THE UNIVERSITY OF CALGARY

The Complexity of Separability Testing

by

Kristopher Luttmer

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

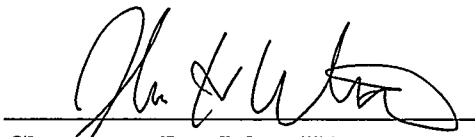
CALGARY, ALBERTA

July, 2005

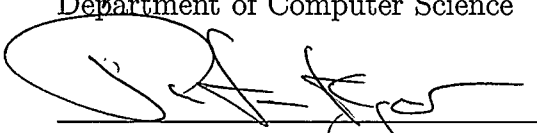
THE UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

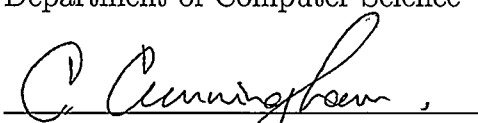
The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "The Complexity of Separability Testing" submitted by Kristopher Luttmer in partial fulfillment of the requirements for the degree of Master of Science.



Chairman, Dr. John Watrous
Department of Computer Science



Dr. Peter Høyer
Department of Computer Science



Dr. Clifton Cunningham
The Department of Mathematics and Statistics

July 11, 2005

Date

Abstract

In this thesis we examine the question of quantum separability testing. We begin by examining some of the properties of the set of separable quantum states and show how these properties can be used to create tests for separability. Unfortunately, the separability criteria we discuss in this thesis are unsatisfactory for one of two reasons. The first reason being that they are difficult or impossible to implement and the second reason is that they are not complete criterion, there are states which they cannot categorize as entangled or separable. The main purpose of this thesis is to give a rigorous proof of a result due to L. Gurvits [14] that quantum separability testing is NP hard.

Table of Contents

List of Figures

Chapter 1

Introduction

Entanglement is defined as a resource used in quantum computing because it can be used to perform tasks that cannot be done classically. For instance, entanglement is an essential ingredient in quantum teleportation and superdense coding. Before we can give a mathematical definition of entanglement we need to discuss what a quantum state is.

Definition 1.1. *A quantum state is a Hermitian matrix, with entries from the complex numbers, whose eigenvalues are non-negative real numbers that sum to one.*

With this definition of quantum state we can begin to investigate what an entangled state is. First, it is important to keep in mind that entangled states can only exist on composite systems. A composite system is, as the name suggests, a system that can be broken into smaller parts. For simplicity, let us consider a system composed of two parts, one part with Alice and another part with Bob. If Alice's system has dimension n and Bob's system has dimension m then a quantum state over the system shared by Alice and Bob will be a $nm \times nm$ quantum state. We will denote the set of all states in this system by $\mathsf{Pos}_1(\mathbb{C}^n \otimes \mathbb{C}^m)$.

Definition 1.2. *A quantum state $\rho \in \mathsf{Pos}_1(\mathbb{C}^n \otimes \mathbb{C}^m)$ is called separable if there exists quantum states $\sigma_1, \sigma_2, \ldots, \sigma_r \in \mathsf{Pos}_1(\mathbb{C}^n)$, $\xi_1, \xi_2, \ldots, \xi_r \in \mathsf{Pos}_1(\mathbb{C}^m)$ and a vector*

$p \in \mathbb{R}^r$, *with positive entries where* $\|p\|_1 = 1$ *such that*

$$\rho = \sum_{i=1}^{r} p[i]\, \sigma_i \otimes \xi_i.$$

If a state is not separable then it is entangled.

Example 1.3. *Consider the state*

$$\rho = \begin{bmatrix} \frac{1}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{bmatrix}$$

The state ρ *is separable because*

$$\rho = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$$

This is an easy example of a separable state. One can see almost immediately that the state is separable.

Example 1.4. *Now, consider the state*

$$\sigma = \begin{bmatrix} \frac{1}{8} & \frac{1}{8} & 0 & 0 \\ \frac{1}{8} & \frac{1}{4} & 0 & \frac{1}{8} \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{8} & 0 & \frac{1}{8} \end{bmatrix}$$

This is a slightly more difficult example. It is not at all clear if the state σ *is separable or entangled. However, if we examine the state closer we will find that*

$$\sigma = \frac{1}{4} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} + \frac{1}{4} \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

and is therefore separable.

Example 1.5. *Finally, let us examine the state*

$$\xi = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix}.$$

After some consideration one would find that it is impossible to write this state as a convex combination of separable states. This state is entangled.

Now that we know what entanglement is, we want to know how we can use it. As mentioned earlier, entanglement is a requirement for quantum teleportation. In quantum teleportation there are two parties, Alice and Bob, and Alice wants to use a classical communication channel to send an arbitrary physical quantum system to Bob. An example of quantum teleportation is Alice teleporting a photon to Bob.

Let us assume that Alice has performed some physical operation on a photon and she wants to send this photon to Bob. If Bob has a photon in the ground state then using quantum teleportation Alice and Bob can engage in a protocol such that at the end of the protocol Bob's photon has the same state as Alice's photon did at the start and the state of Alice's photon is changed to something else. Quantum teleportation allows Alice to send the state of an arbitrary physical system of small size to Bob using only two bits of communication and a shared entangled system. This is a very powerful procedure. Without quantum teleportation we would not be able to efficiently transmit quantum information.

One might wonder if it is possible to perform an operation like quantum teleportation without entanglement. For instance, if Alice knows the quantum state of her

photon, then she can send this to Bob. Bob could then use the quantum state to determine what operations to perform on his photon to create a photon identical to the photon that Alice wants to send him. Depending on the quantum state, the end result of this procedure might be the same as quantum teleportation and it would not require entanglement. However, there are many problems with this approach and we discuss four of them below.

First, even though we may know the quantum state it may still be difficult to create the quantum system. Alice may have more powerful equipment than Bob. Even though Bob knows the state of the photon he may be unable to perform the same operation on his photon as Alice did to her photon. Second, the positive semidefinite matrix may have irrational real or imaginary parts. Alice may only be able to send an approximation of her state to Bob. Bob would not end up with a photon in the exact same state as Alice's. Third, this approach will not work if Alice wants to send one photon of an entangled pair of photons to Bob. An entangled system is more than just the sum of the two parts and so this method cannot be used to distribute an entangled state. Finally, in general we do not know the quantum state that represents a physical system. Furthermore, we cannot determine the quantum state of a physical system without many copies of the physical system.

Now that we know what entanglement is and what we can use it for, we now come to the main part of this thesis. We answer the question, "Given a quantum state, is it possible to efficiently determine if the state is entangled or not?". When working with a quantum state, we can use any mathematical procedure to determine if the quantum state is entangled or not. Does this allow us to successfully test for

entanglement? We know from previous examples that the quantum state

$$\begin{bmatrix} \frac{1}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{bmatrix}$$

is separable and the state

$$\begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

is entangled. If we are given a new state, for instance,

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

can we tell if it is an entangled state or not? In this case the answer is yes.

There is a simple test we can perform on 4×4 quantum states that allows us to determine if they are entangled or not. This is called the partial transpose test. In the 4×4 case, we partition the quantum state into four 2×2 matrices and take the transpose of each matrix. Applying this technique to the above matrix gives the

following,

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \mapsto \left[\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \hline 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] \mapsto \left[\begin{array}{cc|cc} 0 & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & 0 & 0 \\ \hline 0 & 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & 0 \end{array}\right] \mapsto \begin{bmatrix} 0 & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & 0 \end{bmatrix}.$$

We can then determine if the quantum state is entangled by looking at the eigenvalues of the partial transposed state. In this case, the eigenvalues are $-1/2, 1/2, 1/2$, and $1/2$. Since one of the eigenvalues of the partial transposed state is negative we can conclude that the original state was entangled. This is a useful test in the case where our quantum state is a 4×4 matrix or even a 6×6 matrix. However, once our dimension grows beyond this point this test starts to fail. In dimensions above 6×6, there exists entangled states such that the partial transpose of these states will have only positive eigenvalues.

The partial transpose test fails to work in larger dimensions. To make matters even more difficult, quantum states are closed under convex combinations. If X and Y are quantum states of the same dimension and p is any real number between zero and one then $pX + (1-p)Y$ is also a quantum state. If we take the convex combination of a known entangled state and a known separable state, for instance,

$$p \begin{bmatrix} \frac{1}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{bmatrix} + (1-p) \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

then for some values of p we get an entangled state and for other values of p we get a separable state. Determining when we get an entangled state and when we get a

separable state is a very difficult task. In fact, there is no efficient test for all types of entanglement in dimensions above 6.

The first step to proving our main result is to introduce the concepts used in this thesis. Chapter 2 will introduce the background material needed to understand the results in this thesis. We start with a basic description of the notation we will be using and finish the chapter with a discussion of Neumark's theorem [1, 2] and quantum measurements.

Chapter 3 begins the discussion of how to test for entanglement. We cover the main criteria used when trying to determine if a quantum state is entangled or not. There are many tests for entanglement but we only cover the most general tests in Chapter 3. Specifically, we will look at the Woronowicz-Peres criterion [19, 30] and the Peres-Horodecki criterion [3, 19]. This thesis is only concerned with criteria which can help us decide if an unknown quantum state is entangled or not. We will not cover any tests for entanglement that assume any prior knowledge of the input state.

The next major topic we address is the size of the set of separable states. By studying the set of separable states we can learn more about the set of entangled states. Chapter 4 gives the radius of the smallest ball that completely contains the set of separable states and then covers a result due to L. Gurvits and H. Barnum [15] which shows how to construct balls of separable states that completely fit inside the set of separable states. This gives an upper and lower bound on the size of the set of separable states.

Chapter 5 covers some of the earliest results on the hardness of testing for entanglement. In this chapter, we talk about exact entanglement testing [25] and creating

a physical operation that will be able to test for entanglement.

Chapters 6 and 7 contain the result that is the purpose of this thesis. In these two chapters we examine the proof from [14] that shows separability testing is NP hard. Chapter 6 covers the Yudin-Nemirovsky theorem, which plays a vital role in the proof of hardness. Chapter 7 uses the results of Chapter 6 to complete the proof of hardness.

Chapter 2

Background

2.1 Linear Algebra

This thesis does not follow the standard notation used in quantum information. Here, we avoid the use of Dirac notation and instead use the traditional mathematical way of representing vectors and vector spaces, the main elements of quantum information. The notation, beyond the most basic, was used in lecture notes prepared by J. Watrous [28, 29]. Throughout this thesis we will only be dealing with finite dimensional vector spaces over the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$. Vector spaces will be denoted by calligraphic letters such as $\mathcal{F}$ and $\mathcal{G}$ and the notation $\mathcal{F} = \mathbb{C}^n$ means that $\mathcal{F}$ is a n-dimensional vector space over the field $\mathbb{C}$. Let $\mathcal{F} = \mathbb{C}^n$ and let $u \in \mathcal{F}$. Then $\bar{u}$ will be the vector whose entries are the complex conjugates of the entries of u, u^T will be the row vector that is the transpose of the column vector u and $u^* = \bar{u}^T$. The vector u will be indexed by square brackets $[\cdot]$, $u[i]$ will be the i'th entry in the column vector u. The following three vector norms will be used.

$\|u\|_1 = \sum_{i=1}^{n} \|u[i]\|$	The sum norm.
$\|u\|_2 = \sqrt{\sum_{i=1}^{n} \|u[i]\|^2}$	The Euclidean norm.
$\|u\|_\infty = \max\{\|u[i]\| : i = 1, \ldots, n\}$	The max norm.

For convenience, a norm with no subscript $\|\cdot\|$, will be used to denote the Euclidean norm and when we say unit vector we mean a vector with Euclidean norm equal to one. For any two vectors $u, v \in \mathcal{F}$ we will use the inner product $\langle u, v\rangle = u^* v$. The standard basis for $\mathcal{F}$ will be denoted by $\{e_1, \ldots, e_n\}$ where $e_i[i] = 1$ and $e_i[j] = 0$ for all $i \neq j$.

In many cases we will have to consider composite vector spaces. A composite vector space is a space that is composed of more than one part. If we take two vector spaces $\mathcal{G}$ and $\mathcal{H}$ then an example of a composite vector space would be $\mathcal{F} = \mathcal{G} \otimes \mathcal{H}$. If the set $\{u_1, \ldots, u_n\}$ is a basis for $\mathcal{G}$ and the set $\{v_1, \ldots, v_m\}$ is a basis for $\mathcal{H}$ then $\{u_i \otimes v_j : 1 \leq i \leq n \text{ and } 1 \leq j \leq m\}$ is a basis for $\mathcal{F}$ where $\otimes$ denotes the tensor product. It may be possible to write a vector space as a composition of different vector spaces, for instance $\mathbb{C}^{16} = \mathbb{C}^4 \otimes \mathbb{C}^4 = \mathbb{C}^8 \otimes \mathbb{C}^2$. We will call each possible composition a partition. In our example above, $\mathbb{C}^8 \otimes \mathbb{C}^2$ is one possible partitioning of the space $\mathbb{C}^{16}$. When dealing with composite systems we will always specify the way it is partitioned by simply writing the partition we are concerned about. If it does not matter whether the space is composite or not then we will simply write $\mathcal{F}$. There are also instances where we may consider a composite space composed of more than two systems such as $\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n$.

The Schmidt decomposition theorem is useful when working with vectors over composite vector spaces.

Theorem 2.1. Schmidt Decomposition Theorem

Let $\mathcal{F} = \mathbb{C}^n$ and $\mathcal{G} = \mathbb{C}^m$. For any vector $u \in \mathcal{F} \otimes \mathcal{G}$ there exists a positive integer $r \leq \min\{n, m\}$, two sets of orthonormal vectors $\{u_1, u_2, \ldots, u_r\} \subset \mathcal{F}$,

$\{v_1, v_2, \ldots, v_r\} \subset \mathcal{G}$, *and a vector* $p \in \mathbb{R}^n$ *with positive entries where* $\|p\|_2 = 1$ *such that*

$$u = \sum_{i=1}^{r} p[i]\, u_i \otimes v_i.$$

The entries of p are called the Schmidt coefficients of the vector u and the number of Schmidt coefficients is the Schmidt rank of u. The Schmidt coefficients and the Schmidt rank are both uniquely determined by u.

It will also be important in this thesis to consider the space of linear maps from one vector space to another. If $\mathcal{F}$ and $\mathcal{G}$ are vector spaces over the same field then $\mathsf{L}(\mathcal{F}, \mathcal{G})$ will denote the set of all linear maps from $\mathcal{F}$ to $\mathcal{G}$, with $\mathsf{L}(\mathcal{F})$ being shorthand notation for $\mathsf{L}(\mathcal{F}, \mathcal{F})$. If $\dim(\mathcal{F}) = n$ and $\dim(\mathcal{G}) = m$ then the space $\mathsf{L}(\mathcal{F}, \mathcal{G})$ can be identified with the set of all $m \times n$ matrices with entries from the base field of $\mathcal{F}$. The elements of $\mathsf{L}(\mathcal{F})$ will be called operators. $\mathsf{L}(\mathcal{F}, \mathcal{G})$ is also a vector space with standard basis $\{E_{i,j} : 1 \leq i \leq \dim(\mathcal{G}), 1 \leq j \leq \dim(\mathcal{F})\}$ where $E_{i,j}[i, j] = 1$ and $E_{i,j}[k, l] = 0$ when $i \neq k$ or $j \neq l$. We will be using the following norms on the vector space $\mathsf{L}(\mathcal{F}, \mathcal{G})$.

$\|X\|_{tr} = \mathrm{tr}\sqrt{X^*X}$	The Trace norm.
$\|X\|_F = \sqrt{\mathrm{tr}(X^*X)}$	The Frobenius norm.
$\|X\| = \max\{\|Xu\| : u \in \mathcal{F}, \|u\| = 1\}$	The Operator norm.

All our matrix norms listed above fulfill the standard norm axioms. In addition, we have that for any vector space $\mathcal{F}$ and operators $A, B \in \mathsf{L}(\mathcal{F})$

$$\begin{aligned} \|AB\|_{\mathrm{tr}} &\leq \|A\|_{\mathrm{tr}} \|B\|_{\mathrm{tr}} . \\ \|AB\|_F &\leq \|A\|_F \|B\|_F . \\ \|AB\| &\leq \|A\| \|B\| . \end{aligned}$$

The standard inner product we will use for matrices $X, Y \in \mathsf{L}(\mathcal{F}, \mathcal{G})$ is the Hilbert-Schmidt inner product $\langle X, Y \rangle = \mathrm{tr}\,(X^* Y)$.

Throughout this thesis we will encounter many different types of operators on vector spaces. For any operator $X \in \mathsf{L}(\mathcal{F})$ we have that X is normal if $XX^* = X^*X$, X is Hermitian if $X^* = X$, X is unitary if $XX^* = X^*X = I$ and, X is positive semidefinite if X is Hermitian and $u^*Xu \geq 0$ for all $u \in \mathcal{F}$. For all matrices $X \in \mathsf{L}(\mathcal{F}, \mathcal{G})$ the operator $Y = X^*X$ is a positive semidefinite operator. If X is a positive semidefinite operator then there exists a unique operator $Z = \sqrt{X}$ such that $X = Z^2$. If $X \in \mathsf{L}(\mathcal{F}, \mathcal{G})$ is not an operator but $X^*X = I$ then we say that X is norm preserving. This is justified because

$$\|Xu\|_2 = \sqrt{(Xu)^* Xu} = \sqrt{u^*X^*Xu} = \sqrt{u^*u} = \|u\|_2$$

where $u \in \mathcal{F}$ and X is either a unitary operator on $\mathcal{F}$ or a norm preserving matrix $X \in \mathsf{L}(\mathcal{F}, \mathcal{G})$. It is clear from the definitions that all Hermitian operators are normal and all unitary operators are normal. By definition, all positive semidefinite operators are Hermitian and hence normal. One theorem involving normal operators that we will exploit often in this thesis is the Spectral Decomposition Theorem.

Theorem 2.2. Spectral Decomposition Theorem

Let $\mathcal{F} = \mathbb{C}^n$. For any normal operator $X \in \mathsf{L}(\mathcal{F})$ with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$, there exists an orthonormal basis $\{u_1, u_2, \ldots, u_n\}$ for $\mathcal{F}$ such that

$$X = \sum_{i=1}^{n} \lambda_i u_i u_i^*.$$

The spectral decomposition is closely related to another theorem that we will use, the singular value decomposition theorem. In fact, if X is any positive semidefinite operator then the spectral decomposition of X is also a singular value decomposition of X. The difference being the singular value decomposition is more general.

Theorem 2.3. Singular Value Decomposition Theorem.

Let $\mathcal{F} = \mathbb{C}^n$, $\mathcal{G} = \mathbb{C}^m$ and let $X \in \mathsf{L}(\mathcal{F}, \mathcal{G})$ be any matrix with rank r. Then, there exists positive real numbers $s_1, s_2, \ldots, s_r$ and two sets of orthonormal vectors $\{u_1, u_2, \ldots, u_r\} \subset \mathcal{G}$, $\{v_1, v_2, \ldots, v_r\} \subset \mathcal{F}$, such that

$$X = \sum_{i=1}^{r} s_i u_i v_i^*.$$

For a matrix X, the positive real numbers s_i in the theorem are often called the singular values of X. They are equal to the square roots of the positive eigenvalues of XX^*. One important result about the singular values of a matrix is how they can be used to compute the matrix norms discussed earlier. In fact, for any matrix X we have that the trace norm of X is the sum norm of its singular values, the Frobenius norm of X is the Euclidean norm of its singular values and the operator norm of X is the max norm of the singular values of X. These facts can be used to show that for all $X \in \mathsf{L}(\mathcal{F}, \mathcal{G})$

$$\|X\| \leq \|X\|_F \leq \|X\|_{\mathrm{tr}}.$$

If X is normal then the absolute values of the eigenvalues of X are the singular values of X and, if X is a positive semidefinite operator the nonzero eigenvalues are the singular values. This makes computing matrix norms on normal operators simple as we only need to consider the eigenvalues of the operator.

The spectral radius of a matrix X is the max norm of the eigenvalues of X. If X is a normal operator then the spectral radius is equal to the operator norm. If X is not normal then the spectral radius may be less than the operator norm. In the special case where X is unitary, the singular values of X are all one. Conversely, if the singular values of an operator X are all one and X has full rank then X is unitary. More results about normal operators and matrix norms can be found in [18].

The following list introduces notation that we will use for the different sets of matrices.

$\mathsf{L}(\mathcal{F}, \mathcal{G})$	The set of linear maps from $\mathcal{F}$ to $\mathcal{G}$.
$\mathsf{U}(\mathcal{F})$	The set of Unitary operators acting on $\mathcal{F}$.
$\mathsf{Herm}(\mathcal{F})$	The set of Hermitian operators acting on $\mathcal{F}$.
$\mathsf{Pos}(\mathcal{F})$	The set of positive semidefinite operators acting on $\mathcal{F}$.
$\mathsf{Pos}_n(\mathcal{F})$	The set of positive semidefinite operators with trace n acting on $\mathcal{F}$.

$\mathsf{Pos}_1(\mathcal{F})$ is an important set as it is the set of all quantum states over the space $\mathcal{F}$.

In addition to the sets of operators above we will also need to consider sets of transformations which are linear maps from operators to operators. The set of transformations from $\mathsf{L}(\mathcal{F})$ to $\mathsf{L}(\mathcal{G})$ will be denoted by $\mathsf{T}(\mathcal{F}, \mathcal{G})$. Like the previous

sets we have defined, $\mathsf{T}(\mathcal{F})$ will be shorthand notation for $\mathsf{T}(\mathcal{F},\mathcal{F})$. The symbols Φ and Ψ will be used to denote transformations. Given $\Phi \in \mathsf{T}(\mathcal{F},\mathcal{G})$ we say that Φ is,

Trace Preserving	if $\mathrm{tr}(X) = \mathrm{tr}\left(\Phi(X)\right)$ for all $X \in \mathsf{L}(\mathcal{F})$.
Unital	if $\Phi(I) = I$.
Positive	if for all $X \in \mathsf{Pos}(\mathcal{F})$, $\Phi(X) \in \mathsf{Pos}(\mathcal{G})$.
Completely Positive	if $\Phi \otimes I$ is positive for any identity transformation I.

Given a transformation $\Phi \in \mathsf{T}(\mathcal{F},\mathcal{G})$ we define $\Phi^* \in \mathsf{T}(\mathcal{G},\mathcal{F})$ as the unique transformation such that

$$\langle X, \Phi(Y)\rangle = \langle \Phi^*(X), Y\rangle$$

for all $X \in \mathsf{L}(\mathcal{G})$ and $Y \in \mathsf{L}(\mathcal{F})$.

Using the above definitions we can prove a result about transformations that will be useful later in this thesis.

Lemma 2.4. *Let $\Phi \in \mathsf{T}(\mathcal{G},\mathcal{H})$. Then $(I \otimes \Phi^*) = (I \otimes \Phi)^*$ where I is the identity transformation over any space $\mathcal{F}$.*

Proof. Let $X \in \mathsf{L}(\mathcal{F}\otimes\mathcal{G})$ and $Y \in \mathsf{L}(\mathcal{F}\otimes\mathcal{H})$ be any operators. If $\dim(\mathcal{G}) = n$ and $\dim(\mathcal{H}) = m$ then we can represent X and Y as block matrices like so,

$$X = \sum_{i,j=1}^{n} X_{i,j} \otimes E_{i,j}$$
$$Y = \sum_{k,l=1}^{m} Y_{k,l} \otimes E_{k,l}.$$

Using this representation of X and Y we have,

$$\begin{aligned}
\langle X, (I \otimes \Phi^*) Y \rangle &= \sum_{k,l=1}^{m} \sum_{i,j=1}^{n} \langle X_{i,j} \otimes E_{i,j}, Y_{k,l} \otimes \Phi^*(E_{k,l}) \rangle \\
&= \sum_{k,l=1}^{m} \sum_{i,j=1}^{n} \langle X_{i,j}, Y_{k,l} \rangle \langle E_{i,j}, \Phi^*(E_{k,l}) \rangle \\
&= \sum_{k,l=1}^{m} \sum_{i,j=1}^{n} \langle X_{i,j}, Y_{k,l} \rangle \langle \Phi(E_{i,j}), E_{k,l} \rangle \\
&= \sum_{k,l=1}^{m} \sum_{i,j=1}^{n} \langle X_{i,j} \otimes \Phi(E_{i,j}), Y_{k,l} \otimes (E_{k,l}) \rangle \\
&= \langle (I \otimes \Phi) X, Y \rangle .
\end{aligned}$$

□

Transformations will be used throughout this thesis. They are important in the study of quantum systems and entanglement. For instance, any physically realizable operation can be described by a completely positive transformation. We will now give examples of two transformations that we will use later in this thesis.

Example 2.5. *Let $T \in \mathsf{T}(\mathcal{F})$ be the transpose transformation, $T(X) = X^T$. The transpose is a positive, trace preserving, unital transformation. It is not completely positive. When the transpose is combined with the identity transformation for any space $(T \otimes I) \in \mathsf{T}(\mathcal{F} \otimes \mathcal{G})$, we will call it the partial transpose.*

Example 2.6. *The partial trace is another example of a transformation. If we set $\{u_1, u_2, \ldots, u_n\}$ to be a basis for the space $\mathcal{G}$ then the partial trace over the space $\mathcal{G}$, $(I \otimes \mathrm{tr}) \in \mathsf{T}(\mathcal{F} \otimes \mathcal{G}, \mathcal{F})$, is defined by*

$$(I \otimes \mathrm{tr}) X = \sum_{i=1}^{n} (I \otimes u_i^*) X (I \otimes u_i) .$$

For the space $\mathcal{F} \otimes \mathcal{G}$, we will use shorthand notation $\mathrm{tr}_{\mathcal{G}}$ to mean $(I \otimes \mathrm{tr})$ and $\mathrm{tr}_{\mathcal{F}}$ to mean $(\mathrm{tr} \otimes I)$.

We can also consider more general mappings. The purpose of transformations was to map operators into operators. Now, we examine a mapping from transformations to linear maps.

If $\mathcal{F} = \mathbb{C}^n$ and $\mathcal{G} = \mathbb{C}^m$ then the Jamiolkowski Isomorphism [23] defines a linear bijection between the set of all transformations $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$ and the set of all operators $\mathsf{L}(\mathcal{F} \otimes \mathcal{G})$.

Definition 2.7. Jamiolkowski Isomorphism

For any transformation $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$ where $\dim(\mathcal{F}) = n$ we define

$$J(\Phi) = \sum_{i,j=1}^{n} E_{i,j} \otimes \Phi(E_{i,j}).$$

The mapping J defines a linear bijection from $\mathsf{T}(\mathcal{F}, \mathcal{G})$ to $\mathsf{L}(\mathcal{F} \otimes \mathcal{G})$.

The Jamiolkowski Isomorphism is important in the study of quantum entanglement because it maps sets of transformations to sets of operators that are important in the study of quantum entanglement. For instance, a transformation $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$ is completely positive if and only if $J(\Phi) \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$. We now prove a fact about the Jamiolkowski Isomorphism that will be useful later in this thesis.

Lemma 2.8. *[10] Let $\mathcal{F} = \mathbb{C}^n$ and $\mathcal{G} = \mathbb{C}^m$. For all $X \in \mathsf{L}(\mathcal{F})$, $Y \in \mathsf{L}(\mathcal{G})$ and $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$*

$$\left\langle \overline{X} \otimes Y, J(\Phi) \right\rangle = \left\langle Y, \Phi(X) \right\rangle.$$

Proof. From the definition of the Hilbert-Schmidt inner product we have that

$$\left\langle \overline{X} \otimes Y, J(\Phi) \right\rangle = \operatorname{tr} \left(\sum_{i,j=1}^{n} X^T E_{i,j} \otimes Y^* \Phi(E_{i,j}) \right).$$

Since $\operatorname{tr}(X^T E_{i,j} \otimes Y^* \Phi(E_{i,j})) = \operatorname{tr}(X^T E_{i,j}) \operatorname{tr}(Y^* \Phi(E_{i,j}))$ and $\operatorname{tr}(X^T E_{i,j}) = X_{j,i}^T$ we get

$$\begin{aligned} \left\langle \overline{X} \otimes Y, J(\Phi) \right\rangle &= \operatorname{tr} \left(\sum_{i,j=1}^{n} X_{j,i}^T \otimes Y^* \Phi(E_{i,j}) \right) \\ &= \operatorname{tr} Y^* \sum_{i,j=1}^{n} X_{i,j} \Phi(E_{i,j}) \\ &= \langle Y, \Phi(X) \rangle . \end{aligned}$$

□

It was shown in [10] that a transformation Φ is Hermitian preserving (maps Hermitian operators to Hermitian operators) if and only if $J(\Phi)$ is Hermitian. By writing any Hermitian matrix X as $X = Y - Z$ where Y and Z are positive operators we can see that any positive transformation must be Hermitian preserving. Therefore, $J(\Phi)$ is Hermitian for any positive transformation $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$. Also, in [8] it is shown that a transformation $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$ is completely positive if and only if $J(\Phi) \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$. Therefore, if $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$ is a positive but not completely positive transformation then $J(\Phi) \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G}) \setminus \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$. This is stated formally in the following lemma.

Lemma 2.9. *If $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$ is a positive but not completely positive transformation then $J(\Phi) \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G}) \setminus \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$.*

2.2 Convexity

An element u of a vector space $\mathcal{F}$ is called a convex combination of the elements $v_1, v_2, \ldots, v_m$ if there exists coefficients $\alpha_1, \alpha_2, \ldots, \alpha_m \in [0,1]$ such that,

$$u = \sum_{i=1}^{m} \alpha_i v_i \quad \text{and} \quad \sum_{i=1}^{m} \alpha_i = 1.$$

The convex hull of a set $S \subseteq \mathcal{F}$, denoted $\mathsf{Conv}(S)$, is the set consisting of all convex combinations of a finite number of elements in S. S is called convex if $S = \mathsf{Conv}(S)$. Geometrically, a convex set S has the property that for any two elements $u, v \in S$ all elements on the line segment from u to v are in S. If $S \subseteq \mathcal{F}$ is any convex set and $u, v_1, v_2 \in S$ then u is called an extreme point of S if $u = pv_1 + (1-p)v_2$ implies that $v_1 = v_2 = u$. For more on extreme points and their usefulness see Appendix A.

Given a convex set $S \subseteq \mathcal{F}$, we can consider the set of all positive linear combinations of elements in S. This results in a convex cone. We will call this the cone generated by the set S. If S is closed then so is the cone generated by S. Let $C \subseteq \mathcal{F}$ be a cone, then the dual of C, C^d, is the cone of all linear functionals that are nonnegative on C.

$$C^d = \{u \in \mathcal{F} : \langle u, v \rangle \geq 0 \text{ for all } v \in C\}.$$

Example 2.10. *The positive semidefinite operators on a space $\mathcal{F}$, $\mathsf{Pos}(\mathcal{F})$, form a cone. This cone is generated by the set $S = \mathsf{Pos}_1(\mathcal{F})$. The cone $\mathsf{Pos}(\mathcal{F})$ is also self dual, $\mathsf{Pos}(\mathcal{F})^d = \mathsf{Pos}(\mathcal{F})$.*

For any vector space $\mathcal{F}$, vector $u \in \mathcal{F}$ and positive real number ϵ, the set

$$\mathsf{B}(u, \epsilon) = \{v \in \mathcal{F} : \|u - v\| \leq \epsilon\}$$

is called the ball of radius ϵ with center u. For any set S where $S \subseteq \mathcal{F}$,

$$\mathsf{B}(S, \epsilon) = \{v \in \mathcal{F} : \|u - v\| \leq \epsilon \text{ for some } u \in S\}$$

is called the ball of radius ϵ around S. It is possible to use different norms in the above definitions. When doing, so we will use the subscript of the norm as a subscript of B. For instance, $\mathsf{B}_\infty(S, \epsilon)$ is the ball of radius ϵ around S with respect to the max norm.

2.3 Quantum Information

Associated with any quantum system is a vector space $\mathcal{F} = \mathbb{C}^n$. In this thesis we will only be concerned with finite dimensional vector spaces over the complex numbers. From now on unless otherwise specified $\mathcal{F}$ and $\mathcal{G}$ represent finite dimensional vector spaces over the complex numbers. A quantum state is a positive semidefinite operator acting on the space $\mathcal{F}$ with trace equal to one. From our notation in the previous section, $\mathsf{Pos}_1(\mathcal{F})$ is the set of all such states. It is common practice to denote members of $\mathsf{Pos}_1(\mathcal{F})$ by lower case Greek letters such as ρ and σ.

$$\mathsf{Pos}_1(\mathcal{F}) = \{\rho : \rho \in \mathsf{Pos}(\mathcal{F}), \mathrm{tr}(p) = 1\}$$

A pure quantum state, or simply a pure state $\rho \in \mathsf{Pos}_1(\mathcal{F})$ is a quantum state with rank one. Since the set of all positive semidefinite operators with trace equal to one can be expressed as a convex combination of rank one positive semidefinite operators with trace equal to one, it follows that the set $\mathsf{Pos}_1(\mathcal{F})$ is the convex hull of the set of pure states. A pure state $\rho \in \mathcal{F}$ can always be written as $\rho = uu^*$ for some unit vector $u \in \mathcal{F}$ and we will occasionally call such a vector u a pure state.

If a quantum state ρ has rank greater than one then ρ is often called a mixed state. Since every quantum state can be written as a convex combination of pure states, we can associate with any quantum state a set consisting of pairs of real numbers and pure states. We will call such a set an ensemble representing the state. If a state $\rho \in \mathsf{Pos}_1(\mathcal{F})$ can be written as

$$\rho = \sum_{i=1}^{n} p[i]\, u_i u_i^*$$

then one possible ensemble for ρ would be

$$\{(p[1], u_1), (p[2], u_2), \ldots, (p[n], u_n)\}.$$

For any given state ρ there exists many different ensembles for ρ.

A bipartite composite system is a vector space of the form $\mathcal{F} \otimes \mathcal{G}$. We will use the convention that the composite system is shared by two parties, Alice and Bob. In general, $\mathcal{F}$ corresponds to the space in which Alice's part of the system resides and $\mathcal{G}$ corresponds to Bob's part of the system. A more general concept of composite system is a multipartite composite system of the form $\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n$.

Definition 2.11. *A state $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ is called separable if there exist unit vectors $u_1, u_2, \ldots, u_n \in \mathcal{F}$, $v_1, v_2, \ldots, v_n \in \mathcal{G}$ and a vector $p \in \mathbb{R}^n$ with positive entries where $\|p\|_1 = 1$ such that*

$$\rho = \sum_{i=1}^{n} p[i]\, u_i u_i^* \otimes v_i v_i^*.$$

If a state is not separable then it will be called entangled.

It is possible that there is more than one way to write a vector space as a composite system. Each possibility could lead to a different conclusion on whether a

state is entangled or not. Because of this we need to specify which partition we are dealing with when we talk about an entangled state. We will only be concerned with separability with respect to the specified partition of the vector space, in the definition above this partition is $\mathcal{F} \otimes \mathcal{G}$. With this in mind, entangled and inseparable will mean the same thing. We will call a state separable even if it is entangled over some other partition of the space.

The definition of separable does extend to systems composed of more than two parts. In general, if a state $\rho \in \mathsf{Pos}_1(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n)$ can be written as a convex combination of states of the form $u_1u_1^* \otimes u_2u_2^* \otimes \cdots \otimes u_nu_n^*$ where $u_i \in \mathcal{F}_i$ then ρ is separable. States of the form $u_1u_1^* \otimes u_2u_2^* \otimes \cdots \otimes u_nu_n^*$ are called separable pure states. The concept of separability is also easily extended to positive semidefinite operators with trace not equal to one. If an operator $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ can be expressed as a convex combination of positive semidefinite operators with trace m of the form $uu^* \otimes vv^*$ for $u \in \mathcal{F}$ and $v \in \mathcal{G}$, then ρ is separable.

We will use the following notation for sets of separable operators.

$\mathsf{Sep}(\mathcal{F} \otimes \mathcal{G})$	The cone of separable operators in $\mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$.
$\mathsf{Sep}_m(\mathcal{F} \otimes \mathcal{G})$	The set of separable operators in $\mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$.
$\mathsf{Psep}_m(\mathcal{F} \otimes \mathcal{G})$	The set of separable operators with rank one in $\mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$.

Each of the above sets can be generalized to a multipartite system. For instance, if we have m parties then $\mathsf{Sep}(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m)$ represents the cone of separable states in $\mathsf{Pos}(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m)$.

Quantifying entanglement in a given state is a difficult task. There are many

proposed schemes which attempt to quantify entanglement and each have their own advantages and disadvantages. We will not cover measures of entanglement in this thesis but we will require one type of entanglement which most people seem to agree upon. This is the notion of a maximally entangled state.

Definition 2.12. *Let $\mathcal{F} = \mathcal{G} = \mathbb{C}^n$. A pure state $u \in \mathcal{F} \otimes \mathcal{G}$ is said to be maximally entangled if*

$$\mathrm{tr}_G\, uu^* = \frac{1}{n} I.$$

If $\dim(\mathcal{F}) = d$ then we call the state $\frac{1}{d} I \in \mathsf{Pos}_1(\mathcal{F})$ the maximally mixed state and denote it by $\mathbb{I}$. Note that if $\mathbb{I} \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ where $\dim(\mathcal{F}) = n$ and $\dim(\mathcal{G}) = m$ then $\mathbb{I} = \frac{1}{n} I \otimes \frac{1}{m} I$ and so $\mathbb{I} \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$.

Not only do maximally entangled states exist, but given two systems $\mathcal{F}$ and $\mathcal{G}$ of equal dimension it is possible to construct a basis for $\mathcal{F} \otimes \mathcal{G}$ consisting entirely of maximally entangled states. This is demonstrated in lemma 2.13.

Lemma 2.13. *Let $\mathcal{F} = \mathcal{G} = \mathbb{C}^n$. The set of vectors*

$$\{u_{a,b} : 0 \leq a, b \leq n-1\} \subset \mathcal{F} \otimes \mathcal{G}$$

is a maximally entangled orthonormal basis for $\mathcal{F} \otimes \mathcal{G}$ where

$$u_{a,b} = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} e^{\frac{2\pi i a j}{n}} e_{j+1} \otimes e_{(j+b)_n+1}.$$

The notation $(j+b)_n$ means that the addition $j+b$ is done modulo n.

Proof. Clearly, each vector is a unit vector. Also, each vector is maximally entangled

because

$$\begin{aligned}
\mathrm{tr}_{\mathcal{G}}\, u_{a,b}u_{a,b}^* &= \mathrm{tr}_{\mathcal{G}}\, \frac{1}{n}\sum_{j,k=0}^{n-1} e^{\frac{2\pi i a(j-k)}{n}} e_{j+1}e_{k+1}^* \otimes e_{(j+b)_n+1}e_{(k+b)_n+1}^* \\
&= \frac{1}{n}\sum_{j=0}^{n-1} e^{\frac{2\pi i a(j-j)}{n}} e_{j+1}e_{j+1}^* \\
&= \frac{1}{n} I.
\end{aligned}$$

Finally, we show that any two distinct vectors are orthonormal.

$$u_{a,b}^* u_{c,d} = \tfrac{1}{n}\textstyle\sum_{j,k=0}^{n-1} e^{\frac{-2\pi i a j}{n}} e^{\frac{2\pi i c k}{n}} e_{j+1}^* e_{k+1} \otimes e_{(j+b)_n+1}^* e_{(k+d)_n+1}$$

$$= \begin{cases} 1 & \text{if } a{=}c \text{ and } b{=}d \\ 0 & \text{otherwise.} \end{cases}$$

□

2.4 Measurements and Neumark's Theorem

Any physically realizable operation can be described by a completely positive trace preserving transformation. This is an important fact as it allows us to determine what operations can be performed on a quantum system in a laboratory. We have a representation of completely positive maps due to M.D. Choi [8].

Lemma 2.14. *[8] If $\Phi \in \mathsf{T}(\mathcal{F},\mathcal{G})$ is a completely positive transformation then there exists operators $A_1, A_2, \ldots, A_n \in \mathsf{L}(\mathcal{F},\mathcal{G})$ for $n = \dim(\mathcal{F}\otimes\mathcal{G})$ so that*

$$\Phi(X) = \sum_{i=1}^{n} A_i X A_i^*$$

for all $X \in \mathsf{L}(\mathcal{F})$. *Additionally, if* Φ *is trace preserving then*

$$\sum_{i=1}^{n} A_i^* A_i = I.$$

A measurement is one example of a completely positive trace preserving transformation, and therefore a physically realizable operation. A measurement of a system over $\mathcal{F}$ is a collection of operators $\{A_1, A_2, \ldots, A_n\} \subset \mathsf{L}(\mathcal{F})$ such that

$$\sum_{i=1}^{n} A_i^* A_i = I.$$

The possible outcomes of a measurement will be labeled by indices to the operators that define the measurement. For instance, if we measure a state $\rho \in \mathsf{Pos}_1(\mathcal{F})$ with the above measurement, then the possible outcomes are labeled by integers from 1 to n. The resulting state of outcome i is

$$\frac{A_i \rho A_i^*}{\mathrm{tr}(A_i \rho A_i^*)}.$$

In some cases, we are only concerned with the probability of a given outcome and not the resulting state. For a given measurement $\{A_1, \ldots, A_n\}$ on a quantum state ρ, the probability of outcome i is $\mathrm{tr}(A_i \rho A_i^*) = \mathrm{tr}(A_i^* A_i \rho)$. Therefore, we only need to specify the operators $B_i = A_i^* A_i$. With the set $\{B_1, B_2, \ldots, B_n\}$ we can compute the probability of outcome i when measuring ρ by computing $\mathrm{tr}(B_i \rho)$. When we only specify the positive operators required to determine the probability of each outcome we will call this a POVM (positive operator valued measurement).

A projector onto a space $\mathcal{F}$ is an operator of the form

$$P = \sum_{i=1}^{n} u_i u_i^*$$

where $\{u_1, \ldots, u_n\} \subset \mathcal{F}$ is an orthonormal set of vectors. If all the elements of a measurement are projections then we will refer to the measurement as a projective measurement. Projective measurements are easier to work with because $P^2 = P$ and $P^* = P$ for all projectors P. Although not all measurements are projective measurements, the following theorem shows that we can simulate a general measurement with a projective measurement in a larger space.

Theorem 2.15. Neumark's Theorem *[1, 2]*

Given any measurement $\{A_1, A_2, \ldots, A_n\} \subset \mathsf{L}(\mathcal{F})$ *there exists a vector space* $\mathcal{G}$*, a norm preserving linear map* $U \in \mathsf{L}(\mathcal{F}, \mathcal{F} \otimes \mathcal{G})$*, and a set of orthogonal projectors* $\{P_1, P_2, \ldots P_n\} \subset \mathsf{L}(\mathcal{F} \otimes \mathcal{G})$ *where* $\sum_{i=1}^{n} P_i = I$ *so that for all operators* $X \in \mathsf{L}(\mathcal{F})$ *and* $1 \leq i \leq n$ *we have*

$$\mathrm{tr}_{\mathcal{G}}\, P_i U X U^* P_i^* = A_i X A_i^* \text{ and } \mathrm{tr}\, P_i U X U^* P_i^* = \mathrm{tr}\, A_i X A_i^*.$$

Proof. Let $\mathcal{G} = \mathbb{C}^n$. We define U and P_i as

$$U = \sum_{i=1}^{n} A_i \otimes e_i \quad \text{and} \quad P_i = I \otimes E_{i,i}.$$

The matrix U is norm preserving because

$$U^* U = \sum_{i,j=1}^{n} A_i^* A_j \otimes e_i^* e_j = \sum_{i=1}^{n} A_i^* A_i = I.$$

It is also easy to see that the projectors P_i are orthogonal. For any $1 \leq i \neq j \leq n$ we have

$$\langle P_i, P_j \rangle = \mathrm{tr}\,(P_i P_j) = \mathrm{tr}\,(I \otimes E_{i,i} E_{j,j}) = 0.$$

Notice that

$$\begin{aligned}
\mathrm{tr}_{\mathcal{G}}\, P_i U X U^* P_i^* &= \mathrm{tr}_{\mathcal{G}}\,(I \otimes E_{i,i}) \left(\sum_{j=1}^{n} A_j \otimes e_j \right) X \left(\sum_{k=1}^{n} A_k^* \otimes e_k^* \right) (I \otimes E_{i,i}) \\
&= \mathrm{tr}_{\mathcal{G}}\,(A_i \otimes e_i)\, X\, (A_i^* \otimes e_i^*) \\
&= A_i X A_i^*
\end{aligned}$$

where the second line follows from the first because $E_{i,i} e_j = 0$ if $i \neq j$. This establishes the first equality.

Applying the trace to a system $\mathcal{F} \otimes \mathcal{G}$ is the same as applying $\mathrm{tr}_{\mathcal{G}}$ followed by $\mathrm{tr}_{\mathcal{F}}$. Therefore, we have that $\mathrm{tr}\, P_i U X U^* P_i^* = \mathrm{tr}\, A_i X A_i^*$ as desired. □

When we want to apply a projective measurement instead of a more general measurement we simply construct the projectors P_i and the norm preserving matrix U as shown in Neumark's theorem. We then map the input operator $X \in \mathsf{L}(\mathcal{F})$ to $UXU^* \in \mathsf{L}(\mathcal{F} \otimes \mathcal{G})$. It is important to note that the dimension of the space $\mathcal{G}$ is not too large. In fact, it is no larger than the dimension of the original space $\mathcal{F}$ and so the dimension of $\mathcal{F} \otimes \mathcal{G}$ is at most twice as big as the dimension of $\mathcal{F}$. After mapping X to UXU^* we apply the projective measurement. After the projective measurement, we want to take the output state to what would be the output state in our original space $\mathsf{L}(\mathcal{F})$. We can easily do this by applying the partial trace over the space $\mathcal{G}$. Once this is complete, we will have simulated the general measurement with a projective measurement.

If we are only concerned with the probability of a given outcome, that is we want to perform a POVM, then Neumark's theorem tells us that it is sufficient to look at a projective POVM on a larger space. The following corollary tells us exactly how to take a general POVM to a projective POVM on a larger space.

Corollary 2.16. *[29] For any POVM* $\{B_1, B_2, \ldots, B_n\}$ *there exists a space* $\mathcal{G}$*, a norm preserving linear map* $U \in \mathsf{L}(\mathcal{F}, \mathcal{F} \otimes \mathcal{G})$*, and a set of orthogonal projectors* $\{P_1, P_2, \ldots P_n\} \subset \mathsf{L}(\mathcal{F} \otimes \mathcal{G})$ *where* $\sum_{i=1}^{n} P_i = I$ *so that for all* $1 \leq i \leq n$ *we have*

$$U^* P_i U = B_i.$$

Proof. Set $A_i = \sqrt{B_i}$. Then, by Neumark's theorem we have

$$\operatorname{tr} P_i U X U^* P_i = \operatorname{tr} A_i X A_i^*$$

for any $X \in \mathsf{L}(\mathcal{F})$. Using the cyclic properties of the trace gives

$$\begin{aligned} \operatorname{tr} P_i U X U^* P_i = \operatorname{tr} A_i X A_i^* \quad &\Longleftrightarrow \quad \operatorname{tr} P_i U X U^* = \operatorname{tr} A_i^* A_i X \\ &\Longleftrightarrow \quad \operatorname{tr} U^* P_i U X = \operatorname{tr} A_i^* A_i X \\ &\Longleftrightarrow \quad \operatorname{tr} U^* P_i U X = \operatorname{tr} B_i X. \end{aligned}$$

Both $U^* P_i U$ and B_i are Hermitian and so we have that for any $X \in \mathsf{L}(\mathcal{F})$

$$\langle U^* P_i U, X \rangle = \langle B_i, X \rangle .$$

This implies that $U^* P_i U = B_i$. □

This concludes the background section of this thesis. In the next section we examine criteria for determining if a given quantum state is entangled or not.

Chapter 3

Separability Criterion

There are many different criteria one can use to test for separability, each with their own advantages and disadvantages. In some cases, the criteria is very easy to apply but does not work very effectively. For example, the Peres-Horodecki criterion is very simple to execute but there are some entangled states that it cannot detect. Conversely, criteria that are accurate are unfortunately difficult to apply. The Woronowicz-Peres criterion is a necessary and sufficient criterion for separability but it is not feasible to test for separability in this way. This chapter will introduce the separability criterion that we will require later in this thesis.

The first thing we will cover in this chapter is a lemma that shows that the set of separable states is a compact subset of $\mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$. For background information about this lemma and where it applies in quantum information see Appendix C.

Lemma 3.1. *[26] For all operators* $\rho, \sigma \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$

$$\|\mathrm{tr}_{\mathcal{F}}\,\rho - \mathrm{tr}_{\mathcal{F}}\,\sigma\|_{\mathrm{tr}} \leq \|\rho - \sigma\|_{\mathrm{tr}} \qquad \textit{and} \qquad \|\mathrm{tr}_{\mathcal{G}}\,\rho - \mathrm{tr}_{\mathcal{G}}\,\sigma\|_{\mathrm{tr}} \leq \|\rho - \sigma\|_{\mathrm{tr}}\,.$$

We require lemma 3.1 in the proof that the set of separable states is compact. It relates the distance between two operators to the distance between the partial trace of those operators. Since the partial trace is comparable to throwing away part of the operator, the distance between two operators ρ and σ must always be greater than or equal to the distance between the partial trace of ρ and the partial trace of σ. Lemma 3.1 states this in a more formal manner.

Lemma 3.2. *Let $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$. If $\mathrm{tr}_{\mathcal{G}}(\rho) = uu^*$ for some unit vector $u \in \mathcal{F}$ and $\mathrm{tr}_{\mathcal{F}}(\rho) = vv^*$ for some unit vector $v \in \mathcal{G}$ then ρ is a separable pure state.*

Proof. If $\mathrm{tr}_{\mathcal{F}}(\rho) = vv^*$ then by the definition of the partial trace we can represent ρ as $\rho = \sigma_1 \otimes vv^*$ for some $\sigma_1 \in \mathsf{Pos}_1(\mathcal{F})$. Similarly, if $\mathrm{tr}_{\mathcal{G}}(\rho) = uu^*$ we can represent ρ as $\rho = uu^* \otimes \sigma_2$ for some $\sigma_2 \in \mathsf{Pos}_1(\mathcal{G})$. Therefore, it must be the case that $\rho = uu^* \otimes vv^*$ for some unit vectors $u \in \mathcal{F}$ and $v \in \mathcal{G}$, and so ρ is a separable pure state. □

We now have the results required to prove that the set of separable states is compact.

Theorem 3.3. $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ *is a compact subset of* $\mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$.

Proof. From [24] (Section 5.3, theorem 14), the convex hull of a compact set must be compact. Additionally, the Heine-Borel theorem, theorem C.6 tells us that if $\mathsf{Psep}_1(\mathcal{F} \otimes \mathcal{G})$ is closed and bounded then it must be compact. Therefore, to prove the lemma all we need to show is that $\mathsf{Psep}_1(\mathcal{F} \otimes \mathcal{G})$ is a closed and bounded subset of $\mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$. We know that the trace norm of a positive semidefinite operator is just the sum of the eigenvalues and so the set $\mathsf{Psep}_1(\mathcal{F} \otimes \mathcal{G})$ is bounded.

To see that $\mathsf{Psep}_1(\mathcal{F} \otimes \mathcal{G})$ is closed let $\{u_i u_i^* \otimes v_i v_i^*\}$ be a sequence in $\mathsf{Psep}_1(\mathcal{F} \otimes \mathcal{G})$ that converges in $\mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$. We need to show that $\{u_i u_i^* \otimes v_i v_i^*\}$ converges to an element of $\mathsf{Psep}_1(\mathcal{F} \otimes \mathcal{G})$. Since $\{u_i u_i^* \otimes v_i v_i^*\}$ converges, we get that for all $\epsilon > 0$ there exists an operator $\xi \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$ and a integer $N \in \mathbb{N}$, such that for all $n \geq N$ we have that

$$\left\| u_n u_n^* \otimes v_n v_n^* - \xi \right\|_{\mathrm{tr}} \leq \epsilon.$$

Combining this fact with lemma 3.1 we can conclude that for all $n \geq N$,

$$\|u_n u_n^* - \mathrm{tr}_{\mathcal{G}}\,\xi\|_{\mathrm{tr}} \leq \epsilon \text{ and } \|v_n v_n^* - \mathrm{tr}_{\mathcal{F}}\,\xi\|_{\mathrm{tr}} \leq \epsilon.$$

This implies that $\{u_i u_i^*\}$ is a convergent sequence in $\mathsf{Herm}(\mathcal{F})$ and $\{v_i v_i^*\}$ is a convergent sequence in $\mathsf{Herm}(\mathcal{G})$. First, we note that $\mathrm{tr}_{\mathcal{F}}\,\xi$ and $\mathrm{tr}_{\mathcal{G}}\,\xi$ must have trace one. If it does not have trace one then there exists some $\delta > 0$ such that $\|u_n u_n^* - \mathrm{tr}_{\mathcal{G}}\,\xi\|_{\mathrm{tr}} \geq \delta$ and this is a contradiction to the work done above. We can see this by noting that the trace norm of a Hermitian matrix X is the sum norm of the eigenvalues of X. If $\mathrm{tr}_{\mathcal{F}}\,\xi$ does not have unit trace then the smallest value for the trace norm would be $|1-k|$ where k is the trace of $\mathrm{tr}_{\mathcal{F}}\,\xi$.

Recall from Chapter 2 that $\|X\|_F \leq \|X\|_{\mathrm{tr}}$ for all operators $X \in \mathsf{L}(\mathcal{F})$. We will now show that $\mathrm{tr}_{\mathcal{G}}\,\xi \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ and $\|u_n u_n^* - \mathrm{tr}_{\mathcal{G}}\,\xi\|_F \geq \delta$ where $1-\delta$ is the largest eigenvalue of $\mathrm{tr}_{\mathcal{G}}\,\xi$. Since, $\{u_n u_n^*\}$ is a convergent sequence and it converges to $\mathrm{tr}_{\mathcal{G}}\,\xi$, it must be the case that $\delta = 0$ and so $\mathrm{tr}_{\mathcal{G}}\,\xi = uu^*$ for some unit vector $u \in \mathcal{F}$. Similarly, $\mathrm{tr}_{\mathcal{F}}\,\xi = vv^*$ for some unit vector $v \in \mathcal{G}$. Then, by lemma 3.2, we have $\xi = uu^* \otimes vv^*$ for some unit vectors $u \in \mathcal{F}$ and $v \in \mathcal{G}$. Therefore, the sequence $\{u_i u_i^* \otimes v_i v_i^*\}$ converges to a pure separable state and the set $\mathsf{Psep}_1(\mathcal{F} \otimes \mathcal{G})$ is closed. We now show that $\|u_n u_n^* - \mathrm{tr}_{\mathcal{G}}\,\xi\|_F \geq \delta$ where $1-\delta$ is the largest eigenvalue of $\mathrm{tr}_{\mathcal{G}}\,\xi$.

Fix any n and let $X = u_n u_n^* - \mathrm{tr}_{\mathcal{G}}\,\xi$. Since X is Hermitian we have that $XX^* = X^2$ and so $\|X\|_F = \sqrt{\mathrm{tr}(X^2)}$. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the eigenvalues of $\mathrm{tr}_{\mathcal{G}}\,\xi$. Then,

$$\mathrm{tr}_{\mathcal{G}}\,\xi = \sum_{\lambda_i > 0} \lambda_i w_i w_i^* - \sum_{\lambda_i < 0} |\lambda_i| w_i w_i^*$$

where $\{w_1, w_2, \ldots, w_k\} \subset \mathcal{F}$ is an orthonormal set of vectors. We then have

$$\begin{aligned} X^2 &= u_n u_n^* + \sum_{i=1}^{k} \lambda_i^2 w_i w_i^* \\ &- \sum_{\lambda_i>0} \lambda_i |\langle u, w_i\rangle| u w_i^* - \sum_{\lambda_i>0} \lambda_i |\langle u, w_i\rangle| w_i u^* \\ &+ \sum_{\lambda_i<0} \lambda_i |\langle u, w_i\rangle| u w_i^* + \sum_{\lambda_i<0} \lambda_i |\langle u, w_i\rangle| w_i^* u \end{aligned}$$

and so

$$\mathrm{tr}(X^2) = 1 + \sum_{i=1}^{k} \lambda_i^2 - 2 \sum_{\lambda_i>0} \lambda_i |\langle u, w_i\rangle|^2 + 2 \sum_{\lambda_i<0} \lambda_i |\langle u, w_i\rangle|^2.$$

Since we want this value to be small we can take $\sum_{\lambda_i<0} \lambda_i |\langle u, w_i\rangle|^2 = 0$. This means that we only need to consider the case where $\mathrm{tr}_{\mathcal{G}} \xi \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$. Without loss of generality, we let $\lambda_1 = 1 - \delta$ be the largest eigenvalue of $\mathrm{tr}_{\mathcal{G}} \xi$. Then the minimum of $\mathrm{tr}(X^2)$ occurs when $\langle u, w_1\rangle = 1$ and so

$$\mathrm{tr}(X^2) \geq 1 + \sum_{i=1}^{k} \lambda_i^2 - 2 + 2\delta \geq 1 + (1-\delta)^2 - 2 + 2\delta = \delta^2.$$

Therefore, as stated above we have $\|X\|_F \geq \delta$ where $1 - \delta$ is the largest eigenvalue of $\mathrm{tr}_{\mathcal{G}} \xi$. □

3.1 Pure State Entanglement

All quantum states can be expressed as a convex combination of pure states and so to understand entanglement in general it will help to start with pure state entanglement. In the bipartite case, it is quite easy to determine if a pure state is entangled or not. We can use the Schmidt decomposition of a pure state $u \in \mathcal{F} \otimes \mathcal{G}$ to determine if u is separable or not. Since the Schmidt decomposition is easy to compute we can efficiently determine if a pure state is separable or entangled.

Lemma 3.4. *Let $u \in \mathcal{F} \otimes \mathcal{G}$ be a pure state of a bipartite system and let*

$$u = \sum_{i=1}^{r} s_i v_i \otimes w_i$$

be a Schmidt decomposition of u. Then, u is separable if and only if the Schmidt rank of u is one.

Proof. If the Schmidt rank of u is one, $r = 1$, then clearly u is separable. If u is separable, $u = v \otimes w$ is a Schmidt decomposition of u with Schmidt rank one. □

With a criterion as simple as the above case one might ask whether we can extend this criterion to multipartite states. This question reduces down to the problem of extending the definition of the Schmidt decomposition from a bipartite system to a multipartite system. For instance, if we could show that every pure state $u \in \mathcal{F} \otimes \mathcal{G} \otimes \mathcal{H}$ can be written in the form

$$u = \sum_{i=1}^{r} s_i v_i \otimes w_i \otimes x_i$$

then we could have a result analogous to lemma 3.4 for the multipartite case. However, it was shown in [27] that in general, an arbitrary $u \in \mathcal{F} \otimes \mathcal{G} \otimes \mathcal{H}$ cannot be written in the form above. Unfortunately, for multipartite pure state entanglement we do not know of a simple criterion to test for entanglement. Therefore, we must resort to the more general criteria that is used to determine if a mixed state is entangled or not.

3.2 Bipartite Mixed State Entanglement

Unlike the pure state case where there is a simple and straightforward test for entanglement, mixed state entanglement is more difficult to deal with. One might think

that if we can obtain an ensemble that represents ρ, then we can immediately tell if ρ is entangled or not by looking at the Schmidt decomposition of each of the pure states in the ensemble. There is a problem with this approach. For any mixed state ρ there exist an infinite number of different ensembles representing ρ. If a mixed state ρ is separable then there may exist ensembles of ρ that contain entangled states. In fact, it may be the case that the ensemble of a separable mixed state ρ will consist entirely of entangled pure states. However, if we can find an ensemble of ρ that only contains separable pure states then ρ must be separable.

Searching for an ensemble of ρ that contains only separable pure states may result in demonstrating that ρ is separable. However, it is not useful as a separability criterion because there is an infinite number of ensembles representing ρ. Checking an infinite number of ensembles is infeasible so we could never show that ρ is entangled using this approach. We now search for necessary and sufficient criteria for a mixed state ρ to be entangled. This result was first presented in [19] and is based on the idea of an entanglement witness.

Definition 3.5. *An entanglement witness* $X \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G}) \setminus \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$ *is an operator such that for all* $u \in \mathcal{F}$ *and* $v \in \mathcal{G}$, $\langle X, uu^* \otimes vv^* \rangle \geq 0$.

The inner product of an entanglement witness and a separable operator is always nonnegative and, for every entanglement witness X there exists some set of entangled operators S such that the inner product of the entanglement witness and any of the entangled operators in S is negative. Therefore, we know that if the inner product of quantum state $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ and an entanglement witness is negative, then ρ must be entangled.

Given any entangled operator $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$, the Hahn-Banach theorem, theorem C.8, tells us that there exists a hyperplane which separates ρ from the set $\mathsf{Sep}_m(\mathcal{F} \otimes \mathcal{G})$. If we could find this hyperplane then we could use it to construct an entanglement witness for ρ. Unfortunately, in general it is not easy to find a hyperplane separating a state $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ from $\mathsf{Sep}_m(\mathcal{F} \otimes \mathcal{G})$. However, using the fact that a separating hyperplane exists for any entangled operator, it can be shown that for any entangled operator $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ there exists an entanglement witness X such that $\langle X, \rho \rangle < 0$.

Lemma 3.6. *[19] An operator $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ is entangled if and only if there exists an entanglement witness X such that $\langle X, \rho \rangle < 0$.*

We now use the Jamiolkowski Isomorphism to connect this result about entanglement witnesses to positive maps $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$. This was first noticed in [30] and proved in [19]. We will call it the Woronowicz-Peres separability criterion.

Theorem 3.7. The Woronowicz-Peres Separability Criterion *[19, 30]*
An operator $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ is separable, $\rho \in \mathsf{Sep}_m(\mathcal{F} \otimes \mathcal{G})$, if and only if for all positive transformations $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$, it holds that $(I \otimes \Phi)\rho \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$.

Proof. Assume that $\rho \in \mathsf{Sep}_m(\mathcal{F} \otimes \mathcal{G})$. If $\rho \in \mathsf{Sep}_m(\mathcal{F} \otimes \mathcal{G})$ then we can write ρ as $\rho = \sum_{i=1}^{n} p[i]\, u_i u_i^* \otimes v_i v_i^*$ where $u_i \in \mathcal{F}$ and $v_i \in \mathcal{G}$ for $i = 1, \ldots, n$ and $p \in \mathbb{R}^n$ is a vector with nonnegative entries such that $\|p\|_1 = 1$. Therefore, if $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$ is a positive unital transformation then

$$(I \otimes \Phi)\rho = (I \otimes \Phi) \sum_{i=1}^{n} p[i]\, u_i u_i^* \otimes v_i v_i^* = \sum_{i=1}^{n} p[i]\, u_i u_i^* \otimes \Phi(v_i v_i^*) \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F}).$$

Next, we assume that $(I \otimes \Phi)\rho \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$ for any positive unital transformation $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$. Let $n = \dim(\mathcal{F})$, fix some positive but not completely positive transformation $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$ and set

$$\begin{aligned} Y &= \sum_{i,j=1}^{n} E_{i,j} \otimes E_{i,j} \qquad \text{and} \\ X &= (I \otimes \Phi^*)Y = \mathsf{J}(\Phi^*). \end{aligned}$$

Note that $Y \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$ and $X = J(\Phi^*) \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G}) \setminus \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$ from lemma 2.9. We now have

$$\langle \rho, J(\Phi^*) \rangle = \langle \rho, (I \otimes \Phi^*)Y \rangle = \langle (I \otimes \Phi)\rho, Y \rangle \geq 0.$$

We now show that as Φ ranges over all possible positive transformations, $J(\Phi^*)$ ranges over all entanglement witnesses. This will give us a necessary and sufficient criteria for separability by lemma 3.6. To prove this we will use the Jamiolkowski Isomorphism between all positive but not completely positive transformations Φ, and all entanglement witnesses $J(\Phi^*)$. We know from the work done in lemma 2.9 that $J(\Phi^*) \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G}) \setminus \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$. All we need to show is that $\langle J(\Phi^*), uu^* \otimes vv^* \rangle \geq 0$ for all $uu^* \in \mathsf{Pos}(\mathcal{F})$ and $vv^* \in \mathsf{Pos}(\mathcal{G})$.

$$\begin{aligned} \langle J(\Phi^*), uu^* \otimes vv^* \rangle \geq 0 &\iff \langle uu^* \otimes vv^*, J(\Phi^*) \rangle \geq 0 \\ &\iff \left\langle vv^*, \Phi^*(\overline{u}u^T) \right\rangle \geq 0 \\ &\iff \left\langle \Phi(vv^*), \overline{u}u^T \right\rangle \geq 0 \\ &\iff \Phi(vv^*) \in \mathsf{Pos}(\mathcal{F}). \end{aligned}$$

If Φ is positive but not completely positive then $J(\Phi^*)$ is a entanglement witness. Therefore, as Φ ranges over all positive transformations $J(\Phi^*)$ ranges over all entanglement witnesses.

We can now see, via lemma 3.6, that an operator $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ is separable, if and only if $(I \otimes \Phi)\rho \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$ for all positive but not completely positive transformations $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$. □

We can further strengthen the Woronowicz-Peres Separability Criterion by giving the following lemma.

Lemma 3.8. *For any entangled operator $\rho \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$ there exists a positive unital map $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$, such that $(I \otimes \Phi)\rho \notin \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$.*

Proof. Let ρ be any entangled state. By theorem 3.7 there exists some positive map $\Psi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$ such that $(I \otimes \Psi)\rho \notin \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$.

If $\Psi(I)$ does not have full rank then let $\Psi'(X) = \Psi(X) + \epsilon I$ for some small $\epsilon > 0$. First, note that Ψ' is still a positive transformation. Next, since the function $f(\Psi) = (I \otimes \Psi)\rho$ is continuous we can always choose a small enough ϵ so that $(I \otimes \Psi')\rho \notin \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$. Therefore, we can assume without loss of generality that $\Psi(I)$ has full rank.

Since Ψ is positive and $\Psi(I)$ has full rank $\Psi(I)$ is invertible. Let $A = \Psi(I)^{-\frac{1}{2}}$ and let $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$ be the transformation such that $\Phi(X) = A\Psi(X)A^*$. First, we show that Φ is unital.

$$\Phi(I) = A\Psi(I)A = \Psi(I)^{-\frac{1}{2}}\Psi(I)\Psi(I)^{-\frac{1}{2}} = I.$$

Next, we show that for all $\sigma \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$ it holds that $(I \otimes \Psi)\sigma \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$ if and only if $(I \otimes \Phi)\sigma \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$. Using the fact that A is positive semidefinite

we get

$$\begin{aligned}(I \otimes \Psi)\sigma &= (I \otimes A^{-1})(I \otimes A)(I \otimes \Psi)\sigma(I \otimes A)(I \otimes A^{-1}) \\ &= (I \otimes A^{-1})(I \otimes \Phi)\sigma(I \otimes A^{-1}).\end{aligned}$$

Since $I \otimes A^{-1}$ has full rank we can conclude that $(I \otimes \Psi)\sigma \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$ if and only if $(I \otimes \Phi)\sigma \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$. Using this fact it is easy to see $(I \otimes \Phi)\rho \notin \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$. □

The Jamiolkowski Isomorphism allows us to give an equivalence between entanglement witnesses and positive maps. At first this may seem like this is inconsequential and we could easily use the entanglement witness criterion. It will become evident later that it is much easier to work in the context of positive maps when trying to show that a given state is entangled or not. Also, the positive map criterion is stronger than the entanglement witness criteria. It has been shown in [20] that there exists entanglement witnesses $J(\Phi^*)$ and entangled states $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ such that $\langle J(\Phi^*), \rho \rangle \geq 0$ but $(I \otimes \Phi)\,\rho \notin \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$. This means that the entanglement witness corresponding to the positive map Φ does not detect the entanglement in ρ but the positive map Φ does detect the entanglement in ρ.

Unfortunately, one of the big open questions in the study of entanglement deals with positive maps. We do not yet know a good classification scheme for positive maps. This means that in practice we cannot use this criterion to test if a state is separable or not. If we could fully characterize the positive maps then not only would this information be valuable to understanding entanglement in general but it may give some insight into operational criteria for entanglement.

In general we do not know a good characterization of positive maps, but we do know one specific positive map that detects all entanglement in low dimensional

systems of the form $\mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$ where $\dim(\mathcal{F}) = \dim(\mathcal{G}) = 2$ or $\dim(\mathcal{F}) = 2$ and $\dim(\mathcal{G}) = 3$.

Definition 3.9. *Let T be the transpose operator, $T(X) = X^T$. The partial transpose of an operator $\rho \in \mathsf{L}(\mathcal{F} \otimes \mathcal{G})$ is $(I \otimes T)\,\rho$. The partial transpose is a linear transformation $I \otimes T \in \mathsf{T}(\mathcal{F} \otimes \mathcal{G})$.*

If an operator $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ is still positive after applying the partial transpose, $(I \otimes T)\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ then we say that ρ has positive partial transpose and denote this by $\rho \in \mathsf{PPT}_m(\mathcal{F} \otimes \mathcal{G})$. If $\mathcal{F} = \mathbb{C}^2$ and $\mathcal{G} = \mathbb{C}^2$ or $\mathcal{F} = \mathbb{C}^2$ and $\mathcal{G} = \mathbb{C}^3$, all operators $\rho \notin \mathsf{PPT}_m(\mathcal{F} \otimes \mathcal{G})$ are entangled and all operators σ where $\sigma \in \mathsf{PPT}_m(\mathcal{F} \otimes \mathcal{G})$ are separable. Unfortunately, this no longer holds in higher dimensions. In spaces with larger dimensions, $\dim(\mathcal{F})\dim(\mathcal{G}) > 6$, there exists entangled operators with positive partial transpose, $\rho \in \mathsf{PPT}_m(\mathcal{F} \otimes \mathcal{G})$. The positive partial transpose test is often called the Peres-Horodecki criterion [3, 19]. If we discover that an operator $\rho \notin \mathsf{PPT}_m(\mathcal{F} \otimes \mathcal{G})$ (for any spaces $\mathcal{F}$ and $\mathcal{G}$) then we know that ρ is entangled. However, if $\rho \in \mathsf{PPT}_m(\mathcal{F} \otimes \mathcal{G})$ then ρ can be either entangled or separable. This means that the cone of separable operators is a subset of the cone of positive partial transpose operators, $\mathsf{Sep}(\mathcal{F} \otimes \mathcal{G}) \subseteq \mathsf{PPT}(\mathcal{F} \otimes \mathcal{G})$.

3.3 Multipartite Mixed State Entanglement

The separability criteria for multipartite states is very similar to that of bipartite mixed states. Using the same approach as in the bipartite case, we can always construct an entanglement witness for any multipartite entangled operator ρ. Therefore, we can easily extend lemma 3.6 to include multipartite states.

Lemma 3.10. *[20] A state $\rho \in \mathsf{Pos}_m(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n)$ is entangled if and only if there exists an entanglement witness X such that $\langle X, \rho \rangle < 0$.*

We have to be careful when trying to extend the Woronowicz-Peres separability criterion from the bipartite to multipartite setting. If we follow the same approach as in theorem 3.7 we see that the Jamiolkowski Isomorphism gives an isomorphism between all entanglement witnesses $X \in \mathsf{Herm}(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n) \setminus \mathsf{Pos}(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n)$ and linear maps $\Phi(\mathcal{F}_2 \otimes \mathcal{F}_3 \otimes \cdots \otimes \mathcal{F}_n, \mathcal{F}_1)$ which are positive on separable pure states $\rho = u_2 u_2^* \otimes \cdots \otimes u_n u_n^*$ where $\rho_i \in \mathcal{F}_i$ for $i = 2, \ldots, n$. This does not necessarily mean that Φ is positive. Generalizing theorem 3.7 and lemma 3.8 to multipartite states give the following theorem.

Theorem 3.11. *[20] An operator on a multipartite system $\rho \in \mathsf{Pos}_m(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n)$ is separable, $\rho \in \mathsf{Sep}_m(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n)$, if and only if $(I \otimes \Phi)\rho \in \mathsf{Pos}(\mathcal{F}_1 \otimes \mathcal{F}_1)$ for all unital transformations $\Phi \in \mathsf{T}(\mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n, \mathcal{F}_1)$ such that for all separable pure states $\sigma = u_2 u_2^* \otimes \cdots \otimes u_n u_n^* \in \mathsf{Sep}_m(\mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$, $\Phi(\sigma) \in \mathsf{Pos}(\mathcal{F}_1)$.*

We can also consider a generalization of the Peres-Horodecki criterion for bipartite states. We say that an operator ρ on a multipartite system has positive partial transpose, $\rho \in \mathsf{PPT}_m(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n)$, if and only if every bipartite partition of $\rho \in \mathsf{PPT}_m(\mathcal{F} \otimes \mathcal{G})$. A bipartite partition of a multipartite operator $\rho \in \mathsf{Pos}_m(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n)$ is a partition of the parties into two groups. For example, in a system with three parties $\mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G} \otimes \mathcal{H})$ if $\rho \in \mathsf{PPT}_m((\mathcal{F} \otimes \mathcal{G}) \otimes \mathcal{H})$, $\rho \in \mathsf{PPT}_m(\mathcal{F} \otimes (\mathcal{G} \otimes \mathcal{H}))$ and, $\rho \in \mathsf{PPT}_m(\mathcal{G} \otimes (\mathcal{F} \otimes \mathcal{H}))$ then $\rho \in \mathsf{PPT}_m(\mathcal{F} \otimes \mathcal{G} \otimes \mathcal{H})$. For an n party system there are $2^n - 2$ possible bipartite partitions and so the Peres-Horodecki criterion for multipartite states becomes infeasible to check as the number of parties increases.

Chapter 4

The Size of the Set of Separable States

The previous chapter showed us that the set of separable states is a compact set. The purpose of this chapter is to address the question on the size of the set of separable states. To do this we use a well known separable state $\mathbb{I}$, the maximally mixed state. We first give the radius of a ball centered at $\mathbb{I}$ that is completely contained in the set of separable states. Next, we give the radius for a larger ball centered at $\mathbb{I}$ that completely contains the set of separable states. We have to be careful because although we compute the radius of these balls around the maximally mixed state, the set of separable states does not form a ball around the maximally mixed state. This is easily seen by noticing that all the pure states are the same distance from the maximally mixed state. Since $\mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ is the convex hull of the pure states we would have that all states are separable and this is clearly not true.

The results discussed in this chapter are not only matters of curiosity, they are important stepping stones for proving that separability testing is NP hard. The proof that we present on the hardness of separability testing requires that we know the radius of a ball that fits inside the set of bipartite separable states, and the radius of a ball that contains the set of bipartite separable states. In addition, we require each of the radii given be polynomial in the dimension of the space in which we are working.

4.1 Bounds on the Size of $\mathsf{Sep}(\mathcal{F} \otimes \mathcal{G})$

We now present a proof that the set of separable states are completely contained in a ball of radius one around the maximally mixed state.

Lemma 4.1. *Let* $\mathcal{F} = \mathbb{C}^n$ *and* $\mathcal{G} = \mathbb{C}^m$. *Then* $\mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G}) \subseteq \mathsf{B}_F(\mathbb{I}, 1)$.

Proof. Let $d = nm$. Consider the maximal distance any state ρ can be from the totally mixed state $\mathbb{I}$.

$$\begin{aligned}
\|\rho - \mathbb{I}\|_F &= \sqrt{\mathrm{tr}(\rho - \mathbb{I})^\dagger(\rho - \mathbb{I})} \\
&= \sqrt{\mathrm{tr}(\rho - \mathbb{I})^2} \\
&= \sqrt{\mathrm{tr}(\rho^2) - \frac{2}{d}\mathrm{tr}(\rho) + \frac{1}{d}\mathbb{I}} \\
&\leq \sqrt{1 - \frac{2}{d} + \frac{1}{d}} \\
&= \sqrt{\frac{d-1}{d}} \\
&< 1.
\end{aligned}$$

□

Lemma 4.1 has shown us that all states, and therefore the set of separable states, is contained in the ball of radius one around the maximally mixed state. We now show the more difficult result due to Gurvits and Barnum [15] that there exists a ball inside the set of separable states that has a radius that is polynomial in the dimension. We also show that this ball is the largest ball that fits inside the set of separable states. This result is interesting because it gives a lower bound on the size of the set of separable states.

Before we are able to give an upper bound on the radius of a ball that fits completely inside $\mathsf{Sep}_1(\mathcal{F}\otimes\mathcal{G})$ centered at $\mathbb{I}$, we need to cover some important results. The first of these was shown by Bhatia and Kittaneh [7] and relates the norm of a block matrix to the sum of the norms of its blocks.

Lemma 4.2. *[7] Let $\mathcal{F} = \mathbb{C}^n$ and $\mathcal{G} = \mathbb{C}^m$. If we consider the operator $X \in \mathsf{L}(\mathcal{F}\otimes\mathcal{G})$ as the block operator*

$$X = \sum_{i,j=1}^{n} E_{i,j} \otimes X_{i,j}$$

where each $X_{i,j} \in \mathsf{L}(\mathcal{G})$. Then,

$$\|X\|^2 \leq \sum_{i,j=1}^{n} \|X_{i,j}\|^2 .$$

Proof. Let

$$Y_i = \sum_{j=1}^{n} E_{i,j} \otimes X_{i,j}.$$

Using the fact that $Y_i^* Y_j = 0$ when $i \neq j$ we get

$$X^*X = \left(\sum_{i=1}^{n} Y_i\right)^* \left(\sum_{j=1}^{n} Y_j\right) = \sum_{i=1}^{n} Y_i^* Y_i.$$

Applying the triangle inequality and noting that $\|Z\|^2 = \|Z^*Z\|$ for all operators Z gives us that

$$\|X\|^2 \leq \sum_{i=1}^{n} \|Y_i\|^2 .$$

Now, fix some integer $1 \leq k \leq n$ and set $Y = Y_k$. Y is the block matrix

$$Y = \sum_{i,j=1}^{n} E_{i,j} \otimes Y_{i,j}$$

where $Y_{i,j} = X_{i,j}$ if $i = k$ and $Y_{i,j}$ is the zero matrix otherwise. Using the same approach as above we set

$$Z_{k,j} = \sum_{i=1}^{n} E_{i,j} \otimes Y_{i,j}.$$

The only nonzero $Y_{i,j}$ in $Z_{k,j}$ is when $i = k$ and so

$$Z_{k,j} = E_{k,j} \otimes X_{k,j}.$$

We then have that

$$Y^*Y = \left(\sum_{i=1}^{n} Z_{k,i}\right)^* \left(\sum_{j=1}^{n} Z_{k,j}\right) = \sum_{j=1}^{n} Z_{k,j}^* Z_{k,j}.$$

Since k was chosen arbitrarily we can conclude

$$\|Y_i\|^2 \leq \sum_{j=1}^{n} \|Z_{i,j}\|^2 .$$

Combining the two inequalities we get

$$\|X\|^2 \leq \sum_{i=1}^{n} \|Y_i\|^2 \leq \sum_{i,j=1}^{n} \|Z_{i,j}\|^2 = \sum_{i,j=1}^{n} \|E_{i,j} \otimes X_{i,j}\|^2 = \sum_{i,j=1}^{n} \|X_{i,j}\|^2 .$$

□

Next, we need to know what happens to the norm of an operator X when we apply a positive unital transformation Φ to X. The proof given here is due to Gurvits and Barnum [15] and uses Neumark's theorem, theorem 2.15. This theorem also uses the concept of extreme points of convex sets, a reader unfamiliar with these should refer to Appendix A.

Lemma 4.3. *[15] Let $\Phi \in \mathsf{T}(\mathcal{F})$ be a positive unital transformation and let X be any operator $X \in \mathsf{L}(\mathcal{F})$. Then $\|\Phi(X)\| \leq \|X\|$.*

Proof. Consider the set

$$S = \{X \in \mathsf{L}(\mathcal{F}) : \|X\| \leq 1\}.$$

S is the closed unit ball with respect to the operator norm and the extreme points of this ball are the unitary operators. For a proof of this fact see theorem A.3 in Appendix A. Proving that $\|\Phi(X)\| \leq \|X\|$ for all $X \in S$ is sufficient to solve the problem because any operator $X \in S$ can be expressed as ϵY for some $Y \in \mathsf{L}(\mathcal{F})$ and sufficiently small $\epsilon > 0$. The Krein-Millman theorem from analysis tells us that any element of the set S can be expressed as a convex combination of unitary operators. By the triangle inequality we only need to consider the case where X is a unitary operator.

If X is unitary then X is normal and there is a spectral decomposition of X.

$$X = \sum_{i=1}^{n} \lambda_i u_i u_i^*.$$

Since transformations are linear we get

$$\Phi(X) = \sum_{i=1}^{n} \lambda_i \Phi(u_i u_i^*).$$

Let $B_i = \Phi(u_i u_i^*)$. Since Φ is unital and positive we get that B_i is positive semidefinite and that $\sum_{i=1}^{n} B_i = I$. By Corollary 2.16 there exists a vector space $\mathcal{G}$, a norm preserving map $U \in \mathsf{L}(\mathcal{F}, \mathcal{F} \otimes \mathcal{G})$ and a set of projectors $\{P_1, P_2, \ldots P_n\} \subset \mathsf{L}(\mathcal{F} \otimes \mathcal{G})$ where $\sum_{i=1}^{n} P_i = I$ such that $B_i = U^* P_i U$. Now we can conclude

$$\|\Phi(X)\| = \left\| \sum_{i=1}^{n} \lambda_i B_i \right\| \leq \|U^*\| \left\| \sum_{i=1}^{n} \lambda_i P_i \right\| \|U\| \leq \left\| \sum_{i=1}^{n} \lambda_i P_i \right\| = 1 = \|X\|.$$

The second last equality holds because the operator norm of $\sum_{i=1}^{n} \lambda_i P_i$ is just the absolute value of the largest eigenvalue λ_i. This must equal one because X is unitary. □

Now, we have the required knowledge to give a criterion for separability. We first give a general criterion for an operator to be in the set $\mathsf{Sep}_m(\mathcal{F} \otimes \mathcal{G})$. This criterion is based on representing an operator in a specific way, as the sum of the identity and a Hermitian matrix.

Lemma 4.4. *[15] If $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ can be expressed in the form $\rho = k\,(I + \xi)$, for some positive scalar $k \in \mathbb{R}$ and $\xi \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$ where $\|\xi\|_F \leq 1$, then $\rho \in \mathsf{Sep}_m(\mathcal{F} \otimes \mathcal{G})$.*

Proof. Let $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$ be any positive unital transformation. We can view ξ as a block matrix in $\mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$

$$\xi = \sum_{i,j=1}^{n} E_{i,j} \otimes \xi_{i,j}.$$

Combining lemmas 4.2 and 4.3 we have that

$$\|(I \otimes \Phi)\xi\|^2 \leq \sum_{i,j=1}^{n} \|\Phi(\xi_{i,j})\|^2 \leq \sum_{i,j=1}^{n} \|\xi_{i,j}\|^2 \leq \sum_{i,j=1}^{n} \|\xi_{i,j}\|_F^2 = \|\xi\|_F^2 \leq 1.$$

Since $\|(I \otimes \Phi)\xi\| \leq 1$ all eigenvalues, λ, of $(I \otimes \Phi)\xi$ must satisfy $|\lambda| \in [0, 1]$. This is due to the fact that the spectral radius of $(I \otimes \Phi)\xi$ is less than or equal to the operator norm of $(I \otimes \Phi)\xi$ as discussed in the background section. If the absolute value of any eigenvalue of $(I \otimes \Phi)\xi$ is between zero and one then $(I \otimes \Phi)(I + \xi) \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$. The scalar factor k has no effect on the separability of ρ, it just ensures that ρ has trace m. Therefore, $\rho = k\,(I + \xi)$ is separable by the Woronowicz-Peres criterion (theorem 3.7). and lemma 3.8. □

The above criterion is very general and difficult to use. There may be many different values for k and different matrices ξ such that $\rho = k\,(I + \xi)$. For instance,

$$\rho = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} = 2\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} -\frac{3}{4} & 0 \\ 0 & -\frac{3}{4} \end{bmatrix} \right).$$

In this case $\|\xi\|_F = \sqrt{\frac{9}{8}} > 1$ and so it might seem that ρ is entangled. However, by choosing $k = 1/2$ and $\xi = 0$ we can see that ρ is separable. We now show that there exists a real number k and a Hermitian matrix ξ where $\|\xi\|_F \leq 1$ such that any state $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ where $\rho \in \mathsf{B}_F(\mathbb{I}, \frac{1}{\sqrt{d(d-1)}})$ can be written in the form $\rho = k\,(I + \xi)$. In this way we give a lower bound on the radius of the largest ball of separable states in bipartite systems.

Theorem 4.5. *[15] For any quantum state $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ where $d = \dim(\mathcal{F} \otimes \mathcal{G})$, if $\|\rho - \mathbb{I}\|_F \leq 1/\sqrt{d(d-1)}$ then $\rho \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$.*

Proof. Let $\lambda_1, \lambda_2, \ldots, \lambda_d$ be the eigenvalues of ρ. Using the fact that the Frobenius norm of a normal operator is just the Euclidean norm of the eigenvalues we get

$$\|\rho - \mathbb{I}\|_F^2 = \sum_{i=1}^{d} \left(\lambda_i - \frac{1}{d}\right)^2 = \sum_{i=1}^{d} \lambda_i^2 - \frac{2}{d}\sum_{i=1}^{d} \lambda_i + \frac{1}{d} = \sum_{i=1}^{d} \lambda_i^2 - \frac{1}{d}.$$

Let $k = \sum_{i=1}^{d} \lambda_i^2$. Using the assumption that $\|\rho - \mathbb{I}\|_F^2 \leq \frac{1}{d(d-1)}$ we get,

$$k - \frac{1}{d} \leq \frac{1}{d(d-1)} \Rightarrow k \leq \frac{1}{d-1} \Rightarrow \frac{1}{k} \geq d - 1.$$

If we set $\xi = \frac{1}{k}\rho - I$ then by lemma 4.4 we know that ρ is separable if $\|\xi\|_F \leq 1$.

$$\begin{aligned} \|\xi\|_F^2 &= \left\| \frac{1}{k}\rho - I \right\|_F^2 = \sum_{i=1}^{d} \left(\frac{\lambda_i}{k} - 1\right)^2 = \frac{1}{k^2}\sum_{i=1}^{d} \lambda_i^2 - \frac{2}{k}\sum_{i=1}^{d} \lambda_i + d \\ &= d - \frac{1}{k} \leq d - (d-1) = 1 \end{aligned}$$

□

Since a quantum state $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ is normal, we get that the purity of ρ, $\mathrm{tr}(\rho^2)$, is the sum of the squared eigenvalues of ρ. This, along with the work done in theorem 4.5 allows us to realize another sufficient criteria for separability equivalent to theorem 4.5. It is interesting to note that numerical evidence for this criteria was first given in 1998 in [32].

Lemma 4.6. *Let $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ be a quantum state. If $\mathrm{tr}(\rho^2) \leq \frac{1}{d-1}$ then ρ is separable.*

4.2 States Close to the Bipartite Separable Ball

We now show that the lower bound given in section 4.1 is tight. We want to show that for any bipartite system $\mathcal{F} \otimes \mathcal{G}$ and any $\epsilon > 0$ there exists an entangled state ρ such that $\|\rho - \mathbb{I}\|_F \leq \frac{1}{\sqrt{d(d-1)}} + \epsilon$. We will show this for the composite system $\mathcal{F} \otimes \mathcal{G}$ where $\dim(\mathcal{F}) = \dim(\mathcal{G}) = 2$ but the results easily extend to any dimension. Consider the operator

$$\rho = \begin{bmatrix} \frac{a+b}{2} & 0 & 0 & \frac{a-b}{2} \\ 0 & c & 0 & 0 \\ 0 & 0 & c & 0 \\ \frac{a-b}{2} & 0 & 0 & \frac{a+b}{2} \end{bmatrix}$$

where a, b and, c are all positive real numbers. It is easy to verify that a, b and c are the eigenvalues of ρ and this is why we set them to be positive. The requirement that the state ρ is in $\mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ gives us the criterion that $a + b + 2c = 1$. When

we apply the partial transpose to ρ we get

$$\tilde{\rho} = (I \otimes T)\,\rho = \begin{bmatrix} \frac{a+b}{2} & 0 & 0 & 0 \\ 0 & c & \frac{a-b}{2} & 0 \\ 0 & \frac{a-b}{2} & c & 0 \\ 0 & 0 & 0 & \frac{a+b}{2} \end{bmatrix}.$$

The eigenvalues of $\tilde{\rho}$ are

$$\begin{aligned} \lambda_1 &= \lambda_2 = \frac{a+b}{2} \\ \lambda_3 &= \frac{a-b}{2} + c \\ \lambda_4 &= \frac{b-a}{2} + c. \end{aligned}$$

Therefore, we have that $\tilde{\rho} \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ if and only if $2c \geq a - b$. This means that ρ has negative partial transpose and is therefore entangled if $2c < a - b$. Let us consider what happens when we set $a = \frac{1}{2} + \delta$, $b = \frac{1}{6} + \delta$ and $c = \frac{1}{6} - \delta$ for some small $\delta > 0$. If δ is small enough we have that a, b and, c are all positive, the trace condition is satisfied, $a + b + 2c = 1$, and finally $2c < a - b$. Therefore, the operator

$$\sigma = \begin{bmatrix} \frac{2}{6} + \delta & 0 & 0 & \frac{1}{6} \\ 0 & \frac{1}{6} - \delta & 0 & 0 \\ 0 & 0 & \frac{1}{6} - \delta & 0 \\ \frac{1}{6} & 0 & 0 & \frac{2}{6} + \delta \end{bmatrix}$$

is in $\mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ and is entangled. Finally, we compute the distance between σ and $\mathbb{I}$. It is easy to verify that

$$\|\sigma - \mathbb{I}\|_F = \sqrt{\frac{1}{12} + \frac{2\delta}{3} + 4\delta^2}.$$

For the two by two case, the bound we derived earlier tells us that all states with Frobenius distance less than or equal to $\sqrt{1/12}$ from the maximally mixed state are separable. Clearly then, for any given ϵ we can choose δ small enough so that the state σ constructed above is within distance ϵ of the border of the ball of separable states that we constructed earlier.

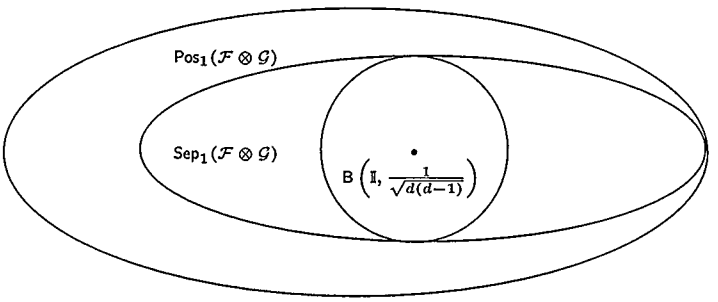


Figure 4.1: The Largest Separable Ball in Bipartite Systems

4.3 Multipartite Separable States

We will now consider the largest separable ball of multipartite quantum states. In this setting we have a quantum state shared by more than just two parties. We want to know the maximum radius of a ball consisting solely of separable states centered around the maximally mixed state. Unlike the bipartite case we do not know the exact radius of the largest separable ball of multipartite quantum states centered around $\mathbb{I}$. We can use the results from the previous section to derive an upper bound on the radius of the largest separable ball in multipartite systems. A state that is separable for multiple parties must still be separable if we combine parties into two groups and consider it to be a bipartite state. Therefore, our bound from the previous section of $1/\sqrt{d(d-1)}$ is an upper bound on the radius of the largest separable ball

in multipartite systems. In this section we will derive a lower bound on the radius of the largest separable ball in multipartite system. We start this section by looking at separability in a general way.

Definition 4.7. *Let* $C_1 \subseteq \mathsf{Pos}(\mathcal{F})$ *and* $C_2 \subseteq \mathsf{Pos}(\mathcal{G})$ *be closed convex cones. A positive semidefinite operator* ρ *is called* (C_1, C_2) *separable,* $\rho \in \mathsf{Sep}(C_1 \otimes C_2)$ *if* $\rho = \sum_{i=1}^{n} X_i \otimes Y_i$ *for some positive integer* $n \geq 1$, *and operators* $X_i \in C_1$, $Y_i \in C_2$ *for* $i = 1, \ldots, n$. *We will use the shorthand notation* $\mathsf{Sep}(\mathcal{F} \otimes C_2)$ *to represent* $(\mathsf{Pos}(\mathcal{F}), C_2)$ *separability. By setting* $C_1 \subseteq \mathsf{Pos}_n(\mathcal{F})$ *and* $C_2 \subseteq \mathsf{Pos}_n(\mathcal{G})$ *to be closed convex sets we can similarly define* $\mathsf{Sep}_n(C_1 \otimes C_2)$, *and* $\mathsf{Sep}_n(\mathcal{F} \otimes C_2)$.

The approach we will take in this section to find a lower bound on the largest ball of separable states is to inductively build a separable ball. That is, for tripartite separability we simply take the cone C_2 generated by all separable bipartite states and consider all $(\mathsf{Pos}(\mathcal{F}), C_2)$ separable states. Then, since this cone is also separable we can continue, increasing the number of parties at each step. The shortcoming of this approach is that at each step when a new party is added to the system we need to shrink the size of the cone of separable states by a constant factor. As we continue to add parties, the lower bound of the radius continues to shrink. After we have added in all the parties we then convert the result about separable cones into separable sets.

Since the size of the separable cone shrinks after adding every party the bound given by using this method is smaller than the bound given in the bipartite case. Recent literature [4, 17] suggests that the radius of the largest separable ball in a multipartite system may be smaller than in a bipartite system with the same total

dimension.

We will now extend and generalize the results that we covered in the previous section on bipartite separable states.

Definition 4.8. *A transformation $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$ is called C positive for some closed convex cone $C \subset \mathsf{L}(\mathcal{F})$ if for all $X \in C$, $\Phi(X) \in \mathsf{Pos}(\mathcal{G})$.*

We now need to consider a generalization of the Woronowicz-Peres criterion, theorem 3.11. The building block of the Woronowicz-Peres criterion was the idea of an entanglement witness. The concept of an entanglement witness still holds in our general definition of separability and is highlighted in the following definition and lemma.

Definition 4.9. *Let $S \subseteq \mathsf{Pos}_m(\mathcal{G})$ be a closed convex set. A Hermitian operator $X \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G}) \setminus \mathsf{Pos}(\mathcal{F} \otimes \mathcal{G})$ is called an $\mathcal{F} \otimes S$ entanglement witness if for every $u \in \mathcal{F}$ and $v \in \mathcal{G}$ where $vv^* \in S$, $\langle X, uu^* \otimes vv^* \rangle \geq 0$.*

Lemma 4.10. *[16] Let $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ and let $S \subseteq \mathsf{Pos}_m(\mathcal{G})$ be a closed convex set. Then, $\rho \in \mathsf{Sep}_m(\mathcal{F} \otimes S)$ if and only if $\langle X, \rho \rangle \geq 0$ for all $\mathcal{F} \otimes S$ witnesses X.*

Basically, lemma 4.10 tells us that if a state $\rho \notin \mathsf{Sep}(\mathcal{F} \otimes S)$ we can always find a hyperplane that separates ρ from $\mathsf{Pos}(\mathcal{F}) \otimes S$. This follows from the same reasoning as before, see Appendix C except we need to show that the set S is compact. By assumption S is closed and since $S \subseteq \mathsf{Pos}_m(\mathcal{G})$, S is bounded by the trace norm. Therefore, S is closed and bounded and must be compact. We can then use the Hahn-Banach theorem to conclude that given any entangled operator we can always construct an entanglement witness. Using this fact, we are now prepared to state a generalization of the Woronowicz-Peres criterion.

Theorem 4.11. *[16] Let $S \subseteq \mathsf{Pos}_m(\mathcal{G})$ be a closed convex set. For any operator $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes S)$ we have $\rho \in \mathsf{Sep}_m(\mathcal{F} \otimes S)$ if and only if $(I \otimes \Phi)\rho \in \mathsf{Pos}(\mathcal{F} \otimes \mathcal{F})$ for all S positive unital transformations $\Phi \in \mathsf{T}(\mathcal{G}, \mathcal{F})$.*

The proof of theorem 4.11 follows (with some very minor changes) exactly like the proof of the Woronowicz-Peres criterion, theorem 3.7. In our proof of the Woronowicz-Peres criterion we implicitly used the fact that if $\Phi(\mathsf{Pos}(\mathcal{F})) \subseteq \mathsf{Pos}(\mathcal{G})$ then $\Phi^*(\mathsf{Pos}(\mathcal{G})) \subseteq \mathsf{Pos}(\mathcal{F})$. The notation $\Phi(\mathsf{Pos}(\mathcal{F}))$ denotes the range of the transformation Φ when the domain is restricted to $\mathsf{Pos}(\mathcal{F})$. All we actually require to prove the theorem is that for any two closed convex cones $C_1 \subseteq \mathsf{Pos}(\mathcal{F})$ and $C_2 \subseteq \mathsf{Pos}(\mathcal{G})$, if $\Phi(C_1) \subseteq C_2$ then $\Phi^*(C_2^d) \subseteq C_1^d$. We can prove this by noting that for all C positive $\Phi \in \mathsf{T}(\mathcal{F}, \mathcal{G})$, $X \in C_1$ and $Y \in C_2^d$,

$$\Phi(X) \in C_2 \iff \langle Y, \Phi(X) \rangle \geq 0 \iff \langle \Phi^*(Y), X \rangle \geq 0 \iff \Phi^*(Y) \in C_1^d.$$

We now introduce the positive cone that we will be interested in for the rest of this section. We used this cone in the previous section when dealing with bipartite entanglement. In that case our value for r was one and the cone generated was a sub-cone of the cone of separable positive semidefinite operators.

Definition 4.12. *Fix any positive real number $0 < r \leq 1$. Then, $C(\mathcal{F}, r)$ is defined to be the cone generated by the set*

$$\{I + \xi : I, \xi \in \mathsf{Herm}(\mathcal{F}) \text{ and } \|\xi\|_F \leq r\}.$$

Like in the previous cases where we were dealing with positive cones, we will let $C_n(\mathcal{F}, r)$ be the convex set that is the set of all operators in $C(\mathcal{F}, r)$ with trace n.

Using our newly defined positive cone we can generalize lemma 4.3 which showed that for any operator $X \in \mathsf{L}(\mathcal{F})$ and any positive unital transformation $\Phi \in \mathsf{T}(\mathcal{F})$, $\|\Phi(X)\| \leq \|X\|$.

Lemma 4.13. *[16] If $\Phi(\mathcal{F}, \mathcal{G})$ is a $C(\mathcal{F}, r)$ positive unital transformation then for all $X \in \mathsf{L}(\mathcal{F})$ we have*

$$\|\Phi(X)\| \leq \frac{\sqrt{2}\,\|X\|_F}{r}.$$

Proof. First, we consider the case where X is a Hermitian operator and $\|X\|_F = r$. If we let $Y = I + X$ then since Φ is a $C(\mathcal{F}, r)$ positive unital transformation we get that $\Phi(Y) = I + \Phi(X) \in \mathsf{Pos}(\mathcal{G})$ and so $\|\Phi(X)\| \leq 1$. Therefore, we get that

$$\|\Phi(X)\| \leq 1 = \frac{\|X\|_F}{r}.$$

Any Hermitian matrix can be written as a scalar multiple of a Hermitian matrix with Frobenius norm r. This follows from the isomorphism between the Hermitian matrices and the real numbers and the equivalence of all norms on finite dimensional vector spaces. We have shown that all Hermitian operators satisfy the inequality.

Consider now, any operator $X \in \mathsf{L}(\mathcal{F})$. We can always write $X = Y + iZ$ for some operators $Y, Z \in \mathsf{Herm}(\mathcal{F})$. We then have that $\Phi(X) = \Phi(Y) + i\Phi(Z)$ which gives

$$\|\Phi(X)\| \leq \|\Phi(Y)\| + \|\Phi(Z)\| = \frac{1}{r}\left(\|Y\|_F + \|Z\|_F\right).$$

The last inequality follows from the initial work on Hermitian operators proved above. Finally, we have that

$$\|\Phi(X)\|^2 \leq \frac{1}{r^2}\left(\|Y\|_F + \|Z\|_F\right)^2 \leq \frac{2}{r^2}\left(\|Y\|_F^2 + \|Z\|_F^2\right) = \frac{2}{r^2}\|X\|_F^2.$$

□

We can now give an analogue to lemma 4.4. The proof of which follows almost exactly like the bipartite case and will be omitted.

Lemma 4.14. *[16] If $\rho \in \mathsf{Pos}_m(\mathcal{F} \otimes \mathcal{G})$ can be expressed in the form $\rho = k\,(I + \xi)$ for some positive scalar $k \in \mathbb{R}$ and $\xi \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$ where $\|\xi\|_F \leq \frac{r}{\sqrt{2}}$, then $\rho \in \mathsf{Sep}_m(\mathcal{F} \otimes C(\mathcal{G}, r))$.*

The result of lemma 4.14 is weaker than lemma 4.4 by factor of $\sqrt{2}$. This is due to the fact that the contraction bound of lemma 4.13 contains a factor of $\sqrt{2}$ in it. There exists examples that show this bound is tight and is the best that can be done. We now use lemma 4.14 to get a more useful result that can be applied directly to multipartite systems.

Lemma 4.15. *[16] If $\rho \in \mathsf{Pos}_m(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$ can be expressed in the form $\rho = k\,(I + \xi)$ for some positive scalar $k \in \mathbb{R}$ and $\xi \in \mathsf{Herm}(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$ where $\|\xi\|_F \leq \frac{1}{2^{n/2-1}}$, then ρ must be separable, $\rho \in \mathsf{Sep}_m(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$.*

Proof. We will prove this by induction on the number of parties. For the base case $(n = 2)$ we can use the bipartite result

$$C_m\left(\mathcal{F}_1 \otimes \mathcal{F}_2, 1\right) \subseteq \mathsf{Sep}_m(\mathcal{F}_1 \otimes \mathcal{F}_2)\,.$$

Next, we assume that the result holds for $n - 1$. That is,

$$C_m\left(\mathcal{F}_2 \otimes \mathcal{F}_3 \otimes \cdots \otimes \mathcal{F}_n, \frac{1}{2^{(n-1)/2-1}}\right) \subseteq \mathsf{Sep}_m\left(\mathcal{F}_2 \otimes \mathcal{F}_3 \otimes \cdots \otimes \mathcal{F}_n\right).$$

Let $r = \frac{1}{2^{(n-1)/2-1}}$. Using lemma 4.14 we see that if $\rho = I + \xi$ where $\|\xi\|_F \leq r/\sqrt{2}$ then $\rho \in \mathsf{Sep}_m\left(\mathcal{F}_1 \otimes C_m\left(\mathcal{F}_2 \otimes \mathcal{F}_3 \otimes \cdots \otimes \mathcal{F}_n, r\right)\right)$. Therefore, we have that

$$C_m\left(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \mathcal{F}_3 \otimes \cdots \otimes \mathcal{F}_n, \frac{1}{2^{n/2-1}}\right) \subseteq \mathsf{Sep}\left(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \mathcal{F}_3 \otimes \cdots \otimes \mathcal{F}_n\right).$$

□

Next, by proceeding along the same lines as theorem 4.5 we can get a bound on the radius of a ball completely contained within the multipartite separable states. This bound is not as good as in the bipartite case. The more parties we have the further this bound gets from the bipartite case. Since the number of parties is in general significantly lower than the dimension this bound is not as bad as it looks.

Theorem 4.16. *[16] Let $\rho \in \mathsf{Pos}_1(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$ be a quantum state and set $d = \dim(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$. If $\|\rho - \mathbb{I}\|_F \leq 1/\left(2^{n/2-1}\sqrt{d(d-2^{-n+2})}\right)$ then $\rho \in \mathsf{Sep}_1(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$.*

Using the same reasoning as in the bipartite case we can use this bound on the size of the ball that fits inside the set of separable states to obtain another equivalent criterion for separability in multipartite systems.

Lemma 4.17. *Let $\rho \in \mathsf{Pos}_1(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$ be any multipartite quantum state. If $\mathrm{tr}(\rho^2) \leq \frac{1}{d-2^{-n+2}}$ then ρ is separable.*

Figure 4.2 compares the radius of the largest ball that can fit inside the set of bipartite separable states (the dashed line) and the largest known radius of the ball that fits inside the set of multipartite separable states. A tight bound on the size of the largest ball that can fit inside the set of multipartite separable states is currently unknown.

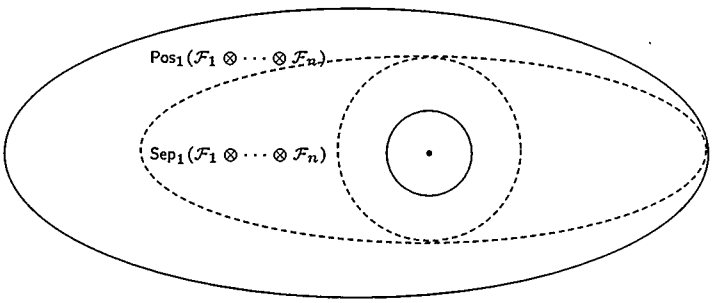


Figure 4.2: The Largest Separable Ball in Multipartite Systems

4.4 States Close to the Multipartite Separable Ball

The exact size of the largest separable ball around the maximally mixed multipartite state is still unknown. The results about bipartite entanglement give us an upper bound on the radius and the results of Section 4.3 give a lower bound on the radius. In this section we will discuss the most recent developments in this area. We first try to find an entangled state that is close to the maximally mixed multipartite state.

If we have a three party quantum state $\rho \in \mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \mathcal{F}_3$ then, by considering the three bipartite partitions of this tripartite system $\mathcal{F}_1 \otimes \mathcal{G}_1 = \mathcal{F}_1 \otimes (\mathcal{F}_2 \otimes \mathcal{F}_3)$, $\mathcal{F}_2 \otimes \mathcal{G}_2 = \mathcal{F}_2 \otimes (\mathcal{F}_1 \otimes \mathcal{F}_3)$, and $\mathcal{F}_3 \otimes \mathcal{G}_3 = \mathcal{F}_3 \otimes (\mathcal{F}_1 \otimes \mathcal{F}_2)$, we know from the results of Section 4.1 that if ρ is within Frobenius distance $\sqrt{\frac{1}{d(d-1)}}$ of the maximally mixed state $\mathbb{I}$ then ρ is separable over all three partitions. Being separable over all bipartite partitions of a multipartite system is not enough to ensure that ρ is separable in the multipartite system. This is one reason why we cannot immediately conclude that a multipartite system with the same total dimension as a bipartite system has the same size largest separable ball. However, we can conclude that any state that would be in the largest separable ball in the bipartite system must be a positive partial transpose state. This is demonstrated in the next lemma.

Lemma 4.18. *Let* $\rho \in \mathsf{Pos}_1(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$ *and set* $d = \dim(\mathcal{F}_1 \otimes \mathcal{F}_2 \otimes \cdots \otimes \mathcal{F}_n)$. *If* $\|\rho - \mathbb{I}\|_F \leq 1/\sqrt{d(d-1)}$ *then* ρ *has positive partial transpose with respect to any bipartite partition* $(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_k) \otimes (\mathcal{F}_{k+1} \otimes \cdots \otimes \mathcal{F}_n)$.

Proof. Setting $\mathcal{F} = (\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_k)$ and $\mathcal{G} = (\mathcal{F}_{k+1} \otimes \cdots \otimes \mathcal{F}_n)$ we can see that $\rho \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ and therefore must be separable with respect to the partition $(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_k) \otimes (\mathcal{F}_{k+1} \otimes \cdots \otimes \mathcal{F}_n)$. If ρ is separable with respect to a partition then ρ must have positive partial transpose with respect to that partition. □

The above lemma tells us that if we are to find a multipartite entangled state that is closer than $\sqrt{\frac{1}{d(d-1)}}$ to the maximally mixed state then this state must have positive partial transpose. We now try to construct a positive partial transpose state that is close to the multipartite separable ball. The method we will use for creating positive partial transpose entangled states is based on the idea of an unextendible product basis [6, 11].

Definition 4.19. *An unextendible product basis* $S \subset \mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m$ *is an orthogonal set of separable pure states such that* $\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m$ *contains no separable pure states that are orthogonal to every state in* S.

Once we have an unextendible product basis for our composite system we can quite easily construct a entangled positive partial transpose state. This is demonstrated in the following lemma.

Lemma 4.20. *[6] Let* $d = \dim(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m)$. *Given any unextendible product basis* $S = \{u_1, u_2, \ldots, u_n\} \subset \mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m$ *the state*

$$\rho_S = \frac{1}{d-n}\left(I - \sum_{i=1}^{n} u_i u_i^*\right)$$

is in $\mathsf{PPT}(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m)$.

Now that we know how to construct an entangled positive partial transpose state we will look at how far away these states are from the maximally mixed state.

Lemma 4.21. *If S is an unextendible product basis in $\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m$ with $|S| = n$ and $d = \dim(\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m)$ then $\|\rho_S - \mathbb{I}\|_F = \sqrt{\frac{n}{d(d-n)}}$.*

Proof.

$$\begin{aligned}
\|\rho_S - \mathbb{I}\|_F &= \left\| \frac{1}{d-n} I - \frac{1}{d} I - \frac{1}{d-n} \sum_{i=1}^{n} u_i u_i^* \right\|_F \\
&= \left\| \frac{n}{d(d-n)} I - \frac{d}{d(d-n)} \sum_{i=1}^{n} u_i u_i^* \right\|_F \\
&= \sqrt{n \left(\frac{n-d}{d(d-n)} \right)^2 + (d-n) \left(\frac{n}{d(d-n)} \right)^2} \\
&= \sqrt{\frac{n}{d^2} + \frac{n^2}{d^2(d-n)}} \\
&= \sqrt{\frac{n}{d(d-n)}}.
\end{aligned}$$

□

It is interesting to note that the distance from the maximally mixed state depends only on the number of states in the unextendible product basis. There does exists a simple lower bound for the number of states in an unextendible product basis. If the composite system is $\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m$ and $\dim(\mathcal{F}_i) = d_i$ then we get that the minimum number of states in an unextendible product basis over $\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_m$ is

$$n = \sum_{i=1}^{m} (d_i - 1) + 1.$$

This shows that any bound entangled state created from a unextendible product basis will not come close to the upper bound of the largest separable ball in multipartite systems.

If we could now prove that all bound entangled states ρ have an associated unextendible product basis S such that $\rho = \rho_S$ then we would could conclude that the bipartite largest separable ball and the multipartite separable ball are the same size. However, this is not the case as there do exist entangled positive partial transpose states which cannot be constructed by using an unextendible product basis, see for instance [21].

Recall how in section 4.2 we proved that the lower bound on the size of the largest separable ball in bipartite systems was tight. We were able to construct an entangled state ρ that was as close as we wanted to the largest separable ball. Perhaps we will be able to use the same technique for multipartite systems. Unfortunately, applying the same techniques as in the bipartite case will not result in an entangled state that is close the maximally mixed multipartite state. This is due to the fact that the bipartite case used a negative partial transpose as a way of determining if a state is entangled. We will not be able to construct a negative partial transpose state that is close to our bound for the largest multipartite separable ball because of lemma 4.18. This means a new approach is necessary. Unfortunately, there seems to be no candidates for a multipartite entangled state close to the maximally mixed state, and constructing such a state has yet to be done.

4.5 Tighter Bounds

In Appendix B we discuss how to construct an isomorphism from the set of $n \times n$ Hermitian matrices to $\mathbb{R}^{n^2}$. In the 2×2 case, the positive operators are mapped into a special sub-cone $C \subset \mathbb{R}^{n^2}$, where

$$C = \left\{ u \in \mathbb{R}^4 : u[1]^2 - \sum_{i=2}^{4} u[i]^2 \geq 0 \text{ and } u[1] \geq 0 \right\}.$$

Therefore, the set of all positive transformations can be represented by linear maps which map C into itself. An analysis of linear maps which map C into itself is done by R. Hildebrand in [17]. By approaching the problem this way the author obtains a tighter bound on the radius of the largest multipartite separable ball. The bound discussed earlier given by Gurvits in [16] was

$$\frac{1}{2^{n/2-1}\sqrt{d(d-2^{-n+2})}}$$

where d is the total dimension of the space and the n is the number of parties. The new bound only applies to the case where the system is composed of two dimensional parts $\mathcal{F} = \mathbb{C}_1^2 \otimes \cdots \otimes \mathbb{C}_n^2$. In this case, we get the tighter bound of

$$\frac{1}{2^{n/2}\sqrt{3^{n-1}+1}}.$$

Unfortunately, this method is not extendible to higher dimensions because of the properties of the Gell-Mann isomorphism. When the dimension of the Hermitian operators increases, the Gell-Mann isomorphism no longer maps positive operators in $\mathsf{Herm}(\mathbb{C}^n)$ into such a simple cone in $\mathbb{R}^{n^2}$. This makes the analysis of positive transformations and separable states more difficult.

Chapter 5

Preliminary Results on Separability Testing

In this chapter, we will cover two results about the complexity of separability testing. The first result we cover was presented by Wayne Myrvold in [25]. Myrvold showed that the separability decision problem was undecidable. Although this result may sound negative, this is not the case. The first section in this chapter will discuss how Myrvold's result fits into the big picture of separability testing. Before reading this chapter, it is important to have some background in computability. For this, the reader is referred to [9].

The second result we will cover is the possibility of testing for entanglement in a laboratory. Up until now we have taken a very mathematical approach to quantum information. We have only considered quantum states as positive semidefinite operators. In the laboratory we have many different physical systems representing a qubit, see for instance Chapter 7 of [26]. In this Chapter, we will show that no matter how we represent a qubit we cannot perform a physical operation that tests for entanglement.

5.1 Exact Separability Testing is Undecidable

Let $S = [0, 1]$, the real numbers from zero to one inclusive, and suppose that your task is to answer queries about whether a given number is in S or not. If you are given a real number, r, you can easily decide if r is in S or not. Now, let us assume

that you are not given the number r but instead you are given an approximation to r, some number x such that $|x - r| < \epsilon$ for some small epsilon. Then, given only the number x you have to decide if r is in S or not. For instance, say you are given the input $x = 1$ as an approximation to some real number r. There are three possible cases for this input. In the first case we have $r = 1 - \delta$ for some $\delta < \epsilon$ and so $r \in S$. Case two is that $r = 1 + \delta$ for some $\delta < \epsilon$. Unlike the previous case, this time $r \notin S$. If it is possible to obtain a better approximation to r, a number y such that $|y - r| < |x - r|$, then doing this may help to distinguish case one from case two. In the last case we have $x = r = 1$. In this case r is in S. However, there is no approximation that we can use to solve this final case. We will never be able to tell if our approximation is exact, $x = r = 1$ or if we need to decrease ϵ to see a difference between x and r. There is no way for us to make an informed decision about whether or not $r \in S$.

The above example illustrates how things might work on a computer. Given a real number r, a computer can only store an approximation to r because there is a finite amount of memory. When working with real numbers, we cannot correctly decide if r is in a set S or not because we may not be able to get the exact value for r. Even worse, if we do have the exact value for r we may not know it. This is the basic idea behind Myrvold's proof of the undecidability of the separability decision problem.

The Separability Decision Problem

Input: A rational approximation to an operator $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$.

Question: Is $\rho \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$?

Theorem 5.1. *[25] The separability decision problem is undecidable.*

We will now sketch a proof of theorem 5.1.

Let us assume that we have some Turing machine M that receives as input a rational approximation to a state $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$. Each entry of ρ will be given with rational real and imaginary parts that approximate the actual entries of ρ to within some predefined accuracy. At any point in the computation M is allowed to use an oracle to get a better approximation of ρ. If we assume that $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ is decidable by M, then by a basic result from computability we have that $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ is partially recursive. Using the same reasoning as at the start of this section we see that $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ is partially recursive if and only if $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ is open. We know that $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ is closed and so we have derived a contradiction.

Before we jump to conclusions about this proof, we should examine it more closely. Instead of dealing with separability testing directly, this result is more about the properties of the vector spaces we are working with. As discussed above, computer memory is finite and because of this we cannot represent certain types of numbers precisely. Myrvold's proof shows that exact separability testing is undecidable but not as a consequence of the problem itself. Instead, the result is based on the impossibility of computing exactly in the vector spaces used for quantum information. If we accept the fact that we cannot compute exactly but can approximate elements of the vector space then there is still progress to be made on the separability problem. Unfortunately, as we will now show, we need the state representing the quantum system in order to make significant progress on separability testing.

5.2 A Physical Test for Entanglement

Now we consider the case of a physically realizable operation to test for entanglement. We assume that we are given one copy of an unknown quantum state $\rho \in \mathsf{Pos}_1(\mathcal{F}\otimes\mathcal{G})$. We want to devise an operation so that at the end of the operation we can tell if ρ is entangled or not. Recall from section 2.4 that we can describe all physically realizable operations by completely positive trace preserving transformations. We would like to have a quantum operation such that when we apply this operation on an entangled state we get one result and when we apply the operation on a separable state we get another result. Performing a measurement is exactly what we need to try to solve this problem. Since we are not concerned with the resulting state, only the probability of the different outcomes, we only need to consider a POVM.

Theorem 5.2. *For any POVM* $\{B_1, B_2, \ldots, B_m\}$ *there does not exist a pair of integers* $1 \leq i, j \leq m$ *such that* $\mathrm{tr}(B_i\rho) > \mathrm{tr}(B_j\rho)$ *for all states* $\rho \notin \mathsf{Sep}_1(\mathcal{F}\otimes\mathcal{G})$ *and* $\mathrm{tr}(B_j\sigma) > \mathrm{tr}(B_i\sigma)$ *for all states* $\sigma \in \mathsf{Sep}_1(\mathcal{F}\otimes\mathcal{G})$.

Proof. We will prove this by contradiction. Assume that there did exist some pair of integers i, j for which it holds that $\mathrm{tr}(B_i\rho) > \mathrm{tr}(B_j\rho)$ for all entangled states ρ and $\mathrm{tr}(B_j\sigma) > \mathrm{tr}(B_i\sigma)$ for all separable states σ. Since the maximally mixed state is separable, we have that $\mathrm{tr}(B_j\mathbb{I}) > \mathrm{tr}(B_i\mathbb{I})$. Using the maximally entangled basis of lemma 2.13 we have that $\mathrm{tr}(B_i u_{a,b} u_{a,b}^*) > \mathrm{tr}(B_j u_{a,b} u_{a,b}^*)$. By linearity of the trace we can derive the contradiction

$$\mathrm{tr}(B_i\mathbb{I}) = \mathrm{tr}\left(\sum_{a,b=0}^{n-1} B_i u_{a,b} u_{a,b}^*\right) > \mathrm{tr}\left(\sum_{a,b=0}^{n-1} B_j u_{a,b} u_{a,b}^*\right) = \mathrm{tr}(B_j\mathbb{I}).$$

□

This theorem tells us that it is impossible to construct a POVM that can be used to test for entanglement in all cases. There is no single measurement that we can perform that will allow us to fully categorize all states as entangled or separable. Therefore, given a single copy of an unknown state we cannot perform a physical experiment that will reliably test if the state is entangled or not.

In the previous result we only considered the case where we are given one copy of an unknown quantum state. We could also consider the possibility that we are given many copies of the state we are trying to test. This information could change the situation quite dramatically. If we are given many copies of a state ρ then it may be possible to devise a physically realizable experiment that can determine if ρ is entangled or not. An example is the work done by P. Horodecki and A. Ekert in [22].

The main result proposed in [22] is that if we take the output of any positive (but not completely positive) transformation and mix it with the maximally mixed state then we can turn a positive transformation into a completely positive transformation. For instance, if we are working with the composite system $\mathcal{F} \otimes \mathcal{G}$ where $\dim(\mathcal{F}) = \dim(\mathcal{G}) = 2$ we can create the completely positive transformation

$$\Phi(\rho) = \frac{8}{9}\mathbb{I} + \frac{1}{9}(I \otimes T)\rho$$

where T is the transpose transformation. The key is that the convex coefficients in the mixture are chosen so that negative one (the minimum eigenvalue of the state $(I \otimes T)\rho$ over all possible states ρ) is shifted to a number greater than or equal to zero. This means that the mixture adds a small number to each eigenvalue of $(I \otimes T)\rho$ to make them nonnegative. This not only makes Φ a completely positive

transformation, but allows us to determine if a state ρ is entangled or not by applying a completely positive transformation. Given an unknown state ρ we simply compute $\Phi(\rho)$. We then determine the minimum eigenvalue of $\Phi(\rho)$. If the state $(I \otimes T)\rho$ is positive semidefinite then all eigenvalues of $(I \otimes T)\rho$ will be greater than or equal to zero and the minimum eigenvalue of $\Phi(\rho)$ will be the minimum eigenvalue of $\frac{8}{9}\mathbb{I}$ which is 2/9. If the state $(I \otimes T)\rho$ is not positive semidefinite then the minimum eigenvalue of $\Phi(\rho)$ will be less than 2/9 but still greater than or equal to zero. Therefore, by examining the minimum eigenvalue of $\Phi(\rho)$ we can determine if ρ is entangled or not.

Given a quantum state in a laboratory, we require many copies of the state in order to determine the smallest eigenvalue of ρ. However, since the Peres-Horodecki criterion is a necessary and sufficient test for entanglement over the $\mathcal{F} \otimes \mathcal{G}$ system, we have created a physically implementable transformation that can detect entanglement.

A problem arises when we try to extend this to larger dimensional spaces. In the low dimensional cases it is easy because the Peres-Horodecki criterion is both a necessary and sufficient criterion for entanglement. In larger dimensions, we require a set of transformations which can detect all types of entanglement. Next, we would have to construct a completely positive version of each transformation and then determine the minimum eigenvalue of the resulting states. As discussed in Chapter 3, we do not have any reasonably sized set of positive transformations that can detect all forms of entanglement. Therefore, this approach will not work on all states in systems with dimension greater than 6.

Chapter 6

The Yudin-Nemirovsky Theorem

The Yudin-Nemirovsky theorem [31] gives a polynomial time Turing reduction between two problems defined on a convex set. In this chapter we use the Yudin-Nemirovsky theorem in the specific case where the convex set in question is the set of separable states $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$. We outline a series of problems that are polynomial time Turing reducible to each other and try to give some intuition about how the reductions work.

Problem A is polynomial time Turing reducible to problem B if we can use a polynomial time Turing machine with an oracle for problem B to decide if any valid input is a YES instance of problem A. We denote a polynomial time Turing reduction by $A \leq B$. For convenience, we will use the term Turing reduction to mean polynomial time Turing reduction and we will specify when the reduction is not polynomial time.

Turing reductions are transitive. That is, if $A \leq B$ and $B \leq C$ then we can conclude that $A \leq C$. This will help us when looking at the Yudin-Nemirovsky theorem as it allows us to examine the theorem in parts. We do not need to cover the Yudin-Nemirovsky theorem in one big step. Instead, we can break it down into smaller, more manageable parts.

The running time of the algorithms in this chapter will be measured in the length of the input and the length of an encoding of the convex set. In Chapter 4 we went to great lengths to give bounds on the size of $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ that were polynomial in

the dimension of $\mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$. Now that we have done this, the length of an encoding of the convex set $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ is dominated by the dimension of $\mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$.

The input to our problem is a positive semidefinite operator ρ and a rational number ϵ representing the error term. For the remainder of this chapter we will assume the positive semidefinite operator is given to us with rational entries. The encoding size of a rational number is how many bits it takes to encode the numerator and denominator of the entry.

Therefore, the running time of the algorithms in this chapter is measured in the dimension of the convex set multiplied by the encoding length of ϵ multiplied by the largest encoding length of the entries of our positive semidefinite operator. With this encoding scheme we can set the error term ϵ to be exponentially small in the dimension and the length of the input would still be polynomial in the dimension.

6.1 Approximate Separability Testing

We already know (via Chapter 5) that exact separability testing is undecidable. Although this is a negative result, it does not rule out the possibility of an algorithm that can test separability with a small amount of error. Therefore, we now define the approximate separability problem.

Approximate Separability Testing

Input:	An operator $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ and $\epsilon \in \mathbb{Q}^+$.
Yes:	$\rho \in \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), -\epsilon)$.
No:	$\rho \notin \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon)$.

The reason why the problems in this chapter are called "weak" or "approximate" has nothing to do with their difficulty but emphasizes the fact that there is a certain small amount of error involved in each problem. For instance, in approximate separability testing we are given a positive semidefinite matrix ρ and we are trying to determine if ρ is in the set of separable states or not. There is an area surrounding the border of the set of separable states for which we may get an incorrect answer to our problem. We already know that exact separability testing is undecidable so without this small error we would be unable to construct a separability testing algorithm that works properly. We have to accept the fact that there will be a small number of states for which we cannot determine if they are separable or not. Therefore, our definition of a correct algorithm is not that the algorithm is correct on all inputs, just that the algorithm is correct on the determined YES and NO inputs. Again using approximate separability testing as an example, if our input ρ is within ϵ (ϵ is an input) of the border of the set of separable states then we may get an incorrect answer. The YES inputs would be where ρ is separable and is at least ϵ away from the border of the set of separable states. The NO inputs would be where ρ is at least ϵ away from the edge of the set of separable states and is entangled.

The solid line in figure 6.1 represents the border of $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$. The area between the two dashed lines represents the area which contains inputs where we allow a correct algorithm to answer YES or NO.

Having an algorithm for approximate separability testing does not imply that we would be able to determine if any given quantum state is separable. However, if we could determine if any given state $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ is separable or entangled then we would be able to solve the approximate separability testing problem. Therefore,

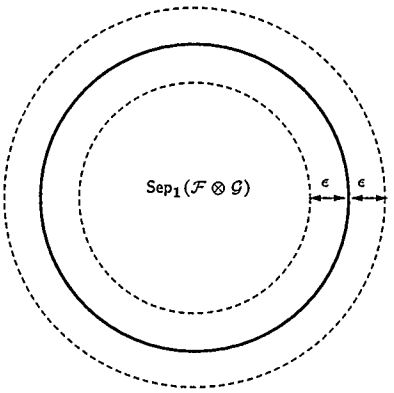


Figure 6.1: Approximate Separability Testing

we have that approximate separability testing reduces to separability testing (ST). In mathematical terms,

$$AST \leq ST.$$

The next problem we will consider is closely related to AST. We will call this problem approximate separability testing with one-sided error (AST-OSE). The difference between AST-OSE and AST is that the area in which an incorrect solution might be obtained in the one-sided error version has been shifted. This means that if the input ρ is separable we no longer require it to be at least distance ϵ from the border of the set of separable states.

Approximate Separability Testing With One-Sided Error

Input: An operator $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ and $\epsilon \in \mathbb{Q}^+$.

Yes: $\rho \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$.

No: $\rho \notin \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon)$.

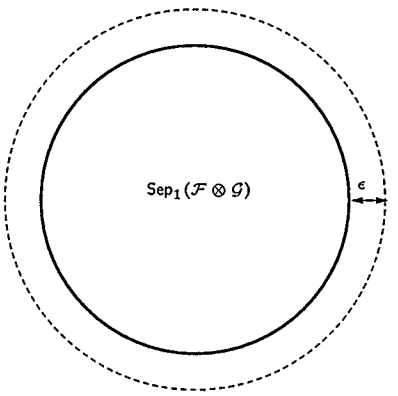


Figure 6.2: Approximate Separability Testing with One-Sided Error

The solid line in figure 6.2 represents the border of $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$. The area between the border of $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ and the dashed line is the area which contains inputs where we allow a correct algorithm to answer YES or NO.

Next, we will show that the problems AST and AST-OSE are in fact equivalent. Given an algorithm that solves one of the problems, we can construct an algorithm that will solve the other. It is easy to see that if we are given an algorithm for AST-OSE then we can solve AST. However, this is not the direction that we need to show that separability testing is NP hard. We need to show the reverse, if we are given an algorithm that solves AST then we can solve AST-OSE. We want a reduction from AST-OSE to AST, we want to show that $AST\text{-}OSE \leq AST$.

Lemma 6.1. *[13] Approximate separability testing with one-sided error Turing reduces to approximate separability testing, $AST\text{-}OSE \leq AST$.*

Proof. Let $\mathcal{F} = \mathbb{C}^n$, $\mathcal{G} = \mathbb{C}^m$ and let $d = nm$. Assume that we have an algorithm that solves the AST problem. We want to use this algorithm to solve AST-OSE. Given the input ϵ and ρ we can do the following,

1. Compute $\delta = \|\rho - \mathbb{I}\|_F$.
   - If $\delta \geq 1$ then $\rho \notin \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ and we can answer NO.
   - If $\delta \leq \sqrt{\frac{1}{d(d-1)}}$ then $\rho \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$, and we can answer YES.
2. Set $\rho_0 = \left(1 - \frac{\epsilon}{4}\right)\rho + \frac{\epsilon}{4}\mathbb{I}$ and $\epsilon_0 = \frac{\epsilon}{4\sqrt{d(d-1)}}$.
3. Run the AST algorithm with input ρ_0 and ϵ_0.
4. If the AST algorithm tells us that $\rho_0 \in \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon_0)$ then we can conclude that $\rho \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ and answer YES.
5. If the AST algorithm concludes that $\rho_0 \notin \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), -\epsilon_0)$ then we can conclude that $\rho \notin \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon)$ and we can answer NO.

This is the first place where the work done in Chapter 4 becomes important. Since we know upper and lower bounds on the size of the set of separable states, computing $\|\rho - \mathbb{I}\|_F$ in step one eliminates cases that would cause us difficulty later. We can now assume that $\sqrt{\frac{1}{d(d-1)}} < \|\rho - \mathbb{I}\|_F < 1$. Using this we can see that

$$\|\rho - \rho_0\|_F = \left\|\frac{\epsilon}{4}\rho - \frac{\epsilon}{4}\mathbb{I}\right\|_F = \frac{\epsilon}{4}\|\rho - \mathbb{I}\|_F < \frac{\epsilon}{4}.$$

If the AST algorithm tells us that $\rho_0 \in \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon_0)$ then it must be the case that $\rho \in \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon_0 + \frac{\epsilon}{4})$. We also have that

$$\epsilon_0 + \frac{\epsilon}{4} = \frac{\epsilon}{4\sqrt{d(d-1)}} + \frac{\epsilon}{4} \leq \epsilon,$$

and so $\mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon_0 + \frac{\epsilon}{4}) \subseteq \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon)$. From this it is easy to see that $\rho \in \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon)$. This means that ρ is either inside $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ or ρ is in the area where a correct algorithm can answer YES or NO. In either case, we are safe in concluding with a YES.

If the AST algorithm tells us that $\rho_0 \notin \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), -\epsilon_0)$, then we need to show that $\rho \notin \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$; we will do this by using a contradiction. Assume that $\rho \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$. Then,

$$\begin{aligned}
\|\rho_0 - \mathbb{I}\|_F &= \left\| \left(1 - \frac{\epsilon}{4}\right) \rho - \left(1 - \frac{\epsilon}{4}\right) \mathbb{I} \right\|_F \\
&= \left(1 - \frac{\epsilon}{4}\right) \|\rho - \mathbb{I}\|_F \\
&= \|\rho - \mathbb{I}\|_F - \frac{\epsilon}{4} \|\rho - \mathbb{I}\|_F \\
&< \|\rho - \mathbb{I}\|_F - \frac{\epsilon}{4\sqrt{d(d-1)}} \\
&= \|\rho - \mathbb{I}\|_F - \epsilon_0.
\end{aligned}$$

The second last line follows from the fact that $\|\rho - \mathbb{I}\|_F > \sqrt{\frac{1}{d(d-1)}}$, which we checked in the first part of our reduction. With all this information we can conclude that $\mathsf{B}_F(\rho_0, \epsilon_0) \subseteq \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ and so $\rho_0 \in \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), -\epsilon_0)$. This is a contradiction to the answer of the AST algorithm. This means that ρ is either far away from separable or ρ is in the area where a correct algorithm is allowed to answer either YES or NO. In either case, we can answer NO. □

6.2 The Approximate Witness Problem

The approximate witness problem is the next step in the Yudin-Nemirovsky theorem. Unlike the previous two problems that we have dealt with, the approximate witness problem is not a simple YES or NO problem. Like the previous problems, we require that a correct algorithm for the approximate witness problem declares YES when the input ρ fulfills some criterion. However, when the input ρ is not a YES instance then we require that a correct algorithm for the approximate witness problem finds

an operator that almost proves this. This is where the error plays an important part. The algorithm does not need to find an operator that proves that ρ is NO instance, it simply needs to find an operator that shows that ρ is close to being a NO instance.

The Approximate Witness Problem

Input: An operator $\rho \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ and two rational numbers $0 < \epsilon, \beta < 1$.

Yes: $\rho \in \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon)$

No: Find a Hermitian operator $Y \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$ such that
$1 \leq \|Y\|_F \leq \dim(\mathcal{F}) \dim(\mathcal{G})$ and $\langle Y, \sigma \rangle \leq \langle Y, \rho \rangle + (\epsilon + \beta \|\sigma - \rho\|_F) \|Y\|_F$
for all $\sigma \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$.

As with all the problems in this chapter we require an area in which a correct algorithm can be right or wrong. In this case, the area is the same as the area in the AST-OSE problem. If our input ρ is within ϵ of the border of $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ and is not contained in $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ then a correct algorithm can either answer YES or give a Hermitian operator that fulfills the criteria. The following theorem can be found in [13] and it demonstrates the connection between AWP and AST-OSE.

Lemma 6.2. *[13] There exists a (non polynomial time) Turing reduction from the AST-OSE problem to AWP; $AWP \leq AST\text{-}OSE$.*

The idea behind the reduction is we can use an algorithm for *AST-OSE* on the set $\mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon)$. If our *AST-OSE* algorithm concludes YES, then we know that $\rho \in \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), \epsilon)$ and we are done. If not, then we know that $\rho \notin \mathsf{B}_F(\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}), 2\epsilon)$. Then, by using a binary search with the *AST-OSE* algorithm we can find an element of $\sigma \in \mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ that is really close to the set

$\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ but is entangled. We then use σ, along with our knowledge about the bounds on the size of the set of separable states, to construct the Hermitian operator Y required in the AWP.

This reduction runs in time that is polynomial in the dimension and $\lceil \frac{1}{\beta} \rceil$. This means that it is not a polynomial time Turing reduction as we had defined in the first part of this chapter. However, we only use this reduction in the case where $\beta \approx \frac{1}{d}$ where d is the dimension of $\mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$. This means that although this reduction is not a polynomial time Turing reduction for all inputs, we only require the reduction on inputs where the reduction will still run in polynomial time.

6.3 The Weak Validity for Separable States Problem

In order to understand the weak validity for separable states problem, we need to know what a valid inequality is. For any $\rho \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$ and $r \in \mathbb{Q}$ an inequality $\langle \rho, Y \rangle \leq r$ is called valid for $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ if

$$\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G}) \subseteq \{Y \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G}) : \langle \rho, Y \rangle \leq r\}.$$

Geometrically, the inequality and the inputs ρ and r define what is called a half-space $H = \{Y \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G}) : \langle \rho, Y \rangle \leq r\}$. The weak validity problem tests whether the convex set in question is contained in this half-space.

The Weak Validity for Separable States Problem

Input: A Hermitian operator $X \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$, $\gamma \in \mathbb{Q}$ and $\epsilon \in \mathbb{Q}^+$.

Yes: $\exists \sigma \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ such that $\langle X, \sigma \rangle \geq \gamma$.

No: $\forall \sigma \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$, $\langle X, \sigma \rangle < \gamma - \epsilon$.

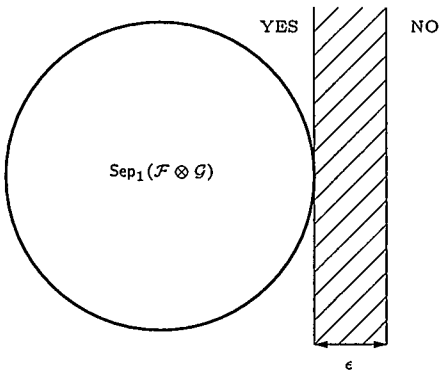


Figure 6.3: Weak Validity for Separable States

Figure 6.3 shows one possible case of the WVSS problem. The YES instances correspond to inputs X that are on the left side of the shaded area and NO instances are inputs X that are on the right side of the shaded area. If the input X is within ϵ of $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ then a correct algorithm for WVSS can answer either YES or NO.

Theorem 6.3. *[13, 31]* **Yudin-Nemirovsky Theorem**

Weak validity for separable states Turing reduces to approximate separability testing, $WVSS \leq AST$.

The first step in the Yudin-Nemirovsky theorem is to build a shallow-cut ellipsoid algorithm. We use the algorithm for AST to get an algorithm for AWP. We then use the algorithm for AWP along with the bounds on the size of the set of separable states, to construct a shallow-cut ellipsoid algorithm.

Given the convex set $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ and input to WVSS of $X \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$, $\gamma \in \mathbb{Q}$ and $\epsilon \in \mathbb{Q}^+$, the shallow-cut ellipsoid method constructs a new convex set S

based on X and $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$, and tries to find an ellipsoid E such that $S \subseteq E$ where the volume of E is less than or equal to ϵ. The first step is to guess any ellipsoid E_1 that has the same center as S. We then check if a smaller scaled version of this ellipsoid fits inside the set S. To do this we require our lower bound on the size of $\mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ which we can use to get a lower bound on the size of S.

If our smaller ellipsoid is not inside the set S then there exists some point s that is in the smaller ellipsoid but not in S. The next step of the algorithm is to construct a hyperplane that separates the point s from the set S. To do this, we use our algorithm for AWP. After we have constructed the hyperplane, we use it to construct a new ellipsoid E_2 and repeat the process. The algorithm halts when we have found an appropriate ellipsoid or we can no longer use the AWP to build the required hyperplane. Figure 6.4 shows an example of one iteration of the shallow-cut ellipsoid method where the smaller ellipsoid is not contained in S.

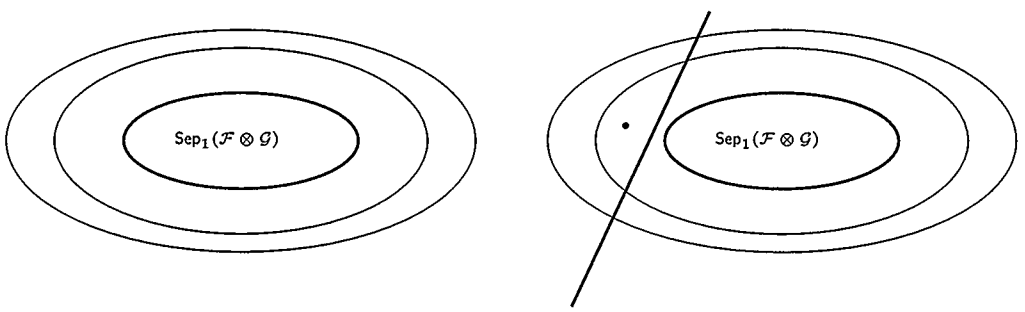


Figure 6.4: Step One and Two of Shallow-Cut Ellipsoid Method

If the shallow-cut ellipsoid algorithm finds an ellipsoid containing S with volume at most ϵ, then it can be shown that the input is a NO instance of WVSS. Conversely, if the shallow-cut ellipsoid algorithm fails then the input is a YES instance of WVSS.

Chapter 7

Approximate Separability Testing is NP hard

This chapter will give a reduction from the NP complete problem of Partition to $WVSS$. This is the final step in showing that AST is NP hard because the Yudin-Nemirovsky theorem gave a reduction between AST and $WVSS$. It is well known that Partition is NP complete (see for instance [12]) and the reduction between $WVSS$ and Partition was first shown by A. Ben-Tal and A. Nemirovsky in [5]. However, it was L. Gurvits in [14] who first combined this result with the results from the previous chapter to establish that separability testing is NP hard.

7.1 Proof of Hardness

The following lemma will be very useful in the proof of hardness.

Lemma 7.1. *[28] Let $\mathcal{F} = \mathbb{C}^n$ and $\mathcal{G} = \mathbb{C}^m$ where $n = \binom{m}{2} + 2$. For any matrices $X_1, X_2, \ldots, X_{n-1} \in \mathsf{Herm}(\mathcal{F})$ and*

$$C = \sum_{i=1}^{n-1} (E_{1,i+1} + E_{i+1,1}) \otimes X_i.$$

it follows that

$$f(C) = \max_{\rho \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})} \operatorname{tr}(C\rho) = \sqrt{\max \left\{ \sum_{i=1}^{n-1} (v^* X_i v)^2 : v \in \mathcal{G}, \|v\|_2 = 1 \right\}}.$$

Proof. First, we note that the function f is well defined because the set of separable states is compact. Lemma C.7 tells us that there does exist some separable state

$\sigma \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ such that the the maximum value of $f(C)$ is $\mathrm{tr}(C\sigma)$. By convexity, it suffices to consider only pure states $uu^* \otimes vv^* \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})$ when attempting to maximize $f(C)$. Given this, it is possible to simplify $f(C)$ as follows,

$$\begin{aligned} f(C) &= \max_{uu^* \otimes vv^* \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})} \mathrm{tr}(C\,(uu^* \otimes vv^*)) \\ &= \mathrm{tr}\left(\sum_{i=1}^{n-1} \left((E_{1,i+1} + E_{i+1,1}) \otimes X_i \right) (uu^* \otimes vv^*) \right) \\ &= \mathrm{tr}\left(\sum_{i=1}^{n-1} (E_{1,i+1}\, uu^* + E_{i+1,1}\, uu^*) \otimes v^* X_i v \right) \\ &= u^* \left(\sum_{i=1}^{n-1} v^* X_i v \, (E_{1,i+1} + E_{i+1,1}) \right) u. \end{aligned}$$

The operator $\sum_{i=1}^{n-1} (E_{1,i+1} + E_{i+1,1})$ is Hermitian and so the Rayleigh-Ritz theorem from matrix analysis implies that the maximum of this last equality is the largest eigenvalue λ, of $\sum_{i=1}^{n-1} v^* X_i v \, (E_{1,i+1} + E_{i+1,1})$. This maximum is obtained when the vector $u = \sum_{i=1}^{n} u[i]\, e_i$ is the corresponding eigenvector. Using the fact that

$$\lambda u = \sum_{i=1}^{n-1} v^* X_i v \, (E_{1,i+1} + E_{i+1,1})\, u$$

we get

$$\begin{aligned} \lambda u &= \sum_{i=1}^{n-1} v^* X_i v \, (E_{1,i+1} + E_{i+1,1})\, u \\ &= \sum_{i=1}^{n-1} v^* X_i v \, (e_1 u[i+1] + e_{i+1} u[1]) \\ &= \sum_{i=1}^{n-1} v^* X_i v \, (e_1 u[i+1]) + \sum_{i=1}^{n-1} v^* X_i v \, (e_{i+1} u[1]). \end{aligned}$$

Therefore, we know that the vector u satisfies

$$\begin{aligned} \lambda u[1] &= \sum_{i=1}^{n-1} u[i+1]\, v^* X_i v \quad \text{and} \\ \lambda u[i+1] &= u[1]\, v^* X_i v \text{ for } i = 1, \ldots, n-1. \end{aligned}$$

Finally, since

$$u[i+1] = \frac{u[1]\, v^* X_i v}{\lambda} \quad \text{for } i = 1, \ldots, n-1$$

we get

$$\lambda u[1] = \sum_{i=1}^{n-1} \frac{u[1]\,(v^* X_i v)^2}{\lambda} \Rightarrow \lambda^2 = \sum_{i=1}^{n-1} (v^* X_i v)^2 .$$

□

The last step before it is shown that Partition reduces to $WVSS$ is to formally introduce the problem of Partition.

Partition

Input: A set S of positive integers.

Yes: There exists some set $S' \subseteq S$ such that

$$\sum_{s \in S'} s = \sum_{s \in S \setminus S'} s.$$

Theorem 7.2. *Partition reduces to the Weak Validity Problem for Separable States,* $PARTITION \leq WVSS$.

Proof. Let the set $S = \{s_1, s_2, \ldots s_m\}$ be the input to the Partition problem. We set $n = \binom{m}{2} + 2$, $\mathcal{F} = \mathbb{Q}^n$ and $\mathcal{G} = \mathbb{Q}^m$. Let $X_1, X_2, \ldots, X_{n-2} \in \mathsf{Herm}(\mathcal{G})$ be an enumeration of the matrices

$$\frac{E_{i,j} + E_{j,i}}{\sqrt{2}}$$

for $1 \leq i < j \leq m$. We then set

$$X_{n-1} = I - \frac{xx^*}{\langle x, x \rangle}$$

where

$$x = \sum_{i=1}^{m} s_i e_i.$$

Now, define $C \in \mathsf{Herm}(\mathcal{F} \otimes \mathcal{G})$ as

$$C = \sum_{i=1}^{n-1} (E_{1,i+1} + E_{i+1,1}) \otimes X_i.$$

We can use lemma 7.1 to get

$$f(C) = \max_{\rho \in \mathsf{Sep}_1(\mathcal{F} \otimes \mathcal{G})} \mathrm{tr}(C\rho) = \sqrt{\max \left\{ \sum_{i=1}^{n-1} (u^* X_i u)^2 : u \in \mathcal{G}, \|u\|_2 = 1 \right\}}.$$

It will be shown below that the maximum value of $f(C)$ will be obtained when the set S is a YES instance of the partition problem. When S is a YES instance of the partition problem, the value of u that yields the maximum value of $f(C)$ will be of the form $u = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} \pm e_i$ and this represents a possible partitioning of S. The sign of $u[i]$ will represent whether we should place s_i in S' or not, a positive sign indicates that we should and a negative sign indicates that s_i should be excluded from the set S'. In this way, if a valid partitioning of S exists then the vector u will describe one of the possible ways that we can partition S. We then show if S is a NO instance of the partition problem then the maximum value of $f(C)$ will be less than optimal by some fixed amount. With this information we show that we can use an algorithm for the WVSS problem to solve the partition problem.

First, define two functions f_1 and f_2 like so

$$f_1(u) = \sum_{i=1}^{n-2} (u^* X_i u)^2 \text{ and } f_2(u) = (u^* X_{n-1} u)^2.$$

From the choice of X_{n-1} it is clear that f_2 is maximized for all unit vectors $u \in \mathcal{F}$ where $\langle x, u \rangle = 0$. The maximum value that f_2 can take when given this input is 1.

Next, notice that

$$\begin{aligned} f_1(u) = \sum_{i=1}^{n-2} (u^* X_i u)^2 &= \sum_{1 \le i < j \le m} 2\left(u^* E_{i,j} u\right)^2 \\ &= \sum_{1 \le i < j \le m} 2u[i]^2 u[j]^2 \\ &= \sum_{i,j=1}^{m} u[i]^2 u[j]^2 - \sum_{i=1}^{m} u[i]^4 \\ &= 1 - \sum_{i=1}^{m} u[i]^4 . \end{aligned}$$

Since $\sum_{i=1}^{m} u[i]^4$ is minimized when each $u[i]$ is as small as possible, in this case $u[i] = \pm\frac{1}{\sqrt{m}}$, the maximum of f_1 occurs when $u = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} \pm e_i$. We can now easily compute the maximum for $f_1(u)$ to be, $f_1(u) = 1 - \sum_{i=1}^{m} \frac{1}{m^2} = 1 - \frac{1}{m}$. Therefore, the maximum of $f_1 + f_2$ is $2 - \frac{1}{m}$ and this maximum occurs when $u = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} \pm e_i$ and $\langle x, u \rangle = 0$.

Consider now, what happens when S is a NO instance of the partition problem. Let

$$d = \min \left\{ \langle u, x \rangle : u \in \mathcal{G}, u = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} \pm e_i \right\}.$$

Since x is an integral vector the smallest value for d is $\frac{1}{\sqrt{m}}$. It is possible to express all unit vectors $u \in \mathcal{G}$ as $u = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} (\pm 1 - \delta_i) e_i$, where each δ_i is some constant between negative one and one. From this, we can get the following equality,

$$d = \frac{1}{\sqrt{m}} \left(\langle x, u \rangle + \sum_{i=1}^{m} \delta_i s_i \right).$$

Using this equality it is now possible to show that there exists some polynomial p such that if S cannot be partitioned then $f(C) \le 2 - \frac{1}{m} - \frac{1}{p(m, \|x\|_2)}$. This will be broken down into two cases. Case one will be when $\langle x, u \rangle \notin \text{poly}\left(\frac{1}{m}, \frac{1}{\|x\|_2}\right)$. In this

case, we have a unit vector u, which scales the entries of the vector x so that when we take the inner product of x and u we get something that is very close to zero. We can then reorder the above equation to get $\sum_{i=1}^{m} \delta_i a_i = d\sqrt{m} - \delta \geq 1 - \delta$ for some small δ. This means that at least one δ_i is greater than or equal to approximately $\frac{1}{\|x\|_1} \geq \frac{1}{\sqrt{m}\|x\|_2}$, and so there exists some polynomial p_1 such that

$$f_1(u) = 1 - \sum_{i=1}^{m} u[i]^4 = 1 - \sum_{i=1}^{m} \left(\pm\frac{1}{\sqrt{m}} - \delta_i \right)^4 \leq 1 - \frac{1}{p_1(m, \|x\|_2)}.$$

In the second case $\sum_{i=1}^{m} \delta_i x_i \notin \text{poly}\left(\frac{1}{m}, \frac{1}{\|x\|_2}\right)$. In this case $\langle x, u \rangle = d - \delta$ for some small δ and so $f_2(u) = 1 - \frac{(1-\delta)^2}{\|x\|_2^2}$. Therefore, there exists some polynomial p_2 such that

$$f_2(u) = 1 - \frac{(1-\delta)^2}{\|x\|_2^2} \leq 1 - \frac{1}{p_2(m, \|x\|_2)}.$$

Choosing $p(m, \|x\|_2) = \max\{p_1(m, \|x\|_2), p_2(m, \|x\|_2)\}$ for given values of m and $\|x\|_2$ yields the result

$$f(C) = f_1(C) + f_2(C) \leq 2 - \frac{1}{m} - \frac{1}{p(m, \|x\|_2)}.$$

Now, it is clear to see that the input C, $\gamma = 2 - \frac{1}{m}$ and $\epsilon = \frac{1}{2p(m, \|x\|_2)}$ is a yes instance of the $WVSS$ problem if and only if S is a YES instance of the partition problem. □

7.2 Overview of the Hardness Result

By the work done in the previous chapter we now have proved that partition Turing reduces to separability testing.

$$PARTITION \leq WVSS \leq AWP \leq AST\text{-}OSE \leq AST \leq ST.$$

Since partition is NP hard it must be the case that separability testing is NP hard.

We now consider the constraint that the dimension $n = \binom{m}{2} + 2$ is fixed given m used in the reduction from partition to WVSS. This does not affect the proof that partition reduces to weak validity for separable states. However, this constraint does "trickle down" and implies that we have only shown that separability testing is NP hard in the case where the composite system is $\mathbb{C}^{\binom{m}{2}+2} \otimes \mathbb{C}^m$ for any integer m. However, if we could solve the general case of separability testing then we could easily solve the constrained version of separability testing. Therefore, it must be the case that separability testing is also NP hard.

One final consideration is we have only shown that bipartite separability testing is NP hard. This is sufficient to conclude that multipartite separability testing is also NP hard. If multipartite separability testing was not NP hard then we could add an extra party to a bipartite quantum state and then use multipartite separability testing to determine if the state is entangled. Therefore, there exists a reduction from bipartite separability testing to multipartite separability testing. Since we have shown that bipartite separability testing is NP hard then multipartite separability testing must also be NP hard.

Chapter 8

Conclusion

This thesis has shown that testing for separability is an NP hard problem. To do this we closely examined how separable states behave when we apply a positive transformation to them and this led to bounds on the size of the set of separable states. We required the bounds on the size of the set of separable states in order to apply a theorem from convex optimization known as the Yudin-Nemirovsky theorem. We then uesd the Yudin-Nemirovsky theorem to give a polynomial time Turing reduction from weak validity for separable states to approximate separability testing, two problems defined on the set of separable states. We concluded the proof by showing that weak validity for separable states was NP hard and so approximate separability testing must also be NP hard.

Although separability testing has been shown to be NP hard this has not discouraged researchers from trying to improve on the best known algorithms for separability testing. Separability testing is NP hard when the complexity parameter is the total dimension of the composite system. If we are working with a system that is composed of a small number of low dimensional systems, then we may be able to test for entanglement in a reasonable time. Although the main result presented in this thesis is a negative one, it does not rule out the possibility of an algorithm that works well enough to test for separability in a composite system with low total dimension. Therefore, there is still work being done and still work that needs to be done on separability testing.

Bibliography

[1] A.Peres. Neumark's theorem and quantum inseparability. *Foundations of Physics*, 20(12):1441–1453, 1990.

[2] A.Peres. *Quantum Theory: Concepts and Methods.* Kluwer Academic Publishers, 1993.

[3] A.Peres. Separability criterion for density matrices. *Physical Review Letters*, 77:1413–1415, 1996.

[4] S. Bandyopadhyay and V. Roychowdhury. Maximally disordered distillable quantum states. *Physical Review A*, 69:040302, 2004.

[5] A. Ben-Tal and A. Nemirovsky. Robust convex optimization. *Mathematics of Operations Research*, 23(4):769–805, 1998.

[6] C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal. Unextendible product bases and bound entanglement. *Physical Review Letters*, 82:5385–5388, 1999.

[7] R. Bhatia and F. Kittaneh. Norm inequalities for partitioned operators and an application. *Math Ann.*, (287):719–726, 1990.

[8] M.D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10:285–290, 1975.

[9] M.D. Davis, R. Sigal, and E.J. Weyuker. *Computability, Camplexity, and Languages.* Morgan Kaufmann Publishers, 1994.

[10] J. de Phillis. Linear transformations which preserve Hermitian and positive semidefinite operators. *Pacific Journal of Mathematics*, 23(1):129–137, 1967.

[11] D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal. Unextendible product bases, uncompletable product bases and bound entanglement. *Communications in Mathematical Physics*, 238:379–410, 2003.

[12] M.R. Garey and D.S. Johnson. *Computers and Intractability.* W.H Freeman and Company, 1979.

[13] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 2 of *Algorithms and Combinatorics.* Springer, second corrected edition edition, 1993.

[14] L. Gurvits. Quantum matching theory (with new complexity theoretic, combinatorial and topological insights on the nature of the quantum entanglement). 2002. quant-ph/0201022.

[15] L. Gurvits and H. Barnum. Largest separable balls around the maximally mixed bipartite quantum state. *Physical Review A*, 66(6):062311, 2002.

[16] L. Gurvits and H. Barnum. Separable balls around the maximally mixed multipartite quantum states. *Physical Review A*, 68:042312, 2003.

[17] R. Hildebrand. Cones of ball-ball separable elements. 2005. quant-ph/0503194.

[18] R.A. Horn and C.R. Johnson. *Matrix Analysis.* Cambridge University Press, 1985.

[19] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physical Letters A*, 223:1–8, 1996.

[20] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps. *Physical Letters A*, 283:1–7, 2001.

[21] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physical Letters A*, 232:333–339, 1997.

[22] P. Horodecki and A. Ekert. Direct detection of quantum entanglement. 2001. quant-ph/0111064.

[23] A. Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.

[24] P.L. Kelly and M.L. Weiss. *Geometry and Convexity.* John Wiley and Sons, 1979.

[25] W. C. Myrvold. The decision problem for entanglement. In R.S. Cohen, M. Horne, and J. Stachel, editors, *Potentiality, Entanglement and Passion-at-a-Distance*, pages 177–190. Kluwer Academic Publishers.

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

[27] A. Peres. Higher order Schmidt decompositions. *Physical Letters A*, (202):16–17, 1995.

[28] J. Watrous. Lecture notes from Advanced Topics in Quantum Information Processing. Winter 2003.

[29] J. Watrous. Lecture notes from Advanced Topics in Quantum Information Processing. Winter 2004.

[30] S.L. Woronowicz. Positive maps of low dimensional matrix algebras. *Reports on Mathematical Physics*, 10(2):165–183, 1976.

[31] D. Yudin and A. Nemirovsky. Computational complexity and efficiency of methods for solving convex extremum problems. *Ekonomika i matem. metody*, (XII-2):357–369, 1976. In Russian.

[32] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Physical Review A*, 58(2):883–892, 1998.

Appendix A

Extreme Points and Convex Sets

Definition A.1. *Let S be a convex set and let $u \in S$. The point u is called an extreme point of S if for all u_1, u_2, $u = pu_1 + (1-p)u_2$ for some real number $0 < p < 1$ implies that $u_1 = u_2 = u$.*

Extreme points can be very useful when trying to solve a problem about a compact convex set. This is due to a well know result in convex analysis called the Krein-Millman theorem. If we know or can easily find the extreme points of a convex compact set S, then we can simply solve the problem on these points. In many cases this is much easier than solving the problem for any point in S as the extreme points are often easier to work with. If the solution on the extreme points works with convex combinations of extreme points and is stable under limits then the Krein-Millman theorem states that it holds for every element in S.

Theorem A.2. Krein-Millman Theorem

Let $\mathcal{F}$ be a normed vector space and S a convex, compact subset of $\mathcal{F}$. S is the closure of the convex hull of its extreme points.

We now prove a result that was required earlier in the thesis about the extreme points of the matrix ball with respect to the operator norm.

Lemma A.3. *Consider the convex set $S = \{X \in \mathsf{L}(\mathcal{F}) : \|X\| \leq 1\}$. The extreme points of S are the unitary matrices.*

Proof. First we will show that any unitary matrix can only be expressed as a trivial convex combination. Let $X \in S$ be a unitary matrix such that $X = pY + (1-p)Z$ where $Y, Z \in S$. This implies that for any unit vector $u \in \mathcal{F}$ we have $\|Yu\|_2 \leq 1$ and $\|Zu\|_2 \leq 1$. Also, using our convex combination we have that

$$1 = \|Xu\|_2 = \|pYu + (1-p)Zu\|_2 \leq p\|Yu\|_2 + (1-p)\|Zu\|_2 .$$

which shows that $\|Yu\|_2 \geq 1$ and $\|Zu\|_2 \geq 1$. Therefore, it must be that case that $\|Yu\|_2 = 1$ and $\|Zu\|_2 = 1$ for all unit vectors $u \in \mathcal{F}$ and so Y and Z are unitary. This also gives that the triangle inequality becomes an equality

$$\|pYu + (1-p)Zu\|_2 = p\|Yu\|_2 + (1-p)\|Zu\|_2$$

which only happens in the case that pYu is a scalar multiple of $(1-p)Zu$. Since Y and Z are unitary this means that $Yu = Zu$ for all $u \in \mathcal{F}$ and therefore $Y = Z$. We have now shown that if X is unitary then X is an extreme point.

Now we will show that if X is an extreme point of S then X is unitary. To do this it will suffice to show that all extreme points have full rank and all the singular values of any extreme point are one.

Let X be any operator in S with rank r. Using the singular value decomposition, theorem 2.3, we can write

$$X = \sum_{i=1}^{r} s_i u_i v_i^*$$

where $\{u_1, u_2, \ldots, u_r\} \subset \mathcal{F}$ and $\{v_1, v_2, \ldots, v_r\} \subset \mathcal{F}$ are orthonormal sets. Using this representation of X, we can write X as a convex combination of two other operators,

$X = \frac{1}{2}Y + \frac{1}{2}Z$ where

$$Y = \sum_{\substack{i \\ s_i < \frac{1}{2}}} 2s_i u_i v_i^* + \sum_{\substack{i \\ s_i \geq \frac{1}{2}}} u_i v_i^* \quad \text{and} \quad Z = \sum_{\substack{i \\ s_i \geq \frac{1}{2}}} (2s_i - 1)\, u_i v_i^*.$$

Clearly Y and Z are distinct operators unless all singular values of X are one.

If the operator X does not have full rank, then there exists at least one vector, u_{r+1}, that can be added to the set $\{u_1, u_2, \ldots, u_r\}$ so that it is still an orthonormal set of vectors. Likewise, there exists a vector, v_{r+1}, that can be added to the set $\{v_1, v_2, \ldots, v_r\}$ so that it is still an orthonormal set of vectors. Using the two vectors u_{r+1} and v_{r+1} we can create two new operators Y and Z where

$$Y = \sum_{i=1}^{r-1} u_i v_i^* + \left(\frac{u_r - u_{r+1}}{\sqrt{2}}\right)\left(\frac{v_r + v_{r+1}}{\sqrt{2}}\right)^* + \left(\frac{u_r + u_{r+1}}{\sqrt{2}}\right)\left(\frac{v_r - v_{r+1}}{\sqrt{2}}\right)^*$$

and

$$Z = \sum_{i=1}^{r-1} u_i v_i^* + \left(\frac{u_r + u_{r+1}}{\sqrt{2}}\right)\left(\frac{v_r + v_{r+1}}{\sqrt{2}}\right)^* + \left(\frac{u_r - u_{r+1}}{\sqrt{2}}\right)\left(\frac{v_r - v_{r+1}}{\sqrt{2}}\right)^*.$$

Each of the added vectors in the decomposition of Y and Z are normalized and can be part of a complete orthonormal basis for $\mathcal{F}$. Therefore, the above decompositions of Y and Z are valid singular value decompositions. It is also important to note that Y and Z are both in S. Simplifying these expressions gives

$$Y = \sum_{i=1}^{r} u_i v_i^* - u_{r+1} v_{r+1}^* \quad \text{and} \quad Z = \sum_{i=1}^{r} u_i v_i^* + u_{r+1} v_{r+1}^*.$$

It is now easy to see that $X = \frac{1}{2}Y + \frac{1}{2}Z$.

We have shown that any extreme point must have full rank and all of its singular values must equal one. Therefore, by the discussion about unitary matrices and singular values given after theorem 2.3, if X is an extreme point then X must be unitary. □

Appendix B

An Isomorphism Between $\mathsf{Herm}(\mathbb{C}^n)$ and $\mathbb{R}^m$

To define an isomorphism from $\mathsf{Herm}(\mathbb{C}^n)$ to $\mathbb{R}^{n^2}$ we need to consider a basis for $\mathsf{Herm}(\mathbb{C}^n)$. One such basis is the Gell-Mann basis, defined as

$$A_{a,b} = \begin{cases} E_{a,b} + E_{b,a} & \text{if } a < b \\ -i\left(E_{b,a} - E_{a,b}\right) & \text{if } a > b \\ I & \text{if } a = b = 1 \\ \sqrt{\frac{2}{a(a-1)}}\left(\sum_{k=1}^{a-1} E_{a-1,a-1} - (a-1)\, E_{a,a}\right) & \text{if } a = b \text{ and } a > 1 \end{cases}$$

for all $1 \leq a, b \leq n$.

Now that we have a basis for $\mathsf{Herm}(\mathbb{C}^n)$ we can define an isomorphism as follows

$$G : \mathsf{Herm}(\mathbb{C}^n) \mapsto \mathbb{R}^{n^2}$$
$$G(X) = \tfrac{1}{n} \sum_{a,b=1}^{n} \langle A_{a,b}, X \rangle\, e_{n(a-1)+b}.$$

It is a simple and straightforward task to verify that the Gell-Mann Isomorphism is actually an isomorphism.

In the case where we map $\mathsf{Herm}(\mathbb{C}^2)$ in $\mathbb{R}^4$ the Gell-Mann isomorphism has some special properties. We look at this example as it will become useful later.

Example B.1. *let $\mathcal{F} = \mathbb{C}^2$. Then, the Gell-Mann basis for $\mathsf{Herm}(\mathcal{F})$ consists of the following four matrices.*

$$A_{1,1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} A_{1,2} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} A_{2,1} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} A_{2,2} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

These matrices may look familiar as they are the widely known Pauli matrices. It may be tempting to think that the Gell-Mann basis can be considered as a generalization of the Pauli matrices. However, the Gell-Mann basis is no longer composed of unitary matrices once $\dim(\mathcal{F}) > 2$. *Any matrix in* $\mathsf{Herm}(\mathcal{F})$ *can be written as*

$$\rho = \begin{bmatrix} a & b+ci \\ b-ci & d \end{bmatrix}$$

and under the Gell-Mann Isomorphism this gets mapped to

$$G(\rho) = \frac{1}{2}\begin{bmatrix} a+d \\ 2b \\ 2c \\ a-d \end{bmatrix}$$

Lemma B.2. *let* $\mathcal{F} = \mathbb{C}^2$. *The Gell-Mann isomorphism maps the cone* $\mathsf{Pos}(\mathcal{F})$ *into the cone*

$$C = \left\{ u \in \mathbb{R}^4 : u[1]^2 - \sum_{i=2}^{4} u[i]^2 \geq 0 \text{ and } u[1] \geq 0 \right\}.$$

Proof. If we set

$$\rho = \begin{bmatrix} a & b+ci \\ b-ci & d \end{bmatrix} \in \mathsf{Herm}(\mathcal{F})$$

then the eigenvalues of ρ are

$$\begin{aligned} \lambda_1 &= \frac{a+d+\sqrt{4b^2+4c^2+(a-d)^2}}{2} \\ \lambda_2 &= \frac{a+d-\sqrt{4b^2+4c^2+(a-d)^2}}{2}. \end{aligned}$$

Since the eigenvalues of ρ must be real numbers we have that $\rho \in \mathsf{Pos}(\mathcal{F})$ if and only if $\lambda_1\lambda_2 \geq 0$ and $\lambda_1 + \lambda_2 \geq 0$. Now, it is easily seen that the condition $\lambda_1 + \lambda_2 \geq 0$ is equivalent to $a+d \geq 0$ and that $\lambda_1\lambda_2 \geq 0$ is equivalent to $(a+d)^2 \geq 4b^2+4c^2+(a-d)^2$. These two conditions are equivalent to saying that $G(\rho) \in C$. $\square$

Appendix C

Analysis

Definition C.1. *For any subset S of a vector space $\mathcal{F}$ we say that S is closed if every sequence of elements from S that has a limit in $\mathcal{F}$, has a limit in S.*

Definition C.2. *A subset S of a vector space $\mathcal{F}$ is called bounded if there exists a real number r such that $\|s\| \leq r$ for all $s \in S$.*

Both of the above definitions depend on the concept of a norm. Is it possible that a set S of a vector space $\mathcal{F}$ is closed with respect to one norm and not another? Can S be bounded by one norm but not another? The following definition and lemma show that the answer to both these questions is no.

Definition C.3. *Let $\mathcal{F}$ be a vector space with at least two norms $\|\cdot\|_a$ and $\|\cdot\|_b$. We say that the norms $\|\cdot\|_a$ and $\|\cdot\|_b$ are equivalent if there exists a positive real number r so that*

$$\frac{1}{r}\|u\|_a \leq \|u\|_b \leq r\|u\|_a$$

for all $u \in \mathcal{F}$.

Lemma C.4. *If $\mathcal{F}$ is a finite dimensional vector space then all norms on $\mathcal{F}$ are equivalent.*

Definition C.3 and lemma C.4 are used implicitly throughout this thesis. For instance, in theorem 3.3 where we show that the set of separable states is compact,

we show that the set of separable states is a bounded subset of $\mathsf{L}(\mathcal{F} \otimes \mathcal{G})$ with respect to the trace norm. Because all norms on finite dimensional vector spaces are equivalent, we have that the set of separable states is a bounded subset of $\mathsf{L}(\mathcal{F} \otimes \mathcal{G})$ with respect to any norm of $\mathsf{L}(\mathcal{F} \otimes \mathcal{G})$.

Appendix B discusses isomorphisms between the vector spaces $\mathsf{Herm}(\mathbb{C}^n)$ and $\mathbb{R}^{n^2}$. Hence, $\mathsf{Pos}_1(\mathcal{F} \otimes \mathcal{G})$ and the set of separable states can both be viewed as subsets of $\mathbb{R}^m$ for some positive integer m. This is important because it allows us to use the Heine-Borel theorem from analysis to equate compactness with closed and bounded.

Definition C.5. *A subset S of a vector space $\mathcal{F}$ is called compact if for every collection of open sets $\{K_i\}$ where $S \subseteq \bigcup_i K_i$ there exists a finite set of positive integers $X = \{x_1, x_2, \ldots, x_n\}$ so that $S \subseteq \bigcup_i^n K_{x_i}$.*

Theorem C.6. Heine-Borel Theorem

If S is a subset of $\mathbb{R}^n$ then S is closed and bounded if and only if S is compact.

We use the Heine-Borel theorem to show that the set of separable states is compact, theorem 3.3. Compactness also gives us some nice results about continuous functions defined on the set of separable states.

Lemma C.7. *If f is a continuous real function on a compact subset S of a vector space $\mathcal{F}$ then there exists elements $s_1, s_2 \in S$ such that*

$$f(s_1) = \sup_{s \in S} f(s) \quad \textit{and} \quad f(s_2) = \inf_{s \in S} f(s).$$

We use the above lemma when we define the function f used in Chapter 7 for lemma 7.1 and theorem 7.2.

Theorem C.8. Geometric Hahn-Banach Theorem *Let S_1 and S_2 be disjoint, closed, convex subsets of $\mathbb{R}^n$ and let S_1 be compact. Then, there exists a vector $a \in \mathbb{R}^n$ and a real number r so that*

$$\langle a, s_1 \rangle < r \text{ for all } s_1 \in S_1 \text{ and } \langle a, s_2 \rangle > r \text{ for all } s_2 \in S_2$$

The vector a and the number r from the Hahn-Banach theorem define a hyperplane. The inequalities given show that the hyperplane lies between the two sets S_1 and S_2. This is what we mean when we say a hyperplane separates two sets.

We use the isomorphism from $\mathsf{Herm}(\mathbb{C}^n)$ to $\mathbb{R}^{n^2}$ in order to apply this theorem to the set of positive semidefinite operators. If we choose S_1 to be the set of separable states (which is compact by theorem 3.3) and S_2 to be a single entangled state then by the Hahn-Banach theorem we can always construct a hyperplane that separates the two.

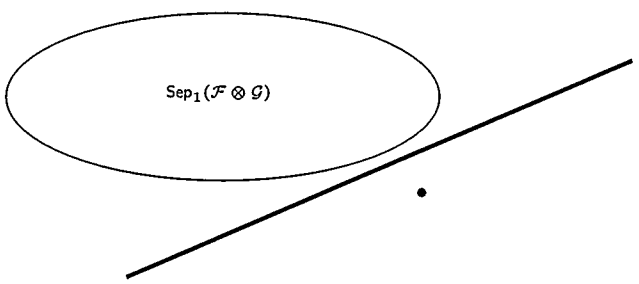


Figure C.1: Separating Hyperplane