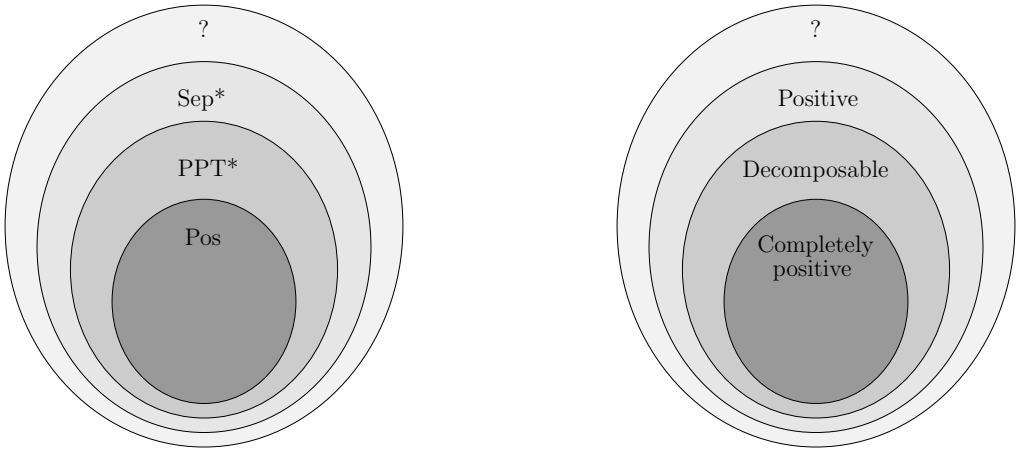

Figure 4.1: Sets of operators that are dual to the sets of Figure 2.1 (on the left) and the corresponding sets of linear mappings via the Choi isomorphism (on the right).

4.2.3 Symmetric extensions

For any given ensemble of states $\mathcal{E}$, the cone program (4.40) for separable measurements outputs a better (not always strictly better) approximation of $\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E})$, compared to the output of the semidefinite program (4.14) for PPT measurements. The drawback is in the computational complexity: on the one extreme, we have polynomial time algorithms to solve the PPT semidefinite program, and on the other extreme, we can prove that optimizing over a set of separable operator is an NP-hard problem (more details in Section 4.4).

Building up on an idea by Doherty, Parrilo, and Spedalieri [DPS02, DPS04], we are able to interpolate between these two extremes and construct a hierarchy of semidefinite programs characterized by the following trade-off: whenever we climb up a level of the hierarchy, the size of the program increases (and so does the running time of the algorithms that solve it), however the outputs of the program gives an approximation closer to $\mathrm{opt}_{\mathrm{Sep}}(\mathcal{E})$.

In order to formally describe the hierarchy of semidefinite programs that approximates $\mathrm{opt}_{\mathrm{Sep}}(\mathcal{E})$, we first need to introduce the concept of symmetric extension of a positive operator. First let us define the set of permutation operators. Let s be a positive integer and let $\mathcal{X}_1, \ldots, \mathcal{X}_s$ be s isomorphic copies of the same complex Euclidean space, that is, for some positive integer d and any $k \in \{1, \ldots, m\}$, $\mathcal{X}_k \simeq \mathbb{C}^d$. Given a permutation

$\pi \in \mathrm{Sym}(s)$, we define a *permutation operator*

$$W_\pi \in \mathrm{U}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_s) \tag{4.45}$$

to be the unitary operator that acts as follows:

$$W_\pi(u_1 \otimes \cdots \otimes u_s) = u_{\pi(1)} \otimes \cdots \otimes u_{\pi(s)}, \tag{4.46}$$

for any choice of vectors $u_1, \ldots, u_s \in \mathbb{C}^d$. We are now ready to give the definition of symmetric extension of a positive semidefinite operator.

Definition 4.5. Suppose we are given complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, and an operator $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$. Moreover, let s be a positive integer and let $\mathcal{Y}_2, \ldots, \mathcal{Y}_s$ be copies of the space $\mathcal{Y}$. An operator

$$X \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_s) \tag{4.47}$$

is called an *s-symmetric extension* of P if the following two properties hold:

(a) $\mathrm{Tr}_{\mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_s}(X) = P$;

(b) $(\mathbb{1}_{\mathcal{X}} \otimes W_\pi) X (\mathbb{1}_{\mathcal{X}} \otimes W_\pi^*) = X$, for every $\pi \in \mathrm{Sym}(s)$.

Any separable operator possesses s-symmetric extensions, for any $s \geq 1$. This is easy to see from the definition of separable operator: given $P \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y})$, there exists a positive integer M, positive semidefinite operators $Q_1, \ldots, Q_M \in \mathrm{Pos}(\mathcal{X})$ and density matrices $\rho_1, \ldots, \rho_M \in \mathrm{D}(\mathcal{Y})$ such that

$$P = \sum_{k=1}^{M} Q_k \otimes \rho_k. \tag{4.48}$$

Then, for any $s \geq 1$,

$$X = \sum_{k=1}^{M} Q_k \otimes \rho_k^{\otimes s} \tag{4.49}$$

is an s-symmetric extension of P.

Interestingly, the converse is also true, that is, for any entangled operator

$$P \in \mathrm{Pos}(\mathcal{X} : \mathcal{Y}) \setminus \mathrm{Sep}(\mathcal{X} : \mathcal{Y}), \tag{4.50}$$

there must exist a value $s > 1$ for which P does not have a s-symmetric extension. For a proof of this fact, which is more involved, we refer the reader to the original paper [DPS02].

It is worthwhile to consider two additional constraints we can add to the definition of symmetric extension. The first one comes from the observation that the symmetric part of the operator X in Eq. (4.49) is supported by the symmetric subspace, which is defined as the set of all vectors in $\mathcal{Y} \otimes \mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_s$ that are invariant under the action of W_π, for every choice of $\pi \in \mathrm{Sym}(s)$. We denote the symmetric subspace by

$$\mathcal{Y} \circledcirc \mathcal{Y}_2 \circledcirc \cdots \circledcirc \mathcal{Y}_s = \{y \in \mathcal{Y} \otimes \mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_s : y = W_\pi y \ \text{ for every } \pi \in \mathrm{Sym}(s)\}, \quad (4.51)$$

and the projection on this subspace by $\Pi_{\mathcal{Y} \circledcirc \mathcal{Y}_2 \circledcirc \cdots \circledcirc \mathcal{Y}_s}$.

Definition 4.6. Suppose we are given complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, and an operator $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$. Moreover, let s be a positive integer and let $\mathcal{Y}_2, \ldots, \mathcal{Y}_s$ be copies of the space $\mathcal{Y}$. An operator

$$X \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_s) \quad (4.52)$$

is called an *s-symmetric bosonic extension* of P if the following two properties hold:

(a) $\mathrm{Tr}_{\mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_s}(X) = P$;

(b) $(\mathbb{1}_{\mathcal{X}} \otimes \Pi_{\mathcal{Y} \circledcirc \mathcal{Y}_2 \circledcirc \cdots \circledcirc \mathcal{Y}_s}) X (\mathbb{1}_{\mathcal{X}} \otimes \Pi_{\mathcal{Y} \circledcirc \mathcal{Y}_2 \circledcirc \cdots \circledcirc \mathcal{Y}_s}) = X$.

A further observation is that we want the semidefinite program at the first level of the symmetric-extension hierarchy to be at least as powerful as the program ($\mathrm{P}_{\mathrm{PPT}}$). In order to do so, we add a third condition to Definition 4.6:

(c) $\mathrm{T}_{\mathcal{X}}(X) \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_s)$, and
$\mathrm{T}_{\mathcal{Y}_j \otimes \mathcal{Y}_{j+1} \otimes \cdots \otimes \mathcal{Y}_s}(X) \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_s)$, for all $j \in \{2, \ldots, s\}$.

Finally, we can put all the constraints together in a hierarchy of semidefinite programs in which, at the s-th level, we optimize over measurements whose operators possess s-symmetric bosonic PPT extensions. The following is the semidefinite program corresponding to the level $s = 2$ of the hierarchy (the programs corresponding to higher levels of the hierarchy can be easily inferred from this one).

Primal ($\mathrm{P}_{\mathrm{Sym}}$)

$$
\begin{aligned}
\text{maximize:} \quad & \sum_{k=1}^{N} p_k \langle \rho_k, \mu(k) \rangle, \\
\text{subject to:} \quad & \sum_{k=1}^{N} \mu(k) = \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}}, \\
& \left.\begin{aligned}
& \mathrm{Tr}_{\mathcal{Y}_2}(X_k) = \mu(k), \\
& (\mathbb{1}_{\mathcal{X}} \otimes \Pi_{\mathcal{Y}\otimes\mathcal{Y}_2}) X_k (\mathbb{1}_{\mathcal{X}} \otimes \Pi_{\mathcal{Y}\otimes\mathcal{Y}_2}) = X_k, \\
& \mathrm{T}_{\mathcal{X}}(X_k) \in \mathrm{Pos}(\mathcal{X}\otimes\mathcal{Y}\otimes\mathcal{Y}_2), \\
& \mathrm{T}_{\mathcal{Y}_2}(X_k) \in \mathrm{Pos}(\mathcal{X}\otimes\mathcal{Y}\otimes\mathcal{Y}_2),
\end{aligned}\right\} \quad (\text{for each } k = 1, \ldots, N), \\
& X_1, \ldots, X_N \in \mathrm{Pos}(\mathcal{X}\otimes\mathcal{Y}\otimes\mathcal{Y}_2).
\end{aligned}
\tag{4.53}
$$

The dual program can be derived by moving to the standard form and by observing that the partial transpose is its own adjoint.

Dual ($\mathrm{D}_{\mathrm{Sym}}$)

$$
\begin{aligned}
\text{minimize:} \quad & \mathrm{Tr}(H), \\
\text{subject to:} \quad & \left.\begin{aligned}
& H - Q_k \geq p_k \rho_k, \\
& Q_k \otimes \mathbb{1}_{\mathcal{Y}_2} + (\mathbb{1}_{\mathcal{X}} \otimes \Pi_{\mathcal{Y}\otimes\mathcal{Y}_2}) R_k (\mathbb{1}_{\mathcal{X}} \otimes \Pi_{\mathcal{Y}\otimes\mathcal{Y}_2}) - R_k \\
& \qquad - \mathrm{T}_{\mathcal{X}}(S_k) - \mathrm{T}_{\mathcal{Y}}(Z_k) \in \mathrm{Pos}(\mathcal{X}\otimes\mathcal{Y}\otimes\mathcal{Y}_2),
\end{aligned}\right\} \quad (\text{for each } k = 1, \ldots, N), \\
& H, Q_1, \ldots, Q_N \in \mathrm{Herm}(\mathcal{X}\otimes\mathcal{Y}), \\
& R_1, \ldots, R_N \in \mathrm{Herm}(\mathcal{X}\otimes\mathcal{Y}\otimes\mathcal{Y}_2) \\
& S_1, \ldots, S_N, Z_1, \ldots, Z_N \in \mathrm{Pos}(\mathcal{X}\otimes\mathcal{Y}\otimes\mathcal{Y}_2).
\end{aligned}
\tag{4.54}
$$

Figure 4.2 pictures the hierarchy of measurements that have s-symmetric extensions and the relationships between the same hierarchy and the classes of global (Pos) and separable measurements (Sep).

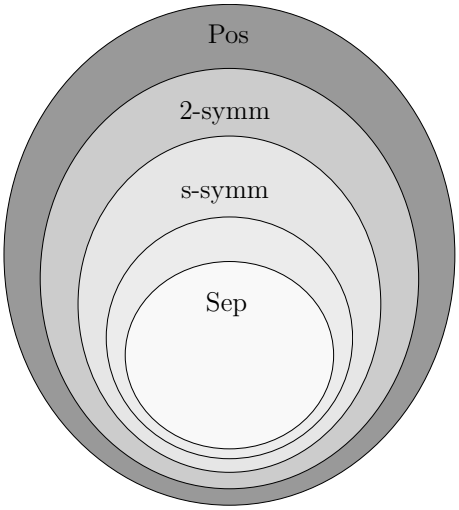

Figure 4.2: Symmetric extension hierarchy.

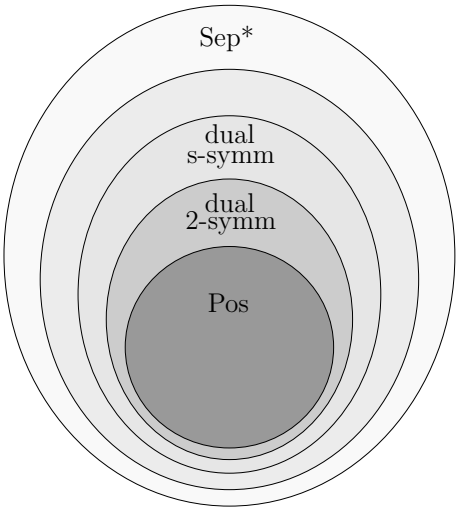

Figure 4.3: Dual of the symmetric extension hierarchy of Figure 4.2.

4.3 An example: Werner hiding pair

In order to demonstrate an analytic method to use the cone programming framework presented above, we apply it here to a simple example. We reprove the result from Example 3.2, that is, a tight bound on the LOCC-distinguishability of a pair of quantum hiding states. For any positive integer $n \leq 2$, consider the equiprobable ensemble $\mathcal{E}^{(n)}$ of the two extremal Werner states $\sigma_0^{(n)}, \sigma_1^{(n)} \in \mathrm{D}(\mathbb{C}^n \otimes \mathbb{C}^n)$ defined in Eq. (3.23). Here we prove that

$$\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}^{(n)}) \leq \frac{1}{2} + \frac{1}{n+1}, \tag{4.55}$$

for any $n \geq 2$. For this particular case, the semidefinite program ($\mathrm{P}_{\mathrm{PPT}}$) is sufficient to prove a tight bound on the distinguishability of the states. This is not always the case, as we will see in the next chapter.

Let the integer n be fixed and let $\mathcal{X}$ and $\mathcal{Y}$ be copies of $\mathbb{C}^n$. First, we instantiate Program (4.25) for the ensemble $\mathcal{E}^{(n)}$:

$$\begin{aligned} \text{minimize:} \quad & \mathrm{Tr}(H) \\ \text{subject to:} \quad & H - \frac{1}{2}\sigma_0^{(n)} \in \mathrm{PPT}^*(\mathcal{X} : \mathcal{Y}), \\ & H - \frac{1}{2}\sigma_1^{(n)} \in \mathrm{PPT}^*(\mathcal{X} : \mathcal{Y}), \\ & H \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y}). \end{aligned} \tag{4.56}$$

Next, we define the Hermitian operator $H \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y})$ as

$$H = \frac{1}{2}\sigma_0^{(n)} + \frac{1}{n+1}\sigma_1^{(n)}, \tag{4.57}$$

and observe that the trace is equal to the bound we seek to prove, that is,

$$\mathrm{Tr}(H) = \frac{1}{2} + \frac{1}{n+1}. \tag{4.58}$$

It is left to be checked that H is a feasible solution of the dual program. By the definition of the cone $\mathrm{PPT}^*(\mathcal{X} \otimes \mathcal{Y})$, we need to show that there exist positive semidefinite operators $R_0, R_1 \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ such that

$$H - \frac{1}{2}\sigma_0^{(n)} \geq \mathrm{T}_{\mathcal{X}}(R_0) \tag{4.59}$$

and

$$H - \frac{1}{2}\sigma_1^{(n)} \geq \mathrm{T}_{\mathcal{X}}(R_1). \tag{4.60}$$

Let

$$u = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle|i\rangle \tag{4.61}$$

be the canonical maximally entangled state in $\mathcal{X} \otimes \mathcal{Y}$ and let

$$R_0 = 0 \qquad \text{and} \qquad R_1 = \frac{1}{n+1} uu^*. \tag{4.62}$$

We have

$$H - \frac{1}{2}\sigma_0^{(n)} = \frac{1}{n+1}\sigma_1^{(n)} \geq 0 = \mathrm{T}_{\mathcal{X}}(R_0), \tag{4.63}$$

and

$$H - \frac{1}{2}\sigma_1^{(n)} = \frac{1}{2}\sigma_0^{(n)} - \frac{n-1}{2(n+1)}\sigma_1^{(n)} = \frac{1}{n(n+1)} W_n = \mathrm{T}_{\mathcal{X}}(R_1), \tag{4.64}$$

where $W_n \in \mathrm{U}(\mathcal{X} \otimes \mathcal{Y})$ in the last equation is the swap operator defined in (2.41).

4.4 A discussion on computational aspects

The proof approach we outlined for the Werner hiding pair (and that we are going to pursue all over in the following chapters) may leave an uneasy feeling to the reader, even though it is mathematically legitimate. We started by defining the operator H in Eq. (4.57) whose trace was exactly equal to the bound we wanted to prove, and then we proved that H is indeed a feasible solution of the dual problem. A posteriori our strategy did work out just fine, but how did we know that H was a good candidate for the solution we were seeking?

For simple problems such as the one above, one could come up with some insights after trying a few candidates that look promising and eventually tweak the solution until things work out. For more complicated instances this is not always a good strategy, and most often we are not blessed by magic insights. What comes to rescue in difficult situations is a numerical approach: we can get a good candidate solution by running an actual computer implementation of one of the programs described above. The output of the program often gives insights on a potential solution, which can be then verified analytically, as we did above for the Werner hiding pair example. When running a particular instance of a convex optimization problem, attention should be paid to the time and the memory space that computer solvers need, which is the topic of discussion of the rest of this section.

Optimizing over separable operators (and therefore over separable measurements) is NP-hard [Gha10], which simply means that solving the cone program ($\mathrm{P}_{\mathrm{Sep}}$) is not feasible. However, there do exist algorithms that solve semidefinite programs efficiently. This very fact motivated us (and [DPS04] before us) to introduce the hierarchy of semidefinite programs in Section 4.2.3. More precisely, let the dimensions of Alice's and Bob's subspaces be $\dim(\mathcal{X}) = n$ and $\dim(\mathcal{Y}) = m$, respectively. Then the *ellipsoid method* [GLS93] solves the program corresponding to the s-th level of the symmetric extension hierarchy in a running time that is *polynomial* in N (the number of states), n, m^s, and the maximum bit-length of the entries of the density matrices specifying the input states[2]. Notice that the value of s needed in order to reach a good approximation of the separable problem can grow larger than a constant (and in fact larger than $m^{o(1)}$), which is why this does not contradict the above-mentioned NP-hardness of the problem (or more precisely, any complexity theory hypothesis).

One way to make the algorithm more efficient in terms of memory used is to observe that ultimately we are really optimizing only over operators in the space

$$\mathcal{X} \otimes \mathcal{Y}_1 \circledcirc \cdots \circledcirc \mathcal{Y}_s, \tag{4.65}$$

which has dimension

$$d = n\binom{s+m-1}{m-1}, \tag{4.66}$$

that is, much smaller than nm^s.

Let us see how this works for the case $s = 2$, the other cases being a straightforward generalization. Let $A \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{Y}_2, \mathcal{Y} \circledcirc \mathcal{Y}_2)$ be the linear isometry such that $AA^* = \Pi_{\mathcal{Y}\circledcirc\mathcal{Y}_2}$, where $\Pi_{\mathcal{Y}\circledcirc\mathcal{Y}_2}$ is the projection on the symmetric subspace $\mathcal{Y} \circledcirc \mathcal{Y}_2$. Then we can replace the two sets of constraints

$$\begin{aligned} &\mathrm{Tr}_{\mathcal{Y}_2}(X_k) = \mu(k), \\ &(\mathbb{1}_{\mathcal{X}} \otimes \Pi_{\mathcal{Y}\circledcirc\mathcal{Y}_2}) X_k (\mathbb{1}_{\mathcal{X}} \otimes \Pi_{\mathcal{Y}\circledcirc\mathcal{Y}_2}) = X_k \end{aligned} \tag{4.67}$$

in the Program (4.53), with a set of constraints of the form

$$\mathrm{Tr}_{\mathcal{Y}_2}((\mathbb{1}_{\mathcal{X}} \otimes A) X_k (\mathbb{1}_{\mathcal{X}} \otimes A^*)) = \mu(k), \tag{4.68}$$

where the only variables of the program are now of the form

$$X_k \in \mathrm{Pos}(\mathbb{C}^d). \tag{4.69}$$

[2] Actual software implementations of semidefinite programming solvers may use other methods that are not guaranteed to run as efficiently in theory, but that behave very well in practice, the *interior point method* being one of those.

A MATLAB function that checks for separable/PPT distinguishability has been developed as part of N. Johnston's QETLAB toolbox [JCR15]. See Appendix A for more details on the implementation, as well as a tutorial on how to use the function.

4.5 Unambiguous state discrimination

In the previous sections, we analyzed the problem of distinguishing quantum states using measurements that minimize the probability of error. Here we consider a strategy in which Alice and Bob can give an inconclusive, yet never incorrect answer. Such measurement strategies are called *unambiguous*.

If there are N states to be distinguished, an unambiguous measurement

$$\mu : \{1, \ldots, N+1\} \to \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$$

consists of $N+1$ operators, where the outcome of the operator $\mu(N+1)$ corresponds to the inconclusive answer.

The cone programming approach has already been used to study unambiguous discrimination by global measurement [Eld03], but never, as far as we know, to study unambiguous local discrimination. In fact, we believe that unambiguous LOCC discrimination in general has not been thoroughly investigated yet.

The optimal value of the following cone program is equal to the success probability of unambiguously distinguishing an ensemble of states $\{\rho_1, \ldots, \rho_k\}$ using measurements whose operators belong to a convex cone $\mathcal{C} \subset \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$. Again, we assume that the states are drawn with a uniform probability.

Primal problem

$$\begin{aligned} \text{maximize:} \quad & \sum_{k=1}^{N} p_k \langle \mu(k), \rho_k \rangle \\ \text{subject to:} \quad & \sum_{k=1}^{N+1} \mu(k) = \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}}, \\ & \mu : \{1, \ldots, N+1\} \to \mathcal{C}, \\ & \langle \mu(i), \rho_j \rangle = 0, \qquad 1 \leq i, j \leq N, \quad i \neq j. \end{aligned} \tag{4.70}$$

The dual program can be derived by routine calculation.

Dual problem

$$\begin{aligned}
\text{minimize:} \quad & \operatorname{Tr}(H) \\
\text{subject to:} \quad & H - p_k \rho_k + \sum_{\substack{1 \leq i \leq N \\ i \neq k}} y_{i,k} \rho_i \in \mathcal{C}^*, \quad k = 1, \ldots, N \,, \\
& H \in \operatorname{Herm}(\mathcal{X} \otimes \mathcal{Y}), \\
& y_{i,j} \in \mathbb{R}, \quad 1 \leq i, j \leq N, \quad i \neq j.
\end{aligned} \tag{4.71}$$

Chapter 5

Distinguishability of maximally entangled states

In this chapter we finally bring the cone programming framework into action, in order to answer some questions about the distinguishability of maximally entangled states. As it was discussed in Section 3.3, sets of maximally entangled states constitute an important testbed for gaging the power of different classes of measurements.

As a warm-up, we first reprove a bound by [YDY12] on the distinguishability of any set of maximally entangled states. Next, we answer an open question regarding the entanglement cost of Bell states that was raised in [YDY14]. In the second part we study the set of states (3.29) introduced in [YDY12].

Contents

5.1 General bound for maximally entangled states

We show that no PPT measurement can perfectly distinguish more than n maximally entangled states in $\mathcal{X} \otimes \mathcal{Y}$, where $\mathcal{X} = \mathcal{Y} = \mathbb{C}^n$. This result appears in [YDY12] and it generalizes a bound by Nathanson, which is valid against LOCC and separable measurements [Nat05]. The following lemma is central to the proof.

Lemma 5.1. *Let $A \in \mathrm{U}(\mathcal{Y}, \mathcal{X})$ be a unitary operator. It holds that*

$$\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - \operatorname{vec}(A) \operatorname{vec}(A)^* \in \mathrm{PPT}^*(\mathcal{X} : \mathcal{Y}). \tag{5.1}$$

Proof. Let $W_n \in \mathrm{U}(\mathcal{X}, \mathcal{Y})$ be the swap operator from Eq. (2.41). Consider the operator

$$U = (\overline{A} \otimes \mathbb{1}_{\mathcal{Y}}) W_n (A^{\mathsf{T}} \otimes \mathbb{1}_{\mathcal{Y}}). \tag{5.2}$$

Since A and W_n are unitary operators, so is U. Notice that U is also Hermitian, and therefore its eigenvalues are either 1 or -1. This implies that

$$\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - U \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}) \tag{5.3}$$

is positive semidefinite. Moreover we have that

$$\begin{aligned} \mathrm{T}_{\mathcal{X}}(\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - U) &= \mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - (A \otimes \mathbb{1}_{\mathcal{Y}}) \operatorname{vec}(\mathbb{1}) \operatorname{vec}(\mathbb{1})^* (A^* \otimes \mathbb{1}_{\mathcal{Y}}) \\ &= \mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - \operatorname{vec}(A) \operatorname{vec}(A)^*, \end{aligned} \tag{5.4}$$

and therefore

$$\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - \operatorname{vec}(A) \operatorname{vec}(A)^* \in \mathrm{PPT}^*(\mathcal{X} : \mathcal{Y}). \tag{5.5}$$

□

Now, suppose that $u_1, \ldots, u_N \in \mathcal{X} \otimes \mathcal{Y}$ are vectors representing maximally entangled pure states. An upper-bound on the probability to distinguish these N states, assuming a uniform selection, is obtained from the dual problem (4.25) by considering

$$H = \frac{\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}}}{nN}. \tag{5.6}$$

It holds that H is a feasible solution to the dual problem: since the states are maximally entangled, for each $k \in \{1, \ldots, N\}$ one may write

$$u_k = \frac{1}{\sqrt{n}} \operatorname{vec}(A_k), \tag{5.7}$$

for some choice of an isometry $A_k \in \mathrm{U}(\mathcal{Y}, \mathcal{X})$, and therefore

$$H - \frac{1}{N} u_k u_k^* = \frac{1}{nN} \left(\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - \mathrm{vec}(A_k)\, \mathrm{vec}(A_k)^* \right) \in \mathrm{PPT}^*(\mathcal{X} : \mathcal{Y}) \tag{5.8}$$

by Lemma 5.1. Finally, the value

$$\mathrm{Tr}(H) = \frac{n}{N} \tag{5.9}$$

is an upper bound on the probability of distinguishing the states and it is smaller than 1 whenever the number of states N is bigger than the dimension n of each subspace.

Remark 5.2. The statement of Lemma 5.1 may become very familiar to the reader, once it is translated in the language of linear mappings via the Choi isomorphism. It is straightforward to see that the operator in Eq. (5.1) is the Choi operator of a mapping $\Phi_A : \mathrm{L}(\mathcal{Y}) \to \mathrm{L}(\mathcal{X})$ defined as

$$\Phi_A(X) = \mathrm{Tr}(X)\mathbb{1} - AXA^*, \tag{5.10}$$

for any $X \in \mathrm{L}(\mathcal{Y})$, which in turn is the composition of a unitary mapping

$$X \to AXA^* \tag{5.11}$$

and the mapping

$$\Phi(X) = \mathrm{Tr}(X)\mathbb{1} - X, \tag{5.12}$$

which is the well-known *reduction map* introduced in [HH99] (it is the mapping at the basis of the reduction criterion for entanglement detection). In brief, we related the fact that PPT measurements can distinguish no more than n maximally entangled states in $\mathbb{C}^n \otimes \mathbb{C}^n$ with the fact that the reduction map from $\mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ is a decomposable map.

5.2 Entanglement cost of distinguishing Bell states

In this section, we study state discrimination problems for sets of three or four Bell states, by LOCC, separable, and PPT measurements, with the assistance of an entangled pair of qubits. In particular, we will assume that Alice and Bob aim to discriminate a set of Bell states given that they share the additional resource state

$$|\tau_\varepsilon\rangle = \sqrt{\frac{1+\varepsilon}{2}}\, |0\rangle|0\rangle + \sqrt{\frac{1-\varepsilon}{2}}\, |1\rangle|1\rangle, \tag{5.13}$$

for some choice of $\varepsilon \in [0,1]$. The parameter ε quantifies the amount of entanglement in the state $|\tau_\varepsilon\rangle$. Up to local unitaries, this family of states represents every pure state of two qubits.

Using the cone programming method discussed in the previous chapter, we obtain exact expressions for the optimal probability with which any set of three or four Bell states can be discriminated with the assistance of the state (5.13) by separable measurements (which match the probabilities obtained by LOCC measurements in all cases).

5.2.1 Discriminating three Bell states

Notice that the state $|\tau_1\rangle = |0\rangle|0\rangle$ is a product state and it does not aid the two parties in discriminating any set of Bell states, so the probability of success for $\varepsilon = 1$ is still at most $2/3$ for a set of three Bell states. If $\varepsilon = 0$, then Alice and Bob can use teleportation to perfectly discriminate all four Bell states perfectly by LOCC measurements, and therefore the same is true for any three Bell states. It was proved in [YDY14] that PPT measurements can perfectly discriminate any set of three Bell states using the resource state (5.13) if and only if $\varepsilon \leq 1/3$.

Here we show that a maximally entangled state ($\varepsilon = 0$) is required to perfectly discriminate any set of three Bell states using separable measurements, and more generally we obtain an expression for the optimal probability of a correct discrimination for all values of ε. Because the permutations of Bell states induced by local unitaries is transitive, there is no loss of generality in fixing the three Bell states to be discriminated to be $|\phi_1\rangle$, $|\phi_2\rangle$, and $|\phi_3\rangle$ (as defined in (2.13)).

Theorem 5.3. *Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_1 = \mathcal{Y}_2 = \mathbb{C}^2$, define $\mathcal{X} = \mathcal{X}_1 \otimes \mathcal{X}_2$ and $\mathcal{Y} = \mathcal{Y}_1 \otimes \mathcal{Y}_2$, and let $\varepsilon \in [0,1]$ be chosen arbitrarily. For any separable measurement $\mu \in \mathrm{Meas}_{\mathrm{Sep}}(3, \mathcal{X} : \mathcal{Y})$, the success probability of correctly discriminating the states corresponding to the set*

$$\big\{|\phi_1\rangle \otimes |\tau_\varepsilon\rangle,\ |\phi_2\rangle \otimes |\tau_\varepsilon\rangle,\ |\phi_3\rangle \otimes |\tau_\varepsilon\rangle\big\} \subset (\mathcal{X}_1 \otimes \mathcal{Y}_1) \otimes (\mathcal{X}_2 \otimes \mathcal{Y}_2), \tag{5.14}$$

assuming a uniform distribution $p_1 = p_2 = p_3 = 1/3$, is at most

$$\frac{1}{3}\left(2 + \sqrt{1 - \varepsilon^2}\right). \tag{5.15}$$

To prove this theorem, we require the following lemma. The lemma introduces a family of positive maps that, to our knowledge, has not previously appeared in the literature.

Lemma 5.4. *Define a linear mapping* $\Xi_t : \mathrm{L}(\mathbb{C}^2 \oplus \mathbb{C}^2) \to \mathrm{L}(\mathbb{C}^2 \oplus \mathbb{C}^2)$ *as*

$$\Xi_t \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} \Psi_t(D) + \Phi(D) & \Psi_t(B) + \Phi(C) \\ \Psi_t(C) + \Phi(B) & \Psi_t(A) + \Phi(A) \end{pmatrix} \tag{5.16}$$

for every $t \in (0, \infty)$ *and* $A, B, C, D \in \mathrm{L}(\mathbb{C}^2)$*, where* $\Psi_t : \mathrm{L}(\mathbb{C}^2) \to \mathrm{L}(\mathbb{C}^2)$ *is defined as*

$$\Psi_t \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} t\alpha & \beta \\ \gamma & t^{-1}\delta \end{pmatrix} \tag{5.17}$$

and $\Phi : \mathrm{L}(\mathbb{C}^2) \to \mathrm{L}(\mathbb{C}^2)$ *is defined as*

$$\Phi \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}, \tag{5.18}$$

for every $\alpha, \beta, \gamma, \delta \in \mathbb{C}$*. It holds that* Ξ_t *is a positive map for all* $t \in (0, \infty)$*.*

Proof. It will first be proved that Ξ_1 is positive. For every vector

$$u = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{5.19}$$

in $\mathbb{C}^2$, define a matrix

$$M_u = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix}. \tag{5.20}$$

Straightforward computations reveal that

$$M_u^* M_v = uv^* + \Phi(vu^*) \qquad \text{and} \qquad M_u^* M_u = \|u\|^2 \mathbb{1} \tag{5.21}$$

for all $u, v \in \mathbb{C}^2$. It follows that

$$\Xi_1 \begin{pmatrix} uu^* & uv^* \\ vu^* & vv^* \end{pmatrix} = \begin{pmatrix} vv^* + \Phi(vv^*) & uv^* + \Phi(vu^*) \\ vu^* + \Phi(uv^*) & uu^* + \Phi(uu^*) \end{pmatrix} = \begin{pmatrix} \|v\|^2 \mathbb{1} & M_u^* M_v \\ M_v^* M_u & \|u\|^2 \mathbb{1} \end{pmatrix}, \tag{5.22}$$

which is positive semidefinite by virtue of the fact that $\|M_u^* M_v\| \leq \|M_u\| \|M_v\| = \|u\| \|v\|$. As every element of $\mathrm{Pos}(\mathbb{C}^2 \oplus \mathbb{C}^2)$ can be written as a positive linear combination of matrices of the form

$$\begin{pmatrix} uu^* & uv^* \\ vu^* & vv^* \end{pmatrix}, \tag{5.23}$$

ranging over all vectors $u, v \in \mathbb{C}^2$, it follows that Ξ_1 is a positive map.

For the general case, observe first that the mapping Ψ_s may be expressed using the Hadamard (or entry-wise) product as

$$\Psi_s \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} s\alpha & \beta \\ \gamma & s^{-1}\delta \end{pmatrix} = \begin{pmatrix} s & 1 \\ 1 & s^{-1} \end{pmatrix} \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{5.24}$$

for every positive real number $s \in (0, \infty)$. The matrix

$$\begin{pmatrix} s & 1 \\ 1 & s^{-1} \end{pmatrix} \tag{5.25}$$

is positive semidefinite, from which it follows (by the Schur product theorem) that Ψ_s is a completely positive map. (See, for instance, Theorem 3.7 of [Pau02].) Also note that $\Phi = \Psi_s \Phi \Psi_s$ for every $s \in (0, \infty)$, which implies that

$$\Xi_t = \big(\mathbb{1}_{\mathrm{L}(\mathbb{C}^2)} \otimes \Psi_s\big)\Xi_1\big(\mathbb{1}_{\mathrm{L}(\mathbb{C}^2)} \otimes \Psi_s\big) \tag{5.26}$$

for $s = \sqrt{t}$. This shows that Ξ_t is a composition of positive maps for every positive real number t, and is therefore positive. □

Proof of Theorem 5.3. For the cases that $\varepsilon = 0$ and $\varepsilon = 1$, the theorem is known, as was discussed previously, so it will be assumed that $\varepsilon \in (0, 1)$. Define a Hermitian operator

$$H_\varepsilon = \frac{1}{3}\left[\frac{\mathbb{1}_{\mathcal{X}_1 \otimes \mathcal{Y}_1} \otimes \tau_\varepsilon}{2} + \sqrt{1 - \varepsilon^2}\, \phi_4 \otimes \mathrm{T}_{\mathcal{X}_2}(\phi_4)\right], \tag{5.27}$$

where $\tau_\varepsilon = |\tau_\varepsilon\rangle\langle\tau_\varepsilon|$, $\phi_4 = |\phi_4\rangle\langle\phi_4|$, and $\mathrm{T}_{\mathcal{X}_2}$ denotes partial transposition with respect to the standard basis of $\mathcal{X}_2$. It holds that

$$\mathrm{Tr}(H_\varepsilon) = \frac{1}{3}\left(2 + \sqrt{1 - \varepsilon^2}\right), \tag{5.28}$$

so to complete the proof it suffices to prove that H_ε is a feasible solution to the dual problem (4.41) for the cone program corresponding to the state discrimination problem being considered.

In order to be more precise about the task at hand, it is helpful to define a unitary operator W, mapping $\mathcal{X}_1 \otimes \mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2$ to $\mathcal{X}_1 \otimes \mathcal{Y}_1 \otimes \mathcal{X}_2 \otimes \mathcal{Y}_2$, that corresponds to swapping the second and third subsystems:

$$W(x_1 \otimes x_2 \otimes y_1 \otimes y_2) = x_1 \otimes y_1 \otimes x_2 \otimes y_2, \tag{5.29}$$

for all vectors $x_1 \in \mathcal{X}_1$, $x_2 \in \mathcal{X}_2$, $y_1 \in \mathcal{Y}_1$, $y_2 \in \mathcal{Y}_2$. We are concerned with the separability of measurement operators with respect to the bipartition between $\mathcal{X}_1 \otimes \mathcal{X}_2$ and $\mathcal{Y}_1 \otimes \mathcal{Y}_2$, so the dual feasibility of H_ε requires that the operators defined as

$$Q_{k,\varepsilon} = W^* \left(H_\varepsilon - \frac{1}{3}\phi_k \otimes \tau_\varepsilon \right) W \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y}) \tag{5.30}$$

be contained in $\mathrm{Sep}^*(\mathcal{X} : \mathcal{Y})$ for $k = 1, 2, 3$.

Let $\Lambda_{k,\varepsilon} : \mathrm{L}(\mathcal{Y}) \to \mathrm{L}(\mathcal{X})$ be the unique linear map whose Choi representation satisfies $J(\Lambda_{k,\varepsilon}) = Q_{k,\varepsilon}$ for each $k = 1, 2, 3$. As discussed in Section 4.2.2, the block positivity of $Q_{k,\varepsilon}$ is equivalent to the positivity of $\Lambda_{k,\varepsilon}$. Consider first the case $k = 1$ and let

$$t = \sqrt{\frac{1+\varepsilon}{1-\varepsilon}}. \tag{5.31}$$

A calculation reveals that

$$\Lambda_{1,\varepsilon}(Y) = \frac{\sqrt{1-\varepsilon^2}}{3} \left(\sigma_3 \otimes \mathbb{1}_{\mathcal{X}_2} \right) \Xi_t(Y) \left(\sigma_3 \otimes \mathbb{1}_{\mathcal{X}_2} \right), \tag{5.32}$$

where $\Xi_t : \mathrm{L}(\mathcal{Y}) \to \mathrm{L}(\mathcal{X})$ is the map defined in Lemma 5.4 and σ_3 denotes one of the Pauli operators (see Eq. (2.11) for an explicit definition). As $\varepsilon \in (0, 1)$, it holds that $t \in (0, \infty)$, and therefore Lemma 5.4 implies that $\Xi_t(Y) \in \mathrm{Pos}(\mathcal{X})$ for every $Y \in \mathrm{Pos}(Y)$. As we are simply conjugating $\Xi_t(Y)$ by a unitary and scaling it by a positive real factor, we also have that $\Lambda_{1,\varepsilon}(Y) \in \mathrm{Pos}(\mathcal{X})$, for any $Y \in \mathrm{Pos}(Y)$, which in turn implies that $Q_{1,\varepsilon} \in \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y})$.

For the case of $k = 2$ and $k = 3$, first define $U, V \in \mathrm{U}(\mathbb{C}^2)$ as follows:

$$U = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \text{and} \quad V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \tag{5.33}$$

These operators transform $\phi_1 = |\phi_1\rangle\langle\phi_1|$ into $\phi_2 = |\phi_2\rangle\langle\phi_2|$ and $\phi_3 = |\phi_3\rangle\langle\phi_3|$, respectively, and leave ϕ_4 unchanged, in the following sense:

$$\begin{aligned} (U^* \otimes U^*)\phi_1(U \otimes U) &= \phi_2, \\ (V^* \otimes V^*)\phi_1(V \otimes V) &= \phi_3, \\ (U^* \otimes U^*)\phi_4(U \otimes U) &= \phi_4, \\ (V^* \otimes V^*)\phi_4(V \otimes V) &= \phi_4. \end{aligned} \tag{5.34}$$

Therefore the following equations hold:

$$\begin{aligned} Q_{2,\varepsilon} &= \left(U^* \otimes \mathbb{1} \otimes U^* \otimes \mathbb{1} \right) Q_{1,\varepsilon} \left(U \otimes \mathbb{1} \otimes U \otimes \mathbb{1} \right), \\ Q_{3,\varepsilon} &= \left(V^* \otimes \mathbb{1} \otimes V^* \otimes \mathbb{1} \right) Q_{1,\varepsilon} \left(V \otimes \mathbb{1} \otimes V \otimes \mathbb{1} \right). \end{aligned} \tag{5.35}$$

It follows that $Q_{2,\varepsilon} \in \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y})$ and $Q_{3,\varepsilon} \in \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y})$, which completes the proof. □

Remark 5.5. The upper bound obtained in Theorem 5.3 is achievable by an LOCC measurement, as it is the probability obtained by using the resource state $|\tau_\varepsilon\rangle$ to teleport the given Bell state from one player to the other, followed by an optimal local measurement to discriminate the resulting states.

5.2.2 Discriminating four Bell states

It is known that, for the perfect LOCC discrimination of all four Bell states using an auxiliary entangled state $|\tau_\varepsilon\rangle$ as above, one requires that $\varepsilon = 0$ (i.e., a maximally entangled pair of qubits is required). This fact follows from the method of [HSSH03], for instance. Here we prove a more precise bound on the optimal probability of a correct discrimination, for every choice of $\varepsilon \in [0,1]$, along similar lines to the bound on three Bell states provided by Theorem 5.3. In the present case, in which all four Bell states are considered, the result is somewhat easier: one obtains an upper bound for PPT measurements that matches a bound that can be obtained by an LOCC measurement, implying that LOCC, separable, and PPT measurements are equivalent for this discrimination problem.

Theorem 5.6. *Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_1 = \mathcal{Y}_2 = \mathbb{C}^2$, define $\mathcal{X} = \mathcal{X}_1 \otimes \mathcal{X}_2$ and $\mathcal{Y} = \mathcal{Y}_1 \otimes \mathcal{Y}_2$, and let $\varepsilon \in [0,1]$. For any PPT measurement $\mu \in \mathrm{Meas}_{\mathrm{PPT}}(4, \mathcal{X} : \mathcal{Y})$, the success probability of discriminating the states in the set*

$$\{|\phi_1\rangle \otimes |\tau_\varepsilon\rangle,\ |\phi_2\rangle \otimes |\tau_\varepsilon\rangle,\ |\phi_3\rangle \otimes |\tau_\varepsilon\rangle,\ |\phi_4\rangle \otimes |\tau_\varepsilon\rangle\} \subset (\mathcal{X}_1 \otimes \mathcal{Y}_1) \otimes (\mathcal{X}_2 \otimes \mathcal{Y}_2), \tag{5.36}$$

assuming a uniform distribution $p_1 = p_2 = p_3 = p_4 = 1/4$, is at most

$$\frac{1}{2}\left(1 + \sqrt{1-\varepsilon^2}\right). \tag{5.37}$$

Proof. Consider the following operator:

$$H_\varepsilon = \frac{1}{8}\Big[\mathbb{1}_{\mathcal{X}_1 \otimes \mathcal{Y}_1} \otimes \tau_\varepsilon + \sqrt{1-\varepsilon^2}\,\mathbb{1}_{\mathcal{X}_1 \otimes \mathcal{Y}_1} \otimes \mathrm{T}_{\mathcal{X}_2}(\phi_4)\Big] \in \mathrm{Herm}(\mathcal{X}_1 \otimes \mathcal{Y}_1 \otimes \mathcal{X}_2 \otimes \mathcal{Y}_2). \tag{5.38}$$

It holds that

$$\mathrm{Tr}(H_\varepsilon) = \frac{1}{2}\left(1 + \sqrt{1-\varepsilon^2}\right), \tag{5.39}$$

so to complete the proof it suffices to prove that H_ε is dual feasible for the Program (4.25). Dual feasibility will follow from the condition (which is sufficient but not necessary for feasibility)

$$(\mathrm{T}_{\mathcal{X}_1} \otimes \mathrm{T}_{\mathcal{X}_2})\Big(H_\varepsilon - \frac{1}{4}\,\phi_k \otimes \tau_\varepsilon\Big) \in \mathrm{Pos}(\mathcal{X}_1 \otimes \mathcal{Y}_1 \otimes \mathcal{X}_2 \otimes \mathcal{Y}_2), \tag{5.40}$$

for $k = 1, 2, 3, 4$. One may observe that

$$\mathrm{T}_{\mathcal{X}_2}(\tau_\varepsilon) + \frac{\sqrt{1-\varepsilon^2}}{2}\phi_4 = \frac{1}{2}\begin{pmatrix} 1+\varepsilon & 0 & 0 & 0 \\ 0 & \frac{\sqrt{1-\varepsilon^2}}{2} & \frac{\sqrt{1-\varepsilon^2}}{2} & 0 \\ 0 & \frac{\sqrt{1-\varepsilon^2}}{2} & \frac{\sqrt{1-\varepsilon^2}}{2} & 0 \\ 0 & 0 & 0 & 1-\varepsilon \end{pmatrix} \tag{5.41}$$

is positive semidefinite, from which it follows that

$$(\mathrm{T}_{\mathcal{X}_1} \otimes \mathrm{T}_{\mathcal{X}_2})\Big(H_\varepsilon - \frac{1}{4}\,\phi_1 \otimes \tau_\varepsilon\Big) = \frac{1}{4}\phi_4 \otimes \mathrm{T}_{\mathcal{X}_2}(\tau_\varepsilon) + \frac{\sqrt{1-\varepsilon^2}}{8}\mathbb{1}_{\mathcal{X}_1\otimes\mathcal{Y}_1} \otimes \phi_4 \tag{5.42}$$

is also positive semidefinite. A similar calculation holds for $k = 2, 3, 4$, which completes the proof. □

Remark 5.7. Similar to Theorem 5.3, one has that the upper bound obtained by Theorem 5.6 is optimal for LOCC measurements, as it is the probability obtained using teleportation.

5.3 Yu-Duan-Ying states

In this section we prove a tight bound of $3/4$ on the maximum success probability for any LOCC measurement to discriminate the set of states (3.29) exhibited by Yu, Duan, and Ying [YDY12], assuming a uniform selection of states. The fact that this bound can be achieved by an LOCC measurement is trivial: if Alice and Bob measure their parts of the states with respect to the standard basis, they can easily discriminate $|\phi_1\rangle$, $|\phi_2\rangle$, and $|\phi_4\rangle$, erring only in the case that they receive $|\phi_3\rangle$. The fact that this bound is optimal will be proved by exhibiting a feasible solution H to the dual problem (4.41) instantiated with the state discrimination problem at hand, such that

$$\mathrm{Tr}(H) = \frac{3}{4}. \tag{5.43}$$

With respect to the vector-operator correspondence, the states (3.29) are given by tensor products of the Pauli operators (2.11) as follows:

$$\begin{aligned} |\phi_1\rangle &= \frac{1}{2}\,\mathrm{vec}(U_1), \quad |\phi_2\rangle = \frac{1}{2}\,\mathrm{vec}(U_2), \\ |\phi_3\rangle &= \frac{1}{2}\,\mathrm{vec}(U_3), \quad |\phi_4\rangle = \frac{1}{2}\,\mathrm{vec}(U_4), \end{aligned} \tag{5.44}$$

for

$$U_1 = \sigma_0 \otimes \sigma_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad U_2 = \sigma_1 \otimes \sigma_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$
$$U_3 = i\sigma_2 \otimes \sigma_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \qquad U_4 = \sigma_3 \otimes \sigma_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}. \tag{5.45}$$

Bound for separable measurements

A feasible solution of the dual problem (4.41) is based on a construction of block positive operators that correspond, via the Choi isomorphism, to the family of positive maps introduced by Breuer and Hall [Bre06, Hal06].

Proposition 5.8 (Breuer–Hall)**.** *Let $\mathcal{X} = \mathcal{Y} = \mathbb{C}^n$ and let $U, V \in \mathrm{U}(\mathcal{Y}, \mathcal{X})$ be unitary operators such that $U^{\mathsf{T}}V \in \mathrm{U}(\mathcal{Y})$ is skew-symmetric: $(V^{\mathsf{T}}U)^{\mathsf{T}} = -V^{\mathsf{T}}U$. It holds that*

$$\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - \operatorname{vec}(U)\operatorname{vec}(U)^* - \mathrm{T}_{\mathcal{X}}(\operatorname{vec}(V)\operatorname{vec}(V)^*) \in \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y}). \tag{5.46}$$

Proof. For every unit vector $y \in \mathcal{Y}$, one has

$$\begin{aligned}(\mathbb{1}_{\mathcal{X}} \otimes y^*)(\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - \operatorname{vec}(U)\operatorname{vec}(U)^* - \mathrm{T}_{\mathcal{X}}(\operatorname{vec}(V)\operatorname{vec}(V)^*))(\mathbb{1}_{\mathcal{X}} \otimes y) \\ = \mathbb{1}_{\mathcal{X}} - U\overline{y}y^{\mathsf{T}}U^* - \overline{V}yy^*V^{\mathsf{T}}.\end{aligned} \tag{5.47}$$

As it holds that $V^{\mathsf{T}}U$ is skew-symmetric, we have

$$\left\langle \overline{V}y, U\overline{y} \right\rangle = y^*V^{\mathsf{T}}U\overline{y} = \left\langle yy^{\mathsf{T}}, V^{\mathsf{T}}U \right\rangle = 0, \tag{5.48}$$

as the last inner product is between a symmetric and a skew-symmetric operator. Because U and V are unitary, it follows that $U\overline{y}y^{\mathsf{T}}U^* + \overline{V}yy^*V^{\mathsf{T}}$ is a rank two orthogonal projection, so the operator represented by (5.47) is also a projection and is therefore positive semidefinite. □

Remark 5.9. The assumption of Proposition 5.8 requires n to be even, as skew-symmetric unitary operators exist only in even dimensions.

Now, for the ensemble

$$\mathcal{E} = \{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle\}, \tag{5.49}$$

one has that the following operator is a feasible solution to the dual problem (4.41):

$$H = \frac{1}{16}(\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} - \mathrm{T}_{\mathcal{X}}(\mathrm{vec}(V)\,\mathrm{vec}(V)^*)) \tag{5.50}$$

for

$$V = i\sigma_2 \otimes \sigma_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{5.51}$$

Due to Proposition 5.8, the feasibility of H follows from the condition

$$(V^{\mathsf{T}}U_k)^{\mathsf{T}} = -V^{\mathsf{T}}U_k, \tag{5.52}$$

which can be checked by inspecting each of the four cases. It is easy to calculate that $\mathrm{Tr}(H) = 3/4$, and so the required bound has been obtained.

Bound for PPT measurements

Interestingly, when it comes to distinguishing the Yu–Duan–Ying states, PPT measurements can do better than separable (and LOCC) measurement, yet without achieving perfect distinguishability. As far as we know, this is the first example of a set consisting only of maximally entangled states for which such a gap holds. In this section we exhibit a tight bound of 7/8 on the probability of distinguishing the Yu–Duan–Ying ensemble by PPT measurements.

Theorem 5.10. *For $\mathcal{E}$ being the ensemble in Eq. (5.49), it holds that* $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) \leq 7/8$.

Proof. We show that there exists a solution of the dual program ($\mathrm{D}_{\mathrm{PPT}}$) which achieves the bound. It is easy to check that the following operator satisfies the constraints in of the program and its trace is equal to 7/8:

$$Y = \frac{1}{16}\mathbb{1} \otimes \mathbb{1} - \frac{1}{8}\left(\psi_2 \otimes \psi_1\right).$$

We will check the constraint $Y \geq \mathrm{T}_{\mathcal{A}}(\rho_1)$ and the reader can check the remaining constraints with a similar calculation. By the equations in (4.28), we have

$$\begin{aligned}\mathrm{T}_{\mathcal{A}}(\rho_1) = \mathrm{T}_{\mathcal{A}}(\psi_0 \otimes \psi_0) &= \left(\frac{1}{2}\mathbb{1} - \psi_2\right) \otimes \left(\frac{1}{2}\mathbb{1} - \psi_2\right) \\ &= \frac{1}{4}\mathbb{1} \otimes \mathbb{1} - \frac{1}{2} \sum_{i \in \{0,1,3\}} (\psi_i \otimes \psi_2 + \psi_2 \otimes \psi_i),\end{aligned}$$

and

$$Y - \frac{1}{4}\mathrm{T}_{\mathcal{A}}(\rho_1) = \frac{1}{8}(\psi_0 \otimes \psi_2 + \psi_1 \otimes \psi_2 + \psi_3 \otimes \psi_2 + \psi_2 \otimes \psi_0 + \psi_2 \otimes \psi_3) \geq 0.$$

□

Theorem 5.11. *For $\mathcal{E}$ being the ensemble in Eq. (5.49), it holds that* $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) \geq 7/8$.

Proof. It is enough to show a feasible solution of the primal program ($\mathrm{P}_{\mathrm{PPT}}$) that achieves the bound. Let $Q \in \mathrm{Pos}(\mathbb{C}^4 \otimes \mathbb{C}^4)$ and $R, S \in \mathrm{Pos}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ be the following operators:

$$Q = \frac{1}{4}\mathbb{1} \otimes (\psi_1 + \psi_2), \qquad R = \frac{7}{8}\psi_0 + \frac{1}{8}\psi_3, \qquad S = \frac{1}{8}\psi_0 + \frac{7}{8}\psi_3.$$

Then the following operators define a PPT measurement that achieves a success probability of 7/8:

$$\begin{aligned}\mu(1) &= Q + (\frac{2}{3}\psi_0 + \frac{1}{3}\mathbb{1}) \otimes R, \\ \mu(2) &= Q + (\frac{1}{3}\psi_0 + \psi_1) \otimes S + \frac{1}{3}(\psi_2 + \psi_3) \otimes R, \\ \mu(3) &= Q + (\frac{1}{3}\psi_0 + \psi_2) \otimes S + \frac{1}{3}(\psi_1 + \psi_3) \otimes R, \\ \mu(4) &= Q + (\frac{1}{3}\psi_0 + \psi_3) \otimes S + \frac{1}{3}(\psi_1 + \psi_2) \otimes R.\end{aligned}$$

It is easy to check that these operators define a valid measurement, that is $\sum_{k=1}^{4} \mu(k) = \mathbb{1}$. Using the equations in (4.28), we can verify that those operators are also PPT. Again, we check this for $\mu(1)$.

$$\mathrm{T}_{\mathcal{A}}(\mu(1)) = (\psi_1 + \psi_2 + \psi_4) \otimes (\frac{1}{3}\psi_1 + \frac{1}{2}\psi_2 + \frac{1}{3}\psi_4) + \frac{1}{4}\psi_3 \otimes (\psi_2 + \psi_3) \geq 0.$$

Finally, we have that $\langle \mu(k), \rho_k \rangle = 7/8$, for each $k \in \{1, \ldots, 4\}$. □

To recap, for $\mathcal{E}$ being the ensemble of Yu–Duan–Ying states selected uniformly at random, we have

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) = \mathrm{opt}_{\mathrm{Sep}}(\mathcal{E}) = \frac{3}{4} < \frac{7}{8} = \mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) < \mathrm{opt}(\mathcal{E}) = 1. \tag{5.53}$$

5.3.1 Generalization to higher dimension

Here we generalize the Yu–Duan–Ying states in order to construct sets of N orthogonal maximally entangled states in $\mathbb{C}^N \otimes \mathbb{C}^N$ that are distinguishable by separable operators only with probability $3/4$, for any $N \geq 4$ that is power of 2.

Let $t \geq 2$ be a positive integer and, for any choice of $k \in \{1, \ldots, 2^t\}$, we recursively define the unitary operator

$$U_k^{(t)} = \begin{cases} \sigma_0 \otimes U_k^{(t-1)} & \text{if } 1 \leq k \leq 2^{t-1}, \\ \sigma_1 \otimes U_{k-2^{t-1}}^{(t-1)} & \text{if } 2^{t-1}+1 \leq k \leq 2^t. \end{cases} \tag{5.54}$$

The base of the recursion, $U_1^{(2)}, \ldots, U_4^{(2)}$, is given by the operators defined in Eq. (5.72). In a paper by the author [CR14], it was shown that the set

$$\left\{ \mathrm{vec}(U_k^{(t)})\, \mathrm{vec}(U_k^{(t)})^* : k = 1, \ldots, 2^t \right\} \tag{5.55}$$

can be distinguished with probability at most $7/8$ by PPT measurements, for any value of $t \geq 2$, when the states are drawn with uniform probability, $p_1, \ldots, p_{2^t} = 1/2^t$. In the rest of this section, we show that the maximum success probability for any separable measurement to distinguish the same set of states under the same assumption is $3/4$ instead.

As in the theme of this thesis, we will exhibit a feasible solution of the dual cone program (4.41) for which the value of the objective function equals $3/4$. However, we first prove a rather general lemma, which shows how to compose a separable operator with a block positive operator, in order to construct another block positive operator in higher dimensions.

Lemma 5.12. *Let $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}_1$, and $\mathcal{Y}_1$ be complex Euclidean spaces. We denote by $W \in \mathrm{U}(\mathcal{X}_1 \otimes \mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2, \mathcal{X}_1 \otimes \mathcal{Y}_1 \otimes \mathcal{X}_2 \otimes \mathcal{Y}_2)$ the linear isometry that swaps the second and the third subsystems, which is defined by the following equation:*

$$W(x_1 \otimes x_2 \otimes y_1 \otimes y_2) = x_1 \otimes y_1 \otimes x_2 \otimes y_2, \tag{5.56}$$

holding for all vectors $x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2, y_1 \in \mathcal{Y}_1, y_2 \in \mathcal{Y}_2$. *Let* $S \in \mathrm{Sep}(\mathcal{X}_1 : \mathcal{Y}_1)$ *be a separable operator and* $Q \in \mathrm{Sep}^*(\mathcal{X}_2 : \mathcal{Y}_2)$ *be a block positive operator. Then the following holds:*

$$W^*(S \otimes Q)W \in \mathrm{Sep}^*(\mathcal{X}_1 \otimes \mathcal{X}_2 : \mathcal{Y}_1 \otimes \mathcal{Y}_2). \tag{5.57}$$

Proof. By the definition of block-positivity, the claim of the lemma is equivalent to the following condition:

$$(\mathbb{1}_{\mathcal{X}_1 \otimes \mathcal{X}_2} \otimes y^*)W^*(S \otimes Q)W(\mathbb{1}_{\mathcal{X}_1 \otimes \mathcal{X}_2} \otimes y) \in \mathrm{Pos}(\mathcal{X}_1 \otimes \mathcal{X}_2), \tag{5.58}$$

for every $y \in \mathcal{Y}_1 \otimes \mathcal{Y}_2$.

For an arbitrary $y \in \mathcal{Y}_1 \otimes \mathcal{Y}_2$, consider its Schmidt decomposition, that is, a positive integer r and orthogonal sets $\{w_1, \ldots, w_r\} \subset \mathcal{Y}_1$ and $\{z_1, \ldots, z_r\} \subset \mathcal{Y}_2$ such that

$$y = \sum_{i=1}^{r} w_i \otimes z_i. \tag{5.59}$$

It holds that

$$\begin{aligned}
&(\mathbb{1} \otimes y^*)W^*(S \otimes Q)W(\mathbb{1} \otimes y) \\
&\qquad = \left(\sum_{i=1}^{r} \mathbb{1}_{\mathcal{X}_1 \otimes \mathcal{X}_2} \otimes w_i^* \otimes z_i^*\right) W^*(S \otimes Q)W \left(\sum_{i=1}^{r} \mathbb{1}_{\mathcal{X}_1 \otimes \mathcal{X}_2} \otimes w_i \otimes z_i\right) \\
&\qquad = \left(\sum_{i=1}^{r} \mathbb{1}_{\mathcal{X}_1} \otimes w_i^* \otimes \mathbb{1}_{\mathcal{X}_2} \otimes z_i^*\right) (S \otimes Q) \left(\sum_{i=1}^{r} \mathbb{1}_{\mathcal{X}_1} \otimes w_i \otimes \mathbb{1}_{\mathcal{X}_2} \otimes z_i\right) \\
&\qquad = \sum_{i,j=1}^{r} (\mathbb{1}_{\mathcal{X}_1} \otimes w_i^*)S(\mathbb{1}_{\mathcal{X}_1} \otimes w_j) \otimes (\mathbb{1}_{\mathcal{X}_2} \otimes z_i^*)Q(\mathbb{1}_{\mathcal{X}_2} \otimes z_j).
\end{aligned} \tag{5.60}$$

The separable operator $S \in \mathrm{Sep}(\mathcal{X}_1 : \mathcal{Y}_1)$ can be expressed as

$$S = \sum_{j=1}^{m} a_j a_j^* \otimes b_j b_j^*, \tag{5.61}$$

for vectors $a_1, \ldots, a_m \in \mathcal{X}_1$ and $b_1, \ldots, b_m \in \mathcal{Y}_1$. By convexity, it is enough to argue about the operator

$$(\mathbb{1} \otimes y^*)W^*(aa^* \otimes bb^* \otimes Q)W(\mathbb{1} \otimes y), \tag{5.62}$$

for any vectors $a \in \mathcal{X}_1$ and $b \in \mathcal{Y}_1$. From Eq. (5.60), we have that

$$\begin{aligned}
&(\mathbb{1} \otimes y^*)W^*(aa^* \otimes bb^* \otimes Q)W(\mathbb{1} \otimes y) \\
&\qquad = \sum_{i,j=1}^{r} (aa^* \otimes w_i^* bb^* w_j) \otimes (\mathbb{1}_{\mathcal{X}_2} \otimes z_i^*) Q (\mathbb{1}_{\mathcal{X}_2} \otimes z_j) \\
&\qquad = aa^* \otimes \left(\mathbb{1}_{\mathcal{X}_2} \otimes \sum_{i=1}^{r} w_i^* a z_i^* \right) Q \left(\mathbb{1}_{\mathcal{X}_2} \otimes \sum_{i=1}^{r} a^* w_i z_i \right) \\
&\qquad = aa^* \otimes (\mathbb{1}_{\mathcal{X}_2} \otimes z^*) Q (\mathbb{1}_{\mathcal{X}_2} \otimes z),
\end{aligned} \tag{5.63}$$

where we have defined the vector $z \in \mathcal{Y}_2$ to be such that $z = \sum_{i=1}^{r} a^* w_i z_i$. From the fact the $Q \in \mathrm{Sep}^*(\mathcal{X}_2 : \mathcal{Y}_2)$, it holds that

$$(\mathbb{1}_{\mathcal{X}_2} \otimes z^*) Q (\mathbb{1}_{\mathcal{X}_2} \otimes z) \in \mathrm{Pos}(\mathcal{X}_2),$$

and therefore we have that

$$(\mathbb{1}_{\mathcal{X}_1 \otimes \mathcal{X}_2} \otimes y^*) W^* (S \otimes Q) W (\mathbb{1}_{\mathcal{X}_1 \otimes \mathcal{X}_2} \otimes y) \in \mathrm{Sep}(\mathcal{X}_1 \otimes \mathcal{X}_2) \tag{5.64}$$

is positive semidefinite. □

Now we are ready to show a feasible solution of the dual problem (4.41) for the set of states (5.55). For any $t \geq 2$, we denote with $\mathcal{X}^{(t)}$ and $\mathcal{Y}^{(t)}$ two isomorphic copies of the complex Euclidean space $\mathbb{C}^{2^t}$, so that the states in (5.55) lie in $\mathcal{X}^{(t)} \otimes \mathcal{Y}^{(t)}$.

Consider the operator

$$S = \frac{1}{2} \operatorname{vec}(\sigma_0 + \sigma_1) \operatorname{vec}(\sigma_0 + \sigma_1)^* \in \mathrm{Pos}(\mathcal{X}^{(1)} \otimes \mathcal{Y}^{(1)}). \tag{5.65}$$

Let $W \in \mathrm{U}(\mathcal{X}^{(t)} \otimes \mathcal{Y}^{(t)}, \mathcal{X}^{(1)} \otimes \mathcal{Y}^{(1)} \otimes \mathcal{X}^{(t-1)} \otimes \mathcal{Y}^{(t-1)})$ be the linear isometry defined in the statement of Lemma 5.12, acting on the specified spaces. The solution of the dual problem may be recursively defined as follows:

$$H^{(t)} = W^* (S \otimes H^{(t-1)}) W, \tag{5.66}$$

for any $t \geq 2$. The base of the recursion $H^{(2)}$ is the operator defined in Eq. (5.50). In the rest of the section we prove, by induction, that the cone program constraint

$$H^{(t)} - \frac{1}{2^t} \operatorname{vec}(U_k^{(t)}) \operatorname{vec}(U_k^{(t)})^* \in \mathrm{Sep}^*(\mathcal{X}^{(t)} : \mathcal{Y}^{(t)}) \tag{5.67}$$

is satisfied for any $k \in \{1, \ldots, 2^t\}$.

Let us consider an arbitrary $1 \leq k \leq 2^{t-1}$ (the case $2^{t-1} \leq k \leq 2^t$ follows from a similar argument). Eq. (5.54) implies that

$$\begin{aligned} \operatorname{vec}(U_k^{(t)}) \operatorname{vec}(U_k^{(t)})^* &= W^*(\operatorname{vec}(\sigma_0) \operatorname{vec}(\sigma_0)^* \otimes \operatorname{vec}(U_k^{(t-1)}) \operatorname{vec}(U_k^{(t-1)})^*)W \\ &\leq W^*(\operatorname{vec}(\sigma_0 + \sigma_1) \operatorname{vec}(\sigma_0 + \sigma_1)^* \otimes \operatorname{vec}(U_k^{(t-1)}) \operatorname{vec}(U_k^{(t-1)})^*)W, \end{aligned} \tag{5.68}$$

and therefore that

$$H^{(t)} - \frac{1}{2^t} \operatorname{vec}(U_k^{(t)}) \operatorname{vec}(U_k^{(t)})^* = W^*(S \otimes H^{(t-1)})W - \frac{1}{2^t} \operatorname{vec}(U_k^{(t)}) \operatorname{vec}(U_k^{(t)})^* \tag{5.69}$$

$$\geq W^*(S \otimes (H^{(t-1)} - \frac{1}{2^{t-1}} \operatorname{vec}(U_k^{(t-1)}) \operatorname{vec}(U_k^{(t-1)})^*)W. \tag{5.70}$$

The Peres-Horodecki criterion, along with the fact that

$$\mathrm{T}_{\mathcal{X}}(S) = S \in \operatorname{Pos}(\mathcal{X}_1 \otimes \mathcal{Y}_1),$$

implies that $S \in \operatorname{Sep}(\mathcal{X}_1 : \mathcal{Y}_1)$. From Lemma 5.12 and the induction hypothesis, we have that

$$W^*(S \otimes (H^{(t-1)} - \frac{1}{2^{t-1}} \operatorname{vec}(U_k^{(t-1)}) \operatorname{vec}(U_k^{(t-1)})^*)W \in \operatorname{Sep}^*(\mathcal{X}^{(t)} : \mathcal{Y}^{(t)}), \tag{5.71}$$

and therefore the constraint (5.67) is satisfied. Moreover, we have that $\operatorname{Tr}(Q) = 1$ and therefore

$$\operatorname{Tr}(H^{(t)}) = \operatorname{Tr}(H^{(2)}) = \frac{3}{4}$$

Small sets of locally indistinguishable orthogonal maximally entangled states

The main corollary of the proof above is that there exist LOCC-indistinguishable sets of $k < n$ maximally entangled states in $\mathbb{C}^n \otimes \mathbb{C}^n$. Asymptotically, our construction allows for the cardinality k of the indistinguishable sets to be as small as Cn, where C is a constant less than 1. In particular, we have that $3/4 \leq C < 1$. It is possible that this constant can be improved by using a different construction than the Yu–Duan–Ying states. A further improvement would be to exhibit indistinguishable sets of maximally entangled states with cardinality $o(n)$. One among the smallest indistinguishable sets that come out

of the above construction consists of the states in $\mathbb{C}^8 \otimes \mathbb{C}^8$ corresponding the following 7 unitary operators:

$$\begin{aligned} U_1 &= \sigma_0 \otimes \sigma_0 \otimes \sigma_0, \\ U_2 &= \sigma_0 \otimes \sigma_1 \otimes \sigma_1, \\ U_3 &= \sigma_0 \otimes \sigma_2 \otimes \sigma_1, \\ U_4 &= \sigma_0 \otimes \sigma_3 \otimes \sigma_1, \\ U_5 &= \sigma_0 \otimes \sigma_0 \otimes \sigma_0, \\ U_6 &= \sigma_0 \otimes \sigma_1 \otimes \sigma_1, \\ U_7 &= \sigma_0 \otimes \sigma_2 \otimes \sigma_1. \end{aligned} \tag{5.72}$$

Remark 5.13. In a very recent result[1], Li et al. [LWFZ15] build up on our proof from [CR14] and show that indistinguishable sets of N orthogonal maximally entangled states in $\mathbb{C}^N \otimes \mathbb{C}^N$ exists for all N and not just when N is a power of 2.

Entanglement Discrimination Catalysis

It is worth noting that the "Entanglement Discrimination Catalysis" phenomenon, observed in [YDY12] for the set (3.29), also applies to the set of states in the above example and to any set derived from our construction. If Alice and Bob are provided with a maximally entangled state as a resource, then they are able to distinguish the states in these sets and, when the protocol ends, they are still left with an untouched maximally entangled state. When $t = 2$, the catalyst is used to teleport the first qubit from one party to the other, say from Alice to Bob. Bob can then measure the first two qubits in the standard Bell basis and identify which of the four states was prepared. Since the third and fourth qubits are not being acted on, they can be used in a new round of the protocol. For the case $t > 2$, let us recall the recursive construction of the states from (5.54). Distinguishing between the two cases of the recursion is equivalent to distinguishing between two Bell states. And the base case is exactly the case $t = 2$ described above, with only one maximally entangled state involved in the catalysis.

PPT vs. separable in the perfect discrimination of maximally entangled states

Michael Nathanson (personal communication) raised the question whether there always exists a separable measurement that *perfectly* distinguishes maximally entangled states

[1] A similar result (obtained via a different approach) appears also in a preprint by Yu and Oh [YO15]. Notice that this has not been published yet, neither I have verified it myself yet.

that are known to be *perfectly* distinguishable by PPT. The construction that generalize Yu–Duan–Ying states in high dimension provides a negative answer to Michael's question. It turns out that if we take only 7 out of the 8 states coming from the construction for $t = 3$ (for example, the ones corresponding to the operators in Eq. (5.72)), they are distinguishable by separable measurement with probability at most $6/7$, but they are perfectly distinguishable by PPT. Unfortunately we do not have a nice-looking closed form for the PPT measurement operators that achieve perfect distinguishability, but know, by running a semidefinite programming solver, that such operators exist.

5.3.2 Unambiguous discrimination

Interestingly, the optimal probability of unambiguously distinguish the set of Yu–Duan-Ying states with PPT measurements is $3/4$, which should be compared with the success probability of $7/8$ that can be achieved with a minimum-error strategy (see Theorem 5.11). Using a semidefinite program solver, we were also able to verify that this bound is actually tight.

Theorem 5.14. *The maximum success probability of* unambiguously *distinguishing the ensemble in Eq.* (5.49) *with PPT measurements is equal to* $3/4$.

Proof. We show a feasible solution of the dual problem (4.71) for which the value of the objective function is $3/4$. Let

$$Y = \frac{1}{16}[(\mathbb{1} - \psi_1) \otimes (\mathbb{1} - 2\psi_4) + \psi_1 \otimes (-\psi_1 + 3\psi_2 + 3\psi_3 + \psi_4)]. \tag{5.73}$$

and

$$\begin{aligned} Q_1 &= [(\mathbb{1} - \psi_3) \otimes \psi_3 + \psi_3 \otimes (\psi_2 + \psi_3)]/4, \\ Q_2 &= [(\psi_1 + \psi_2) \otimes \psi_2 + \psi_4 \otimes (\mathbb{1} - \psi_2)]/4, \\ Q_3 &= [(\psi_2 + \psi_4) \otimes \psi_2 + \psi_1 \otimes (\mathbb{1} - \psi_2)]/4, \\ Q_4 &= [(\psi_1 + \psi_4) \otimes \psi_2 + \psi_2 \otimes (\mathbb{1} - \psi_2)]/4, \\ Q_5 &= (\psi_3 \otimes \psi_2)/4. \end{aligned} \tag{5.74}$$

We can use the equations in (4.28) to verify that the constraints of the program (4.71) are satisfied:

$$Y - \frac{1}{4}\rho_j + \sum_{\substack{1 \le i \le k \\ i \ne j}} \rho_i = \mathrm{T}_{\mathcal{A}}(Q_j), \quad j = 1, \ldots, 4 \quad \text{and} \quad Y \ge \mathrm{T}_{\mathcal{A}}(Q_5), \tag{5.75}$$

Finally, we have $\mathrm{Tr}(Y) = 3/4$. □

Chapter 6

Distinguishability of unextendable product sets

In this chapter, we study the state discrimination problem for collections of states formed by unextendable product sets. An orthonormal collection of product vectors

$$\mathcal{A} = \{u_k \otimes v_k : k = 1, \ldots, N\} \subset \mathcal{X} \otimes \mathcal{Y}, \tag{6.1}$$

for complex Euclidean spaces $\mathcal{X} = \mathbb{C}^n$ and $\mathcal{Y} = \mathbb{C}^m$, is said to be an *unextendable product set* if it is impossible to find a nonzero product vector $u \otimes v \in \mathcal{X} \otimes \mathcal{Y}$ that is orthogonal to every element of $\mathcal{A}$ [BDM+99]. That is, $\mathcal{A}$ is an unextendable product set if, for every choice of vectors $u \in \mathcal{X}$ and $v \in \mathcal{Y}$ satisfying either $\langle u, u_k \rangle = 0$ or $\langle v, v_k \rangle = 0$ for each $k \in \{1, \ldots, N\}$, one has that either $u = 0$ or $v = 0$ (or both).

The first section establishes a simple criterion for the states formed by any unextendable product set to be perfectly discriminated by separable measurements, and the second subsection proves that any set of states formed by taking the union of an unextendable product set $\mathcal{A} \subset \mathcal{X} \otimes \mathcal{Y}$ together with any pure state $z \in \mathcal{X} \otimes \mathcal{Y}$ orthogonal to every element of $\mathcal{A}$ cannot be perfectly discriminated by a separable measurement. (It is evident that PPT measurements allow a perfect discrimination in both cases.)

Contents

6.1 A criterion for perfect separable discrimination of unextendable product sets

Here we provide a simple criterion for when an unextendable product set can be perfectly discriminated by separable measurements, and we use this criterion to show that there is an unextendable product set $\mathcal{A} \subset \mathcal{X} \otimes \mathcal{Y}$ that is not perfectly discriminated by any separable measurement when $\mathcal{X} = \mathcal{Y} = \mathbb{C}^4$. It is known that no unextendable product set $\mathcal{A} \subset \mathcal{X} \otimes \mathcal{Y}$ spanning a proper subspace of $\mathcal{X} \otimes \mathcal{Y}$ can be perfectly discriminated by an LOCC measurement [BDM+99], while every unextendable product set can be discriminated perfectly by a PPT measurement. It is also known that every unextendable product set $\mathcal{A} \subset \mathcal{X} \otimes \mathcal{Y}$ can be perfectly discriminated by separable measurements in the case $\mathcal{X} = \mathcal{Y} = \mathbb{C}^3$ [DMS+03].

The following notation will be used throughout this section. For $\mathcal{X} = \mathbb{C}^n$, $\mathcal{Y} = \mathbb{C}^m$, and $\mathcal{A} = \{u_k \otimes v_k : k = 1, \ldots, N\} \subset \mathcal{X} \otimes \mathcal{Y}$ being an unextendable product set, we will write

$$\mathcal{A}_k = \mathcal{A} \backslash \{u_k \otimes v_k\}, \tag{6.2}$$

and define a set of rank-one product projections

$$\mathcal{P}_k = \left\{ xx^* \otimes yy^* \,:\, x \in \mathcal{X},\, y \in \mathcal{Y},\, \|x\| = \|y\| = 1,\, \text{and } x \otimes y \perp \mathcal{A}_k \right\} \tag{6.3}$$

for each $k = 1, \ldots, N$. One may interpret each element $xx^* \otimes yy^*$ of $\mathcal{P}_k$ as corresponding to a product vector $x \otimes y$ that could replace $u_k \otimes v_k$ in $\mathcal{A}$, yielding a (not necessarily unextendable) orthonormal product set.

The following theorem states that the sets $\mathcal{P}_1, \ldots, \mathcal{P}_N$ defined above determine whether or not an unextendable product set can be perfectly discriminated by separable measurements.

Theorem 6.1. *Let $\mathcal{X} = \mathbb{C}^n$ and $\mathcal{Y} = \mathbb{C}^m$ be complex Euclidean spaces and let*

$$\mathcal{A} = \{u_k \otimes v_k : k = 1, \ldots, N\} \subset \mathcal{X} \otimes \mathcal{Y} \tag{6.4}$$

be an unextendable product set. The following two statements are equivalent:

1. *There exists a separable measurement $\mu \in \mathrm{Meas}_{\mathrm{Sep}}(N, \mathcal{X} : \mathcal{Y})$ that perfectly discriminates the states represented by $\mathcal{A}$ (for any choice of nonzero probabilities $p_1, \ldots, p_N$).*
2. *For $\mathcal{P}_1, \ldots, \mathcal{P}_N$ as defined in (6.3), one has that the identity operator $\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}}$ can be written as a nonnegative linear combination of projections in the set $\mathcal{P}_1 \cup \cdots \cup \mathcal{P}_N$.*

Proof. Assume first that statement 2 holds, so that one may write

$$\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}} = \sum_{k=1}^{N} \sum_{j=1}^{M_k} \lambda_{k,j}\, x_{k,j} x_{k,j}^* \otimes y_{k,j} y_{k,j}^* \tag{6.5}$$

for some choice of positive integers $M_1, \ldots, M_N$, nonnegative real numbers $\{\lambda_{k,j}\}$, and product vectors $\{x_{k,j} \otimes y_{k,j}\}$ satisfying

$$x_{k,j} x_{k,j}^* \otimes y_{k,j} y_{k,j}^* \in \mathcal{P}_k \tag{6.6}$$

for each $k \in \{1, \ldots, N\}$ and $j \in \{1, \ldots, M_k\}$. Define

$$\mu(k) = \sum_{j=1}^{M_k} \lambda_{k,j}\, x_{k,j} x_{k,j}^* \otimes y_{k,j} y_{k,j}^* \tag{6.7}$$

for each $k \in \{1, \ldots, N\}$. It is clear that μ is a separable measurement, and by the definition of the sets $\mathcal{P}_1, \ldots, \mathcal{P}_N$ it necessarily holds that

$$\langle \mu(k), u_\ell u_\ell^* \otimes v_\ell v_\ell^* \rangle = 0, \tag{6.8}$$

when $k \neq \ell$. This implies that μ perfectly discriminates the states represented by $\mathcal{A}$, and therefore implies that statement 1 holds.

Now assume that statement 1 holds: there exists a separable measurement

$$\mu \in \mathrm{Meas}_{\mathrm{Sep}}(N, \mathcal{X} : \mathcal{Y})$$

that perfectly discriminates the states represented by $\mathcal{A}$. As each measurement operator $\mu(k)$ is separable, it is possible to write

$$\mu(k) = \sum_{j=1}^{M_k} \lambda_{k,j}\, x_{k,j} x_{k,j}^* \otimes y_{k,j} y_{k,j}^* \tag{6.9}$$

for some choice of nonnegative integers $\{M_k\}$, positive real numbers $\{\lambda_{k,j}\}$, and unit vectors $\{x_{k,j} : j = 1, \ldots, M_k\} \subset \mathcal{X}$ and $\{y_{k,j} : j = 1, \ldots, M_k\} \subset \mathcal{Y}$. The assumption that this measurement perfectly discriminates $\mathcal{A}$ implies that $x_{k,j} \otimes y_{k,j} \perp \mathcal{A}_k$, and therefore $x_{k,j} x_{k,j}^* \otimes y_{k,j} y_{k,j}^* \in \mathcal{P}_k$, for each $k = 1, \ldots, N$ and $j = 1, \ldots, M_k$. As we have that $\mu(1) + \cdots + \mu(N) = \mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}}$, it follows that statement 2 holds. □

It is not immediately clear that Theorem 6.1 is useful for determining whether or not any particular unextendable product set can be discriminated by separable measurements, but indeed it is. What makes this so is the fact that each set $\mathcal{P}_k$ is necessarily finite, as the following proposition establishes.

Proposition 6.2. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let*

$$\mathcal{A} = \{u_k \otimes v_k : k = 1, \ldots, N\} \subset \mathcal{X} \otimes \mathcal{Y}$$

be an unextendable product set, and let $\mathcal{P}_1, \ldots, \mathcal{P}_N$ be as defined in (6.3). The sets $\mathcal{P}_1, \ldots, \mathcal{P}_N$ are finite.

Proof. Assume toward contradiction that $\mathcal{P}_k$ is infinite for some choice of $k \in \{1, \ldots, N\}$. There are finitely many subsets $S \subseteq \{1, \ldots, k-1, k+1, \ldots, N\}$, so there must exist at least one such subset S with the property that there are infinitely many pairwise nonparallel product vectors of the form $x \otimes y$ such that $x \perp u_j$ for every $j \in S$ and $y \perp v_j$ for every $j \notin \mathcal{S}$. This implies that both the subspace of $\mathcal{X}$ orthogonal to $\{u_j : j \in S\}$ and the subspace of $\mathcal{Y}$ orthogonal to $\{v_j : j \notin S\}$ have dimension at least 1, and at least one of them has dimension at least 2. It follows that there must exist a unit product vector $x \otimes y$ with three properties: (i) $x \perp u_j$ for every $j \in S$, (ii) $y \perp v_j$ for every $j \notin \mathcal{S}$, and (iii) $x \otimes y \perp u_k \otimes v_k$. This contradicts the fact that $\mathcal{A}$ is unextendable, and therefore completes the proof. □

Given Proposition 6.2, it becomes straightforward to make use of Theorem 6.1 computationally. The sets $\mathcal{P}_1, \ldots, \mathcal{P}_N$ can be computed by iterating over all

$$S \subseteq \{1, \ldots, k-1, k+1, \ldots, N\}$$

and finding the (at most one) product state orthogonal to $\{u_j : j \in S\}$ on $\mathcal{X}$ and $\{v_j : j \notin S\}$ on $\mathcal{Y}$. Then, the second statement in Theorem 6.1 can be checked through the use of linear programming (and even by hand in some cases).

Example 6.3 (Feng's unextendable product set)**.** We now present an example of an unextendable product set in $\mathcal{X} \otimes \mathcal{Y}$, for $\mathcal{X} = \mathcal{Y} = \mathbb{C}^4$, that cannot be perfectly discriminated by separable measurements. In particular, let $\mathcal{A}$ be the unextendable product set consisting

of 8 states that were found in [Fen06]:

$$\begin{aligned}
|\phi_1\rangle &= |0\rangle|0\rangle, \\
|\phi_2\rangle &= |1\rangle\left(|0\rangle - |2\rangle + |3\rangle\right)/\sqrt{3}, \\
|\phi_3\rangle &= |2\rangle\left(|0\rangle + |1\rangle - |3\rangle\right)/\sqrt{3}, \\
|\phi_4\rangle &= |3\rangle|3\rangle, \\
|\phi_5\rangle &= \left(|1\rangle + |2\rangle + |3\rangle\right)\left(|0\rangle - |1\rangle + |2\rangle\right)/3, \\
|\phi_6\rangle &= \left(|0\rangle - |2\rangle + |3\rangle\right)|2\rangle/\sqrt{3}, \\
|\phi_7\rangle &= \left(|0\rangle + |1\rangle - |3\rangle\right)|1\rangle/\sqrt{3}, \\
|\phi_8\rangle &= \left(|0\rangle - |1\rangle + |2\rangle\right)\left(|0\rangle + |1\rangle + |2\rangle\right)/3.
\end{aligned} \tag{6.10}$$

For each $k = 1, \ldots, 8$, there are exactly 6 product states contained in $\mathcal{P}_k$ for each choice of k, which we represent by product vectors $|\phi_{k,j}\rangle$ for $j = 1, \ldots, 6$. To be explicit, these states are as follows (where we have omitted normalization factors for brevity):

$$\begin{aligned}
|\phi_{1,1}\rangle &= |0\rangle|0\rangle, \\
|\phi_{1,2}\rangle &= \left(|0\rangle + |1\rangle - |3\rangle\right)\left(|0\rangle + |2\rangle\right), \\
|\phi_{1,3}\rangle &= \left(|0\rangle - |1\rangle\right)\left(|0\rangle + |1\rangle - |3\rangle\right), \\
|\phi_{1,4}\rangle &= \left(|0\rangle - |1\rangle + |2\rangle\right)\left(|0\rangle - |1\rangle + |2\rangle\right), \\
|\phi_{1,5}\rangle &= \left(|0\rangle + |2\rangle\right)\left(|0\rangle - |2\rangle + |3\rangle\right), \\
|\phi_{1,6}\rangle &= \left(|0\rangle - |2\rangle + |3\rangle\right)\left(|0\rangle - |1\rangle\right),
\end{aligned}$$

$$\begin{aligned}
|\phi_{2,1}\rangle &= |1\rangle\left(|0\rangle - |2\rangle + |3\rangle\right), \\
|\phi_{2,2}\rangle &= \left(|0\rangle + |1\rangle - |3\rangle\right)|2\rangle, \\
|\phi_{2,3}\rangle &= \left(|0\rangle + |1\rangle\right)|3\rangle, \\
|\phi_{2,4}\rangle &= \left(|0\rangle - |1\rangle + |2\rangle\right)\left(|1\rangle - 2|2\rangle + |3\rangle\right), \\
|\phi_{2,5}\rangle &= \left(|1\rangle + |2\rangle + |3\rangle\right)\left(|0\rangle - |1\rangle - 2|2\rangle\right), \\
|\phi_{2,6}\rangle &= \left(|1\rangle - |3\rangle\right)|0\rangle,
\end{aligned}$$

$$\begin{aligned}
|\phi_{3,1}\rangle &= |2\rangle\left(|0\rangle + |1\rangle - |3\rangle\right), \\
|\phi_{3,2}\rangle &= \left(|0\rangle - |2\rangle + |3\rangle\right)|1\rangle, \\
|\phi_{3,3}\rangle &= \left(|2\rangle - |3\rangle\right)|0\rangle, \\
|\phi_{3,4}\rangle &= \left(|1\rangle + |2\rangle + |3\rangle\right)\left(|0\rangle + 2|1\rangle + |2\rangle\right), \\
|\phi_{3,5}\rangle &= \left(|0\rangle - |1\rangle + |2\rangle\right)\left(2|1\rangle - |2\rangle - |3\rangle\right), \\
|\phi_{3,6}\rangle &= \left(|0\rangle - |2\rangle\right)|3\rangle,
\end{aligned}$$

$$\begin{aligned}
|\phi_{4,1}\rangle &= |3\rangle|3\rangle, \\
|\phi_{4,2}\rangle &= \left(|0\rangle + |1\rangle - |2\rangle\right)\left(|2\rangle + |3\rangle\right), \\
|\phi_{4,3}\rangle &= \left(|1\rangle + |3\rangle\right)\left(|0\rangle + |1\rangle - |3\rangle\right), \\
|\phi_{4,4}\rangle &= \left(|2\rangle + |3\rangle\right)\left(|0\rangle - |2\rangle + |3\rangle\right), \\
|\phi_{4,5}\rangle &= \left(|1\rangle + |2\rangle + |3\rangle\right)\left(|1\rangle + |2\rangle + |3\rangle\right), \\
|\phi_{4,6}\rangle &= \left(|0\rangle - |2\rangle + |3\rangle\right)\left(|1\rangle + |3\rangle\right),
\end{aligned}$$

$$\begin{aligned}
|\phi_{5,1}\rangle &= \left(|1\rangle + |2\rangle + |3\rangle\right)\left(|0\rangle - |1\rangle + |2\rangle\right), \\
|\phi_{5,2}\rangle &= |1\rangle\left(2|0\rangle + |2\rangle - |3\rangle\right), \\
|\phi_{5,3}\rangle &= |3\rangle|0\rangle, \\
|\phi_{5,4}\rangle &= \left(|0\rangle - |2\rangle - 2|3\rangle\right)|2\rangle, \\
|\phi_{5,5}\rangle &= |2\rangle\left(2|0\rangle - |1\rangle + |3\rangle\right), \\
|\phi_{5,6}\rangle &= \left(|0\rangle + |1\rangle + 2|3\rangle\right)|1\rangle,
\end{aligned}$$

$$\begin{aligned}
|\phi_{6,1}\rangle &= \left(|0\rangle - |2\rangle + |3\rangle\right)|2\rangle, \\
|\phi_{6,2}\rangle &= |3\rangle\left(|0\rangle - |2\rangle\right), \\
|\phi_{6,3}\rangle &= |0\rangle\left(|2\rangle - |3\rangle\right), \\
|\phi_{6,4}\rangle &= \left(|0\rangle - |1\rangle - 2|2\rangle\right)\left(|1\rangle + |2\rangle + |3\rangle\right), \\
|\phi_{6,5}\rangle &= |2\rangle\left(|0\rangle - |2\rangle + |3\rangle\right), \\
|\phi_{6,6}\rangle &= \left(|1\rangle - 2|2\rangle + |3\rangle\right)\left(|0\rangle - |1\rangle + |2\rangle\right),
\end{aligned}$$

$$
\begin{aligned}
|\phi_{7,1}\rangle &= (|0\rangle + |1\rangle - |3\rangle)\,|1\rangle, & |\phi_{7,4}\rangle &= (|0\rangle + 2|1\rangle + |2\rangle)\,(|1\rangle + |2\rangle + |3\rangle),\\
|\phi_{7,2}\rangle &= |0\rangle\,(|1\rangle - |3\rangle), & |\phi_{7,5}\rangle &= (2|1\rangle - |2\rangle - |3\rangle)\,(|0\rangle - |1\rangle + |2\rangle),\\
|\phi_{7,3}\rangle &= |1\rangle\,(|0\rangle + |1\rangle - |3\rangle), & |\phi_{7,6}\rangle &= |3\rangle\,(|0\rangle + |1\rangle),
\end{aligned}
$$

$$
\begin{aligned}
|\phi_{8,1}\rangle &= (|0\rangle - |1\rangle + |2\rangle)\,(|0\rangle + |1\rangle + |2\rangle), & |\phi_{8,4}\rangle &= |0\rangle|3\rangle,\\
|\phi_{8,2}\rangle &= |1\rangle\,(|0\rangle - |2\rangle - 2|3\rangle), & |\phi_{8,5}\rangle &= (2|0\rangle + |2\rangle - |3\rangle)\,|2\rangle,\\
|\phi_{8,3}\rangle &= (2|0\rangle - |1\rangle + |3\rangle)\,|1\rangle, & |\phi_{8,6}\rangle &= |2\rangle\,(|0\rangle + |1\rangle + 2|3\rangle).
\end{aligned}
$$

One may verify by a computer that $\mathbb{1} \otimes \mathbb{1}$ is not contained in the convex cone generated by

$$\big\{|\phi_{k,j}\rangle\langle\phi_{k,j}| \,:\, k = 1, \ldots, 8,\ j = 1, \ldots, 6\big\}. \tag{6.11}$$

(In fact, $\mathbb{1}\otimes\mathbb{1}$ is not in the linear span of the set (6.11).) Theorem 6.1 therefore implies that this unextendable product set is not perfectly discriminated by separable measurements.

The computational procedure described above was implemented in MATLAB as part of the QETLAB Toolbox ([JCR15], `UPBSepDistinguishable` function).

6.2 Impossibility to distinguish an unextendable product set plus one more pure state

Next, we prove an upper bound on the probability to correctly discriminate any unextendable product set, together with one extra pure state orthogonal to the members of the unextendable product set, by a separable measurement. Central to the proof of this statement is a family of positive linear maps previously studied in the literature [Ter01, BGR05].

Before proving this fact, we note that it is fairly straightforward to obtain a qualitative result along similar lines: if a separable measurement were able to perfectly discriminate a particular product set from any state orthogonal to this product set, there would necessarily be a separable measurement operator orthogonal to the space spanned by the product set, implying that some nonzero product state must be orthogonal to the product set (and therefore the product set must be extendable). Related results based on this sort of argument may be found in [Ban11]. An advantage of the method described here is that one obtains precise bounds on the optimal discrimination probability, as opposed to a statement that a perfect discrimination is not possible.

The following lemma is required for the proof of the theorem below.

Lemma 6.4 (Terhal)**.** *For given complex Euclidean spaces $\mathcal{X} = \mathbb{C}^n$ and $\mathcal{Y} = \mathbb{C}^m$, and any unextendable product set*

$$\mathcal{A} = \{u_k \otimes v_k : k = 1, \ldots, N\} \subset \mathcal{X} \otimes \mathcal{Y}, \tag{6.12}$$

there exists a positive real number $\lambda_{\mathcal{A}} > 0$ such that

$$(\mathbb{1}_{\mathcal{X}} \otimes y^*) \left(\sum_{k=1}^{N} u_k u_k^* \otimes v_k v_k^* \right) (\mathbb{1}_{\mathcal{X}} \otimes y) - \lambda_{\mathcal{A}} \|y\|^2 \mathbb{1}_{\mathcal{X}} \in \mathrm{Pos}(\mathcal{X}), \tag{6.13}$$

for every $y \in \mathcal{Y}$.

A proof of the lemma, as well as a constructive procedure to calculate a bound on $\lambda_{\mathcal{A}}$, can be found in [Ter01].

Theorem 6.5. *Let $\mathcal{X} = \mathbb{C}^n$ and $\mathcal{Y} = \mathbb{C}^m$ be complex Euclidean spaces, let*

$$\mathcal{A} = \{u_k \otimes v_k : k = 1, \ldots, N\} \subset \mathcal{X} \otimes \mathcal{Y} \tag{6.14}$$

be an unextendable product set, and let

$$z \in \mathcal{X} \otimes \mathcal{Y} \tag{6.15}$$

be a unit vector orthogonal to $\mathcal{A}$. We have that

$$\mathrm{opt}_{\mathrm{Sep}}(\mathcal{A} \cup \{z\}) \leq 1 - \frac{\lambda_{\mathcal{A}}}{(N+1)\delta}, \tag{6.16}$$

where $\lambda_{\mathcal{A}}$ is a positive real number satisfying the requirements of Lemma 6.4 and

$$\delta = \|\mathrm{Tr}_{\mathcal{X}}(zz^*)\|.$$

Proof. Consider the following Hermitian operator:

$$H = \frac{1}{N+1} \left(\sum_{k=1}^{N} u_k u_k^* \otimes v_k v_k^* + \left(1 - \frac{\lambda_{\mathcal{A}}}{\delta}\right) zz^* \right). \tag{6.17}$$

We want to show that H is a feasible solution of the dual problem (4.41) for the state discrimination problem under consideration. It is clear that

$$H - \frac{1}{N+1} u_k u_k^* \otimes v_k v_k^* \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y}) \subset \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y}) \tag{6.18}$$

for $k = 1, \ldots, N$. The remaining constraint left to be checked is the following:

$$H - \frac{1}{N+1} zz^* = \frac{1}{N+1} \left(\sum_{k=1}^{N} u_k u_k^* \otimes v_k v_k^* - \frac{\lambda_{\mathcal{A}}}{\delta} zz^* \right) \in \mathrm{Sep}^*(\mathcal{X} : \mathcal{Y}). \tag{6.19}$$

Using the fact that

$$\delta \|y\|^2 \mathbb{1}_{\mathcal{X}} - (\mathbb{1}_{\mathcal{X}} \otimes y^*)\, zz^*\, (\mathbb{1}_{\mathcal{X}} \otimes y) \in \mathrm{Pos}(\mathcal{X}), \tag{6.20}$$

for any $y \in \mathcal{Y}$, together with Lemma 6.4, one has that

$$(\mathbb{1} \otimes y)^* \left(\sum_{k=1}^{N} u_k u_k^* \otimes v_k v_k^* - \frac{\lambda_{\mathcal{A}}}{\delta} zz^* \right) (\mathbb{1} \otimes y) \in \mathrm{Pos}(\mathcal{X}) \tag{6.21}$$

and therefore the constraint (6.19) is satisfied. Finally, it holds that

$$\mathrm{Tr}(H) = 1 - \frac{\lambda_{\mathcal{A}}}{(N+1)\delta}, \tag{6.22}$$

which completes the proof. □

Example 6.6 (Tiles set)**.** Theorem 6.5 allow us to find specific bounds for the probability of correctly discriminating certain sets of states. For instance, here we consider the following unextendable product set $\mathcal{A} \subset \mathcal{X} \otimes \mathcal{Y}$ for $\mathcal{X} = \mathcal{Y} = \mathbb{C}^3$, commonly known as the *tiles set*:

$$\begin{gathered} |\phi_1\rangle = |0\rangle \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}} \right), \quad |\phi_2\rangle = |2\rangle \left(\tfrac{|1\rangle - |2\rangle}{\sqrt{2}} \right), \quad |\phi_3\rangle = \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}} \right) |2\rangle, \quad |\phi_4\rangle = \left(\tfrac{|1\rangle - |2\rangle}{\sqrt{2}} \right) |0\rangle, \\ |\phi_5\rangle = \tfrac{1}{3} \left(|0\rangle + |1\rangle + |2\rangle \right) \left(|0\rangle + |1\rangle + |2\rangle \right). \end{gathered} \tag{6.23}$$

For a pure state orthogonal to this set, one may take

$$|\psi\rangle = \frac{1}{2} \left(|0\rangle|0\rangle + |0\rangle|1\rangle - |0\rangle|2\rangle - |1\rangle|2\rangle \right). \tag{6.24}$$

Using the procedure described in [Ter01], one obtains

$$\lambda_{\mathcal{A}} \geq \frac{1}{9} \left(1 - \sqrt{\frac{5}{6}} \right)^2. \tag{6.25}$$

Therefore, if we assume that each state is selected with probability $1/6$, the maximum probability of correctly discriminating the set $\{|\phi_1\rangle, \ldots, |\phi_5\rangle, |\psi\rangle\}$ by a separable measurement is at most

$$\text{opt}_{\text{Sep}}(\mathcal{A}) \leq 1 - \frac{1}{54} \frac{\left(1 - \sqrt{\frac{5}{6}}\right)^2}{\cos\left(\frac{\pi}{8}\right)^2} < 1 - 1.647 \times 10^{-4}. \tag{6.26}$$

This bound is not tight, as numerical optimization (see Appendix A) shows that

$$\text{opt}_{\text{Sep}}(\mathcal{A}) < 0.9861. \tag{6.27}$$

Chapter 7

Conclusions and open problems

In this thesis we have used techniques from convex optimization to study the limitations of LOCC, separable, and PPT measurements for the task of distinguishing sets of bipartite states. Compared to previous approaches, our techniques turned out to be effective in providing precise bounds on the maximum probability of locally distinguishing some interesting sets of maximally entangled states and unextendable product sets.

Several specific questions regarding the local distinguishability of sets of bipartite states remain unsolved.

In Chapter 5 we proved a tight bound on the entanglement cost of discriminating sets of Bell states by means of LOCC protocols. One could ask the following more general question.

Question 7.1. How much entanglement does it cost to distinguish maximally entangled states in $\mathbb{C}^n \otimes \mathbb{C}^n$?

Ghosh et al. [GKRS04] have shown that orthogonal maximally entangled states, which are in canonical form, can always be discriminated, by means of LOCC protocols, if two copies of each of the states are provided. One could ask if two copies are always sufficient. In fact, this question is open even for separable and PPT measurement.

Question 7.2. Are two copies sufficient to discriminate any set of orthogonal pure states by PPT measurements?

The techniques presented in the paper are not intrinsically limited to the setting of bipartite pure states, and applications of these techniques to the *multipartite* setting are topics for possible future work.

Global distinguishability of random states was studied by A. Montanaro [Mon07]. More precisely, he put a lower bound on the probability of distinguishing (by global measurements) an ensembles of n random quantum states in $\mathbb{C}^d$, in the asymptotic regime where n/d approaches a constant. A similar question on the distinguishability of random states by PPT and separable measurements could be investigated by using the convex optimization approach developed in the thesis.

Apart from quantum states, one could also study the LOCC distinguishability of quantum operations [MPW10]. It is a topic that has not been studied as throughly as in the case of states, but once again, one could approach it through the lens of convex optimization.

A more speculative project, yet very exciting, is to give a somewhat useful characterization of the set dual to the set of LOCC measurement and its corresponding set of linear mappings (both labeled by a question mark in the diagrams of Figure 4.1). As we do not have a nice characterization of the LOCC set itself, we suppose this is a difficult project. One direction to approach this problem can be to consider smaller sets that are contained in the LOCC set, such as one-way LOCC, where the communication is only in one direction, say from Alice to Bob, or LOCC-r , in which the communication is limited to r rounds. Let us fantasize we had a characterization of the set dual to the set of LOCC measurement and let us denote it as $\text{Meas}^*_{\text{LOCC}}(N, \mathcal{X} : \mathcal{Y})$. Then we could plug it in the following cone program and proceed as we did for all the cone programs analyzed on this thesis.

Dual (LOCC measurements)

$$\begin{aligned} \text{minimize:} \quad & \text{Tr}(H) \\ \text{subject to:} \quad & \begin{pmatrix} H - p_1\rho_1 & & \\ & \ddots & \\ & & H - p_N\rho_N \end{pmatrix} \in \text{Meas}^*_{\text{LOCC}}(N, \mathcal{X} : \mathcal{Y}), \\ & H \in \text{Herm}(\mathcal{X} \otimes \mathcal{Y}). \end{aligned} \tag{7.1}$$

Finally, apart from [GSU13], I am not aware of any results where cone programming is explicitly used in quantum computing for any cones different than the cone of semidefinite operators. I hope this work helps toward the rise of more applications of cone programming in quantum information theory.

APPENDICES

Appendix A

Local distinguishability in Matlab

Setup

Requirements

- MATLAB[1];
- CVX >= 2.1 [GB14];
- QETLAB >= 0.7 [JCR15];

List of functions

- `Distinguishability` (by N. Johnston) — given an ensemble $\mathcal{E}$, computes $\mathrm{opt}(\mathcal{E})$;
- `LocalDistinguishability` — given an ensemble $\mathcal{E}$, computes $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E})$ or $\mathrm{opt}_{\mathrm{Sym}}(\mathcal{E})$;
- `UPBSepDistinguishable` (by N. Johnston) – an implementation of the criterion described in Sec. 6.1;

[1] Unfortunately at the time of writing this, the package CVX only runs on Matlab. I solemnly promise that I will port all the code to GNU Octave once the Octave port of CVX will be completed.

Examples

The code for the following examples can be found in the repository [Cos15].

Yu–Duan–Ying states

```
states = 1/2*[vec(kron(Pauli(0),Pauli(0)))'; ...
              vec(kron(Pauli(1),Pauli(1)))'; ...
              vec(kron(Pauli(2),Pauli(1)))'; ...
              vec(kron(Pauli(3),Pauli(1)))'];

disp(Distinguishability(states));
disp(LocalDistinguishability(states, 'copies', 1));
disp(LocalDistinguishability(states));
```

```
    1
    0.8750
    0.7500
```

Tiles set plus extra orthogonal state (Example 6.6)

```
extra_state = 1/2*[1 1 -1 0 0 -1 0 0 0];
set = [UPB('Tiles') extra_state'];

disp(LocalDistinguishability(UPB('Tiles')))
disp(LocalDistinguishability(states, 'copies', 1));
disp(LocalDistinguishability(states));
```

```
    1.0000
    1.0000
    0.9860
```

Bell state discrimination

```
bells_m = [Bell(1) Bell(2) Bell(3) Bell(4)]';

disp(Distinguishability(bells_m));
disp(LocalDistinguishability(bells_m, 'copies', 1));
```

```
    1
    0.5000
```

Entanglement cost (Section 5.2)

```
eps = 1/2; % takes a value between 0 and 1
eps_state = [sqrt((1+eps)/2) 0 0 sqrt((1-eps)/2)]';
```

4 Bell states

```
d = 4;
n = 4;

bells_m = zeros(d^2, n);

for k=1:n
    % makes sure we are considering the right partition
    bells_m(:, k) = Swap(kron(Bell(k), eps_state), [2 3], [2 2 2 2]);
end

disp(Distinguishability(bells_m));
disp(LocalDistinguishability(bells_m, 'copies', 1));
```

```
    1
    0.9330
```

3 Bell states

```
n = 3;
disp(Distinguishability(bells_m(:, 1:n)));
disp(LocalDistinguishability(bells_m(:, 1:n), 'copies', 1));
disp(LocalDistinguishability(bells_m(:, 1:n), 'copies', 2));
```

```
    1
    0.9916
    0.9586
```

Generalized Bell states (Examples from [GKRS04])

In the code that follows, the function `GenPauli(a,b,n)` generates the matrix corresponding to the operator $W_{a,b} \in \mathrm{U}(\mathbb{C}^n)$ defined in Eq. (2.17).

5 states in $\mathbb{C}^5 \otimes \mathbb{C}^5$

```
n = 5;
gen_bells = [vec(GenPauli(0,0,n)), ...
             vec(GenPauli(1,1,n)), ...
             vec(GenPauli(1,2,n)), ...
             vec(GenPauli(3,1,n)), ...
             vec(GenPauli(3,2,n))];

disp(Distinguishability(gen_bells));
disp(LocalDistinguishability(gen_bells, 'copies', 1));
```

```
    1
    0.9898
```

6 states in $\mathbb{C}^6 \otimes \mathbb{C}^6$

```
n = 6;
gen_bells = [vec(GenPauli(0,0,n)), ...
             vec(GenPauli(1,1,n)), ...
             vec(GenPauli(0,2,n)), ...
             vec(GenPauli(0,3,n)), ...
             vec(GenPauli(0,4,n)), ...
             vec(GenPauli(3,0,n))];

disp(Distinguishability(gen_bells));
disp(LocalDistinguishability(gen_bells, 'copies', 1));
```

```
    1
    0.9905
```

References

[AL15] Guillaume Aubrun and Cecilia Lancien. Locally restricted measurements on a multipartite quantum system: data hiding is generic. *Quantum Information & Computation*, 15(5&6):513–540, 2015. arXiv:1406.1959. 26

[Ban11] Somshubhro Bandyopadhyay. More nonlocality with less purity. *Physical Review Letters*, 106:210402, May 2011. arXiv:1106.0104, doi:10.1103/PhysRevLett.106.210402. 80

[BBKW09] Somshubhro Bandyopadhyay, Gilles Brassard, Shelby Kimmel, and William K. Wootters. Entanglement cost of nonlocal measurements. *Physical Review A*, 80:012313, Jul 2009. arXiv:0809.2264, doi:10.1103/PhysRevA.80.012313. 31

[BCJ+15] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu. Limitations on separable measurements by convex optimization. *Information Theory, IEEE Transactions on*, 61(6):3593–3604, June 2015. arXiv:1408.6981, doi:10.1109/TIT.2015.2417755. ii, 5, 30

[BDM+99] Charles H. Bennett, David P. DiVincenzo, Tal Mor, Peter W. Shor, John A. Smolin, and Barbara M. Terhal. Unextendible product bases and bound entanglement. *Physical Review Letters*, 82:5385–5388, Jun 1999. arXiv:quant-ph/9808030, doi:10.1103/PhysRevLett.82.5385. 2, 29, 75, 76

[BGK11] Somshubhro Bandyopadhyay, Sibasish Ghosh, and Guruprasad Kar. LOCC distinguishability of unilaterally transformable quantum states. *New Journal of Physics*, 13(12):123013, 2011. URL: http://stacks.iop.org/1367-2630/13/i=12/a=123013, arXiv:1102.0841. 28

[BGR05] Somshubhro Bandyopadhyay, Sibasish Ghosh, and Vwani Roychowdhury. Non-full-rank bound entangled states satisfying the range criterion. *Physical Review*

A, 71:012316, Jan 2005. arXiv:quant-ph/0406023, doi:10.1103/PhysRevA.71.012316. 80

[BHH04] János A. Bergou, Ulrike Herzog, and Mark Hillery. Discrimination of quantum states. In Matteo Paris and Jaroslav Řeháček, editors, *Quantum State Estimation*, volume 649 of *Lecture Notes in Physics*, chapter 11, pages 417–465. Springer Berlin Heidelberg, 2004. doi:10.1007/978-3-540-44481-7_11. 24

[Bre06] Heinz-Peter Breuer. Optimal entanglement criterion for mixed quantum states. *Physical Review Letters*, 97:080501, 2006. arXiv:quant-ph/0605036, doi:10.1103/PhysRevLett.97.080501. 66

[BRW10] Somshubhro Bandyopadhyay, Ramij Rahaman, and William K Wootters. Entanglement cost of two-qubit orthogonal measurements. *Journal of Physics A: Mathematical and Theoretical*, 43(45):455303, 2010. URL: http://stacks.iop.org/1751-8121/43/i=45/a=455303, arXiv:1005.5236. 31

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge University Press, 2004. 17

[CGL99] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Physical Review Letters*, 83:648–651, Jul 1999. URL: http://link.aps.org/doi/10.1103/PhysRevLett.83.648, arXiv:9901025, doi:10.1103/PhysRevLett.83.648. 2

[Che00] Anthony Chefles. Quantum state discrimination. *Contemporary Physics*, 41(6):401–424, 2000. arXiv:quant-ph/0010114, doi:10.1080/00107510010002599. 24

[CLM+14] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about locc (but were afraid to ask). *Communications in Mathematical Physics*, 328(1):303–326, 2014. arXiv:1210.4583, doi:10.1007/s00220-014-1953-9. 38

[CLMO13] Andrew M. Childs, Debbie Leung, Laura Mančinska, and Maris Ozols. A framework for bounding nonlocality of state discrimination. *Communications in Mathematical Physics*, 323:1121–1153, 2013. arXiv:1206.5822. 30

[Coh08] Scott M. Cohen. Understanding entanglement as resource: Locally distinguishing unextendible product bases. *Physical Review A*, 77:012304,

Jan 2008. URL: http://link.aps.org/doi/10.1103/PhysRevA.77.012304, doi:10.1103/PhysRevA.77.012304. 31

[Cos13] Alessandro Cosentino. Positive-partial-transpose-indistinguishable states via semidefinite programming. *Physical Review A*, 87:012321, Jan 2013. arXiv:1205.1031, doi:10.1103/PhysRevA.87.012321. ii, 5, 30

[Cos15] Alessandro Cosentino. Code repository for local-distinguishability examples, June 2015. URL: https://github.com/cosenal/local-distinguishability. 88

[CR14] Alessandro Cosentino and Vincent Russo. Small sets of locally indistinguishable orthogonal maximally entangled states. *Quantum Information & Computation*, 14(13-14):1098–1106, October 2014. arXiv:1307.3232. ii, 5, 30, 69, 73

[CS14] Dariusz Chruściński and Gniewomir Sarbicki. Entanglement witnesses: construction, analysis and classification. *Journal of Physics A: Mathematical and Theoretical*, 47(48):483001, 2014. URL: http://stacks.iop.org/1751-8121/47/i=48/a=483001. 46

[DFXY09] R. Duan, Yuan Feng, Yu Xin, and M. Ying. Distinguishability of quantum states by separable operations. *Information Theory, IEEE Transactions on*, 55(3):1320–1330, March 2009. arXiv:0705.0795, doi:10.1109/TIT.2008.2011524. 4, 28, 30

[DLT02] David P. DiVincenzo, D.W. Leung, and B.M. Terhal. Quantum data hiding. *Information Theory, IEEE Transactions on*, 48(3):580–598, Mar 2002. doi:10.1109/18.985948. 2, 27

[DMS+03] David P. DiVincenzo, Tal Mor, Peter W. Shor, John A. Smolin, and Barbara M. Terhal. Unextendible product bases, uncompletable product bases and bound entanglement. *Communications in Mathematical Physics*, 238(3):379–410, 2003. URL: http://dx.doi.org/10.1007/s00220-003-0877-6, doi:10.1007/s00220-003-0877-6. 76

[DPS02] A. C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Distinguishing separable and entangled states. *Physical Review Letters*, 88:187904, Apr 2002. URL: http://link.aps.org/doi/10.1103/PhysRevLett.88.187904, doi:10.1103/PhysRevLett.88.187904. 3, 39, 47, 48

[DPS04] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. *Physical Review A*, 69:022308, Feb 2004. URL: http://link.aps.org/doi/10.1103/PhysRevA.69.022308, doi:10.1103/PhysRevA.69.022308. 39, 47, 54

[Eld03] Yonina C. Eldar. A semidefinite programming approach to optimal unambiguous discrimination of quantum states. *Information Theory, IEEE Transactions on*, 49(2):446–456, February 2003. 55

[EMV03] Y.C. Eldar, A. Megretski, and George C. Verghese. Designing optimal quantum detectors via semidefinite programming. *Information Theory, IEEE Transactions on*, 49(4):1007–1012, April 2003. arXiv:quant-ph/0205178, doi:10.1109/TIT.2003.809510. 35

[Fan04] Heng Fan. Distinguishability and indistinguishability by local operations and classical communication. *Physical Review Letters*, 92:177905, Apr 2004. doi:10.1103/PhysRevLett.92.177905. 2, 29

[Fen06] Keqin Feng. Unextendible product bases and 1-factorization of complete graphs. *Discrete Applied Mathematics*, 154(6):942 – 949, 2006. doi:10.1016/j.dam.2005.10.011. 79

[GB14] Michael Grant and Stephen Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. http://cvxr.com/cvx, March 2014. 87

[Gha10] Sevag Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Information & Computation*, 10(3&4):343–360, 2010. arXiv:0810.4507. 54

[GKR+01] Sibasish Ghosh, Guruprasad Kar, Anirban Roy, Aditi Sen(De), and Ujjwal Sen. Distinguishability of Bell states. *Physical Review Letters*, 87:277902, Dec 2001. arXiv:quant-ph/0106148, doi:10.1103/PhysRevLett.87.277902. 2, 28, 32

[GKRS04] Sibasish Ghosh, Guruprasad Kar, Anirban Roy, and Debasis Sarkar. Distinguishability of maximally entangled states. *Physical Review A*, 70:022304, Aug 2004. arXiv:quant-ph/0205105, doi:10.1103/PhysRevA.70.022304. 2, 28, 30, 32, 84, 90

[GLS93] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Springer-Verlag Berlin Heidelberg, 1993. doi:10.1007/978-3-642-78240-4. 54

[Got00] Daniel Gottesman. Theory of quantum secret sharing. *Physical Review A*, 61:042311, Mar 2000. URL: http://link.aps.org/doi/10.1103/PhysRevA.61.042311, arXiv:9910067, doi:10.1103/PhysRevA.61.042311. 2

[GSU13] Sevag Gharibian, Jamie Sikora, and Sarvagya Upadhyay. QMA variants with polynomially many provers. *Quantum Information & Computation*, 13(1 & 2):0135–0157, 2013. 45, 85

[Hal06] W. Hall. A new criterion for indecomposability of positive maps. *Journal of Physics A: Mathematical and General*, 39(45):14119, 2006. 66

[Hel69] Carl W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969. URL: http://dx.doi.org/10.1007/BF01007479, doi:10.1007/BF01007479. 2

[HH99] Michał Horodecki and Paweł Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Physical Review A*, 59:4206–4216, Jun 1999. arXiv:quant-ph/9708015, doi:10.1103/PhysRevA.59.4206. 59

[HHH96] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1–2):1 – 8, 1996. URL: http://www.sciencedirect.com/science/article/pii/S0375960196007062, doi:http://dx.doi.org/10.1016/S0375-9601(96)00706-2. 16

[HSSH03] Michał Horodecki, Aditi Sen(De), Ujjwal Sen, and Karol Horodecki. Local indistinguishability: More nonlocality with less entanglement. *Physical Review Letters*, 90:047902, Jan 2003. arXiv:quant-ph/0301106, doi:10.1103/PhysRevLett.90.047902. 2, 32, 33, 64

[JCR15] Nathaniel Johnston, Alessandro Cosentino, and Vincent Russo. Qetlab: Qetlab v0.7, January 2015. URL: http://dx.doi.org/10.5281/zenodo.14186, doi:10.5281/zenodo.14186. 55, 80, 87

[JP99] Daniel Jonathan and Martin B. Plenio. Minimal conditions for local pure-state entanglement manipulation. *Physical Review Letters*, 83:1455–1458, Aug 1999. arXiv:quant-ph/9903054, doi:10.1103/PhysRevLett.83.1455. 33

[LWFZ15] Mao-Sheng Li, Yan-Ling Wang, Shao-Ming Fei, and Zhu-Jun Zheng. d locally indistinguishable maximally entangled states in ${}^{d}\bigotimes{}^{d}$. *Physical Review A*, 91:042318, Apr 2015. arXiv:1411.6702, doi:10.1103/PhysRevA.91.042318. 73

[Man13] Laura Mančinska. *Separable State Discrimination Using Local Quantum Operations and Classical Communication*. PhD thesis, University of Waterloo, 2013. URL: http://hdl.handle.net/10012/7792. 13

[Mon07] Ashley Montanaro. On the distinguishability of random quantum states. *Communications in Mathematical Physics*, 273(3):619–636, 2007. arXiv:quant-ph/0607011, doi:10.1007/s00220-007-0221-7. 85

[MPW10] William Matthews, Marco Piani, and John Watrous. Entanglement in channel discrimination with restricted measurements. *Physical Review A*, 82:032302, Sep 2010. arXiv:1004.0888, doi:10.1103/PhysRevA.82.032302. 85

[MWW09] William Matthews, Stephanie Wehner, and Andreas Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Communications in Mathematical Physics*, 291(3):813–843, 2009. URL: http://dx.doi.org/10.1007/s00220-009-0890-5, doi:10.1007/s00220-009-0890-5. 26

[Nat05] M. Nathanson. Distinguishing bipartitite orthogonal states using LOCC: Best and worst cases. *Journal of Mathematical Physics*, 46:062103, 2005. 2, 28, 30, 58

[Nat13] Michael Nathanson. Three maximally entangled states can require two-way local operations and classical communication for local discrimination. *Physical Review A*, 88:062316, Dec 2013. URL: http://link.aps.org/doi/10.1103/PhysRevA.88.062316, doi:10.1103/PhysRevA.88.062316. 28

[Nav08] Miguel Navascués. Pure state estimation and the characterization of entanglement. *Physical Review Letters*, 100:070503, Feb 2008. URL: http://link.aps.org/doi/10.1103/PhysRevLett.100.070503, doi:10.1103/PhysRevLett.100.070503.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011. 2, 4, 6

[Nie99] M. A. Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83:436–439, Jul 1999. arXiv:quant-ph/9811053, doi:10.1103/PhysRevLett.83.436. 33

[Pau02] Vern Paulsen. *Completely Bounded Maps and Operator Algebras*. Cambridge University Press, 2002. 62

[Per96] Asher Peres. Separability criterion for density matrices. *Physical Review Letters*, 77:1413–1415, Aug 1996. URL: http://link.aps.org/doi/10.1103/PhysRevLett.77.1413, doi:10.1103/PhysRevLett.77.1413. 16

[Pia06] Marco Piani. Class of bound entangled states of $n + n$ qubits revealed by nondecomposable maps. *Physical Review A*, 73:012345, Jan 2006. URL: http://link.aps.org/doi/10.1103/PhysRevA.73.012345, doi:10.1103/PhysRevA.73.012345. 42

[Rai01] E.M. Rains. A semidefinite program for distillable entanglement. *Information Theory, IEEE Transactions on*, 47(7):2921–2933, Nov 2001. doi:10.1109/18.959270. 39

[SSŻ09] Łukasz Skowronek, Erling Størmer, and Karol Życzkowski. Cones of positive maps and their duality relations. *Journal of Mathematical Physics*, 50(062106), 2009. URL: http://scitation.aip.org/content/aip/journal/jmp/50/6/10.1063/1.3155378, doi:http://dx.doi.org/10.1063/1.3155378.

[TDL01] Barbara M. Terhal, David P. DiVincenzo, and Debbie W. Leung. Hiding bits in bell states. *Physical Review Letters*, 86:5807–5810, Jun 2001. arXiv:quant-ph/0011042, doi:10.1103/PhysRevLett.86.5807. 2, 27, 33

[Ter01] Barbara M. Terhal. A family of indecomposable positive linear maps based on entangled quantum states. *Linear Algebra and its Applications*, 323(1–3):61–73, 2001. doi:10.1016/S0024-3795(00)00251-2. 80, 81, 82

[TW12] Levent Tunçel and Henry Wolkowicz. Strong duality and minimal representations for cone optimization. *Computational Optimization and Applications*, 53(2):619–648, 2012. doi:10.1007/s10589-012-9480-0. 6

[Wat05] John Watrous. Bipartite subspaces having no bases distinguishable by local operations and classical communication. *Physical Review Letters*, 95:080505, Aug 2005. arXiv:quant-ph/0503092, doi:10.1103/PhysRevLett.95.080505. 2

[Wat15] John Watrous. *Theory of Quantum Information*. 2015. Draft of the book available at https://cs.uwaterloo.ca/~watrous/CS766/. 4, 6, 13, 14

[WH02] Jonathan Walgate and Lucien Hardy. Nonlocality, asymmetry, and distinguishing bipartite states. *Physical Review Letters*, 89:147901, Sep 2002. arXiv:0202034, doi:10.1103/PhysRevLett.89.147901. 32

[WSHV00] Jonathan Walgate, Anthony J. Short, Lucien Hardy, and Vlatko Vedral. Local distinguishability of multipartite orthogonal quantum states. *Physical Review Letters*, 85:4972–4975, Dec 2000. URL: http://link.aps.org/doi/10.1103/PhysRevLett.85.4972, doi:10.1103/PhysRevLett.85.4972. 2, 26, 30

[WSV00] Henry Wolkowicz, Romesh Saigal, and Lieven Vandenberghe, editors. *Handbook of Semidefinite Programming*. Springer US, 2000. doi:10.1007/978-1-4615-4381-7. 6

[YDY11] Nengkun Yu, Runyao Duan, and Mingsheng Ying. Any $2 \bigotimes n$ subspace is locally distinguishable. *Physical Review A*, 84:012304, Jul 2011. arXiv:1010.2664, doi:10.1103/PhysRevA.84.012304. 2

[YDY12] Nengkun Yu, Runyao Duan, and Mingsheng Ying. Four locally indistinguishable ququad-ququad orthogonal maximally entangled states. *Physical Review Letters*, 109:020506, 2012. arXiv:1107.3224. 2, 4, 28, 29, 30, 33, 57, 58, 65, 73

[YDY14] Nengkun Yu, Runyao Duan, and Mingsheng Ying. Distinguishability of quantum states by positive operator-valued measures with positive partial transpose. *Information Theory, IEEE Transactions on*, 60(4):2069–2079, April 2014. arXiv:1209.4222v2, doi:10.1109/TIT.2014.2307575. 3, 31, 33, 57, 60

[YO15] Sixia Yu and C.H. Oh. Detecting the local indistinguishability of maximally entangled states. Feb 2015. arXiv:1502.01274. 73