DISCRIMINATION OF QUANTUM STATES UNDER LOCAL OPERATIONS AND CLASSICAL COMMUNICATION

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ÖZENÇ GÜNGÖR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
PHYSICS

JULY 2015

Approval of the thesis:

DISCRIMINATION OF QUANTUM STATES UNDER LOCAL OPERATIONS AND CLASSICAL COMMUNICATION

submitted by **ÖZENÇ GÜNGÖR** in partial fulfillment of the requirements for the degree of **Master of Science in Physics Department, Middle East Technical University** by,

Prof. Dr. Gülbin Dural Ünver _____
Dean, Graduate School of **Natural and Applied Sciences**

Prof. Dr. Mehmet T. Zeyrek _____
Head of Department, **Physics**

Prof. Dr. Sadi Turgut _____
Supervisor, **Physics Department, METU**

Examining Committee Members:

Prof. Dr. Yiğit Gündüç
Physics Engineering Department, Hacettepe University _____

Prof. Dr. Sadi Turgut
Physics Department, METU _____

Prof. Dr. Namık Kemal Pak
Physics Department, METU _____

Assoc. Prof. Dr. Yusuf İpekoğlu
Physics Department, METU _____

Assoc. Prof. Dr. Seçkin Kürkçüoğlu
Physics Department, METU _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: ÖZENÇ GÜNGÖR

Signature :

ABSTRACT

DISCRIMINATION OF QUANTUM STATES UNDER LOCAL OPERATIONS AND CLASSICAL COMMUNICATION

Güngör, Özenç
M.S., Department of Physics
Supervisor : Prof. Dr. Sadi Turgut

July 2015, 72 pages

The problem of quantum state discrimination, which is a foundational aspect of quantum information theory, and its relation to the theory of majorization are discussed. The purpose of this study is to review different approaches to the problem and analyze different cases of quantum-state discrimination, most importantly the discrimination of bipartite entangled quantum states under local operations and classical communication. Two partial results on using entanglement as a resource for quantum-state discrimination and discrimination with remaining entanglement is given. The important points are also summarized and the results are discussed.

Keywords: Quantum state discrimination, LOCC, entanglement

ÖZ

KUANTUM DURUMLARININ YEREL OPERASYONLAR VE KLASİK İLETİŞİM ALTINDA AYIRT EDİLMESİ

Güngör, Özenç
Yüksek Lisans, Fizik Bölümü
Tez Yöneticisi : Prof. Dr. Sadi Turgut

Temmuz 2015 , 72 sayfa

Kuantum kuramında temel bir yeri olan kuantum durumlarının belirlenmesi problemi irdelenmiş ve bu problemin majorizasyon kuramı ile bağlantısı araştırılmıştır. Bu çalışmanın ana amacı belirtilmiş problemi çözmek için uygulanan farklı yöntemleri ve bu problemin farklı alt durumlarını, en önemlisi iki-taraflı dolanık kuantum durumlarının yerel operasyonlar ve klasik iletişim altında ayırt edilmesi problemini incelemektir. Dolanıklığın kuantum durumlarının ayırt edilmesi işi için bir kaynak olarak kullanılması ve durumların dolanıklığını koruyarak bu işin gerçekleştşrşlmesi ile ilgili bazı sonuçlar elde edilmiştir. Önemli noktalar özetlenmiş, sonuçlar tartışılmıştır.

Anahtar Kelimeler: Kuantum durumlarının ayırt edilmesi, yerel operasyonlar ve klasik iletişim, dolanıklık

To all scientists and to be scientists held captive

ACKNOWLEDGMENTS

I am very grateful to my tutor, Prof. Dr. Sadi Turgut for his supervision, patience, encouragement and for the fruitful discussions throughout this study. He has introduced me to the beautiful subject of quantum information theory and his insight has proven invaluable on lots of occasions.

I also would like to thank my friend Zeki Seskir for the discussions we held on quantum information theory and his help in using this thesis template, Utku Göreke who provided assistance in numerical calculations and plotting the results and Diren Maraba, my roommate of 4 years for his friendship and endless support.

Last but not the least, I also would like to thank all my friends and family for being there for me when I needed them.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

LOCC	Local Operations and Classical Communication
UQDS	Unambiguous Quantum State Discrimination
QSS	Quantum State Seperation
EPR	Einstein-Podolsky-Rosen

CHAPTER 1

INTRODUCTION

One of the biggest paradigm shifts in the history of science is undoubtedly the Quantum revolution and along with it came many unanswered questions and "paradoxes " and scientists and philosophers alike debated the very nature of reality as quantum mechanics challenged the old, classical ideas. The most famous of these debates are the Bohr-Einstein debates and the papers of EPR (Einstein-Podolsky-Rosen) [1], Bohr [2], Bohm and Aharonov [3]. It was in the first EPR paper that the notion that is nowadays known as quantum entanglement was introduced. These papers explored the fundamental concept of physical reality and in a manner, paved the way for J. S. Bell's famous papers [4] on the nature of physical reality and the pivotal role quantum entanglement plays. It was after the works of J. S. Bell and his collaborators that researchers began to see entanglement as something other than just a peculiarity of quantum mechanics and started to question the nature of information and its physical meaning. The theory of quantum information was born.

Quantum information theory explores the physical nature of information and investigates information processing tasks using quantum mechanical systems. These tasks range from computational ones dealing with using quantum mechanics and quantum entanglement to solve computational problems, a subject which is of great theoretical and experimental interest, and information theoretical tasks such as cryptography, coding, data hiding etc. Entanglement, as a standalone subject is also researched in great detail, particularly the theory of entanglement monotones is a focus of interest.

The main subject of this thesis is the state discrimination problem in quantum mechanics. Quantum state discrimination is a very fundamental problem in quantum theory and it is a great area to explore the very nature of quantum mechanics. The problem is very simple to state: given a quantum system in a known ensemble of quantum states, can the quantum state of the system be determined? It turns out that the answer is not a simple yes or no and the problem is very intimately related with the theory of quantum measurements. The applications of quantum state discrimination are wide, during any process where the state of the system must be determined by an observer, a quantum state discrimination scheme must be implemented. These situations arise particularly in quantum cryptography where the reciever of the message or the key must distinguish the state of the quantum systems which in fact are the carriers of information themselves, and in quantum computation, where the observer might be in a situation in which in order to learn the result of the computation, she must determine the state of the quantum system on which the result of the computation is encoded.

In the following chapters, many aspects of quantum state discrimination will be explored in detail, different strategies will be reviewed and the connection and the usefulness of the theory of majorization in characterizing quantum state discrimination problems will be presented. The possibility of discrimination of entangled quantum states while preserving their entanglement will also be discussed and the processes will be characterized using majorization and some partial results about the subject will be given.

In the opening chapter, some preliminary information about quantum mechanics, quantum measurements and entanglement will be presented. The review will be short and dense and its only purpose is to help the already familiar reader remember some key concepts.

In chapter 3, the quantum state discrimination problem will be presented and various aspects of it will be worked out. Several different cases of the problem such as monopartite and multipartite state discrimination will be investigated and different cases of the problem will be reviewed. Also, the theory of majoriza-

tion and its connections with quantum information theory, more specifically its connections with quantum state discrimination will be explored.

In chapter 4, the problem of discrimination of entangled states with remaining entanglement will be presented and some special cases of the problem will be characterized using majorization and some partial results about the problem will be presented. Also the validity of the results will be discussed.

Lastly, in chapter 5, a short and concise review of the subjects covered in this work will be given and the results found in chapter 4 will be discussed and compared with the existing work in literature if applicable and the study will be concluded with some final remarks. Some fundamental results of probability theory relevant to the work are collected as an appendix.

CHAPTER 2

PRELIMINARIES

2.1 Density Operators

Central to the discussion of quantum mechanics and state discrimination problems is the mathematical tool of density matrices. The need for density matrices is straightforward, on many occasions the system in question is not in a definite quantum system but rather it is a statistical ensemble of different quantum states. An electron, for example might have its spin along the $+z$ direction with probability p_1 and along the $-z$ direction with probability p_2. The state of the electron cannot be represented as

$$|\psi\rangle = \sqrt{p_1}\,|0\rangle + \sqrt{p_2}\,|1\rangle\,, \tag{2.1}$$

where $|0\rangle$ is identified with the spin state along the $+z$ direction and $|1\rangle$ with the spin state along the $-z$ direction. The quantum state $|\psi\rangle$ in eq. (1.1) is in a coherent superposition of $|0\rangle$ and $|1\rangle$. The electron's spin is neither in the $+z$ direction nor in the $-z$ direction but, when one measures the spin along the z direction, the electron will be in the state $|0\rangle$ with probability p_0 and it will be in the state $|1\rangle$ with probability p_1. But, the electron is not in a statistical mixture of states, the electron is in the state $|\psi\rangle$ with probability 1. In other words, the electron is in a "pure" state. Suppose now the spin along the z direction is measured. The outcomes are $+1$ and -1 with probabilities p_1 and p_2 respectively. If an observer performs the measurement but does not record the outcome, the quantum state of the electron must be represented by

an ensemble

$$\mathcal{E} = \{(p_1, |0\rangle); (p_2, |1\rangle)\}. \tag{2.2}$$

More generally, an ensemble of pure states is a set of pairs

$$\mathcal{E} = \{(p_i, |\phi_i\rangle)\}_{i=1}^{n} \text{ and } \sum p_i = 1. \tag{2.3}$$

with the meaning that the system is in the state $|\phi_i\rangle$ with probability p_i. A convenient way to express ensembles is to use the density operator defined as

$$\rho = \sum_{i=1}^{n} p_i \, |\phi_i\rangle\langle\phi_i| \, , \, \langle\phi_i|\phi_i\rangle = 1. \tag{2.4}$$

If the states $|\phi_i\rangle$ are re-expressed as a superposition of some orthogonal basis kets,

$$\rho = \sum_{i,n,m} p_i c_{ni} c^*_{mi} \, |n\rangle\langle m| \, , \, |\phi_i\rangle = \sum_{n} c_{ni} \, |n\rangle \, , \, \langle n|m\rangle = \delta_{nm}. \tag{2.5}$$

Since p_i are real numbers, it is trivial to see that density operators are hermitian.

The expectation value of observables are also easy to calculate

$$\begin{aligned} \langle A\rangle &= \sum_i p_i \langle A\rangle_i, \\ &= \sum_i p_i \, \langle\phi_i|A|\phi_i\rangle \, , \\ &= \mathrm{Tr}\left(\sum_i A p_i \, |\phi_i\rangle\langle\phi_i|\right), \\ &= \mathrm{Tr}(\rho A). \end{aligned} \tag{2.6}$$

where the identity

$$\langle\psi|\phi\rangle = \mathrm{Tr}(|\phi\rangle\langle\psi|) \tag{2.7}$$

is used. The trace of the density operator gives the normalization condition

$$\begin{aligned} \mathrm{Tr}(\rho) &= \mathrm{Tr}\left(\sum_i p_i \, |\phi_i\rangle\langle\phi_i|\right), \\ &= \sum_i p_i \, \mathrm{Tr}(|\phi_i\rangle\langle\phi_i|), \\ &= \sum_i p_i \, \langle\phi_i|\phi_i\rangle \, , \\ &= \sum_i p_i, \\ &= 1 \end{aligned} \tag{2.8}$$

since $\langle\phi_i|\phi_i\rangle = 1$. The density operator is also a positive semidefinite operator, $\rho \geq 0$. This is quite easy to prove, for any arbitrary state ket $|\psi\rangle$

$$\begin{aligned}\langle\psi|\rho|\psi\rangle &= \sum_i p_i \langle\psi|\phi_i\rangle \langle\phi_i|\psi\rangle\,, \\ &= \sum_i p_i |\langle\psi|\phi_i\rangle|^2, \\ &\geq 0.\end{aligned} \tag{2.9}$$

Thus, any positive semidefinite operator with trace equal to one represents an ensemble of pure quantum states. The correspondence between density operators and ensembles is not one-to-one, it is one-to-many. The same density operator might represent different ensembles with different pure quantum states. To see this, looking at the spectral decomposition of the density operator is enough;

$$\begin{aligned}\rho &= \sum_i p_i \,|\phi_i\rangle\langle\phi_i|\,, \\ &= \sum_i \omega_i \,|i\rangle\langle i| \;\text{ where }\; \langle i|j\rangle = \delta_{ij} \text{ and } \rho\,|i\rangle = \omega_i\,|i\rangle\,.\end{aligned} \tag{2.10}$$

Owing to the freedom of choosing the eigenvectors, different ensembles can be represented by the same density operator. The evolution of density matrices under unitary transformations is also easy to construct. Let $|\phi_i'\rangle = U\,|\phi_i\rangle\,,$

$$\begin{aligned}\rho' &= \sum_i p_i \,|\phi_i'\rangle\langle\phi_i'|\,, \\ &= \sum_i p_i U\,|\phi_i\rangle\langle\phi_i|\,U^\dagger, \\ &= U\rho U^\dagger.\end{aligned} \tag{2.11}$$

Density operators are also a convenient way to describe composite systems; systems whose quantum states live in a Hilbert space which is a direct product of two or more Hilbert spaces. The use of density matrices to describe composite systems and subsystems is through the reduced density matrix formalism. Suppose the system to be described lives in the Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. The density operator ρ_{AB} is a linear operator on $\mathcal{H}_A \otimes \mathcal{H}_B$. The operator ρ_{AB} describes the ensemble of pure quantum states that are elements of the composite Hilbert space. To reach the description of a subsystem of the composite system, the reduced density matrix is used and it is defined through the partial trace operation

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}), \tag{2.12}$$

and the map of operators Tr_B is defined as

$$\begin{aligned}\mathrm{Tr}_B(|\alpha_1\rangle_A\langle\alpha_2| \otimes |\beta_1\rangle_B\langle\beta_2|) &= |\alpha_1\rangle_A\langle\alpha_2| \,\mathrm{Tr}(|\beta_1\rangle_B\langle\beta_2|), \\ &= |\alpha_1\rangle_A\langle\alpha_2|({}_B\langle\beta_2|\beta_1\rangle_B).\end{aligned} \tag{2.13}$$

For quantum states which can be expressed as $\rho_{AB} = \rho_A \otimes \rho_B$, the reduced density matrices are simply ρ_A and ρ_B due to the trace condition.

All mixed states represented by a density operator can be "purified" with the help of an ancilla system. The system is imagined to be entangled with an ancilla system, the ancilla might be the environment that the system is interacting with. An ancilla in the context of quantum information science is a system which is discarded at the end of the computation, it is merely a mathematical tool of no physical significance. Purification of a density operator is very straightforward, if $\rho = \sum_i p_i \left|\phi_i\right\rangle \left\langle\phi_i\right|$, then $\left|\psi\right\rangle_{AB} = \sum_i \sqrt{p_i} \left|\phi_i\right\rangle_A \otimes \left|i\right\rangle_B$ is a purification of ρ meaning that the state of the quantum system in question can be expressed as a pure state of the system and the ancilla.

The density operator ρ can be obtained by taking the partial trace over B

$$\begin{aligned}\mathrm{Tr}_B(|\psi\rangle\langle\psi|) &= \sum_{i,j} \sqrt{p_i p_j} \left|\phi_i\right\rangle\!\left\langle\phi_j\right| (\langle i|j\rangle), \\ &= \sum_{i,j} \sqrt{p_i p_j} \left|\phi_i\right\rangle\!\left\langle\phi_j\right| \delta_{ij}. \\ &= \sum_i p_i \left|\phi_i\right\rangle\!\left\langle\phi_i\right| = \rho.\end{aligned} \tag{2.14}$$

Note that, due to the freedom of choosing the ancilla, purifications are not unique, but they are related by a unitary transformation on the ancilla.

2.2 Quantum Measurements

One of the main ways that quantum mechanics differ from its classical counterpart is the effect of measurements performed on quantum systems. Quantum mechanics is a perfectly deterministic theory unless measurements are included, states evolve unitarily and knowing the state of the system at time t_1 and the Hamiltonian H of the system gives the description of the state of the system at a

later time t_2 through the use of the unitary time evolution operator. But, measurement breaks the determinism, measurement outcomes in quantum mechanics is indeterministic, they give rise to a probability distribution of outcomes. To mathematically describe the process of measurement, the measurement formalism is introduced.

Quantum measurements are described by a set of measurement operators $\mathcal{M} = \{M_m\}$ which are linear operators defined on the Hilbert space of the system to be measured. The index m is a label for possible outcomes.

Suppose that the quantum state of the system immediately before measurement is represented by the ket $|\psi\rangle$. The probability to obtain the outcome m is given by

$$p_m = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{2.15}$$

and the quantum state of the system after measurement, corresponding to the m^{th} outcome becomes

$$|\phi_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{2.16}$$

There is one equality that the measurement operators must satisfy which arises from the fact that probabilities must sum up to one;

$$1 = \sum_m p_m = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle\,. \tag{2.17}$$

Since the above condition must be satisfied for all $|\psi\rangle$, it is equivalent to

$$\sum_m M_m^\dagger M_m = \mathbb{1} \tag{2.18}$$

The completeness relation can be satisfied in many ways, the simplest one is to use a complete set of orthogonal projectors P_m which satisfy

$$\sum_m P_m = \mathbb{1} \text{ and } P_m P_n = \delta_{mn} P_n. \tag{2.19}$$

The second condition is simply the idempotence and orthogonality relations combined. Any hermitian operator, in other words an observable can be decomposed into its eigenvalues and projectors $M = \sum_m mP_m$ and the probability that the outcome m is obtained in a measurement is simply

$$p_m = \langle\psi|P_m|\psi\rangle \tag{2.20}$$

and the resultant state corresponding to the m^{th} outcome is

$$|\phi_m\rangle = \frac{P_m |\psi\rangle}{\sqrt{\langle\psi|P_m|\psi\rangle}}. \tag{2.21}$$

These type of measurements are called von Neumann or projective measurements and they are a special case of a broader class of measurements. The effect of measurements on density matrices is also important and easy to formulate. Measurements map density operators to density operators.

Consider an ensemble $\mathcal{E} = \{(p_i, |\phi_i\rangle)\}_{i=1}^n$. Defining the conditional probability $p(m|i)$ as the probability that outcome m is obtained given that the state is $|\phi_i\rangle$

$$\begin{aligned} p(m|i) &= \langle\phi_i|P_m|\phi_i\rangle\,, \\ &= \mathrm{Tr}(P_m\,|\phi_i\rangle\langle\phi_i|). \end{aligned} \tag{2.22}$$

Using the law of total probability (see Appendix),

$$\begin{aligned} p_m &= \sum_i p(m|i)p_i, \\ &= \sum_i p_i\,\mathrm{Tr}(P_m\,|\phi_i\rangle\langle\phi_i|), \\ &= \mathrm{Tr}(P_m\rho) \end{aligned} \tag{2.23}$$

is obtained, which is the probability of obtaining the outcome m after measurement. Noting that the post measurement states are given as

$$|\phi_i^m\rangle = \frac{P_m\,|\phi_i\rangle}{\sqrt{expval P_m \phi_i}}. \tag{2.24}$$

The posterior density operator corresponding to the outcome m is found to be;

$$\begin{aligned} \rho_m &= \sum_i p(i|m)\,|\phi_i^m\rangle\langle\phi_i^m|\,, \\ &= \sum_i p(i|m)\frac{P_m\,|\phi_i\rangle\langle\phi_i|\,P_m}{\langle\phi_i|P_m|\phi_i\rangle}, \\ &= \sum_i \frac{p(m|i)p_i}{p_m}\frac{P_m\,|\phi_i\rangle\langle\phi_i|\,P_m}{p(m|i)}, \\ &= \frac{1}{p_m}\sum_i p_i P_m\,|\phi_i\rangle\langle\phi_i|\,P_m, \\ \rho_m &= \frac{P_m\rho P_m}{\mathrm{Tr}(P_m\rho)} \end{aligned} \tag{2.25}$$

where the Bayes rule, expressed as

$$p(i|m) = \frac{p(m|i)p_i}{p_m} \tag{2.26}$$

is used, giving the probability that the state is $|\phi_i\rangle$ given that the outcome is m. (Refer to the Appendix for a brief review of probability theory.)

Sometimes, in the discussion of quantum information theory, the concept of forgetful measurements gain importance. The idea is that, after performing the measurement, the observer does not record the outcome. The resultant quantum state is then a density operator formed by the corresponding outcomes and the associated probabilities, Suppose the posterior state corresponding to outcome m are called as ρ_m. The outcome m has a probability of p_m. The density operator after a forgetful measurement can be expressed as;

$$\begin{aligned} \rho' &= \sum_m p_m \rho_m, \\ &= \sum_m \mathrm{Tr}(P_m \rho) \frac{P_m \rho P_m}{Tr(P_m \rho)}, \\ \rho' &= \sum_m P_m \rho P_m. \end{aligned} \tag{2.27}$$

The discussion above covers all aspects of the measurement formalism known as projective measurements or von Neumann measurements. However, more general measurement formalism can be constructed which is much more powerful than its projective counterpart. This more general is called the generalized measurement formalism, or when only the probabilities of obtaining the outcomes are concerned, it is sometimes called the POVM formalism where POVM stands for Positive Operator-Valued Measure [5].

A measurement described by the operators $\mathcal{M} = \{M_m\}$ must always satisfy the rule that probabilities p_m corresponding to the outcomes m must satisfy $\sum_m p_m = 1$. In terms of the operators themselves, this can be expressed as,

$$E_m \equiv M_m^\dagger M_m \ , \ \sum_m E_m = \mathbb{1} \tag{2.28}$$

where the probability of obtaining m is given by $p_m = \langle\psi|E_m|\psi\rangle$. It is easy to see that the operators E_m are positive operators since $p_m \geq 0$. Since any

positive operator can be decomposed as $A = B^\dagger B$, the set of operators E_m are sufficient to describe a measurement $\mathcal{M}$. The operators E_m are known as the POVM elements associated with the outcome m for a measurement $\mathcal{M} = \{M_m\}$. Choosing E_m to be projectors $P_m = |\phi_m\rangle\langle\phi_m|$ is a special case where the number of different outcomes must be equal to or smaller than the dimension of the Hilbert space $\mathcal{H}$. For a POVM however, the number of outcomes m can be bigger than $\dim \mathcal{H}$ since the general measurement elements $E_m = M_m^\dagger M_m$ do not obey any orthogonality relation. This fact will be quite important when quantum state discrimination is discussed.

The effect of measurement on quantum states and density operators should also be stated. The results will be generalized from the projective case.

The posterior state after the measurement and the probability corresponding to outcome m is simply

$$|\phi_m\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \ , \ p_m = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{2.29}$$

For density operators, the expressions can be obtained by generalizing the results for projective measurements. The probability of obtaining outcome m is given by

$$p_m = \mathrm{Tr}\big(M_m^\dagger M_m \rho\big) \tag{2.30}$$

and the density operator corresponding to outcome m is given by

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}\Big(M_m^\dagger M_m \rho\Big)} \tag{2.31}$$

and, for a forgetful measurement in which the outcome is not recorded by the observer,

$$\rho' = \sum_m M_m \rho M_m^\dagger. \tag{2.32}$$

The measurement formalism in quantum mechanics can be extended to measurements done on composite systems. In that case, the measurement operators act only on the designated subspace of the total Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. A measurement $\mathcal{M} = M_m$ is separable if all the operators M_m are of the form

$$M_m = F_m^A \otimes F_m^B \tag{2.33}$$

where the superscripts A and B denote the subspaces that the operators F_m act on. When dealing with composite systems, an operator M_m^A is a shorthand for $M_m^A \otimes \mathbb{1}^B$. Certain types of measurements in which the result that one party obtains after measuring her subsystem is conditional on the result of the other party are called LOCC protocols where LOCC stands for Local Operations and Classical Communication which are a subset of separable measurements but mathematically cannot in general be expressed as easily and cleanly as separable measurements. LOCC protocols will be explained in detail in chapter 3.

2.3 Entanglement

Quantum entanglement is the most interesting and baffling aspect of quantum mechanics. Since the foundation of quantum mechanics in its modern form, much debate has been centered on the subject of entanglement and there is an impressive amount of literature devoted to the subject. Stated in words, quantum entanglement is the phenomena in which the measurement results obtained from the different subsystems are correlated in a way that is much stronger than classical correlations. Although the statement above might seem imprecise and confusing, the mathematical framework of quantum entanglement is well founded and rigorous. The framework will be explored in detail below.

Composite quantum states might come in various forms, the simplest form is what is called as the "product" form, meaning that if a state $|\psi\rangle_{AB}$ can be expressed as

$$|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\varphi\rangle_B \tag{2.34}$$

then, $|\psi\rangle_{AB}$ is a product state. A general definition can be made, any pure quantum state that cannot be expressed in product form is an entangled state.

An entangled state lives in the direct product space of the respective Hilbert spaces of the subsystems. For a bipartite (two subsystems) state, the most general expression for the state can be written as

$$|\psi\rangle = \sum_{i,j} c_{ij} |i\rangle_A |j\rangle_B \tag{2.35}$$

where the $\otimes$ symbol has been omitted as the meaning is clear. The set of vectors $\{|i\rangle_A |j\rangle_B\}_{i=1,j=1}^{n,m}$ is an orthonormal basis for the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

The concept of reduced density matrices is widely used when dealing with entangled states and the rank of the reduced density operators is directly related with the entanglement in the following way: a quantum state for which the reduced density operators rank is greater than 1 is an entangled state.

To better understand the statement, the Schmidt decomposition of entangled states must be understood. The Schmidt decomposition is a procedure after which the state is expressed as a superposition of pairwise matched vectors of two orthonormal bases of the Hilbert spaces of the subsystems. Any bipartite quantum state can be expressed in Schmidt form;

$$|\psi\rangle = \sum_i \lambda_i |i\rangle_A |i\rangle_B \tag{2.36}$$

where $|i\rangle_A$ and $|i\rangle_B$ are complete orthonormal bases for their respective Hilbert spaces and λ_i are known as the Schmidt coefficients and they are also the square roots of the eigenvalues of the reduced density matrices. A quick note is in order here, $|i\rangle_A$ and $|i\rangle_B$ might represent states of different physical nature; and i here is just a label. If a quantum state has only one Schmidt coefficient in its Schmidt decomposition, than it is a product state and since the Schmidt coefficients are square roots of the eigenvalues of the reduced density matrices, a state having a rank 1 reduced density matrix is a product state.

The Schmidt decomposition is formally achieved through the singular value decomposition procedure: if c is an arbitrary (possibly rectangular) matrix, than there are unitary matrices u and v and the possibly rectangular, diagonal matrix d with diagonal elements being the singular values, the singular value decomposition is

$$c = udv \text{ or } c_{ij} = \sum_k u_{ik} d_{kk} v_{kj}. \tag{2.37}$$

The proof of the Schmidt decomposition is as follows;

$$\begin{aligned} |\psi\rangle &= \sum_{i,j} c_{ij} |a_i\rangle |b_j\rangle , \\ &= \sum_{i,j,k} u_{ik} d_{kk} v_{kj} |a_i\rangle |b_j\rangle \text{ after singular value decomposition} \\ &= \sum_{k} \lambda_k |k\rangle_A |k\rangle_B \end{aligned} \tag{2.38}$$

after defining $\sum_k u_{ik} |a_i\rangle = |k\rangle_A$, $\sum_j v_{kj} |b_j\rangle = |k\rangle_B$ and $d_{kk} = \lambda_k$.

The density operator associated with $|\psi\rangle$ is $\rho_{AB} = |\psi\rangle \langle\psi|$. Partial tracing over B gives;

$$\begin{aligned} \mathrm{Tr}_B \, \rho_{AB} &= \sum_{i,j} \lambda_i \lambda_j |i\rangle_A \langle j| (\langle i|j\rangle), \\ &= \sum_i \lambda_i^2 |i\rangle\langle i| . \end{aligned} \tag{2.39}$$

Note that the expression on the last line of eq. (2.39) is the spectral decomposition for ρ_A with λ_i^2 as the eigenvalues and the rank of the reduced density operator is the number of Schmidt coefficients. A rank 1 reduced density operator will correspond to a product state since the state will be of the form $|\psi\rangle = |k\rangle_A \otimes |k\rangle_B$. It is clear from here that the Schmidt coefficients for a bipartite state is the square roots of the eigenvalues of the reduced density matrices. Note that the above result doesn't change when the trace is taken over A, the eigenvalues of both reduced density operators are the same. In general the Schmidt decomposition can only be applied to bipartite states, it fails for states with more than two subsystems bar a few special cases like the GHZ state [6].

The amount of entanglement that a state possesses can be quantified by a few methods. These quantifiers are called entanglement monotones and they are required not to increase in any way during LOCC protocols. The study of entanglement monotones is a rich and broad subject in itself so not much detail is going to be given here but two of those monotones; entanglement entropy and concurrence are going to be explained in a quick fashion.

Entanglement entropy is defined as

$$\begin{aligned}\mathcal{E}(\rho_{AB}) &= -\operatorname{Tr}(\rho_A \log_2 \rho_A), \\ &= -\sum_i p_i \log_2 p_i\end{aligned} \tag{2.40}$$

where ρ_A, ρ_B are the reduced density matrices of the quantum state and p_i are the eigenvalues of the reduced density matrix. The unit of entanglement is usually called ebit and a bipartite state can have at most 1 ebit of entanglement. For two level systems, or qubits, the maximally entangled states are also called as the Bell states and in the computational basis $\{|0\rangle, |1\rangle\}$, they can be expressed as follows,

$$\begin{aligned}\left|\psi^+\right\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle, \\ \left|\psi^-\right\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle, \\ \left|\phi^+\right\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle, \\ \left|\phi^-\right\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle.\end{aligned} \tag{2.41}$$

Note that the reduced density matrix for each of these states is $\rho_A = \frac{1}{2}\mathbb{1}$, the maximally mixed ensemble. Hence the following statement can be made, a state is maximally entangled if its reduced density matrix corresponding to one of the systems is $\frac{1}{N}\mathbb{1}$ where N is the dimension of the corresponding Hilbert space.

Another easy to calculate entanglement monotone is the concurrence defined for a mixed state of two qubits (2 level systems) as;

$$\mathcal{C}(\rho) = \max(0, \lambda_1, \lambda_2, \lambda_3, \lambda_4) \tag{2.42}$$

where λ_i are the eigenvalues of the hermitian matrix $\sigma = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$ and $\tilde{\rho}$ is defined as $\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^\star(\sigma_y \otimes \sigma_y)$. For pure states which can be written in the Bell form $|\psi\rangle = a|00\rangle + b|11\rangle$, the concurrence reduces to;

$$\mathcal{C}(\psi) = 2|a||b|. \tag{2.43}$$

There are various other quantifiers of the amount of entanglement in a quantum state, in fact, any concave function of the squares of the Schmidt coefficients of

a state is an entanglement monotone, but they are not useful for the purposes of this work. For the discussion here, concurrence and entanglement entropy will be sufficient.

CHAPTER 3

QUANTUM STATE DISCRIMINATION

Quantum state discrimination is a fundamental problem in the theory of quantum information and much research has been devoted to this subject over the years. The problem was first noticed by Helstrom [7] in 1976 and Holevo [8] in 1979. Later in 1987-1988, Ivanovic [9], Peres [10] and Dieks [11] showed that unambiguous discrimination of linearly independent states is possible and Chefles [12] in 1998 generalized the problem to quantum state separation. Nowadays, the research is more focused on LOCC discrimination of multipartite states, started by Walgate [13] and his colleagues. In itself, quantum state discrimination is a simple, easy to state problem; given an ensemble of quantum states, can the observer determine the state of the system? It turns out that the solution is trivial if the states to be discriminated are orthogonal to each other but if they are linearly independent but not orthogonal, the solution is not that easy and in most cases, due to the very nature of quantum mechanics, the only possibility is to discriminate with some error. It also turns out that for general cases the problem cannot be analytically solved, the analytical solutions only exist for a few special cases.

There are many approaches developed to solve the problem of state discrimination such as minimum error discrimination, unambiguous discrimination and others but all the methods carry an inherent probability of failure in different aspects. It turns out that the problem is actually a linear optimization problem, the task is to minimize the probability of error for a given ensemble.

In this chapter, the problem of state discrimination will be formally defined and

it will be shown that why perfect (error less) discrimination is not possible for non-orthogonal states and then review the minimum error discrimination and unambiguous discrimination strategies for monopartite states. The discussion will than move on to the discrimination of bipartite, possibly entangled, orthogonal states under LOCC. There are many more approaches for solving the stated problem but they are not relevant for the purposes of this study. The body of the chapter will be based on a tutorial review by J. A. Bergou[14].

3.1 Statement of the Problem

In a formal mathematical setting, the quantum state discrimination problem is easy to describe: given an ensemble $\mathcal{E} = \{(p_i, |\psi_i\rangle)\}_{i=1}^{n}$, can the state of the system be determined? The answer is easy if $|\psi_i\rangle$ are mutually orthogonal, it is possible to perfectly discriminate between the states without any error. But, if they are not mutually orthogonal but linearly independent, than it is still possible to determine the state of the system with some probability of error. In the most general setting, the states $|\psi_i\rangle$ are upgraded to density operators ρ_i.

First, the notion of perfect discrimination will be defined and the cases when it is possible will be explained. For an ensemble $\mathcal{E} = \{(p_i, |\psi_i\rangle)\}$ and the measurement $M = \{M_j\}$ with POVM elements $E_i = M_i^\dagger M_i$, perfect discrimination is possible if

$$M_j |\psi_i\rangle = 0 \text{ when } i \neq j. \tag{3.1}$$

In other words, when the measurement is performed, for the state $|\psi_i\rangle$ if all the measurement outcomes other than the i^{th} one occur with 0 probability, then it is concluded that the state was originally $|\psi_i\rangle$. If $|\psi_i\rangle$ are mutually orthogonal, a complete projective measurement with elements P_j can be constructed such that $P_j |\psi_i\rangle = 0$ when $i \neq j$. A quick note, if the given states $|\psi_i\rangle$ do not form a complete orthogonal set, the missing kets can be added to the ensemble with 0 probability and add the projector $P_0 = \mathbb{1} - \sum_i P_i$ to the list of projectors and construct a complete projective measurement. Since the added states occur with zero probability, the conditional probabilities of the corresponding outcomes are 0 enabling us to express that outcome with a single POVM element. Thus, if

the given states are orthogonal, perfect discrimination using projectors is always possible. Showing that perfect discrimination is not possible if the states are not orthogonal is also easy. Suppose that the ensemble in question consists of two states $|\psi_1\rangle$ and $|\psi_2\rangle$, not necessarily orthogonal and two operators, M_1 and M_2 are constructed to discriminate these states obeying $M_1 + M_2 = \mathbb{1}$. For perfect discrimination, the following must hold

$$\begin{aligned} M_1 |\psi_2\rangle &= 0, \\ M_2 |\psi_1\rangle &= 0. \end{aligned} \tag{3.2}$$

The conditional probabilities are defined as

$$\begin{aligned} p(1|1) &= \langle\psi_1|E_1|\psi_1\rangle\,, \\ p(2|2) &= \langle\psi_2|E_2|\psi_2\rangle\,, \end{aligned} \tag{3.3}$$

and the others are 0 due to orthogonality. If the relation $M_1 + M_2 = \mathbb{1}$is multiplied with $\langle\psi_1|$ from the left and with $|\psi_2\rangle$ from the right,

$$\langle\psi_1| E_1 |\psi_2\rangle + \langle\psi_1| E_2 |\psi_2\rangle = \langle\psi_1|\psi_2\rangle\,. \tag{3.4}$$

Taking into account eq.(3.2), it is seen that the above expression must be zero, which is only possible for orthogonal states. Thus, for perfect discrimination to be possible, the states to be discriminated should be orthogonal to each other. Below, the two main strategies to follow when the states are not orthogonal are going to be explained.

3.2 Minimum Error Discrimination

The minimum error strategy was first coined by Helstrom [7] in 1976. The minimum error strategy aims to eliminate inconclusive results but permits errors in the measurement scheme. The problem than transforms into a linear optimization problem, finding the measurement operators that minimize the probability of error. As in all state discrimination problems, an ensemble of states $\mathcal{E} = \{(p_i, \rho_i)\}_{i=1}^n$ is given where each state ρ_i occurs with prior probability p_i. A suitable measurement $\mathcal{M} = \{M_j\}$ where $\sum_j M_j^\dagger M_j = \mathbb{1}$ with $E_i = M_i^\dagger M_i$ being the POVM elements, is used to discriminate between the states. The measurement operators are defined such that if it has been prepared in the state ρ

where $\rho = \sum_i p_i \rho_i$, the probability to conclude that the system is in the state ρ_i is $\mathrm{Tr}(E_i \rho)$. The number of the measurement operators is also equal to the number of states to be discriminated since the measurement needs to be exhaustive, meaning that the measurement should cover all the outcomes and should not give inconclusive results.

The overall probability of error, where the error is the probability that the state is concluded to be ρ_j but it was in fact ρ_i where $i \neq j$ can be simply defined using the fact that probabilities add up to one.

$$p_{er} = 1 - \sum_i p_i \,\mathrm{Tr}(E_i \rho_i). \tag{3.5}$$

The trace term $\mathrm{Tr}(E_i \rho_i)$ is the probability of correctly identifying the state ρ_i and the p_i are the prior probabilities of the states, hence the second term in the right hand side of eq.(3.5) is the probability that the result is correct. The best protocol is achieved when the probability of error is minimized by finding the optimal set of operators M_m. This, however, is no easy task and there is not any general solution for an arbitrary number of states. But, an analytical solution for 2 states can be found.

Consider an ensemble $\mathcal{E} = \{(p_i, \rho_i)\}_{i=1}^2$ and the POVM elements E_1 and E_2 which satisfy $E_1 + E_2 = \mathbb{1}$. Using eq. (3.5), the error probability can be found as

$$\begin{aligned} p_{er} &= 1 - p_1 \,\mathrm{Tr}(E_1 \rho_1) - p_2 \,\mathrm{Tr}(E_2 \rho_2), \\ &= p_1 \,\mathrm{Tr}(E_2 \rho_1) + p_2 \,\mathrm{Tr}(E_1 \rho_2). \end{aligned} \tag{3.6}$$

The second line is also equal to the total probability of an erroneous detection since the trace terms are the probability of false detection events. The error probability can be cast in another form with the help of a new hermitian operator defined as

$$\begin{aligned} \Lambda &= p_2 \rho_2 - p_1 \rho_1, \\ &= \sum_j^D \lambda_k \left|k\right\rangle\!\left\langle k\right|, \end{aligned} \tag{3.7}$$

where the second line in eq. (3.7) is the spectral decomposition of Λ. Inserting

$p_1\rho_1 = \Lambda - p_2\rho_2$ into the second line of eq. (2.6),

$$\begin{aligned} p_{er} &= \mathrm{Tr}[(p_2\rho_2 - \Lambda)E_2] + p_2\,\mathrm{Tr}(\rho_2 E_1), \\ &= p_2 - \mathrm{Tr}[\rho_2(E_1 + E_2)] - \mathrm{Tr}(\Lambda E_2), \\ p_{er} &= p_2 - \mathrm{Tr}(\Lambda E_2) \end{aligned} \tag{3.8}$$

where the facts that $E_1 + E_2 = \mathbb{1}$ and $\mathrm{Tr}\,\rho = 1$ were used. Note that $p_{er} = p_1 + \mathrm{Tr}(\Lambda E_1)$ if $p_2\rho_2 = \Lambda + p_1\rho_1$ is inserted into eq. (3.6).

Since Λ is hermitian, its eigenvalues are all real, hence its eigenvalues can be classified into 3 subgroups without loss of any generality

$$\begin{aligned} &\lambda_k < 0 \text{ for } 1 \leq k < k_-, \\ &\lambda_k = 0 \text{ for } k_- \leq k \leq k_0. \\ &\lambda_k > 0 \text{ for } k_0 < k \leq D. \end{aligned} \tag{3.9}$$

where D is the dimension of the Hilbert space. Inserting the spectral decomposition of Λ into the expression for the probability of error in eq. (3.8), the following expression is obtained after using $\langle\alpha|\beta\rangle = \mathrm{Tr}(|\beta\rangle\langle\alpha|)$

$$\begin{aligned} p_{er} &= p_2 - \sum_{k=1}^{D} \mathrm{Tr}(\lambda_k\,|k\rangle\langle k|\,E_2), \\ p_{er} &= p_2 - \sum_{k=1}^{D} \lambda_k\,\langle k|\,M_2\,|k\rangle = p_1 + \sum_{k=1}^{D} \lambda_k\,\langle k|\,E_1\,|k\rangle\,. \end{aligned} \tag{3.10}$$

Since the expectation values involving the operators E_1 and E_2 are probabilities, the measurement operators hence the expectation value terms in eq. (3.10) are positive semi-definite by construction. To minimize the error expression in eq. (3.10), the following equalities must hold.

$$\begin{aligned} &\langle k|E_2|k\rangle = 0 \text{ and } \langle k|E_1|k\rangle = 1 \text{ for } \lambda_k < 0, \\ &\langle k|E_2|k\rangle = 1 \text{ and } \langle k|E_1|k\rangle = 0 \text{ for } \lambda_k > 0. \end{aligned} \tag{3.11}$$

The minimizing conditions can also be understood in the following way, since the error probability is a linear function of the expectation values $\langle k|E_1|k\rangle$ and $\langle k|E_2|k\rangle$, the extrema happen at the end points of these functions. The true minima happen to be the case described above. These conditions allow the operators E_i constructed as

$$E_1 = \sum_{k=1}^{k_- - 1} |k\rangle\langle k| \text{ and } E_2 = \sum_{k=k_-}^{D} |k\rangle\langle k| \tag{3.12}$$

Note that the operator E_2 also includes the eigenkets corresponding to 0 eigenvalues but the 0 eigenvalues have no effect on the error probability whatsoever. The eigenkets corresponding to the eigenvalues 0 can also be included into E_1, meaning that the solution is not unique. To find the minimum error probability, the expressions for the operators E_1 and E_2 are inserted into the last line of eq. (3.8)

$$\begin{aligned} p_{er} &= p_2 - \mathrm{Tr}\left(\sum_{k=1}^{D} \lambda_k \left|k\right\rangle\!\left\langle k\right| \sum_{k=k_-}^{D} \left|k\right\rangle\!\left\langle k\right|\right),\ \lambda_k \geq 0 \text{ for } k_- \leq k \leq D, \\ &= p_2 - \sum_{k=k_-}^{D} |\lambda_k|, \\ p_{er} &= p_1 + \mathrm{Tr}\left(\sum_{k=1}^{D} \lambda_k \left|k\right\rangle\!\left\langle k\right| \sum_{k=1}^{k_-} \left|k\right\rangle\!\left\langle k\right|\right),\ \lambda_k < 0 \text{ for } 1 \leq k < k_-, \\ p_{er} &= p_1 - \sum_{k=1}^{k_-} |\lambda_k|. \end{aligned} \tag{3.13}$$

Adding up the two alternative expressions found in eq. (3.13) and dividing by two, the final expression can be reached

$$\begin{aligned} p_{er} &= \frac{1}{2}(1 - \sum_{k} |\lambda_k|), \\ &= \frac{1}{2}(1 - \mathrm{Tr}\,|\Lambda|), \end{aligned} \tag{3.14}$$

where $|A|$ is defined as $\sqrt{A^\dagger A}$ and it is trivial to see that all its eigenvalues are the norms of the original eigenvalues. Inserting the expression for Λ from eq. (3.7), the lower bound for the error probability is found, also known as the Helstrom bound

$$p_{er} = \frac{1}{2}(1 - \mathrm{Tr}\,|p_2\rho_2 - p_1\rho_1|). \tag{3.15}$$

This equation can be cast in another form if the states to be discriminated are pure states $|\psi_1\rangle$, $|\psi_2\rangle$ and thus $\rho_1 = |\psi_1\rangle\langle\psi_1|$ and $\rho_2 = |\psi_2\rangle\langle\psi_2|$. In this case, the minimum attainable probability of error can be expressed as

$$p_{er} = \frac{1}{2}(1 - (1 - 4p_1p_2|\langle\psi_1|\psi_2\rangle|^2)^{1/2}). \tag{3.16}$$

To get this result, first note that when the states to be discriminated are pure, the hermitian operator Λ has the form

$$\Lambda = p_2 \left|\psi_2\right\rangle\!\left\langle\psi_2\right| - p_1 \left|\psi_1\right\rangle\!\left\langle\psi_1\right|. \tag{3.17}$$

Since any two state defines a 2 dimensional Hilbert space, without loss of any generality $|\psi_1\rangle$ and $|\psi_2\rangle$ can be expressed as superpositions of arbitrary basis kets $\{|0\rangle, |1\rangle\}$

$$\begin{aligned} |\psi_1\rangle &= \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\,, \\ |\psi_2\rangle &= \cos\theta\,|0\rangle - \sin\theta\,|1\rangle\,. \end{aligned} \tag{3.18}$$

Inserting the expressions for the states in eq. (3.18) into eq. (3.17)

$$\Lambda = \begin{pmatrix} (p_2 - p_1)\cos^2\theta & -(p_2 + p_1)\cos\theta\sin\theta \\ -(p_2 + p_1)\cos\theta\sin\theta & (p_2 - p_1)\sin^2\theta \end{pmatrix}. \tag{3.19}$$

is obtained. The eigenvalues of this matrix can be calculated easily and they are

$$\lambda_\pm = \frac{1}{2}(p_2 - p_1 \pm (1 - 4p_1p_2|\langle\psi_1|\psi_2\rangle|^2)^{1/2}) \tag{3.20}$$

where $|\langle\psi_1|\psi_2\rangle|^2 = \cos^2 2\theta$ Now, note that in the minimum error expression $p_{er} = p_2 - \mathrm{Tr}(\Lambda M_2)$, the operator M_2 projects onto the positive eigenvalue eigenstates of Λ by construction. Using the positive eigenvalue in eq. (3.20) and inserting it into the last line of eq. (3.8), the minimum error probability for 2 pure states is shown to be

$$p_{er} = \frac{1}{2}(1 - (1 - 4p_1p_2|\langle\psi_1|\psi_2\rangle|^2)^{1/2}) \tag{3.21}$$

which is the same as in eq. (3.16). There is an interesting result when $\Lambda \geq 0$, in that case $M_1 = 0$ and $M_2 = \mathbb{1}$, meaning that the minimum probability of error can always be attained by simply guessing that the state is ρ_2 or $|\psi_2\rangle$.

There are other select cases for which an analytical solution for a minimum error discrimination scheme is possible like symmetric states and mirror symmetric states but they will not be explored here. For general problems, the necessary and sufficient conditions for a POVM that realizes a minimum error discrimination to exist are known

$$\begin{aligned} \sum_i p_i\rho_i M_i - p_j\rho_j \leq 0,\ \forall j, \\ M_i(p_i\rho_i - p_j\rho_j)M_j = 0,\ \forall i, j, \end{aligned} \tag{3.22}$$

but these results are not going to be proven. A proof of these conditions can be found in [15]. The discussion above covers the general aspects and the idea of the minimum error discrimination strategy.

3.3 Unambiguous Discrimination

The main difference between the unambiguous discrimination and the minimum error strategies are straightforward, given an ensemble $\mathcal{E} = \{(p_i, |\psi_i\rangle\}$ in UQSD (Unambiguous Quantum State Discrimination) the observer is not allowed to make an erroneous decision, if she states that the state is $|\psi_1\rangle$, the state is $|\psi_1\rangle$ with probability 1, unlike the minimum error discrimination strategy. In mathematical terms, this idea can be expressed as

$$\langle\psi_i|E_j|\psi_i\rangle = 0 \ \forall j \neq i, \tag{3.23}$$

where E_j are the POVM elements. As it was shown at the beginning of this chapter in eq. (3.4), non-orthogonal states cannot be perfectly distinguished from each other. This means that the operators M_j cannot satisfy the completeness condition $\sum_j M_j^\dagger M_j = \mathbb{1}$. To satisfy the completeness requirement, other POVM elements $E_{F\lambda} = M_{F\lambda}^\dagger M_{F\lambda}$ are introduced, which are sometimes also known as the failure operator, and for the general case the number of failure operators can be more than 1. These operators correspond to the outcomes for which no conclusion can be drawn about the state of the system. The POVM elements E_j are the operators to identify the states $|\psi_j\rangle$, such that $\langle\psi_j|E_j|\psi_j\rangle = p(j|j)$ is the probability of successfully identifying the state $|\psi_j\rangle$ and $\sum_\lambda \langle\psi_i|E_{F\lambda}|\psi_i\rangle = p_i^F$ is the probability of failing to identify the state $|\psi_i\rangle$. As usual the POVM elements must satisfy the following conditions

$$\begin{aligned} \sum_j E_j + \sum_\lambda E_{F\lambda} &= \mathbb{1}, \\ E_j &\geq 0, \ \forall j, \\ E_{F\lambda} &\geq 0, \ \forall \lambda. \end{aligned} \tag{3.24}$$

Finding the optimal unambiguous discrimination scheme for a given ensemble is again a linear optimization problem over the POVM elements achieving the lowest probability of failure for a given ensemble. The general idea behind UQSD is pretty simple. For a given ensemble, with the state set $\{\psi_i\}_{i=1}^N$, a reciprocal set $\{\psi_i^\perp\}_{i=1}^N$ can be constructed where $\langle\psi_i^\perp|\psi_j\rangle = 0$, if $i \neq j$ by construction. The general idea is to project the states to be discriminated onto the reciprocal states, since the expectation value of a reciprocal projector in the non-conjugate

state is 0 for all the states other than the corresponding state in the original set, the detection is unambiguous but to satisfy the completeness condition of POVMs, operators corresponding to inconclusive results must be added to the measurement set. To understand the idea better, an analytical solution for two states will be presented.

Suppose the initial ensemble consists of two linearly independent but not necessarily orthogonal states $\mathcal{E} = \{(p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle\}$. The reciprocal set of states is defined as, $\{|\psi_1^\perp\rangle, |\psi_2^\perp\rangle\}$ where $\langle\psi_i^\perp|\psi_j\rangle = 0$, if $i \neq j$. The measurement operators corresponding to successful identification must satisfy

$$\langle\psi_j|E_i|\psi_j\rangle = 0, \ \forall i \neq j. \tag{3.25}$$

Using the idea to project onto the conjugate pair, the operators E_1 and E_2 can be written as

$$\begin{aligned} E_1 &= c_1 \left|\psi_1^\perp\right\rangle\!\left\langle\psi_1^\perp\right|, \\ E_2 &= c_2 \left|\psi_2^\perp\right\rangle\!\left\langle\psi_2^\perp\right|. \end{aligned} \tag{3.26}$$

It is easy to check that these operators satisfy the condition in eq. (3.25). That condition can also be used to solve for the coefficients c_1 and c_2 in eq. (3.26). It gives

$$\begin{aligned} E_1 &= \frac{\langle\psi_1|E_1|\psi_1\rangle}{\left|\langle\psi_1|\psi_1^\perp\rangle\right|^2} \left|\psi_1^\perp\right\rangle\!\left\langle\psi_1^\perp\right|, \\ E_2 &= \frac{\langle\psi_2|E_2|\psi_2\rangle}{\left|\langle\psi_2|\psi_2^\perp\rangle\right|^2} \left|\psi_2^\perp\right\rangle\!\left\langle\psi_2^\perp\right|. \end{aligned} \tag{3.27}$$

These operators are positive semi-definite by construction but for the existence of a POVM that can realize the discrimination scheme, the operator corresponding to the inconclusive outcome $E_F = \mathbb{1} - E_1 - E_2$ must also be positive semi-definite. The positive semi-definiteness of the failure operator can be thought as the following inequality

$$E_1 + E_2 \leq \mathbb{1} \tag{3.28}$$

Since the set $\{|\psi_1\rangle, |\psi_2\rangle\}$ defines a 2 dimensional Hilbert space, any arbitrary state $|\Psi\rangle$ can be expanded as a superposition of the states $|\psi_1\rangle, |\psi_2\rangle$ as

$$|\Psi\rangle = \frac{1}{(\sum_{j,k=1}^{2} c_j^\star c_k \langle\psi_j|\psi_k\rangle)^{1/2}} \sum_{i=1}^{2} c_i |\psi_i\rangle. \tag{3.29}$$

After taking the expectation value of both sides of eq. (3.28), it can be expressed as a matrix equation

$$\begin{pmatrix} c_1^\star & c_2^\star \end{pmatrix} \begin{pmatrix} p(1|1) & -\langle\psi_1|\psi_2\rangle \\ -\langle\psi_2|\psi_1\rangle & p(2|2) \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \leq 1 \tag{3.30}$$

where the off diagonal terms arise due to the non-trivial normalization of the state $|\Psi\rangle$. The statement that $E_1 + E_2 \leq \mathbb{1}$ can be rewritten as $\mathbb{1} - E_1 - E_2 \geq 0$. Using Sylvester's rule, for $\mathbb{1} - E_1 - E_2 \geq 0$, the element on the first row and first column and the determinant of the matrix must be greater than or equal to zero. Since $(\mathbb{1} - M_1 - M_2)_{11})$ is a probability, the determinant of the matrix being greater than or equal to zero will suffice.

$$(1 - p(1|1))(1 - p(2|2)) \geq |\langle\psi_1|\psi_2\rangle|^2. \tag{3.31}$$

Note that $p_i^F = 1 - p(i|i)$ due to the law of probability and using it, the constraint on individual failure probabilities can be found as

$$p_1^F p_2^F \geq |\langle\psi_1|\psi_2\rangle|^2. \tag{3.32}$$

To find the minimum attainable probability for failure, $p_F = p_1 p_1^F + p_2 p_2^F$ must be minimized with respect to the constraint in eq. (3.32). The minimum of p_F happens when the product $p_1^F p_2^F$ is at its lowest possible value $p_1^F p_2^F = |\langle\psi_1|\psi_2\rangle|^2$. This allows us to express the individual failure probabilities in terms of the other one

$$p_2^F = \frac{|\langle\psi_1|\psi_2\rangle|^2}{p_1^F}. \tag{3.33}$$

Inserting this expression into the total failure probability, p_1^F can be treated as an independent variable and p_F can be easily extremized. Doing the same procedure for p_1^F and p_2^F gives

$$\begin{aligned} p_1^F &= \sqrt{\frac{p_2}{p_1}}|\langle\psi_1|\psi_2\rangle|^2, \\ p_2^F &= \sqrt{\frac{p_1}{p_2}}|\langle\psi_1|\psi_2\rangle|^2. \end{aligned} \tag{3.34}$$

These values, when inserted into the general expression for the total failure probability $p_F = p_1 p_1^F + p_2 p_2^F$ will yield

$$p_F = 2\sqrt{p_1 p_2}|\langle\psi_1|\psi_2\rangle|. \tag{3.35}$$

This bound is also known as the IDP bound after Ivanovic, Dieks and Peres. Note that this bound is only applicable if a POVM exists. The existence of the POVM depends on the eigenvalues of the failure operator which are the individual failure probabilities and they both must satisfy $p_1^F \leq 1$ and $p_2^F \leq 1$. This condition can be transformed into an inequality depending on the initial properties of the ensemble like the probabilities and the overlap. The existence range of the POVM is the interval

$$\frac{|\langle\psi_1|\psi_2\rangle|^2}{1+|\langle\psi_1|\psi_2\rangle|^2} \leq p_1 \leq \frac{1}{1+|\langle\psi_1|\psi_2\rangle|^2}. \tag{3.36}$$

This fact can be seen by examining the expressions for the optimal values of p_1^F and p_2^F after making the substitution $p_2 = 1 - p_1$. If the inequality in eq. (3.36) is not satisfied, a POVM with elements E_1, E_2 and E_0 cannot be constructed and a projective measurement which will be explained below must be used instead. Using the conjugate states $\left|\psi_1^{\perp}\right\rangle$ and $\left|\psi_2^{\perp}\right\rangle$, a measurement scheme can be constructed as follows. Suppose a measurement is performed using two projectors $P_1 = |\psi_1\rangle\langle\psi_1|$ and $\bar{P}_1 = \left|\psi_1^{\perp}\right\rangle\left\langle\psi_1^{\perp}\right|$, and the operators corresponding to $|\psi_2\rangle$ and $\left|\psi_2^{\perp}\right\rangle$. When the measurement $\{P_1, \bar{P}_1\}$ is performed, if the outcome $\bar{1}$ is obtained then the conclusion that the state was originally $|\psi_2\rangle$ can be made without error, but if the outcome 1 is inconclusive where the same idea can also be applied for the state $|\psi_2\rangle$. The probability of the inconclusive result for the measurement $\{P_1, \bar{P}_1\}$ is simply

$$p_{F1} = p_1 + p_2|\langle\psi_1|\psi_2\rangle|^2. \tag{3.37}$$

In the above equation, the p_2 term corresponds to $\langle\psi_1|P_1|\psi_1\rangle$, which has a probability of p_1 and the second term corresponds to the $\langle\psi_2|P_1|\psi_2\rangle$ which has a probability of p_2. The same argument can be applied to the probability of an inconclusive result for the measurement $\{P_2, \bar{P}_2\}$

$$p_{F2} = p_2 + p_1|\langle\psi_1|\psi_2\rangle|^2. \tag{3.38}$$

In total, there are three measurement options for UQSD, the POVM with elements $\{E_1, E_2, E_0\}$, and the projective measurements $\{P_1, \bar{P}_1\}$ and $\{P_2, \bar{P}_2\}$. By checking the values of the failure probabilities for different values of p_1 while keeping the overlap between the states the same, it can be seen that when p_1 satisfies the inequality in eq. (3.36), POVM is optimal, when p_1 is smaller than the

lower bound in eq. (3.36) the first projective measurement is optimal and when p_1 exceeds the upper bound, the second projective measurement is optimal.

The UQSD scheme can be generalized to a procedure what is known as QSS (Quantum State Separation). QSS is a procedure which aims to decrease the square overlaps of a given set of states, in other words $\left|\left\langle\psi_i'\middle|\psi_j'\right\rangle\right|^2 \leq |\langle\psi_i|\psi_j\rangle|^2$ is the procedure is successful. The construction is straightforward; a QSS procedure can be thought of as a state transformation problem, transforming the initial set of states $\{|\psi_i\rangle\}$ with the overlap matrix $A_{ij} = \langle\psi_i|\psi_j\rangle$ into the set $\{|\psi_i'\rangle\}$ with the overlap matrix $A'_{ij} = \left\langle\psi_i'\middle|\psi_j'\right\rangle$. If $A_{ij} \neq A'_{ij}$, this transformation can only be realized with a finite probability of failure if $\left|\left\langle\psi_i'\middle|\psi_j'\right\rangle\right|^2 \leq |\langle\psi_i|\psi_j\rangle|^2$ corresponding to the probability of inconclusive result for QSS. If the inner products are to be made smaller, it can be performed without any probability of failure. In this context, UQSD is just a QSS procedure where the final overlap matrix $A'_{ij} = \delta_{ij}$. If the transformation is successful, a set of states with an overlap matrix of δ_{ij} means that the states are mutually orthogonal and discrimination can be realized trivially, via simple orthogonal projective measurements. The measurement that is going to perform the state separation procedure is defined as follows, $\mathcal{M} = \{M_{S\lambda}, M_{F\lambda}\}$ where S denotes success and F denotes failure and the operators act in the following way

$$\begin{aligned} M_{S\lambda}\,|\psi_i\rangle &= c_{\lambda i}\,|\psi_i'\rangle\,, \\ M_{F\lambda}\,|\psi_i\rangle &= f_{\lambda i}\,|\phi_{\lambda i}\rangle \end{aligned} \tag{3.39}$$

for some $|\phi_{\lambda i}\rangle$ and the conditional probabilities are defined as

$$\begin{aligned} p(\lambda|i) &= \langle\psi_i|M_{S\lambda}^\dagger M_{S\lambda}|\psi_i\rangle\,, \\ p^F(\lambda|i) &= \langle\psi_i|M_{F\lambda}^\dagger M_{F\lambda}|\psi_i\rangle\,. \end{aligned} \tag{3.40}$$

The measurement $\mathcal{M}$ must obey the completeness relation

$$\sum_\lambda M_{S\lambda}^\dagger M_{S\lambda} + \sum_\lambda M_{F\lambda}^\dagger M_{F\lambda} = \mathbb{1} \tag{3.41}$$

and the matrix elements of this matrix equation can be found easily

$$\begin{aligned}\sum_{\lambda}\langle\psi_i|\,M_{S\lambda}^{\dagger}M_{S\lambda}\,|\psi_j\rangle+\sum_{\lambda}\langle\psi_i|\,M_{F\lambda}^{\dagger}M_{F\lambda}\,|\psi_j\rangle&=\langle\psi_i|\psi_j\rangle\,,\\ \sum_{\lambda}c_{\lambda i}^{\star}c_{\lambda i}\,\langle\psi_i'|\psi_j'\rangle+\sum_{\lambda}f_{\lambda i}^{\star}f_{\lambda i}\,\langle\phi_{\lambda i}|\phi_{\lambda j}\rangle&=\langle\psi_i|\psi_j\rangle\,,\\ \sum_{\lambda}c_{\lambda i}^{\star}c_{\lambda i}A_{ij}'+\sum_{\lambda}f_{\lambda i}^{\star}f_{\lambda i}\,\langle\phi_{\lambda i}|\phi_{\lambda j}\rangle&=A_{ij}.\end{aligned}\tag{3.42}$$

The following definitions are made to express the above equation in a more compact form

$$K_{ij}=\sum_{\lambda}c_{\lambda i}^{\star}c_{\lambda i},\;\;F_{ij}=\sum_{\lambda}f_{\lambda i}^{\star}f_{\lambda i}\,\langle\phi_{\lambda i}|\phi_{\lambda j}\rangle\,.\tag{3.43}$$

Using these definitions, the last line of eq. (3.42) can be expressed as

$$A_{ij}=K_{ij}A_{ij}'+F_{ij}\tag{3.44}$$

or in matrix form

$$A=K\circ A'+F\tag{3.45}$$

where $\circ$ denotes the entry-wise product also known as the Hadamard product. Since the matrices K and F are related to success and failure probabilities, there is a constraint that both K and F must be positive semi-definite. To define the operators themselves, the conjugate set must be defined as

$$\begin{aligned}\{|\psi_i^{\perp}\rangle\}_{i=1}^{N},\;\text{where}\;\;|\psi_i^{\perp}\rangle=\sum_j A_{ji}^{-1}\,|\psi_i\rangle\,,\;\text{and}\;\;\langle\psi_k|\psi_i^{\perp}\rangle&=\sum_j A_{ji}^{-1}A_{kj},\\ &=\delta_{ki}.\end{aligned}\tag{3.46}$$

Since K is a hermitian matrix, it can be expressed as follows

$$K=\sum_{\lambda}^{m}a_{\lambda}a_{\lambda}^{\dagger}\tag{3.47}$$

where a_λ is an unnormalized column matrix and m is greater than or equal to the rank of K. Using these definitions, the operators corresponding to successful state separation can be constructed as follows

$$M_{S\lambda}=\sum_i a_{\lambda i}^{\star}\,|\psi_i'\rangle\langle\psi_i^{\perp}|\,.\tag{3.48}$$

Checking the effect of $M_{S\lambda}$ on $|\psi_i\rangle$,

$$\begin{aligned} M_{S\lambda}|\psi_i\rangle &= \sum_j a^{\star}_{\lambda j} |\psi'_j\rangle \langle\psi^{\perp}_j|\psi_i\rangle , \\ &= a^{\star}_{\lambda i} |\psi'_i\rangle . \end{aligned} \tag{3.49}$$

The conditional probability $p(\lambda|i)$ is then $|a_{\lambda i}|^2$. Comparing it with the initial definition, it is seen that $c_{\lambda i} = a^{\star}_{\lambda i}$ and the success operators are $M_{S\lambda} = \sum_i c_{\lambda i} |\psi'_i\rangle \langle\psi^{\perp}_i|$. The total probability of successfully transforming the state $|\psi_i\rangle$ into $|\psi'_i\rangle$ is

$$\begin{aligned} p_s(i) &= \sum_{\lambda} p(\lambda|i), \\ &= \sum_{\lambda} c^{\star}_{\lambda i} c_{\lambda i}, \\ &= K_{ii} \end{aligned} \tag{3.50}$$

meaning that the diagonal elements of the matrix K are the individual probabilities of success for each state. The total probability of success is then simply

$$\begin{aligned} p_S &= \sum_i p_i p_s(i), \\ p_S &= \sum_i p_i K_{ii}. \end{aligned} \tag{3.51}$$

The QSS idea was first put forward by Chefles and Barnett [12] for two states and the problem was solved analytically for the special case of two states. Unfortunately, for an arbitrary number of states, this optimization problem is not analytically solvable but it is a nice generalization of the UQSD procedure.

Up to now, the two main discrimination strategies for monopartite states were covered. A very important problem which has also attracted much attention by the scientific community nowadays is the discrimination of multipartite states, especially under LOCC. In the next sections, perfect discrimination of multipartite, possibly entangled states under LOCC will be covered.

3.4 Discrimination of Multi-Partite States Under LOCC

Entanglement plays a central role in the field of quantum information and computation. Entanglement is the cornerstone of many achievements of quantum information theory such as quantum key distribution, quantum teleportation and quantum algorithms. In the context of quantum state discrimination, this translates into the question of the possibility of discriminating between entangled quantum states and the problem has been explored to great depth in the last decade. The problem is not as easy as monopartite state discrimination however and it is filled with negative results. Many authors such as Walgate [13], Virmani [16], Bandyopadhyay [17], Ghosh [18] have worked on the subject and found various results about the problem. These results have a common feature, after the discrimination procedure the states are transformed into product states with no entanglement but since entanglement is in the cornerstone of many applications in quantum information theory, in recent years some attention was focused on achieving discrimination with remaining entanglement in the posterior states. Cohen [19, 20] and Bandyopadhyay [21, 22] have shown that it is indeed possible if the parties agree to use up some entanglement of previously shared states. Discrimination of entangled states is also closely related with the theory of entanglement transformations and the mathematical theory of majorization. In this section, the results of various authors will be reviewed in depth and the relation of the theory of majorization to the state discrimination problem will be examined.

First, the LOCC procedure should be explained. A LOCC procedure means that the parties sharing a system are only allowed to act on their respective subsystem and share the results of the action by classical communication. It is quite hard to represent a general LOCC procedure generally in a purely mathematical language but a mathematical description can be given as the following. Suppose there are two parties, Alice and Bob and they implement a LOCC scheme. Alice starts the procedure by a measurement $\mathcal{M}_A \otimes \mathbb{1}_B$ with the possible outcomes labeled by the index i. After Alice obtains her outcome, she transmit the result via a classical channel (telephone) to Bob then Bob measures $\mathbb{1}_A \otimes \mathcal{M}_B^i$ where the

i denotes the i^{th} measurement option Bob chooses according to Alice's result. The procedure goes on in the following way until both parties agree to stop. Unfortunately, LOCC procedures are hard to express by pure mathematics and the procedures examined here will usually be explained in a somewhat high-level language.

It is a trivial procedure to discriminate two monopartite orthogonal states as it was shown in the previous sections but it is not that trivial to show that it is possible for multipartite states. To show that it is indeed possible, it has to be shown that the states in question can always be transformed into a desirable form. Consider the two states

$$\begin{aligned} |\psi_1\rangle &= \sum_i |i\rangle_A |\mu_i\rangle_B , \\ |\psi_2\rangle &= \sum_i |i\rangle_A |\nu_i\rangle_B , \end{aligned} \tag{3.52}$$

where the set $\{|i\rangle\}_{i=1}^N$ is an orthonormal basis for the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ but the states $\{|\mu_i\rangle\}_{i=1}^N$ and $\{|\nu_i\rangle\}_{i=1}^N$ are not necessarily normalized nor mutually orthogonal. Any bipartite state can be expressed in the form above since it is a general superposition of states where the superposition coefficients have been absorbed in the states of the subsystem B. There exists a basis for the Hilbert space $\mathcal{H}_A$, $\{|i'\rangle\}$ for which the states $|\psi_1\rangle$ and $|\psi_2\rangle$ take the form

$$\begin{aligned} |\psi_1\rangle &= \sum_i |i'\rangle_A |\mu_i\rangle_B , \\ |\psi_2\rangle &= \sum_i |i'\rangle_A \left|\mu_i^{\perp}\right\rangle_B , \end{aligned} \tag{3.53}$$

where $\langle \mu_i | \mu_i^{\perp} \rangle = 0$, $\{|i'\rangle\}_{i=1}^N$ is an orthonormal basis for $\mathcal{H}_A$, $\{|\mu_i\rangle\}_{i=1}^N$ and $\{|\mu_i^{\perp}\rangle\}_{i=1}^N$ are not necessarily orthogonal nor normalized, it is clear that a local projective measurement can perfectly distinguish between the states since after Alice performs a measurement using the projectors $\{|i'\rangle_A \langle i'|\}_{i=1}^N$, Bob can perform a projective measurement using two projectors $P_1 = |\mu_i\rangle_B \langle \mu_i|$ and $P_2 = |\mu_i^{\perp}\rangle_B \langle \mu_i^{\perp}|$ conditional on the outcome of Alice's measurement i. If Bob gets the outcome 1 than it is certain that the state was $|\psi_1\rangle$ and vice-versa. Hence, it is sufficient to show that there always exists a basis $\{|i'\rangle\}$ that enables the states to be expressed as in eq. (3.53).

The states $|\mu_i\rangle_B$ and $|\nu_i\rangle_B$ can be expressed as a superposition of the elements of an orthonormal basis for the Hilbert space $\mathcal{H}_B$ as

$$\begin{aligned} |\mu_i\rangle_B &= \sum_j (\psi_1)_{ij} |j\rangle_B , \\ |\nu_i\rangle_B &= \sum_j (\psi_2)_{ij} |j\rangle_B , \end{aligned} \tag{3.54}$$

thus, the states $|\psi_1\rangle$ and $|\psi_2\rangle$ take the form

$$\begin{aligned} |\psi_1\rangle &= \sum_{i,j} (\psi_1)_{ij} |i\rangle_A |j\rangle_B , \\ |\psi_2\rangle &= \sum_{i,j} (\psi_2)_{ij} |i\rangle_A |j\rangle_B . \end{aligned} \tag{3.55}$$

The above equation can also be understood in the way that the states in eq. (3.52) are indeed a general form to express two multipartite entangled states. The matrices ψ_1 and ψ_2 encode all the necessary information about the states to be discriminated

$$\begin{aligned} \langle \nu_i | \mu_j \rangle &= \sum_{k,l} (\psi_2)^\star_{ik} (\psi_1)_{jl} \langle k|l\rangle , \\ &= \sum_k (\psi_1)_{jk} (\psi_2)^\star_{ik}, \\ &= (\psi_1 \psi_2^\dagger)_{ji}, \end{aligned} \tag{3.56}$$

and since $\langle \psi_2 | \psi_1 \rangle = \sum_i \langle \nu_i | \mu_i \rangle$ than if $\langle \psi_2 | \psi_1 \rangle = 0$, $\mathrm{Tr}\left(\psi_1 \psi_2^\dagger\right) = 0$. But for discrimination purposes, $\mathrm{Tr}\left(\psi_1 \psi_2^\dagger\right) = 0$ condition is not enough. The condition for discrimination is the following

$$\langle \nu_i | \mu_i \rangle = 0 \ \forall i. \tag{3.57}$$

This means that for some initial traceless matrix $\psi_1 \psi_2^\dagger$, if Alice can find a local unitary transformation under which $\psi_1 \psi_2^\dagger$ transforms into a matrix with all the diagonal elements 0, discrimination can be achieved. To prove that it is indeed possible, the existence of a unitary transformation that transforms a matrix to an equi-diagonal matrix must be proven. Since $\psi_1 \psi_2^\dagger$ is traceless by construction, any transformation that makes it equi-diagonal thus makes it a zero-diagonal matrix. Suppose Alice carries out a unitary transformation (a rotation) on her

respective orthonormal basis $|i\rangle_A = \sum_j (U_A)^\dagger_{ij} |j'\rangle_A$. Under such a transformation, the state $|\psi_1\rangle$ and thus $|\psi_2\rangle$ transform as

$$|\psi_1\rangle = \sum_{i,j,k} (U_A)^\dagger_{ij} |j'\rangle_A (\psi_1)_{ik} |k\rangle_B . \tag{3.58}$$

For the sake of generality, the case that Bob also carries out a transformation must also be considered, $|i\rangle_B = \sum_j (U_B)^\dagger_{ij} |j'\rangle_B$. Under both transformations, the states transform into

$$|\psi_1\rangle = \sum_{i,j,k,l} |j'\rangle_A |k'\rangle_B (U_A)^\star_{ji} (\psi_1)_{ik} (U_B)^\dagger_{kl}. \tag{3.59}$$

From eq. (3.59), it can be concluded that under such unitary transformations, the matrices ψ_1 and ψ_2 transform as

$$\psi_1' = U_A^\star \psi_1 U_B^\dagger, \ \psi_2' = U_A^\star \psi_2 U_B^\dagger. \tag{3.60}$$

The important matrix however is $\psi_1 \psi_2^\dagger$. Under such a transformation it becomes

$$\begin{aligned} \psi_1' \psi_2'^\dagger &= U_A^\star \psi_1 U_B^\dagger (U_A^\star \psi_2 U_B^\dagger)^\dagger, \\ &= U_A^\star \psi_1 U_B^\dagger U_B \psi_2^\dagger U_A^{\star\dagger}, \\ &= U_A^\star \psi_1 \psi_2^\dagger U_A^{\star\dagger}. \end{aligned} \tag{3.61}$$

The above equation tells that such a transformation can be carried out by Alice alone and if U is unitary than $U^\star$ is also unitary. Now the proof that such a unitary U can transform $\psi_1 \psi_2^\dagger$ into a matrix with equal diagonal elements should be proven. To that end, suppose Ψ is a general 2×2 matrix and U is a general unitary

$$\Psi = \begin{pmatrix} x & y \\ z & t \end{pmatrix}, \ U = \begin{pmatrix} \cos\theta & \sin\theta e^{i\phi} \\ \sin\theta e^{-i\phi} & -\cos\theta \end{pmatrix}. \tag{3.62}$$

U is a rotation matrix and it is unitary by construction. The condition that $U\Psi U^\dagger$ has equal diagonal elements means that

$$(x - t)\cos 2\theta + (y e^{-i\phi} + z e^{i\phi}) \sin 2\theta = 0. \tag{3.63}$$

As true for any equation with complex variables, this equation can be split into its real and imaginary parts and solved. The real and the imaginary parts of eq.

(3.64) are respectively

$$\begin{aligned}\mathrm{Re}\{x-t\}\cos 2\theta + \mathrm{Re}\{y+z\}\cos\phi\sin 2\theta + \mathrm{Im}\{y-z\}\sin\phi\sin 2\theta = 0,\\ \mathrm{Im}\{x-t\}\cos 2\theta + \mathrm{Im}\{y+z\}\cos\phi\sin 2\theta + \mathrm{Re}\{z-y\}\sin\phi\sin 2\theta = 0.\end{aligned} \tag{3.64}$$

Dividing the equations by $\sin 2\theta$ gives

$$\begin{aligned}\tan 2\theta &= \frac{\mathrm{Re}\{x-t\}}{\mathrm{Re}\{y+z\}\cos\phi - \mathrm{Im}\{z-y\}\sin\phi},\\ &= \frac{\mathrm{Im}\{x-t\}}{\mathrm{Re}\{y-z\}\sin\phi - \mathrm{Im}\{y-z\}\cos\phi},\end{aligned} \tag{3.65}$$

and combining these two and solving for ϕ will give

$$\tan\phi = \frac{\mathrm{Im}\{x-t\}\,\mathrm{Re}\{z+y\} - \mathrm{Re}\{x-t\}\,\mathrm{Im}\{z+y\}}{\mathrm{Re}\{x-t\}\,\mathrm{Re}\{z-y\} + \mathrm{Im}\{x-t\}\,\mathrm{Im}\{z-y\}}. \tag{3.66}$$

Since eq. (3.66) is real, it can always be solved for ϕ and thus eq. (3.65) is always solvable for θ. Hence for any Ψ, a unitary transformation realized by the unitary matrix U always exists and can be constructed using eqs. (3.65-66). This result however applies to 2×2 matrices but it can be used for any $2^n \times 2^n$ matrices since the diagonal elements can be grouped into 2^{n-1} pairs and then 2^{n-2} quartets can be created and pairs in these quartets can be equalized. Continuing in this manner, any $2^k \times 2^k$ matrix can be equi-diagonalized by Alice if she applies $k2^{k-1}$ times a unitary 2×2 transformation. If the matrix $\psi_1\psi_2^\dagger$ is not $2^k \times 2^k$, an ancilla qubit known to be in the state $|0\rangle_{A'}$ can be used to enlarge the dimension of the Hilbert space as follows. The ancilla is introduced in the following manner and the states $|\psi_1\rangle$ and $|\psi_2\rangle$ can be expressed as

$$\begin{aligned}|\psi_1\rangle &= \sum_{i=1}^{n} |i0\rangle_{AA'} |\mu_i\rangle_B + \sum_{i=1}^{n} |i1\rangle_{AA'} |\mu_{i+n}\rangle_B ,\\ |\psi_2\rangle &= \sum_{i=1}^{n} |i0\rangle_{AA'} |\nu_i\rangle_B + \sum_{i=1}^{n} |i1\rangle_{AA'} |\nu_{i+n}\rangle_B .\end{aligned} \tag{3.67}$$

Since the state of the ancilla is known to be in $|0\rangle_{A'}$, $|\mu_i\rangle$, $i > n$ and $|\nu_i\rangle$, $i > n$ have an amplitude of 0. Number theory tells us that $n \leq 2^k \leq 2n$ for some k, hence Alice can pick a $2^k \times 2^k$ sub matrix of the expanded $\psi_1\psi_2^\dagger$ and proceed with the equi-diagonalization in the manner described above.

This concludes the proof that any two bipartite orthogonal quantum state can always be perfectly discriminated. The idea can easily be generalized to multi-partite states with the party number larger than 2. Using a larger Hilbert space

as explained above, the measurement procedure can first be applied by Alice, leaving other parties to continue the discrimination. Than, some other party does the same type of measurement Alice performs and this continues until only 2 parties are left after which the problem reduces to the 2 party version. If they are not orthogonal, the minimum error discrimination strategy can be used. The result is due to Virmani et. al. [16] and an outline of the idea will be presented. If $\langle\psi_1|\psi_2\rangle \neq 0$, than it will not be possible to bring the states into the form in eq. (3.53). The parties however can adopt the following strategy. After Alice performs her projective measurement, Bob will be left with two states conditional on the outcome of Alice. These states, since $\langle\psi_1|\psi_2\rangle \neq 0$, will not be orthogonal but Bob will know the states he possesses. After the measurement of Alice, Bob will be left with two states $|\mu_i'\rangle$ and $|\nu_i'\rangle$ conditional on the outcome i of Alice. Now, using eq. (3.56), it can be seen that the elements of the matrix $(\psi_1\psi_2)$ are the inner products, $\langle\nu_i'|\mu_j'\rangle$. After the equi-diagonalization of $(\psi_1\psi_2)$, all inner products $\langle\nu_i'|\mu_i'\rangle$ will be equal. He can then carry out a minimum error discrimination procedure as explained in sec. (2.2) or a UQSD procedure explained in sec. (2.3). This idea shows that two bipartite states can be distinguished even if they are not orthogonal to each other.

The case for 3 or more states is not as easy to explore as the 2 state case however. Ghosh and his colleagues [18] have shown that for three bipartite orthogonal pure states, discrimination is only possible for certain intervals and discrimination of 4 mutually orthogonal states is impossible. Their result will be reviewed in detail in the following discussion and its connections with the theory of local entanglement transformations and thus majorization will be explained.

Consider the set of conjugate states

$$\begin{aligned}
|\psi_1\rangle &= a\,|00\rangle + b\,|11\rangle\,,\\
|\psi_2\rangle &= b\,|00\rangle - a\,|11\rangle\,,\\
|\psi_3\rangle &= c\,|01\rangle + d\,|10\rangle\,,\\
|\psi_4\rangle &= d\,|00\rangle - c\,|11\rangle\,,
\end{aligned} \tag{3.68}$$

where a, b, c, d are chosen to be real without losing any generality. It will be shown in the next discussion that these 4 states cannot be distinguished. To

prove it, a few definitions about entanglement monotones must be made. A widely used entanglement monotone is the logarithmic negativity which is defined as

$$E_N(\rho) = \log_2 \left\|\rho^{T_A}\right\|_1 \tag{3.69}$$

where $\|\rho\|_1$ is the trace norm defined as $\|\rho\|_1 = \mathrm{Tr}\left(\sqrt{\rho^\dagger \rho}\right)$ and ρ^{T_A} is the partial transpose over the Hilbert space $\mathcal{H}_A$ defined in the following way

$$\begin{aligned} \rho_{AB}^{T_A} &= (\sum_{ijkl} c_{ij} c_{kl}^\star \left|i\right\rangle_A \left\langle k\right| \otimes \left|j\right\rangle_B \left\langle l\right|)^{T_A}, \\ &= \sum_{ijkl} c_{ij} c_{kl}^\star \left|k\right\rangle_A \left\langle i\right| \otimes \left|j\right\rangle_B \left\langle l\right|. \end{aligned} \tag{3.70}$$

As defined in chapter 1, entanglement monotones are functions of the Schmidt coefficients of the states such that they don't increase under LOCC. Also, the concept of distillable entanglement is a useful concept and should be defined. Entanglement distillation [23] is a much used idea in quantum information theory and it is conceptually very simple. Two observers, say Alice and Bob share n entangled states each having less entanglement than a Bell state. Instead of having n copies of a state that has less than 1 ebit of entanglement, using LOCC, these observers can create m Bell states with $m < n$. The procedure can be mathematically outlined in the following way.

Suppose that Alice and Bob share n copies of a partially entangled state. The state they share can be expressed in the following completely general way

$$\begin{aligned} \left|\Psi\right\rangle_{AB} &= (\cos\theta \left|\alpha_1\beta_1\right\rangle + \sin\theta \left|\alpha_2\beta_2\right\rangle)^{\otimes n}, \\ &= \bigotimes_{i=1}^{n} (\cos\theta \left|\alpha_{1i}\beta_{1i}\right\rangle + \sin\theta \left|\alpha_{2i}\beta_{2i}\right\rangle), \\ &= \sum_{k=0}^{n} (\cos\theta)^{n-k} (\sin\theta)^k [\sum_{\substack{|n=1|=n-k \\ |n=2|=k}} (\bigotimes_{i=1}^{n} \left|\alpha_{ni}, \beta_{ni}\right\rangle) \end{aligned} \tag{3.71}$$

where $\otimes n$ denotes the n^{th} power of the state in parenthesis with respect to the Kronecker product and the limits $|n=1| = n-k$ and $|n=2| = k$ means that the index n takes the value 1 for $n-k$ terms and the value 2 for k terms. To obtain a maximally entangled pair, one of the parties will carry out an incomplete projective measurement projecting the states into the subspaces formed by the

states having a coefficient of $\sin^k\theta$ where $k = 0 \ldots n$ using the projectors

$$P_k = \sum_{\substack{|n=1|=n-k \\ |n=2|=k}} (\bigotimes_{i=1}^{n} |\alpha_{ni}\rangle\langle\alpha_{ni}|), \tag{3.72}$$

where these projectors are the ones Alice would use. There are $n+1$ such subspaces and the probability of obtaining the outcome k has a probability of

$$p_k = \binom{n}{k} (\cos^2\theta)^{n-k} (\sin^2\theta)^k. \tag{3.73}$$

The combination symbol counts the number of Kronecker product terms with coefficients $(\cos\theta)^{n-k}(\sin\theta)^k$ in the expansion of the state $|\Psi\rangle_{AB}$ and it can easily be justified, there are $\binom{n}{k}$ ways of choosing k different items out of n items. After learning the result of Alice's measurement, Bob carries out the same projective measurement but due to the entanglement between them, he will always obtain the outcome k. Now, note that after Bob's measurement, Alice and Bob will share a maximally entangled state living in a $\binom{n}{k}$ dimensional subspace of the original 2^n dimensional one. Any maximally entangled state can be transformed into a standard form such as a singlet state with LOCC and after such a transformation, Alice and Bob will share a maximally entangled state. The proof will not be taken any further, the interested reader can follow these papers [23, 24].

The property that the logarithmic negativity is the upper bound for distillable entanglement can be used to show that the states $\{|\psi_i\rangle\}_{i=1}^4$ are not distinguishable. The proof that it is indeed the case is quite long and very non-trivial, so only the reference will be given: the proof can be found in [25].

For the sake of notational simplicity, the Bell states will be denoted as $\{|\phi_i\rangle\}_{i=1}^4$ where the states are ordered from 1 to 4 in the order of appearance in eq. (1.41). Consider the following state that is shared between 4 parties, Alice, Bob, Charlie and Daniel.

$$\rho_{ABCD} = \frac{1}{4} \sum_{i,j=1}^{4} |\psi_i\rangle_{AB} \langle\psi_j| \otimes |\phi_i\rangle_{CD} \langle\phi_j| . \tag{3.74}$$

The initial probabilities have been chosen to be equal to make calculations easier and the result more clear. If it were possible to distinguish the states $|\psi_i\rangle$ with certainty, Alice and Bob could implement a discrimination scheme after which

Charlie and Daniel would share a Bell state which has an entanglement of 1 ebit. This can be interpreted in the context of distillable entanglement to mean that the distillable entanglement between Charlie - Daniel and Alice - Bob, or the AC:BD cut is 1 ebit. Now, use the fact that logarithmic negativity is an upper bound for distillable entanglement. The logarithmic negativity of ρ_{ABCD} in the AC:BD cut is

$$\begin{aligned} E_N(\rho) &= \log_2 \left\| \rho^{T_{AC}} \right\|_1, \\ &= \log_2 \mathrm{Tr}\big((\rho^{T_{AC}})^\dagger \rho^{T_{AC}} \big)^{1/2}). \end{aligned} \tag{3.75}$$

ρ is given by $\rho = \frac{1}{4} \sum_{i,j=1}^{4} |\psi_i\rangle_{AB} \langle\psi_j| \otimes |\phi_i\rangle_{CD} \langle\phi_j|$ and when $E_N(\rho)$ is calculated it gives

$$E_N(\rho) = \log_2(a^2 + c^2). \tag{3.76}$$

The terms in the logarith is just squares since it was assumed that $a, b, c, d \in \mathbb{R}$. The contradiction is clear. Using the fact that the logarithmic negativity is the upper bound for distillable entanglement, $E_N(\rho) \geq 1$, both a and c must be 1, where 1 is the distillable entanglement in the $AC : BD$ cut. If $a = c = 1$, the states $\{|\psi_i\rangle\}_{i=1}^4$ become product states. The conclusion to be drawn here is that 4 entangled, mutually orthogonal states cannot be distinguished. Also, note that when the states $\{|\psi_i\rangle\}_{i=1}^N$ are chosen as the Bell states, the bound can not be satisfied meaning that the Bell states cannot also be discriminated. If this test is applied to the case where only 3 states of the 4 original ones are to be discriminated, it turns out that discrimination is possible for some range of the parameters a, b, c, d. The density operator to be used in the test is constructed as follows

$$\rho_{ABCD} = \frac{1}{4} \sum_{i,j=1}^{3} |\psi_i\rangle_{AB} \langle\psi_j| \otimes |\phi_i\rangle_{CD} \langle\phi_j| , \tag{3.77}$$

and when the logarithmic negativity is calculated for the density operator in eq. (3.77), it gives

$$E_N(\rho) = \log_2[1 + \frac{1}{3}(1 + 16a^2b^2 - 4c^2d^2)^{1/2} + 2(1 - 4a^2b^2 + c^2d^2)^{1/2}]. \tag{3.78}$$

For three states to be discriminated, $E_N(\rho) \geq 1$ must be satisfied, if else there is a contradiction with the fact that logarithmic negativity is the upper bound for distillable entanglement. The bound is satisfied if

$$4a^2b^2 - c^2d^2 > \frac{3}{4}. \tag{3.79}$$

A quick note, the constraint in eq. (3.79) is reached when the states $|\psi_i\rangle$, $i = 1, 2, 3$ are used or, in a more qualitative description, two parallel and one anti-parallel state is used. Since the Schmidt coefficients are same for $|\psi_1\rangle$ and $|\psi_2\rangle$, and $|\psi_3\rangle$ and for $|\psi_4\rangle$, there are only 2 different ways of picking the 3 states to be discriminated among the 4. If two anti parallel and 1 parallel state is chosen, the constraint is found by swapping a with c and b with d, giving

$$4c^2d^2 - a^2b^2 > \frac{3}{4}. \tag{3.80}$$

This is a good point to start discussing the theory of majorization and its connections to entanglement transforms and hence the state discrimination problem. In the next section, the theory of majorization will be introduced and its connections to the state discrimination problem will be made clear.

3.5 Majorization, Entanglement Transformations and State Discrimination

The theory of majorization is a widely studied subject in mathematics, particularly in the field of linear algebra. The applications of majorization are widespread, but for quantum information theory, the main attraction of the theory comes from the ability to compare the mixedness of two probability distributions. The connection between quantum information theory and the theory of majorization is explained in great detail in Nielsen's papers [26, 27]. Majorization is a powerful tool which completely characterizes transformations of pure entangled states and gives important relations about the quantum state of a system before and after measurement and the outcome probabilities. The focus in this section and the rest of this document will be on the first main application of majorization and it will be explained in detail below.

Majorization defines a partial order between vectors whose elements sum up to the same value. Majorization can be defined in the following way. Let x and y

be d dimensional vectors

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{pmatrix}, \; y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_d \end{pmatrix}. \tag{3.81}$$

Than, y majorizes x, or $x \prec y$ if the following inequality holds for every $k = 1, 2, \ldots, d$ and equality holds for $k = d$

$$\sum_{i=1}^{k} x_i^{\downarrow} \leq \sum_{i=1}^{k} y_i^{\downarrow}, \tag{3.82}$$

where $x_i^{\downarrow}$ denotes the components of the vector x are organized in a descending order and specifically, $x_i^{\downarrow}$ is the i^{th} largest component of x. This partial order can be extended to matrices with equal traces constructing a vector λ_A using the eigenvalues of the matrix A and sorting the eigenvalues in a descending order. Note that when two vectors of unequal dimension but equal sum of elements are going to be compared, the lesser dimensional can be padded with zeros until its dimension equals the larger dimensional vector and this idea is going to be used a lot.

The connection of majorization with quantum information theory is made through comparing the eigenvalue vectors of the reduced density operators of various quantum states. There are three important results that realize the connection. These results will be explained in detail below.

The first connection with information theory can be made by using the notion of Schur convex and Schur concave functions. A Schur convex function is a function such that

$$f : \mathbb{R}^d \to \mathbb{R}^d, \; f(x) \leq f(y) \text{ iff } x \prec y, \; \forall x, y, \in \mathbb{R}^d. \tag{3.83}$$

If f is Schur convex, than $-f$ is Schur concave. All Schur convex functions are symmetric under the permutations of its arguments. A criteria for Schur convexity can be expressed as follows. Let $f(x_1, \ldots, x_d)$ be a function on $\mathbb{R}^d$ with continuous partial derivatives. Then f is Schur convex if

$$(x_i - x_j)(\frac{\partial f}{\partial x_i} - \frac{\partial f}{\partial x_j}) \geq 0, \; \forall x_i, x_j \in \mathbb{R}^d. \tag{3.84}$$

It can be seen from inspection that the function $f(x_i) = \sum_{i=1}^{d} x_i \log_2 x_i$ is Schur convex. Then, the function $H(x_i) = -\sum_{i=1}^{d} x_i \log_2 x_i$ is Schur concave which is also the Shannon entropy function. Remembering the definition of Schur concavity, the connection can be made. If $p(x) \prec p(y)$ where $p(x), p(y)$ are probability distributions, $H(x) \geq H(y)$. In other words, x is more mixed than y. Note that, for density operators, the von Neumann entropy reduces to the Shannon entropy with x_i becoming the eigenvalues of the density operator. Using majorization, a partial order can be constructed amongst density operators ranking their mixedness. Also remember that the entanglement entropy is defined as the von Neumann entropy of the reduced density operator. Also, using majorization, a partial order among quantum states can be constructed, ranking their entanglement amount.

Nielsen's theorem and the theorem due to Jonathan and Plenio [28] produce a fascinating connection between majorization and transformations of pure entangled states under LOCC. Let $|\psi\rangle_{AB}$ and $|\phi\rangle_{AB}$ be two bipartite states and let $\rho_\psi = \mathrm{Tr}_B |\psi\rangle \langle\psi|$ and ρ_ϕ defined accordingly. The theorem states that if $|\psi\rangle$ is can be converted into $|\phi\rangle$ under LOCC, then the following must hold

$$\begin{aligned} |\psi\rangle \to |\phi\rangle \text{ iff } \lambda(\psi) \prec \lambda(\phi), \\ |\psi\rangle \to \{(p_i, |\phi_i\rangle\} \text{ iff } \lambda(\psi) \prec \sum_i p_i \lambda(\phi_i), \end{aligned} \tag{3.85}$$

where $\lambda(\psi)$ is the vector with the components being the eigenvalues of ρ_ψ. The second relation is for a probabilistic transformation where the state $|\psi\rangle$ is transformed into $|\phi_i\rangle$ with probability p_i. There are, however some states for which neither $\lambda(\psi) \prec \lambda(\phi)$ nor $\lambda(\phi) \prec \lambda(\psi)$. These states will be said to have incompatible entanglement.

$\lambda(\psi)$ can also be seen as a quantifier of entanglement as it does not increase under LOCC. Also, it can be inferred from eq. (3.85) that a maximally entangled state can be transformed to any state with same dimensionality since

$$\begin{pmatrix} \frac{1}{d} \\ \frac{1}{d} \\ \vdots \\ \frac{1}{d} \end{pmatrix} \prec \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{pmatrix}, \tag{3.86}$$

where $\sum_{i=1}^{d} x_i = 1$. The proof of eq. (3.85) uses several facts which are not going to be proven here:

(i) Any matrix A can be expressed as a polar decomposed form $A = (A^\dagger A)^{1/2} U$ where U is some unitary.

(ii) If $\rho' = \sum_i p_i U_i \rho U_i^\dagger$ where p_i are probabilities, $\lambda(\rho') \prec \lambda(\rho)$.

(iii) If $x \prec y$, then $x = Dy$ where D is a product of at most $d-1$ T transforms where $d = \dim x$ and a T transforms acts on at most 2 components of a matrix and for those two components it has the form

$$T = \begin{pmatrix} t & 1-t \\ 1-t & t \end{pmatrix}. \tag{3.87}$$

(iv) $|\psi\rangle \sim |\phi\rangle$ will be used if they have the same Schmidt coefficients. Two states with the same Schmidt coefficients are equivalent under local unitaries.

The LOCC protocol can be thought of the following way; Alice performs a general measurement $\mathcal{M} = \{M_m\}$ and Bob performs a quantum operation $\mathcal{E}_m$ conditional on the outcome m

$$|\phi\rangle \langle\phi| = \sum_m \mathcal{E}_m(M_m |\psi\rangle \langle\psi| M_m^\dagger). \tag{3.88}$$

A note, Alice and Bob can also realize the transformation using general measurements and arbitrary amount of classical communication or Bob can perform a possibly non unitary operation where Alice and Bob only communicate once.

Tracing out the subsystem B and noting that the states in question are pure, the relation

$$M_m \rho_\psi M_m^\dagger = p_m \rho_\phi \tag{3.89}$$

can be obtained. Using fact (i) and $\rho \geq 0$ for any density operator

$$\begin{aligned} M_m \sqrt{\rho_\psi} &= (M_m \rho_m M_m^\dagger)^{1/2} U_m, \\ &= \sqrt{p_m \rho_\phi} U_m. \end{aligned} \tag{3.90}$$

Since the measurement $\mathcal{M}$ is complete ρ_ψ can be expressed as

$$\rho_\psi = \sum_m \sqrt{\rho_\psi} M_m M_m^\dagger \sqrt{\rho_\psi}. \tag{3.91}$$

Now, eq. (3.90) can be substituted in eq. (3.91) to get

$$\rho_\psi = \sum_m p_m U_m \rho_\phi U_m^\dagger \tag{3.92}$$

and using fact (ii), $\lambda(\psi) \prec \lambda(\phi)$. This shows that if $|\psi\rangle \to |\phi\rangle$ then $\lambda(\psi) \prec \lambda(\phi)$. Now the converse statement, if $\lambda(\psi) \prec \lambda(\phi)$, then $|\psi\rangle \to |\phi\rangle$ must be proven.

Without losing any generality, the quantum states $|\psi\rangle$ and $|\phi\rangle$ can be written in their Schmidt decomposed form using the computational basis

$$\begin{aligned} |\psi\rangle \sim |\psi'\rangle &= \sqrt{p_1}\,|00\rangle + \sqrt{p_2}\,|11\rangle\,, \\ |\phi\rangle \sim |\phi'\rangle &= \sqrt{q_1}\,|00\rangle + \sqrt{q_2}\,|11\rangle\,, \end{aligned} \tag{3.93}$$

where it is assumed that $p_1 \geq p_2$ and $q_1 \geq q_2$, and to satisfy the majorization relation $p_2 \geq q_2$ and $p_1 \leq q_1$.

Alice and Bob will first try to transform the state $|\psi'\rangle$ to

$$|\psi''\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |1\rangle\,(\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle). \tag{3.94}$$

For this to be possible, α must satisfy $p_1 = \frac{1}{2}(1+\cos\alpha)$ so that the states have the same Schmidt coefficients. Then, Alice performs a general measurement defined through the operators

$$M_1 = \begin{pmatrix} \cos\beta & 0 \\ 0 & \sin\beta \end{pmatrix},\ M_2 = \begin{pmatrix} \sin\beta & 0 \\ 0 & \cos\beta \end{pmatrix}. \tag{3.95}$$

It can be checked that $M_1^\dagger M_1 + M_2^\dagger M_2 = \mathbb{1}$. The post measurement states corresponding to M_1 and M_2 are

$$\begin{aligned} |\psi_1'''\rangle &= \cos\beta\,|00\rangle + \sin\beta\,|1\rangle\,(\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle), \\ |\psi_2'''\rangle &= \sin\beta\,|00\rangle + \cos\beta\,|1\rangle\,(\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle). \end{aligned} \tag{3.96}$$

Note that the operators M_1 and M_2 are constructed in such a way that the Schmidt coefficients of $|\psi_1'''\rangle$ and $|\psi_2'''\rangle$ are the same. Using fact (iv), it is possible to ensure that the post measurement state is $|\psi_1'''\rangle$ after some local unitary transformations and classical communication. The Schmidt coefficients of the state $|\psi_1'''\rangle$ can be calculated easily

$$\lambda_\pm = \frac{1 \pm (1 - \sin^2 2\beta \sin^2\alpha)^{1/2}}{2}. \tag{3.97}$$

If there exists a solution such that $\lambda_+ = q_1$, it means that the state $|\psi_1'''\rangle$ is equivalent to $|\phi'\rangle$ under unitary transformations. This equation can be solved easily and gives

$$\beta = \frac{1}{2}\arcsin[\frac{2(q_1 - q_1^2)}{\sin\alpha}]. \tag{3.98}$$

For systems of dimensionality greater than 2, the procedure is to apply M_1^i and M_2^i where i refers to a block of two components and acting them in succession to the states

$$|\psi\rangle \sim |\psi'\rangle = \cos\gamma(\sqrt{p_1}\,|00\rangle + \sqrt{p_2}\,|11\rangle) + \sin\gamma\,|\psi^{\perp}\rangle \tag{3.99}$$

and $|\phi'\rangle$ is expressed in the same fashion.

This completes the proof of the claim in eq. (3.85). For the proof of the second relation

$$\lambda(\psi) \prec \sum_i p_i\lambda(\phi_i), \tag{3.100}$$

some theorems in the theory of majorization will be used without proof [29].

(i)Ky Fan's maximum principle: $\sum_{j=1}^{k}\lambda_j(A) = \max_P \mathrm{Tr}(AP)$ where P are k-dimensional projectors.

(ii)$\lambda(A+B) \prec \lambda(A) + \lambda(B)$ which is a consequence of the Ky Fan's maximum principle.

An immediate result of (ii) is for $\rho = \sum_i p_i\rho_i$,

$$\lambda(\rho) \prec \sum_i p_i\lambda(\rho_i). \tag{3.101}$$

To prove the relation in eq. (3.100), first, it will be proved that if a measurement M_i transforms $|\psi\rangle$ into $|\phi_i\rangle$ with probability p_i then $\lambda(\psi) \prec \sum_i p_i\lambda(\phi_i)$ must hold.

Suppose that the measurement is performed locally on a subsystem of a pure state $|\psi\rangle$ where $\rho_A = \mathrm{Tr}_B\,|\psi\rangle\langle\psi|$. The posterior states are:

$$\begin{aligned} |\psi_i\rangle &= \frac{(M_i \otimes \mathbb{1}_B)\,|\psi\rangle}{\sqrt{p_i}}, \\ \rho_{B,i} &= \mathrm{Tr}_A\,|\psi_i\rangle\langle\psi_i|\,. \end{aligned} \tag{3.102}$$

No communication theorem prevents the faster than light propagation of information or in other words, it prevents Bob from learning whether Alice has performed a measurement or nor or the outcome of Alice's measurement without Alice telling him. The statement can be expressed as follows

$$\begin{aligned}\rho_B = \mathrm{Tr}_A \left|\psi\right\rangle\!\left\langle\psi\right| &= \mathrm{Tr}_A[(M_i \otimes \mathbb{1}_B) \left|\psi\right\rangle\!\left\langle\psi\right| (M_i^\dagger \otimes \mathbb{1}_B)], \\ &= \sum_i p_i \rho_{B,i}.\end{aligned} \tag{3.103}$$

Note that the statement above is equivalent to the one in eq. (3.101) since all reduced density operators of a pure state have identical spectrum.

Now suppose that ρ and ρ_i are density operators and p_i are probabilities such that eq. (3.101) holds. It will be shown that there exists a transformation

$$\sum_{i,j} M_{ij}^\dagger M_{ij} = \mathbb{1},\ M_{ij}\rho M_{ij}^\dagger = p_{ij}\rho_i \text{ and } \sum_j p_{ij} = p_i. \tag{3.104}$$

Fact (iii) can be re expressed in the following way. $\lambda(\rho) = \sum_{i,j} p_i q_j P_j \lambda(\rho_i)$ if $\lambda(\rho) \prec \sum_i p_i \lambda(\rho_i)$ where P_j are permutation matrices. It is easy to justify since T transformations are convex combinations of permutation matrices.

The operators M_{ij} are defined as follows

$$M_{ij}\sqrt{\rho} = \sqrt{p_i q_j}\sqrt{\rho_i} P_j^\dagger \tag{3.105}$$

after assuming that ρ and ρ_i are diagonalizable in the same basis and their eigenvalues are sorted decreasingly. This can be achieved by local unitary transformations before the measurement M_{ij}.

$$\sum_{i,j} \sqrt{\rho}(M_{ij}^\dagger M_{ij})\sqrt{\rho} = \sum_{ij} p_i q_j P_j \rho_i P_j^\dagger. \tag{3.106}$$

Since ρ and ρ_i are diagonal and the diagonal elements are in decreasing order, the above equation is equivalent to $\lambda(\rho) = \sum_{i,j} p_i q_j P_j \lambda(\rho_i)$ meaning that M_{ij} satisfy the completeness relation.

It also follows that

$$M_{ij}\rho M_{ij}^\dagger = p_i q_j \rho_i \tag{3.107}$$

where $p_{ij} = p_i q_j$ and $\sum_j p_i q_j = p_i$. Combining with the proof of the converse relation, the second theorem is proved.

Using eq. (3.100), the feasibility of state discrimination problems can be investigated by the theory of majorization. Majorization relations can be found for state discrimination problems and the relations will help in understanding whether discrimination of a given set of states is possible or not. However, since majorization covers all kinds of LOCC procedures and does not limit itself to one-way communication, constructing a protocol and the measurement operators that do the job is quite hard in most cases.

The result of Ghosh et. al. can be investigated using majorization using eq. (3.100). The set of states to be discriminated are the ones in eq. (3.68), and $|\phi_i\rangle$ are the Bell states. Construct the multipartite state

$$|\Psi\rangle = \frac{1}{2}\sum_{i=1}^{4} |\psi_i\rangle_{AB} |\phi_i\rangle_{CD} \,. \tag{3.108}$$

If discrimination is successful, The parties C, D will share a maximally entangled state. This procedure can be thought of as an entanglement transformation under LOCC with the majorization relation

$$\lambda(\mathrm{Tr}_{BD} |\Psi\rangle\langle\Psi|) \prec \lambda(\frac{1}{2}\mathbb{1}). \tag{3.109}$$

This is actually the majorization relation for an entanglement transformation that takes the the state $|\Psi\rangle$ and converts it into a Bell state $|\phi_i\rangle$ with probability $p_i = \frac{1}{4}$ and i is identified. Being able to identify the index i means that the states $|\psi_i\rangle$ are distinguished from each other and the parties C and D now know which Bell state they share. The equation above is just eq. (3.100) with relevant information inserted. The partial trace can be calculated and gives

$$\mathrm{Tr}_{BD} |\Psi\rangle\langle\Psi| = \frac{1}{8}\begin{pmatrix} (a+b)^2+(c+d)^2 & 0 & 0 & 2(a+b)(c+d) \\ 0 & (a-b)^2+(c-d)^2 & 2(a-b)(c-d) & 0 \\ 0 & 2(a-b)(c-d) & (a-b)^2+(c-d)^2 & 0 \\ 2(a+b)(c+d) & 0 & 0 & (a+b)^2+(c+d)^2 \end{pmatrix} \tag{3.110}$$

with the eigenvalues

$$\begin{aligned} \lambda_1 &= \frac{1}{8}(a+b+c+d)^2, \\ \lambda_2 &= \frac{1}{8}(a-b+c-d)^2, \\ \lambda_3 &= \frac{1}{8}(a-b-c+d)^2, \\ \lambda_4 &= \frac{1}{8}(a+b-c-d)^2. \end{aligned} \tag{3.111}$$

Without losing any generality, it can be assumed that $a \geq b$ and $c \geq d$ and $a, b, c, d \geq 0$. The largest among the eigenvalues is surely λ_1 and for the majorization relation to hold, the following must be satisfied.

$$\frac{1}{2} \geq \frac{1}{8}(a+b+c+d)^2. \tag{3.112}$$

The function $a+\sqrt{1-a^2}-1$ has only one root in the interval $a \in [0,1]$, it is $a = 0$ and that point is also the local minimum hence the function $a + \sqrt{1-a^2} - 1$ is always greater than or equal to zero with the equality satisfied at the endpoints hence $a + \sqrt{1-a^2} \geq 1$. This means that the inequality in eq. (3.112) can only be satisfied for $a = c = 0$ or $a = c = 1$ and that means that the states $|\psi_i\rangle$ are unentangled. The result that 4 mutually orthogonal entangled pure states cannot be distinguished with LOCC. The same idea can be applied for the three state case where

$$|\Psi\rangle = \frac{1}{\sqrt{3}} \sum_{i=1}^{3} |\psi_i\rangle_{AB} |\phi_i\rangle_{CD} \tag{3.113}$$

and the majorization relation is as in eq. (3.109). The reduced density matrix for the state $|\Psi\rangle$ becomes

$$\mathrm{Tr}_{BD} |\Psi\rangle\langle\Psi| = \frac{1}{6} \begin{pmatrix} (a+b)^2+c^2 & 0 & 0 & (a+b)(c+d) \\ 0 & (a-b)^2+c^2 & (a-b)(d-c) & 0 \\ 0 & (a-b)(d-c) & (a-b)^2-d^2 & 0 \\ (a+b)(c+d) & 0 & 0 & (a+b)^2+d^2 \end{pmatrix}. \tag{3.114}$$

The eigenvalue expressions are not simple but numerical calculations show that discrimination is possible for a range of values for a and c.

Majorization can also be used to investigate a different problem. Suppose Alice and Bob share the states $|\psi_i\rangle$ and they also share an entangled pair

$$|\phi\rangle = \alpha |00\rangle + \beta |11\rangle \tag{3.115}$$

and they can use the entanglement of $|\phi\rangle$ to achieve discrimination of the states $|\psi_i\rangle$. If the parties are able to distinguish between the individual $|\psi_i\rangle$, then they will be able to implement a probabilistic entanglement transformation that takes the state $|\phi\rangle \otimes |\Psi\rangle$ to a Bell state $|\phi_i\rangle$ with equal probability for each i and identifying the index i. Using this idea, a majorization relation for that transformation constructed using eq. (3.100).

$$\lambda(\mathrm{Tr}_B |\phi\rangle\langle\phi|) \otimes \lambda(\mathrm{Tr}_{BD} |\Psi\rangle\langle\Psi|) \prec \lambda(\frac{1}{2}\mathbb{1}), \tag{3.116}$$

where $|\Psi\rangle$ is defined as before and $\alpha \geq \beta$ is assumed. Using the eigenvalues of $\mathrm{Tr}_{BD} |\Psi\rangle \langle\Psi|$, the first two terms of the vector in the left hand side of eq. (3.109) is

$$\lambda(\mathrm{Tr}_B |\phi\rangle\langle\phi|) \otimes \lambda(\mathrm{Tr}_{BD} |\Psi\rangle\langle\Psi|) = \frac{1}{8} \begin{pmatrix} \alpha^2(a+b+c+d)^2 \\ \alpha^2(a-b+c-d)^2 \\ \vdots \end{pmatrix}. \tag{3.117}$$

Note that the sum of the first two terms are always smaller than or equal to one hence for the majorization relation to hold

$$\begin{aligned} \frac{1}{8}\alpha^2(a+b+c+d)^2 &\leq \frac{1}{2}, \\ \alpha^2 &\leq \frac{4}{(a+b+c+d)^2}. \end{aligned} \tag{3.118}$$

The limits of this equation can be checked and gives expected results. If the states $|\psi_i\rangle$ are maximally entangled, $|\phi\rangle$ is maximally entangled too and if $|\psi_i\rangle$ are product states, $|\phi\rangle$ is not needed to succeed. The amount of entanglement that $|\phi\rangle$ should have for successful discrimination can be calculated using the entanglement entropy formula and for $|\psi_i\rangle$ having equal prior probabilities, numerical results show that the entanglement of $|\phi\rangle$ is always larger than the average entanglement of the states. An analytical solution however for the entanglement of $|\phi\rangle$ in terms of the average entanglement is not possible. Also, a one-way protocol couldn't be found that realizes these results and it is believed that a one-way protocol in which both parties carry out generalized measurements is impossible for the above relation and it is nearly impossible to express all the possible LOCC procedures in a mathematical way. However, this result is still valid in the sense that it shows that entanglement can be used as a resource to perform otherwise impossible results.

This concludes the discussion of quantum state discrimination. In this chapter, various strategies and different cases of the problem has been examined and it has been shown that entanglement can be used to help discriminate states. In the next chapter, the possibility of preserving the entanglement of the states during discrimination will be discussed.

CHAPTER 4

DISCRIMINATION WITH REMAINING ENTANGLEMENT

In many applications of quantum information theory, the entanglement of the quantum state is of crucial importance and it has many uses. It is therefore only natural to try to preserve the entanglement under various procedures. In the context of quantum state discrimination, this means answering the following question; is it possible to achieve discrimination of quantum states while preserving the entanglement? The answer is, yes if the parties are willing to use the entanglement of a preshared state. This is proven in a number of papers in literature, examples can be found in Cohen's works like [19] and Cohen also proves that for some specific sets of product states called as unextendible product bases, entanglement is also necessary to succeed [20].

The procedure of achieving discrimination with remaining entanglement also has a very intimate connection with the ability to realize non-local measurements. The connection is quite easy to grasp, imagine a set of multipartite entangled states $|\psi_i\rangle$, if the parties can come together and implement a projective measurement using the projectors $P_i = |\psi_i\rangle\langle\psi_i|$ and then separate, the states will remain entangled. If they cannot physically come together, one of the parties can teleport his part to the other party and they can realize a projective measurement projecting onto the states. This protocol will cost 1 ebit of entanglement, but a protocol using up less entanglement are possible [21].

For a procedure achieving discrimination with entanglement preservation, the upper bound on the cost is 2 ebits since the most inefficient way to achieve it is

to perform 2 quantum teleportations. Alice teleports her part of the states to Bob using 1 ebit of entanglement, Bob performs a projective measurement and teleports the respective part of the state to Alice, recovering the original state.

In this chapter, the lower bounds of entanglement for various cases will be calculated using techniques of majorization and the results will be discussed. In some cases, instead of the direct entanglement amounts, the bounds on the Schmidt coefficients of the preshared entangled state will be given and the values corresponding to the maximally entangled and product states will be discussed. As in the previous chapter, the protocols will not be constructed, only the inequalities that a protocol which can realize the discrimination will be given.

In the context of this work, preservation of entanglement is understood in the sense that the amount of entanglement the state has is the same after discrimination which means that the posterior states have the same Schmidt coefficients as the initial states. Two states with the same Schmidt coefficients are equivalent upto local unitary transformations or basis changes meaning that the posterior states can be rotated into the initial states without losing any entanglement.

The way to calculate the bounds on Schmidt coefficients using majorization is very similar to the calculation performed at the last section of chapter 2. The main difference lies in the posterior states. If the entanglement remaining in the states is of no concern, the calculation can proceed as in before otherwise, the relation has to be modified.

This idea can be illustrated in a simple example. Suppose Alice and Bob want to discriminate between the states

$$\begin{aligned} |\psi_1\rangle &= a\,|00\rangle + b\,|11\rangle\,, \\ |\psi_2\rangle &= c\,|01\rangle + d\,|10\rangle\,, \end{aligned} \tag{4.1}$$

where a, b, c, d are assumed to be real and $a \geq b$ and $c \geq d$. Alice and Bob share an entangled state

$$|\phi\rangle = \alpha\,|00\rangle + \beta\,|11\rangle\,. \tag{4.2}$$

A quick note, the only important parameters for the state $|\phi\rangle$ are the Schmidt coefficients. The choice of basis is not important since a simple rotation will transform between two different orthonormal bases.

To construct a majorization relation that completely characterizes such a procedure, it must be seen as an entanglement transformation process. If the parties can discriminate between the states, the following probabilistic entanglement transformation is implementable.

$$|\phi\rangle \otimes (\sqrt{p_1}\,|\psi_1\rangle + \sqrt{p_2}\,|\psi_2\rangle) \to |\psi_i\rangle\,, \text{ with probability } p_i. \tag{4.3}$$

The majorization relation then can be constructed as follows

$$\lambda(\phi) \otimes \lambda(\sqrt{p_1}\,|\psi_1\rangle + \sqrt{p_2}\,|\psi_2\rangle) \prec p_1\lambda(\psi_1) + p_2\lambda(p_2). \tag{4.4}$$

To find the lowest possible bound on the Schmidt coefficients of $|\phi\rangle$ The state

$$|\Psi\rangle = \sqrt{p_1}\,|\psi_1\rangle + \sqrt{p_2}\,|\psi_2\rangle \tag{4.5}$$

should be made a product state by a proper choice of the coefficients $\sqrt{p_1}, \sqrt{p_2}$. The reason is as follows; in the majorization relation, the coefficients of $|\phi\rangle$ will be multiplied by the coefficients of $|\Psi\rangle$, getting them closer to 0 and closer to each other which means higher entanglement. Therefore, to find the lowest possible bound, the state $|\Psi\rangle$ must be made product. In the first chapter, it was proven that if the reduced density matrix of a quantum state is rank 1, than the corresponding state will be a product state. Since the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are two dimensional, the reduced density matrix of $|\Psi\rangle$ will be 2×2. If the determinant of a 2×2 matrix vanishes, it means that the matrix in question is a rank 1 matrix and for reduced density operators, it means that the state is a product state.

The reduced density matrix for the state $|\Psi\rangle$ is

$$\begin{aligned}
\rho_A &= \mathrm{Tr}_B\,|\Psi\rangle\langle\Psi|\,, \\
&= \mathrm{Tr}_B[p_1\,|\psi_1\rangle\langle\psi_1| + p_2\,|\psi_2\rangle\langle\psi_2| + \sqrt{p_1p_2}(|\psi_1\rangle\langle\psi_2| + |\psi_2\rangle\langle\psi_1|)], \\
&= \begin{pmatrix} p_1a^2 + p_2c^2 & \sqrt{p_1p_2}(ad+bc) \\ \sqrt{p_1p_2}(ad+bc) & p_1b^2 + p_2d^2 \end{pmatrix}.
\end{aligned} \tag{4.6}$$

The condition that $\det \rho_A = 0$ gives

$$p_1 = \frac{cd}{ab+cd},\ p_2 = \frac{ab}{ab+cd}. \tag{4.7}$$

Since $|\Psi\rangle$ is a product state, the left side of the majorization relation becomes

$$\lambda(\phi) \otimes \lambda(\Psi) = \begin{pmatrix} \lambda(\phi) \\ 0 \end{pmatrix} \tag{4.8}$$

in block format. The relation, then becomes

$$\begin{pmatrix} \alpha^2 \\ \beta^2 \end{pmatrix} \prec \frac{cd}{ab+cd} \begin{pmatrix} a^2 \\ b^2 \end{pmatrix} + \frac{cd}{ab+cd} \begin{pmatrix} c^2 \\ d^2 \end{pmatrix}, \tag{4.9}$$

giving the following upper bound on α

$$\alpha \leq \frac{a^2cd + c^2ab}{ab+cd}. \tag{4.10}$$

The bound states that if the states $|\psi_1\rangle, |\psi_2\rangle$ are maximally entangled, then $|\phi\rangle$ is also maximally entangled and if $|\psi_1\rangle, |\psi_2\rangle$ are product than $|\phi\rangle$ is also a product state. Converting this bound into a bound for entanglement entropy is not trivial and numerical techniques will in general be needed but in terms of concurrence, the entanglement of the state $|\phi\rangle$ has a simple, elegant form

$$\mathcal{C}(\phi) = \sqrt{\mathcal{C}(\psi_1)\mathcal{C}(\psi_2)}, \tag{4.11}$$

it is simply the geometric mean of the entanglements of the states.

The same kind of majorization relation can be used to find a lower bound on the Schmidt coefficients of a preshared state in the case of a 4 state discrimination scheme where the states $|\psi_i\rangle$ to be discriminated form a complete orthonormal basis

$$\begin{aligned} |\psi_1\rangle &= a\,|00\rangle + b\,|11\rangle, \\ |\psi_2\rangle &= b\,|00\rangle - a\,|11\rangle, \\ |\psi_3\rangle &= c\,|01\rangle + d\,|10\rangle, \\ |\psi_4\rangle &= d\,|00\rangle - c\,|11\rangle, \end{aligned} \tag{4.12}$$

where $a, b, c, d \in \mathbb{R}$ and $a \geq b$, $c \geq d$. As before, the parties also share the state $|\phi\rangle = \alpha\,|00\rangle + \beta\,|11\rangle$ and $\alpha, \beta \in \mathbb{R}$, $\alpha \geq \beta$. The entanglement transformation procedure is $|\phi\rangle \otimes \sum_i \sqrt{p_i}\,|\psi_i\rangle \to |\psi_i\rangle$ with probability p_i and i identified, using the idea explained above. The majorization relation is constructed as

$$\lambda(\phi) \otimes \lambda(\sum_i \sqrt{p_i}\,|\psi_i\rangle) \prec \sum_i p_i \lambda(\psi_i). \tag{4.13}$$

However, the method of finding the values of p_i that make the determinant of the reduced density operator won't work here. Instead the state $|\Psi\rangle = \sum_i \sqrt{p_i}\,|\psi_i\rangle$ can be made product explicitly by construction.

Let $|\Psi\rangle = |A\rangle \otimes |B\rangle$ where

$$\begin{aligned} |A\rangle &= x_A\,|0\rangle + y_A\,|1\rangle\,, \\ |B\rangle &= x_B\,|0\rangle + y_B\,|1\rangle\,. \end{aligned} \tag{4.14}$$

The coefficients $\sqrt{p_i}$ are given by

$$\sqrt{p_i} = \langle \psi_i | A \otimes B \rangle \tag{4.15}$$

where $|A \otimes B\rangle$ is a shorthand for $|A\rangle \otimes |B\rangle$. Using eq. (4.15) the coefficients for the set of states in eq. (4.12) are found as

$$\begin{aligned} \sqrt{p_1} &= x_A x_B a + y_A y_B b, \\ \sqrt{p_2} &= x_A x_B b - y_A y_B a, \\ \sqrt{p_3} &= x_A y_B c + y_A x_B d, \\ \sqrt{p_4} &= x_A y_B d - y_A x_B c, \end{aligned} \tag{4.16}$$

which make the state $|\Psi\rangle = \sum_i \sqrt{p_i}\,|\psi_i\rangle$ a product state. The majorization relation in eq. (4.13) becomes

$$\begin{pmatrix} \lambda(\phi) \\ 0 \end{pmatrix} \prec \sum_i p_i \lambda(\psi_i) \tag{4.17}$$

since $|\Psi\rangle$ is a product state. Therefore

$$\lambda(\sum_i \sqrt{p_i}\,|\psi_i\rangle) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{4.18}$$

Since it was assumed that $\alpha \geq \beta$, only the first term of the column matrix in the left hand side of eq. (4.17), the inequality transforms into

$$\alpha^2 \leq a^2(x_A^2 x_B^2 + (1-x_A^2)^2(1-x_B^2)^2 + c^2(x_A^2(1-x_B^2)^2 + (1-x_A^2)^2 x_B^2) \tag{4.19}$$

after the insertion of the normalization conditions for the states $|A\rangle$ and $|B\rangle$.

In order to find the lowest possible upper bound on α^2, the right hand side of eq. (4.19) should be minimized. The minimization procedure is easy since the

equation is linear in x_A^2 and x_B^2 and a linear function has its extrema at the endpoints. This fact gives the bound on α^2 as

$$\alpha^2 \leq \min(a^2, c^2). \tag{4.20}$$

In other words, the state $|\phi\rangle$ should at least have the same amount of entanglement as the most entangled state in the set $\{|\psi_i\rangle\}$. Note that this bound is a lower bound for this task. The entanglement cost of such an entanglement preserving procedure can be higher than the bound found here which will be shown in the following part.

To find the lowest possible upper bound and the highest possible lower bound on the Schmidt coefficients of the preshared state $|\phi\rangle$ by using the method of making the state $|\Psi\rangle$ a product state, the construction of the product state $|\Psi\rangle$ is reconsidered. It is constructed as follows

$$|\Psi\rangle = \sum_{\mu} |\psi_\mu\rangle_{AB} \otimes |\varphi_\mu\rangle_{\bar{A}\bar{B}}\,. \tag{4.21}$$

where $A, \bar{A}, A', \ldots$ etc. represent various Hilbert spaces on Alice's side and the same goes for Bob. The procedure, as stated above can be considered as an entanglement transformation if Alice and Bob are able to go through with the discrimination. The entanglement transformation is as follows

$$|\phi\rangle_{AB} \otimes (\sum_{\mu} |\psi_\mu\rangle_{AB} \otimes |\varphi_\mu\rangle_{\bar{A}\bar{B}}) \rightarrow \frac{|\psi_\mu\rangle_{AB} \otimes |\varphi_\mu\rangle_{\bar{A}\bar{B}}}{\|\varphi_\mu\|} \tag{4.22}$$

with the index μ identified with probability $p_\mu = \|\varphi_\mu\|^2$, meaning that the discrimination is successful. The majorization relation for this process can be expressed as follows

$$\lambda(\phi) \otimes \lambda(\sum_{\mu} |\psi_\mu\rangle_{AB} \otimes |\varphi_\mu\rangle_{\bar{A}\bar{B}}) \prec \sum_{\mu} \|\varphi_\mu\|^2 \lambda(\frac{\psi_\mu \otimes \varphi_\mu}{\|\varphi_\mu\|}). \tag{4.23}$$

The same argument used in the preceding parts of this chapter applies here, to find the lowest possible upper bound, the state $|\Psi\rangle = \sum_\mu |\psi_\mu\rangle_{AB} \otimes |\varphi_\mu\rangle_{\bar{A}\bar{B}}$ must be made a product state, in this case the state $|\Psi\rangle$ must be unentangled in the $A\bar{A} : B\bar{B}$ cut to ensure that the state $|\Psi\rangle$ is unentangled between Alice and Bob.

A new type of product between kets and bras will be defined here

$$|\varphi_\mu\rangle = \langle\psi_\mu|\Psi\rangle\rangle. \tag{4.24}$$

If the state $|\Psi\rangle$ is unentangled in the $A\bar{A} : B\bar{B}$ cut, it can be expressed as $|\Psi\rangle = |u\rangle_{A\bar{A}} \otimes |v\rangle_{B\bar{B}}$. In order for this to be accomplished, the states $|u\rangle_{A\bar{A}}$ and $|v\rangle_{B\bar{B}}$ must be maximally entangled, this fact stems from the monogamy of entanglement. Since all maximally entangled states are unitarily equivalent to each other under LOCC, the states $|u\rangle, |v\rangle$ can be chosen as one of the bell states, choose them as

$$\begin{aligned} |u\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\sum_{i,j=0}^{1} \delta_{ij} |ij\rangle_{A\bar{A}}), \\ |v\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\sum_{i,j=0}^{1} \delta_{ij} |ij\rangle_{B\bar{B}}). \end{aligned} \tag{4.25}$$

Using eq. (4.25), the state $|\Psi\rangle$ can be re-expressed as

$$|\Psi\rangle = \frac{1}{2} \sum_{i,j,k,l=0}^{1} \delta_{ij}\delta_{kl} |ik\rangle_{AB} \otimes |jl\rangle_{\bar{A}\bar{B}} . \tag{4.26}$$

The states $|\psi_\mu\rangle$ can be expressed generally as

$$|\psi_\mu\rangle = \sum_{i,k} (\psi_\mu)_{ik} |ik\rangle_{AB} . \tag{4.27}$$

Then, the states $|\varphi_\mu\rangle$ can be found as

$$\begin{aligned} |\varphi_\mu\rangle = \langle\psi_\mu|\Psi\rangle\rangle &= \frac{1}{2} \sum_{i,j,k,l} (\psi_\mu)^\star_{ik}\delta_{ij}\delta_{kl} |jl\rangle_{\bar{A}\bar{B}} , \\ &= \frac{1}{2} \sum_{i,k} (\psi_\mu)^\star_{ik} |ik\rangle_{\bar{A}\bar{B}} , \\ |\varphi_\mu\rangle &= \frac{1}{2} \left|\psi^\star_\mu\right\rangle . \end{aligned} \tag{4.28}$$

Finally, the state $|\Psi\rangle$ becomes

$$|\Psi\rangle = \frac{1}{2} \sum_{\mu} |\psi_\mu\rangle_{AB} \otimes \left|\psi^\star_\mu\right\rangle_{\bar{A}\bar{B}} . \tag{4.29}$$

Inserting the expression for $|\varphi_\mu\rangle$, the majorization relation in eq. (4.23) becomes

$$\lambda(\phi) \prec \frac{1}{4} \sum_{\mu} \lambda(\psi_\mu) \otimes \lambda(\psi_\mu) \tag{4.30}$$

after using the facts that;

(i) $\|\varphi\| = \frac{1}{2}$,

(ii) $|\Psi\rangle$ is a product state hence $\lambda(\Psi) = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$,

(iii) $\lambda(\psi_\mu) = \lambda(\psi_\mu^\star)$.

Assuming that $a \geq b \geq 0$ and $c \geq d \geq 0$,

$$\begin{aligned} \lambda(\psi_1) = \lambda(\psi_2) &= \begin{pmatrix} a^2 \\ b^2 \end{pmatrix}, \\ \lambda(\psi_3) = \lambda(\psi_4) &= \begin{pmatrix} c^2 \\ d^2 \end{pmatrix}, \end{aligned} \tag{4.31}$$

the majorization relation can be written as

$$\lambda(\phi) \prec \frac{1}{2} \begin{pmatrix} a^4 + c^4 \\ a^2b^2 + c^2d^2 \\ a^2b^2 + c^2d^2 \\ b^4 + d^4 \end{pmatrix}. \tag{4.32}$$

It can be inferred from the above equation that the state $|\phi\rangle$ should have a Schmidt rank of at least 4 if a, b, c, d are all different from 0, otherwise the relation is not satisfiable by any means. The limiting cases that all the states are maximally entangled and all the states are product give the following results: $|\phi\rangle$ possesses 2 ebits of entanglement for the first case and $|\phi\rangle$ is a product state for the second case. The 2 ebit result is interesting but the explanation is quite simple. Suppose Alice and Bob, instead of realizing the discrimination by an entanglement transformation scheme opt to use quantum teleportation. Alice can teleport her part of the states to Bob using 1 ebit of entanglement and than Bob can implement a projective measurement to realize the discrimination of states. But, after the discrimination, the states are no longer shared between Alice and Bob and in order to preserve the states exactly as they were before, Bob needs to teleport the state back to Alice using 1 ebit. In total, it costs 2

ebits to discriminate the state while preserving it.

The minimum amount of entanglement that the state $|\phi\rangle$ possesses for successful discrimination can be calculated using the Schmidt coefficients as follows

$$\mathcal{E}(\phi) = -\sum_{i=1}^{4} \lambda_i \log_2 \lambda_i \tag{4.33}$$

but the expression is not one-to-one since different values of a, c will always yield different values for the entanglement amount of the state $|\phi\rangle$ but the same amount of average entanglement of the states to be discriminated. Instead, a numerical calculation can be performed to plot the entanglement cost with respect to the average entanglement of the states assuming that the states have equal prior probabilities and it is shown in figure 4.1.

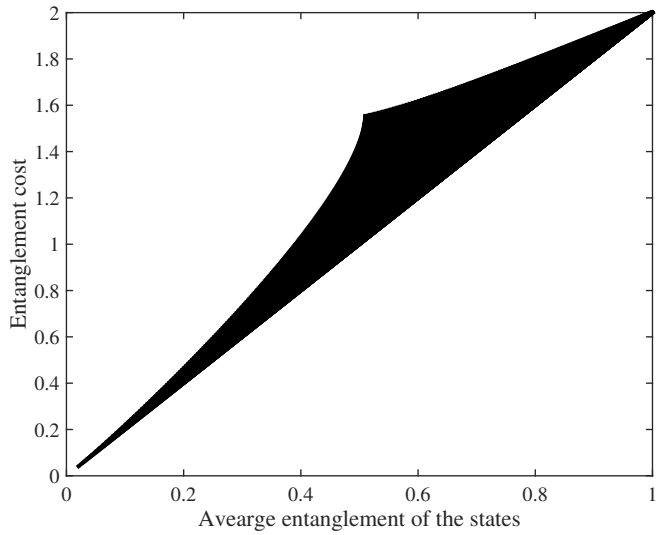

Figure 4.1: Plot of the entanglement cost versus the average entanglement of the states. The diagonal line is when all the states have equal entanglement and the cusp is when 2 of the states are maximally entangled and the others are product states. The entanglement cost is not a simple function of the average entanglement as the average entanglement is not a one-to-one function of the parameters a and c.

In this work, it is claimed that the bound on the Schmidt coefficients of $|\phi\rangle$ in eq. (4.32) is the best possible bound to be found using majorization to characterize the discrimination process.

This last result concludes the discussion of discrimination with remaining entanglement in this thesis. The work done here is in no ways a general calculation as the states to be discriminated are all in very specific forms and the protocols to achieve discrimination are not constructed explicitly. Some problems arise during the generalization of the calculations performed in this chapter. For Hilbert spaces having a dimensionality greater than 2, the expressions for Bell-like maximally entangled states and complete bases tend to get complicated very quickly. The results found here are presented to show that the idea is indeed possible and to introduce the readers to the usefulness of majorization in state discrimination problems. Majorization is a very powerful tool and it completely characterizes any pure state entanglement manipulation under LOCC.

CHAPTER 5

DISCUSSION AND CONCLUSION

There have been many achievements in the field of quantum state discrimination, especially for problems involving monopartite states. To this date, nearly all cases of monopartite state discrimination have been researched and solutions for specific cases have been found and optimized although to the knowledge of the author, a general, optimized solution hasn't been found yet. On the multipartite state discrimination front, necessary conditions that the states to be discriminated have been found[30] and the class of problems not solvable by LOCC but solvable by separable measurements have been characterized recently[31]. The idea of preserving entanglement after discrimination is somewhat new and some progress have been made. Cohen, in his papers[19, 20] introduced the idea but haven't calculated the amount of entanglement needed to achieve discrimination. On a very related subject, authors such as Bandyopadhyay [22, 21] has calculated the entanglement cost of non-local measurements, which can also be used to achieve perfect discrimination of entangled states with remaining entanglement after a teleportation or, if a number of states can be discriminated with remaining entanglement, a projective measurement projecting onto those states can be constructed. In this thesis, characterization of such procedures using majorization was performed and the exact bounds on the Schmidt coefficients of the preshared entangled state were found. This is the original part in this thesis.

The problem of discriminating 2 or 3 monopartite states was solved exactly in the literature during the early 2000s. The main ideas and the solutions

presented in the opening sections of the third chapter of this thesis are for 2 state problems but they can easily be generalized to 3 states. Using the QSS procedure, which generalizes UQSD, solutions for 3 state problems can be found but as the number of states to be discriminated increase, finding the optimal solution gets increasingly harder. As of now, there is no general, optimal solution for the state discrimination problem neither for UQSD nor for minimum error discrimination.

Also, in chapter three, majorization was introduced and it was shown that majorization can characterize state discrimination problems after the problems are reformulated as entanglement transformation problems. The most widely used and central majorization relation is

$$\lambda(\psi) \prec \sum_i p_i \lambda(\phi_i), \tag{5.1}$$

which governs a probabilistic entanglement transformation $|\psi\rangle \rightarrow |\phi_i\rangle$, with probability p_i. As a quick example, majorization was used to show indistinguishability of 4, orthogonal entangled qubit states with ease.

Majorization is a great tool to analyze processes which use entanglement as a resource. To that end, in chapter three, it was shown that, using up some entanglement, 2 parties can distinguish between 4 orthogonal, entangled qubit states. In all the cases examined in this thesis, protocols to achieve the process were not explicitly constructed due to difficulty of generalizing LOCC measurements.

The main aim of this thesis is to show that discrimination while preserving entanglement is possible. In chapter four, several cases of discrimination with remaining entanglement are inspected and it was shown that it is only possible if the parties agree upon using up some entanglement. Using majorization, the bounds on the Schmidt coefficients for the pre-shared state is found. Transforming these bounds into an analytical bounds for the entanglement of the preshared state in terms of the Schmidt coefficients of the states to be discriminated is not always possible but numerical methods were used to see the behavior.

As stated above, Bandyopadhyay and his collaborators have performed the entanglement cost of nonlocal measurements using a different method. The result

that was found in this thesis differs from their result but the explanation for the difference is straightforward. In their work, the procedure does not care about the preservation of the entanglement of the states thus the cost of a projective measurement projecting onto entangled states can be realized by a single teleportation at the worst case. As it was shown in the previous chapter, the cost of preserving entanglement after discrimination is always higher than the cost of a nonlocal measurement because of the need of another teleportation to preserve the original form of the states.

In this thesis, the close relationship of transformation of pure entangled states and quantum state discrimination was also shown. The relation is easy to see for the monopartite case, the QSS generalization of UQSD is just a probabilistic state transformation procedure. For multipartite states, the general idea is the same and it is because of this connection that the theory of majorization and Nielsen's theorem can be applied to multipartite state discrimination problems to completely characterize the discrimination procedure.

In conclusion, in this thesis, the state discrimination problem in quantum mechanics was presented and different cases of the problem were examined. The theory of majorization and its connections with the discrimination problem of multipartite states were also shown. Discrimination with entanglement preservation was also investigated and the possibility of such a procedure was shown and for some special cases, the procedure was completely characterized using majorization relations.

REFERENCES

[1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[2] N. Bohr. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 48:696–702, Oct 1935.

[3] D. Bohm and Y. Aharonov. Discussion of experimental proof for the paradox of einstein, rosen, and podolsky. *Phys. Rev.*, 108:1070–1076, Nov 1957.

[4] J. S. Bell. *Speakable and Unspeakable in Quantum Mechanics*. Cambridge University Press, second edition, 2004. Cambridge Books Online.

[5] 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.

[6] A. Zeilinger D. M. Greenberger, M. A. Horne. Going beyond bell's theorem. pages 69–72, 1989.

[7] CarlW. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969.

[8] A.S. Holevo. *Probabilistic and Statistical Aspects of Quantum Theory*. Publications of the Scuola Normale Superiore. Scuola Normale Superiore, 2011.

[9] I.D. Ivanovic. How to differentiate between non-orthogonal states. *Physics Letters A*, 123(6):257 – 259, 1987.

[10] Asher Peres. How to differentiate between non-orthogonal states. *Physics Letters A*, 128(1 - 2):19 –, 1988.

[11] D. Dieks. Overlap and distinguishability of quantum states. *Physics Letters A*, 126(5 - 6):303 – 306, 1988.

[12] S. M. Barnett A. Chefles. Quantum state seperation, unambiguous discrimination and exact cloning. *J. Phys. A: Math. Gen.*, 31(50), 1998.

[13] Jonathan Walgate, Anthony J. Short, Lucien Hardy, and Vlatko Vedral. Local distinguishability of multipartite orthogonal quantum states. *Phys. Rev. Lett.*, 85:4972–4975, Dec 2000.

[14] János A. Bergou. Discrimination of quantum states. *Journal of Modern Optics*, 57(3):160–180, 2010.

[15] Stephen M Barnett and Sarah Croke. On the conditions for discrimination between quantum states with minimum error. *Journal of Physics A: Mathematical and Theoretical*, 42(6):062001, 2009.

[16] S Virmani, M.F Sacchi, M.B Plenio, and D Markham. Optimal local discrimination of two multipartite pure states. *Physics Letters A*, 288(2):62 – 68, 2001.

[17] Somshubhro Bandyopadhyay. Entanglement and perfect discrimination of a class of multiqubit states by local operations and classical communication. *Phys. Rev. A*, 81:022327, Feb 2010.

[18] Sibasish Ghosh, Guruprasad Kar, Anirban Roy, Debasis Sarkar, Aditi Sen(De), and Ujjwal Sen. Local indistinguishability of orthogonal pure states by using a bound on distillable entanglement. *Phys. Rev. A*, 65:062307, Jun 2002.

[19] Scott M. Cohen. Local distinguishability with preservation of entanglement. *Phys. Rev. A*, 75:052313, May 2007.

[20] Scott M. Cohen. Understanding entanglement as resource: Locally distinguishing unextendible product bases. *Phys. Rev. A*, 77:012304, Jan 2008.

[21] Somshubhro Bandyopadhyay, Gilles Brassard, Shelby Kimmel, and William K. Wootters. Entanglement cost of nonlocal measurements. *Phys. Rev. A*, 80:012313, Jul 2009.

[22] 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.

[23] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046–2052, Apr 1996.

[24] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, Nov 1996.

[25] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:032314, Feb 2002.

[26] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83:436–439, Jul 1999.

[27] M. A. Nielsen. Characterizing mixing and measurement in quantum mechanics. *Physical Review A - Atomic, Molecular, and Optical Physics*, 63(2):1–11, 2001.

[28] Daniel Jonathan and Martin B. Plenio. Minimal conditions for local pure-state entanglement manipulation. *Phys. Rev. Lett.*, 83:1455–1458, Aug 1999.

[29] Michael A. Nielsen and Guifré Vidal. Majorization and the interconversion of bipartite states. *Quantum Info. Comput.*, 1(1):76–93, January 2001.

[30] Anthony Chefles. Condition for unambiguous state discrimination using local operations and classical communication. *Phys. Rev. A*, 69:050307, May 2004.

[31] Scott M. Cohen. Class of unambiguous state discrimination problems achievable by separable measurements but impossible by local operations and classical communication. *Phys. Rev. A*, 91:012321, Jan 2015.

APPENDIX A

PROBABILITY THEORY FUNDAMENTALS

Notions of probability theory are used extensively in quantum mechanics and quantum information theory. Some of the relations in this appendix have been used widely in this thesis and they should be introduced or proven. The aim of this short appendix is to introduce some basic rules, definitions and relations of probability theory.

The fundamental object in the theory of probability is the random variable. A random variable is defined in the following way, a random variable X takes the value x with probability $p(X = x)$. $p(X = x)$ will be called just $p(x)$ as a shorthand notation when the meaning is clear.

The joint probability notion is important and it is usually shown as $p(X = x, Y = y)$, or in shorthand $p(x, y)$ and it is the probability that $X = x$ and $Y = y$.

An important concept in probability theory is the conditional probability. It means the probability that $Y = y$ given $X = x$ and it is defined as

$$p(y|x) = \frac{p(x, y)}{p(x)}. \tag{A.1}$$

A very widely used rule in probability theory is the Bayes' rule. It relates the conditional probabilities $p(x|y)$ and $p(y|x)$ with the formula

$$p(x|y) = \frac{p(y|x)p(x)}{p(y)}. \tag{A.2}$$

The derivation is quite simple and uses the relation for joint probability

$$\begin{aligned} p(x,y) &= p(x)p(x|y) = p(y)p(y|x), \\ p(x)p(x|y) &= p(y)p(y|x), \\ p(x|y) &= \frac{p(y|x)p(x)}{p(y)}. \end{aligned} \tag{A.3}$$

Another widely used and important relation in the theory of probability is the law of total probability. It expresses the probability of $Y = y$ in terms of the probability of $X = x$ and $Y = y$ given $X = x$ with the following relation

$$p(y) = \sum_x p(y|x)p(x). \tag{A.4}$$

To see this result, the joint probability expression must be used. For different values of X, the joint probability can be written as

$$\begin{aligned} p(y, x_1) &= p(y|x_1)p(x_1), \\ p(y, x_2) &= p(y|x_2)p(x_2), \\ &\vdots \end{aligned} \tag{A.5}$$

Note that, if all these probabilities are summed for all possible values of X, it gives the joint probability of $Y = y$ and $X = x_1, x_2, \ldots, x_N$ which is just the probability $p(y)$.

The mean of a random variable, usually called the expectation value in quantum mechanics is the average of all the values a random variable X can have weighted with respect to the probabilities $p(x)$ and it is equal to

$$\langle X \rangle = \sum_x p(x)x. \tag{A.6}$$

This short review of probability theory is enough for the purposes of this work. The interested reader can refer to one of the many textbooks on this subject.