Semidefinite Programs in Quantum Information Theory

Semidefinite Programs in Quantum Information Theory

Written by *Jeppe Johan Waarkjær Olsen* and *Anna Wulff Christensen*

August 4, 2019

Supervised by
Matthias Christandl, Roberto Ferrara & Alexander Gerd C. Müller-Hermes

University of Copenhagen

UNIVERSITY OF COPENHAGEN

Name of Institute:	The University of Copenhagen
Name of Department:	Department of Mathematical Sciences
Author(s):	Jeppe Johan Waarkjær Olsen and Anna Wulff Christensen
Email:	Jeppe: jzl302@alumni.ku.dk, Anna: aw@himalaya.dk
Title and subtitle:	Semidefinite Programs in Quantum Information Theory -
Supervisor(s):	Matthias Christandl, Roberto Ferrara & Alexander Gerd C. Müller-Hermes
Handed in:	09.06.2017
Defended:	19.06.2017

Name ______________________________

Signature _________________________

Date ______________________________

Abstract

This thesis discusses detection of entanglement of states in quantum information theory as well as some of the underlying principles necessary to understand this subject.

Two methods for detecting entanglement are discussed: The PPT-criterion [13] and extendibility of states [6]. The former is a sufficient test only for systems of small dimensions.

Extendibility is first introduced in its most general form. The problem with this form of extendibility is that the dimension of the problem scales exponentially with the number of extensions. With the introduction of the symmetric subspace, we are able to define the Bose-symmetric extensions, improving the performance of the test by reducing the scaling of the dimension to polynomial. This detection protocol is implemented in Python as an SDP. We also show that extendibility for the Bose-symmetric subspace is a sufficient test as is stated in the De-Finetti theorem for Bose-symmetric states [19].

We also give a brief explanation of two applications of entanglement in quantum information theory, namely superdense coding and quantum teleportation.

Contents

1 Introduction **2**

2 Linear Algebra **3**

2.1 Operators . . . 3
2.2 The tensor product . . . 3
2.3 Positive and completely positive maps . . . 4
2.4 Choi-Jamiolkowski representation . . . 5
2.5 Matrix representation . . . 6

3 Quantum Information Theory **7**

3.1 Quantum states . . . 7
3.2 Entanglement . . . 7
3.3 Measurements . . . 8
3.4 Applications of entanglement . . . 8
3.4.1 Superdense coding . . . 8
3.4.2 Quantum teleportation . . . 9

4 Detection of Entanglement **9**

4.1 PPT criterion . . . 11
4.2 Extendibility . . . 11

5 Semidefinite Programming **12**

6 Symmetric Subspace **13**

7 Symmetric Extensions **16**

8 Examples **23**

8.1 Werner state . . . 24
8.2 Horodecki state . . . 24
8.3 PPT edge . . . 24

9 Conclusion **25**

10 Appendix **26**

1 Introduction

Entanglement is an effect in quantum mechanics not present for classical mechanics. Entanglement is important to quantum information theory, for example in quantum teleportation, and as such experimental (and thus theoretical) methods to detecting entanglement are required. This project discusses two such detection methods, namely the PPT-criterion (Peres-Horodecki) [13] and extendibility of states [6][2]. We discuss these two tests in Section 4, starting with the former. The PPT-criterion is only a sufficient test for small dimensions as it follows from the Woronowicz theorem shown in [23]. The first goal of the thesis is to implement the PPT-criterion in Python.

Extendibility utilizes semi-definite programming (SDP), which is a subfield of convex optimization [6]. In this project we use a library for solving SDPs, which is already implemented to Python. The second goal of the project is to introduce the symmetric subspace [11], and use this to formulate the hierarchy of symmetric extendibility as an SDP to be solved in Python.

To show how the symmetric extendible states converge to separable states, we discuss the De-Finetti theorem. This theorem is originally a classical result, but it has been adapted to quantum information theory [5].

2 Linear Algebra

The formalism of quantum mechanics is based on linear algebra and this section introduces the concepts of linear algebra relevant to this thesis.

Definition 1 (Hilbert space)**.** *A Hilbert space is a complex or real vector space with an inner product.*

When referring to Hilbert spaces in this project, we refer only to finite dimensional complex Hilbert spaces. When dealing with multiple systems we will use $\mathbb{C}^{d_A}$ to denote the Hilbert space of system A.

Definition 2 (The computational basis)**.** *The computational basis for $\mathbb{C}^d$ is defined by $\{|i\rangle, i = 1, \ldots, d\}$, where $|i\rangle$ is the d-dimensional vector for which the i'th element is equal to 1, and all other elements are 0.*

2.1 Operators

As we only consider a finite dimensional Hilbert space, all linear operators on this space can be represented as matrices. We denote the space of linear operators, or matrices, on Hilbert space $\mathbb{C}^d$ by $\mathcal{L}(\mathbb{C}^d)$.

The vector space of matrices is also a Hilbert space, called the Hilbert-Schmidt space, when equipped with the Hilbert-Schmidt inner product defined by

$$\langle Y, X\rangle = \mathrm{tr}(Y^\dagger X). \tag{1}$$

Definition 3 (Positive Semidefiniteness)**.** *A linear operator $X \in \mathcal{L}(\mathbb{C}^d)$ is called positive semidefinite if*

$$\langle a| X |a\rangle \geq 0 \; \forall \, |a\rangle \in \mathbb{C}^d$$

We denote a positive semidefinite matrix by $X \geq 0$. The set of positive semidefinite matrices is denoted by $\mathcal{P}(\mathbb{C}^d) = \{X \in \mathcal{L}(\mathbb{C}^d) \mid X \geq 0\}$

Definition 4 (Density Matrix)**.** *A linear operator $\rho \in \mathcal{L}(\mathbb{C}^d)$ is called a density operator if it is positive semidefinite and has trace 1. The set of density operators is denoted*

$$\mathcal{D}(\mathbb{C}^d) = \{\rho \in \mathcal{P}(\mathbb{C}^d) \; |\mathrm{tr}(\rho) = 1\}.$$

2.2 The tensor product

Definition 5 (The tensor product of vectors)**.** *The tensor product of $|a\rangle \in \mathbb{C}^{d_A}$ and $|b\rangle \in \mathbb{C}^{d_B}$ is:*

$$|a\rangle \otimes |b\rangle = \begin{pmatrix} a_1 b_1 \\ \vdots \\ a_1 b_{d_B} \\ \vdots \\ a_{d_A} b_1 \\ \vdots \\ a_{d_A} b_{d_B} \end{pmatrix}, \tag{2}$$

where a_i and b_i are the coefficients of $|a\rangle$ and $|b\rangle$ in the computational basis on systems A and B respectively. We denote the tensor product of two vectors as $|ab\rangle = |a\rangle \otimes |b\rangle$. The tensor product of $\mathbb{C}^{d_A}$ and $\mathbb{C}^{d_B}$ is defined by

$$\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} = \mathrm{span}\left\{|ab\rangle \; : |a\rangle \in \mathbb{C}^{d_A}, |b\rangle \in \mathbb{C}^{d_B}\right\} \tag{3}$$

This space has dimension, $\dim(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}) = d_A \cdot d_A$.

An example of a vector, $|\Omega\rangle \in (\mathbb{C}^d \otimes \mathbb{C}^d)$ which can not be written as a product vector like equation (2) is

$$|\Omega\rangle = \sum_i^d |i\rangle \otimes |i\rangle \tag{4}$$

This vector will be relevant later.

Definition 6 (Tensor product of matrices). *For matrices $X \in \mathcal{L}(\mathbb{C}^{d_A})$ and $Y \in \mathcal{L}(\mathbb{C}^{d_B})$ the tensor product is defined as*

$$X \otimes Y = \begin{bmatrix} X_{11} \cdot \begin{bmatrix} Y_{11} & \cdots & Y_{1d_B} \\ \vdots & \ddots & \vdots \\ Y_{d_B 1} & \cdots & Y_{d_B d_B} \end{bmatrix} & \cdots & X_{1d_A} \cdot \begin{bmatrix} Y_{11} & \cdots & Y_{1d_B} \\ \vdots & \ddots & \vdots \\ Y_{d_B 1} & \cdots & Y_{d_B d_B} \end{bmatrix} \\ \vdots & \ddots & \vdots \\ X_{d_A 1} \cdot \begin{bmatrix} Y_{11} & \cdots & Y_{1d_B} \\ \vdots & \ddots & \vdots \\ Y_{d_B 1} & \cdots & Y_{d_B d_B} \end{bmatrix} & \cdots & X_{d_A d_A} \cdot \begin{bmatrix} Y_{11} & \cdots & Y_{1d_B} \\ \vdots & \ddots & \vdots \\ Y_{d_B 1} & \cdots & Y_{d_B d_B} \end{bmatrix} \end{bmatrix} \tag{5}$$

The tensor product of $\mathcal{L}(\mathbb{C}^{d_A})$ and $\mathcal{L}(\mathbb{C}^{d_B})$ is defined by

$$\mathcal{L}(\mathbb{C}^{A}) \otimes \mathcal{L}(\mathbb{C}^{d_B}) = \operatorname{span}\{X \otimes Y : X \in \mathcal{L}(\mathbb{C}^{d_A}), Y \in \mathcal{L}(\mathbb{C}^{d_B})\} \tag{6}$$

There also is a natural tensor product for linear maps.

Definition 7 (The tensor product of linear maps). *The tensor product of linear maps $T : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_{A'}})$ and $S : \mathcal{L}(\mathbb{C}^{d_B}) \to \mathcal{L}(\mathbb{C}^{d_{B'}})$ is defined by*

$$(T \otimes S)(X \otimes Y) = T(X) \otimes S(Y), \ \forall X \in \mathcal{L}(\mathbb{C}^{d_A}) \text{ and } Y \in \mathcal{L}(\mathbb{C}^{d_B})$$

and extended to all matrices $Z \in \mathcal{L}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ by linearity.

The identity map $\mathrm{id} : \mathcal{L}(\mathbb{C}^{d}) \to \mathcal{L}(\mathbb{C}^{d})$,

$$\mathrm{id}(X) = X \tag{7}$$

can be used to define partial operations on bipartite systems.

Definition 8 (Partial trace). *Let $X \in \mathcal{L}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$, then the trace applied to system B is:*

$$\mathrm{tr}_B : \mathcal{L}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}) \to \mathcal{L}(\mathbb{C}^{d_A})$$

$$\mathrm{tr}_B(X) := (\mathrm{id}_A \otimes \mathrm{tr})(X)$$

If $X_{AB} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ then the partial trace gives the density matrix of the reduced system denoted by $X_A \in \mathcal{D}(\mathbb{C}^{d_A})$.

2.3 Positive and completely positive maps

Definition 9 (Positive map). *A map $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ is positive iff*

$$P(X) \geq 0 \quad \forall X \in \mathcal{P}(\mathbb{C}^{d_A}).$$

We note that an equivalent definition for positive maps is that

$$\langle b| P(|a\rangle \langle a|) |b\rangle \geq 0 \quad \forall |a\rangle \in \mathbb{C}^{d_A}, |b\rangle \in \mathbb{C}^{d_B} \tag{8}$$

Definition 10 (Completely positive maps). *A map $P : \mathcal{L}(\mathbb{C}^{d_B}) \to \mathcal{L}(\mathbb{C}^{d_{B'}})$ is completely positive if and only if*

$$(\mathrm{id}_{d_A} \otimes P)(X) \geq 0 \quad \forall X \in \mathcal{P}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$$

A positive but not completely positive map is the transposition map $\vartheta : \mathcal{L}(\mathbb{C}^{d}) \to \mathcal{L}(\mathbb{C}^{d})$ with respect to the computational basis defined as

$$\vartheta(X) = X^T. \tag{9}$$

We see that ϑ is not completely positive by applying $(\mathrm{id} \otimes \vartheta)$ to the vector defined in equation (4).

$$(\mathrm{id} \otimes \vartheta)(|\Omega\rangle \langle\Omega|) = \sum_{ij} (\mathrm{id} \otimes \vartheta)(|ii\rangle \langle jj|) = \sum_{ij} |ij\rangle \langle ji| \tag{10}$$

which has eigenvalues ±1. ϑ is therefore not completely positive.

Definition 11 (Trace preserving map). *A map $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ is called trace preserving if*

$$\mathrm{tr}(P(X)) = \mathrm{tr}(X), \ \forall X \in \mathcal{L}(\mathbb{C}^{d_A}). \tag{11}$$

Definition 12 (Unital map)**.** *A map $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ is called unital if*

$$P(\mathbb{1}_{d_A}) = \mathbb{1}_{d_B} \tag{12}$$

Another useful definition is the adjoint of a map

Definition 13 (Adjoint map)**.** *Let $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ be a linear map. Then the adjoint of the map P is the map $P^* : \mathcal{L}(\mathbb{C}^{d_B}) \to \mathcal{L}(\mathbb{C}^{d_A})$ such that*

$$\langle X^\dagger P(Y)\rangle = \langle P^*(X)^\dagger Y\rangle \;\forall X \in \mathcal{L}(\mathbb{C}^{d_B}),\; Y \in \mathcal{L}(\mathbb{C}^{d_A}). \tag{13}$$

If P is trace preserving, then P^* is unital. This is seen by

$$\mathrm{tr}(\mathbb{1}_{d_A}\rho) = 1 = \mathrm{tr}(\mathbb{1}_{d_B}P(\rho)) = \mathrm{tr}(P^*(\mathbb{1}_{d_B})\rho),\; \forall\; \rho \in \mathcal{D}(\mathbb{C}^{d_A}). \tag{14}$$

Then

$$P^*(\mathbb{1}_{d_B}) = \mathbb{1}_{d_A}. \tag{15}$$

Another property is that a map P is positive iff P^* is positive. This can be seen by using the definition of a positive map from Equation (8)

$$0 \le \langle b|\, P(|a\rangle\langle a|)\, |b\rangle \quad \forall\, |a\rangle \in \mathbb{C}^{d_A}, |b\rangle \in \mathbb{C}^{d_B}. \tag{16}$$

Rewriting this using the trace, and the adjoint map P^*

$$0 \le \langle b|\, P(|a\rangle\langle a|)\, |b\rangle = \mathrm{tr}(|b\rangle\langle b|\, P(|a\rangle\langle a|)) = \mathrm{tr}(P^*(|b\rangle\langle b|)\, |a\rangle\langle a|) = \langle a|\, P^*(|b\rangle\langle b|)\, |a\rangle\,. \tag{17}$$

2.4 Choi-Jamiolkowski representation

Definition 14 (Choi-Jamiolkowski representation of maps [22])**.** *The Choi representation of a linear map $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ is the operator $C_P \in \mathcal{L}(\mathbb{C}^{d_B} \otimes \mathbb{C}^{d_A})$ given by:*

$$C_P = (\mathrm{id} \otimes \mathrm{P})\,(|\Omega\rangle\langle\Omega|)\,, \tag{18}$$

where $|\Omega\rangle$ is the vector defined in equation (4).

Lemma 1. *The inverse of the map $P \mapsto C_P$ is given by*

$$P(\rho) = (\mathrm{tr} \otimes \mathrm{id})\Big((\rho^T \otimes \mathbb{1})C_P\Big) \tag{19}$$

where ρ^T is the transpose of ρ in the computational basis.

Proof. This can be seen by inserting the definition of the Choi-Jamiolkowski representation

$$\begin{aligned} P(\rho) &= (\mathrm{tr} \otimes \mathrm{id})[(\rho^T \otimes \mathbb{1})\,((\mathrm{id} \otimes P)(|\Omega\rangle\langle\Omega|))] \\ &= (\mathrm{tr} \otimes \mathrm{id})\Big((\rho^T \otimes \mathbb{1})\sum_{ij} |i\rangle\langle j| \otimes P(|i\rangle\langle j|)\Big) \\ &= \sum_{ij} \mathrm{tr}(\rho^T\, |i\rangle\langle j|) \cdot P(|i\rangle\langle j|) \\ &= \sum_{ij} \rho_{ij} P(|i\rangle\langle j|) = \sum_{ij} P(\rho_{ij}\, |i\rangle\langle j|) = P(\rho), \end{aligned} \tag{20}$$

where ρ_{ij} are the coefficients of the density matrix ρ in the computational basis. □

Lemma 2 ([22])**.** *The Choi-Jamiolkowski has the following properties*

1. *A map P is positive iff*

$$tr((|b\rangle\langle b| \otimes |a\rangle\langle a|)C_P) \ge 0 \quad \forall\, |b\rangle \in \mathbb{C}^{d_B}, |a\rangle \in \mathbb{C}^{d_A} \tag{21}$$

2. *A map P is completely positive iff $C_P \ge 0$.*

3. *There is a one-to-one correspondence between a linear map and its Choi-Jamiolkowski representation.*

Proof. To prove property 1, we use that a map $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$, by equation (8) is positive iff

$$\langle b| P(|a\rangle\langle a|) |b\rangle \geq 0 \quad \forall |b\rangle \in \mathbb{C}^{d_B}, |a\rangle \in \mathbb{C}^{d_A} \tag{22}$$

This can rewritten using Lemma 1

$$\begin{aligned} 0 &\leq \langle b| P(|a\rangle\langle a|) |b\rangle && (23)\\ &= \langle b| (\mathrm{tr} \otimes \mathrm{id})\Big((|a\rangle\langle a|^T \otimes \mathbb{1})C_P\Big) |b\rangle && (24)\\ &= \mathrm{tr}\Big((\mathrm{tr} \otimes \mathrm{id})\Big((|a\rangle\langle a|^T \otimes \mathbb{1})C_P\Big) |b\rangle\langle b|\Big) && (25)\\ &= \mathrm{tr}\Big(\Big(|a\rangle\langle a|^T \otimes |b\rangle\langle b|\Big) C_P\Big). && (26) \end{aligned}$$

As $|a\rangle\langle a|$ is Hermitian it follows that $|a\rangle\langle a|^T = \overline{|a\rangle\langle a|}$, and $\overline{|a\rangle} \in \mathbb{C}^{d_A}$.

Property 2 is proved by using that if a map $P : \mathcal{L}(\mathbb{C}^{d_B}) \to \mathcal{L}(\mathbb{C}^{d_{B'}})$ is completely positive, then by Definition 10

$$(\mathrm{id}_{d_A} \otimes P)(\rho) \geq 0, \quad \rho \in \mathcal{P}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}) \tag{27}$$

We can write ρ using the spectral decomposition, with eigenvectors $|a_i\rangle \in (\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$. Equation (27) is then only true if

$$(\mathrm{id}_{d_A} \otimes P)(|a_i\rangle\langle a_i|) \geq 0 \quad \forall i. \tag{28}$$

Finally using that $|a_i\rangle$ can be written using the vector from Equation (4) as is stated in [22]

$$|a_i\rangle = (\mathbb{1}_{d_A} \otimes B) |\Omega\rangle \quad \text{for some } B \in \mathcal{L}(\mathbb{C}^{d_B}) \tag{29}$$

Equation (28) is thefore only true if

$$(id_{d_A} \otimes P)(|\Omega\rangle\langle\Omega|) \geq 0. \tag{30}$$

To prove property 3 we argue that the map $P \mapsto C_P$ is surjective. Any operator $C_P \in \mathcal{L}(\mathbb{C}^{d_B} \otimes \mathbb{C}^{d_A})$ can be written using the block form

$$C_P = \begin{bmatrix} X_{11} & \dots & X_{1d_A} \\ \vdots & \ddots & \vdots \\ X_{d_A 1} & \dots & X_{d_A d_A} \end{bmatrix}, \quad \text{for } X_{ij} \in \mathcal{L}(\mathbb{C}^{d_B}). \tag{31}$$

Using Definition 14, C_P can however also be written using a linear map $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ as

$$C_P = \begin{bmatrix} P(|1\rangle\langle 1|) & \dots & P(|1\rangle\langle d_A|) \\ \vdots & \ddots & \vdots \\ P(|d_A\rangle\langle 1|) & \dots & P(|d_A\rangle\langle d_A|) \end{bmatrix}. \tag{32}$$

We can now choose the map $P(\rho) = \sum_{ij} \rho_{ij} P(|i\rangle\langle j|) = \sum_{ij} \rho_{ij} X_{ij}$, where ρ_{ij} are the coefficients of ρ in the computational basis. This shows that there exists a linear map for every linear operator. □

2.5 Matrix representation

In the following we describe how linear maps are represented as matrices in PICOS [9].

First, we are going to need a new operator.

Definition 15 (Hat operator on matrices). *The hat operator of $X \in \mathcal{L}(\mathbb{C}^d)$ is a vector defined by*

$$\widehat{X} = \sum_{i,j} x_{ij} \widehat{|i\rangle\langle j|} = \sum_{i,j} x_{ij} |ij\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d \tag{33}$$

where x_{ij} are the coefficients of X in the computational basis.

Definition 16 (Hat operator on maps). *The hat operator of a linear map $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ is defined as the matrix*

$$\widehat{P} = \sum_{ijkl} P(|i\rangle\langle j|)_{kl} |kl\rangle\langle ij| \tag{34}$$

where $P(|i\rangle\langle j|)_{kl} = \langle k| P(|i\rangle\langle j|) |l\rangle$.

Now we can define the matrix representation

Theorem 1. *Let $X \in \mathcal{L}(\mathbb{C}^{d_A})$ and $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$. Then*

$$\widehat{P(X)} = \widehat{P} \cdot \widehat{X}.$$

Proof. It is seen by the definition of the two matrices

$$\begin{aligned} \widehat{P} \cdot \widehat{X} &= \sum_{ijklmn} P(|i\rangle \langle j|)_{kl} |kl\rangle \langle ij| X_{mn} |mn\rangle \\ &= \sum_{ijklmn} X_{mn} P(|i\rangle \langle j|)_{kl} |kl\rangle \langle ij|mn\rangle \\ &= \sum_{klmn} P(X_{mn} |m\rangle \langle n|)_{kl} |kl\rangle = \widehat{P(X)}. \end{aligned} \tag{35}$$

□

3 Quantum Information Theory

Quantum information theory is the study of how to store, process and communicate information using quantum systems. This section aims to introduce and explain some of the most basic definitions, as well as two examples of quantum information theory: superdense coding and quantum teleportation.

3.1 Quantum states

Associated to any isolated quantum system is a Hilbert space $\mathbb{C}^d$. Vectors $|\psi\rangle \in \mathbb{C}^d$, are called pure states. The system can be completely described by a density operator on the relevant Hilbert space as $|\psi\rangle \langle\psi|$.

Definition 17 (Density matrix for an ensemble of states)**.** *The density matrix of an ensemble of states $\{p_i, |\psi_i\rangle\}$ is a convex combination of states*

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$$

where $\{p_i \geq 0\}$ form a probability distribution.

The above definition describes a single quantum system. To combine systems, the tensor product as defined in Definition 6 is used.

Definition 18 (Bipartite state)**.** *The state of two combined systems, A and B, is described by a density matrix*

$$\rho_{AB} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}).$$

We call this a bipartite state.

Similarly, a multipartite state on systems $A, B \dots N$ is described by a density matrix

$$\rho_{AB\dots N} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \dots \otimes \mathbb{C}^{d_N}).$$

Definition 19 (Quantum channel)**.** *A quantum channel is a completely positive trace-preserving linear map $P : \mathcal{D}(\mathbb{C}^{d_A}) \to \mathcal{D}(\mathbb{C}^{d_B})$.*

The properties of quantum channels ensure that if the input in the channel is a density matrix, then so is the output. Clearly, then, the quantum channel must be trace preserving so that if the input is a density matrix, the output must have trace 1, too. If a quantum channel is applied partially to a bipartite state, the output must still be positive, which implies complete positivity.

3.2 Entanglement

Definition 20 (Separability)**.** *A bipartite state $\rho \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ is called separable if and only if it can be written as a convex combination of product states:*

$$\rho_{AB} = \sum_i p_i \phi_i^A \otimes \tau_i^B \tag{36}$$

Where $\phi_i^A \in \mathcal{D}(\mathbb{C}^{d_A})$ and $\tau_i^B \in \mathcal{D}(\mathbb{C}^{d_B})$, and $p_i \geq 0$ and $\sum_i p_i = 1$. If a state is not separable it is called entangled.

The set of separable states in $\mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ is denoted SEP(A:B), where A:B denotes the bipartition into systems A and B.

An example of an entangled state is the maximally entangled state

$$\omega = \frac{1}{d} |\Omega\rangle \langle\Omega| , \tag{37}$$

where $|\Omega\rangle$ is the vector defined in equation (4).

3.3 Measurements

Definition 21 (POVM operators)**.** *A positive operator valued measure (POVM) is a set of positive operators $\{P_i\} \subseteq \mathcal{P}(\mathbb{C}^d)$ which satisfy $\sum_i P_i = \mathbb{1}$.*

Definition 22 (Probability of measurement)**.** *The probability of obtaining outcome i when measuring with $\{P_i\}$ on some state $\rho \in \mathcal{D}(\mathbb{C}^d)$ is given by*

$$p(i) = \mathrm{tr}(P_i\rho) \tag{38}$$

The properties of the measurement operators ensures that the probabilities are normalised on quantum states

$$\sum_i p(i) = \sum_i \mathrm{tr}(P_i\rho) = \mathrm{tr}(\mathbb{1}_d\rho) = 1. \tag{39}$$

Definition 23 (Measurement-prepare map)**.** *Let $\{P_i\}$ be a set of POVM operators. Then the map that prepares the state $\sigma_i \in \mathcal{D}(\mathbb{C}^d)$ conditioned on the measurement outcome i, is*

$$M(\rho) = \sum_i \mathrm{tr}(P_i\rho)\sigma_i \tag{40}$$

Definition 24 (Entanglement breaking map)**.** *A map $P : \mathcal{D}(\mathbb{C}^{d_B}) \to \mathcal{D}(\mathbb{C}^{d_{B'}})$ is called entanglement breaking if*

$$(\mathrm{id}_A \otimes P)(\rho_{AB}) \in \mathit{SEP}(A:B') \; \forall \rho_{AB} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}). \tag{41}$$

Theorem 2 (Measurement-prepare map as entanglement breaking map [12])**.** *A map $P : \mathcal{D}(\mathbb{C}^d) \to \mathcal{D}(\mathbb{C}^{d'})$ is entanglement breaking iff it is a measurement-prepare map.*

3.4 Applications of entanglement

3.4.1 Superdense coding

We follow the superdense coding protocol described in [17].

Superdense coding is a protocol that allows two parties, Alice and Bob, to transmit two classical bits from Alice to Bob, by only sending one qubit.The protocol requires Alice and Bob to share a pair of qubits in the maximally entangled state defined in equation (4)

$$|\omega\rangle = \frac{1}{\sqrt{2}} |\Omega\rangle , \tag{42}$$

The protocol also requires two operators, called the Pauli matrices:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad\qquad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

By applying a combination of these matrices to her qubit, Alice can encode two classical bits as follows:

$$00 : |\omega\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{43}$$

$$01 : (\sigma_x \otimes \mathbb{1}_B) |\omega\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{44}$$

$$10 : (\sigma_z \otimes \mathbb{1}_B) |\omega\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{45}$$

$$11 : (\sigma_x\sigma_z \otimes \mathbb{1}_B) |\omega\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}} \tag{46}$$

These four states form an orthonormal basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$ called the Bell basis. If Alice sends her qubit to Bob, so he is in possession of both, he can distinguish which two bits Alice encoded by a measurement in this Bell basis because of the orthonormality.

3.4.2 Quantum teleportation

Whereas superdense coding requires the two parties to send quantum information, the quantum teleportation protocol allows the transferring of quantum information from one system to another, using only classical communication, and shared entanglement. The protocol was first proposed in [1].

The protocol uses three systems: Alice's two systems, A′ and A, and Bob's system B. Systems A and B are in the maximally entangled state ω_{AB} from Equation (37). The state Alice wishes to send to Bob is described by the density operator ρ. We will denote who is in possession of ρ by the subscript $\rho_{A'}$. The protocol can be divided into three steps as follows:

1. Alice measures system $A'A$ in the Bell basis, that is, with operators: $P_{ij} = \frac{1}{\sqrt{d}} |\phi_{ij}\rangle \langle\phi_{ij}|$, where

$$|\phi_{ij}\rangle = \frac{1}{\sqrt{2}}(\sigma_x^i \sigma_z^j \otimes \mathbb{1}_A) |\Omega\rangle_{A'A}, i, j \in \{0, 1\} \tag{47}$$

and where $|\Omega\rangle_{A'A} \in (\mathbb{C}^2 \otimes \mathbb{C}^2)$ is the vector from Equation (4). This can described by the measurement prepare map from Definition 23, but where the prepare part is classical. We only measure on system A and A′ using the Bell basis and apply the identity on system B.

$$\begin{aligned}
&(M \otimes \mathrm{id}_B)(\rho_{A'} \otimes \omega_{AB}) = \sum_{ij} \mathrm{tr}_{A'A}(|\phi_{ij}\rangle \langle\phi_{ij}| \otimes \mathbb{1}_B(\rho_{A'} \otimes \omega_{AB})) \otimes |ij\rangle \langle ij|_{A'A} \\
=&\frac{1}{2} \sum_{ij}(\langle\phi_{ij}| \otimes \mathbb{1}_B)(\rho_{A'} \otimes \omega_{AB})(|\phi_{ij}\rangle \otimes \mathbb{1}_B) \otimes |ij\rangle \langle ij|_{A'A} \\
=&\sum_{ij} \Big(\big[\langle\Omega|_{A'A} ((\sigma_x^i \sigma_z^j)^\dagger \otimes \mathbb{1}_A)\big] \otimes \mathbb{1}_B \Big)(\rho_{A'} \otimes \omega_{AB})\Big(\big[(\sigma_x^i \sigma_z^j \otimes \mathbb{1}_A) |\Omega\rangle_{A'A}\big] \otimes \mathbb{1}_B \Big) \otimes |ij\rangle \langle ij|_{A'A} \\
=&\frac{1}{4} \sum_{ijklmn} \Big(\langle k|_{A'} (\sigma_x^i \sigma_z^j)^\dagger \otimes \langle k|_A \otimes \mathbb{1}_B \Big)(\rho_{A'} \otimes |ll\rangle \langle mm|_{AB})\Big((\sigma_x^i \sigma_z^j) |n\rangle_{A'} \otimes |n\rangle_A \otimes \mathbb{1}_B \Big) \otimes |ij\rangle \langle ij|_{A'A} \\
=&\frac{1}{4} \left(\sum_{ijklmn} \langle k|_{A'} (\sigma_x^i \sigma_z^j)^\dagger \rho_{A'} (\sigma_x^i \sigma_z^j) |n\rangle_{A'} \langle k|l\rangle \langle m|n\rangle |l\rangle \langle m|_B \right) \otimes |ij\rangle \langle ij|_{A'A} \\
=&\frac{1}{4} \left(\sum_{ijkl} \langle k|_{A'} (\sigma_x^i \sigma_z^j)^\dagger \rho_{A'} (\sigma_x^i \sigma_z^j) |n\rangle_{A'} |k\rangle \langle n|_B \right) \otimes |ij\rangle \langle ij|_{A'A} \\
=&\frac{1}{4} \sum_{ij}(\sigma_x^i \sigma_z^j)^\dagger \rho_B (\sigma_x^i \sigma_z^j) \otimes |ij\rangle \langle ij|_{A'A}
\end{aligned} \tag{48}$$

2. Alice sends outcome i,j of the measurement to Bob.

3. Bob corrects his state with $C_{ij}(\rho) = (\sigma_x^i \sigma_z^j)\rho(\sigma_x^i \sigma_z^j)^\dagger$ conditioned on the outcome i,j:

$$C_{ij}((\sigma_x^i \sigma_z^j)^\dagger \rho_B (\sigma_x^i \sigma_z^j)) = (\sigma_x^i \sigma_z^j)(\sigma_x^i \sigma_z^j)^\dagger \rho_B (\sigma_x^i \sigma_z^j)(\sigma_x^i \sigma_z^j)^\dagger = \rho_B \tag{49}$$

Now state ρ is in system B instead of A′.

4 Detection of Entanglement

Checking if a state is separable is an NP-hard problem [10], which, according to common belief, means that there exists cases which are not possible to solve in polynomial time on a Turing machine. This section will describe two ways to check for entanglement. The "Peres-Horodecki criterion", which is also known as the PPT (Positive Partial Transpose) criterion [13], and the hierarchy of extendibility [6].

Theorem 3 (Hahn-Banach [7]). *Let S be a closed convex set in an complex inner product vector space V, and $x \notin S$ then $\exists w \in V, c \in \mathbb{R}$ such that*

$$\begin{aligned}
&Re(\langle w, x\rangle) < c \\
&Re(\langle w, s\rangle) \geq c, \quad \forall s \in S.
\end{aligned} \tag{50}$$

Theorem 4 (Entanglement witness)**.** *Let $\sigma \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$. If $\sigma \notin SEP(A:B)$, then there exists an Hermitian $W \in \mathcal{L}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$, such that*

$$\begin{aligned} &\operatorname{tr}(W\sigma) < c \\ &\operatorname{tr}(W\rho) \geq c. \quad \forall \rho \in \mathit{SEP(A{:}B)}. \end{aligned} \tag{51}$$

Proof. The set of separable states is per definition a closed convex set. Let $\sigma \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ be an entangled state. Let the Hilbert-Schmidt space be V, and SEP(A:B) our set S, then Theorem 3 states that there exists a $W \in \mathcal{L}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ such that

$$\begin{aligned} &\operatorname{Re}(\langle W, x\rangle) = \operatorname{Re}(\operatorname{tr}(W^\dagger \sigma)) < c \\ &\operatorname{Re}(\langle W, x\rangle) = \operatorname{Re}(\operatorname{tr}(W^\dagger \rho)) \geq c, \forall \rho \in \text{SEP(A:B)}. \end{aligned} \tag{52}$$

W can be choosen to be Hermitian, if we note that

$$\operatorname{Re}(\operatorname{tr}(W^\dagger \sigma)) = \frac{1}{2}\left(\operatorname{tr}(W^\dagger\sigma) + \overline{\operatorname{tr}(W^\dagger\sigma)}\right) \tag{53}$$

$$= \frac{1}{2}\left(\operatorname{tr}(W^\dagger\sigma) + \operatorname{tr}(W^\dagger\sigma^\dagger)\right) \tag{54}$$

$$= \operatorname{tr}\left(\frac{W^\dagger + W}{2}\sigma\right) \tag{55}$$

We can let $c = 0$ if we chose $\widetilde{W} = W - c\mathbb{1}$. Then

$$\operatorname{tr}(\widetilde{W}\sigma) = \operatorname{tr}(W\sigma) - c < 0 \tag{56}$$

and

$$\operatorname{tr}(\widetilde{W}\rho) = \operatorname{tr}(W\rho) - c \geq 0. \tag{57}$$

□

Theorem 5 (Entanglement witness for maps)**.** *A state $\rho \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ is separable if and only if*

$$(\mathrm{id} \otimes P)(\rho) \geq 0, \quad \forall P \textit{ positive map.} \tag{58}$$

Proof. If ρ is separable then by Definition 20

$$\begin{aligned} (\mathrm{id} \otimes P)(\rho) &= (\mathrm{id} \otimes P)\left(\sum_i p_i \phi_i^A \otimes \tau_i^B\right) \\ &= \sum_i p_i \phi_i^A \otimes P(\tau_i^B) \\ &= \sum_i p_i \phi_i^A \otimes P(\tau_i^B) \geq 0 \end{aligned} \tag{59}$$

since $\phi_i^A \geq 0$, $p_i \geq 0$ and $P(\tau_i^B) \geq 0$. Now we need to show that for any σ that is not separable, a positive map P exists such that $(\mathrm{id}_A \otimes P)(\sigma) \geq 0$. For $\sigma \notin SEP(A:B)$, Theorem 4 yields W

$$\operatorname{tr}(W\sigma) < 0 \tag{60}$$

$$\operatorname{tr}(W\rho) \geq 0 \quad \forall \rho \in \text{SEP(A:B)} \tag{61}$$

Now define a linear map $P : \mathcal{L}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ by $W = C_{P^*}$. By Definition 14

$$0 > \operatorname{tr}(C_{P^*}\sigma) = \operatorname{tr}\Big((\mathrm{id} \otimes P^*)(|\Omega\rangle\langle\Omega|)\sigma\Big) = \operatorname{tr}\Big(|\Omega\rangle\langle\Omega|(\mathrm{id} \otimes P)(\sigma)\Big) = \langle\Omega|(\mathrm{id} \otimes P)(\sigma)|\Omega\rangle. \tag{62}$$

This implies that $(id \otimes P)(\sigma) \not\geq 0$.

As discussed in Equation (17), P is positive iff P^*. Using the condition for a positive map from equation (21) we need to check

$$0 \leq \operatorname{tr}((|a\rangle\langle a| \otimes |b\rangle\langle b|)C_{P^*}) \quad \forall\, |a\rangle \in \mathbb{C}^{d_A}, |b\rangle \in \mathbb{C}^{d_B}. \tag{63}$$

We note that $(|a\rangle\langle a| \otimes |b\rangle\langle b|)$ is a separable state for all $|a\rangle, |b\rangle$, so by Equation (61) this proves that P^* and thereby P is positive. □

4.1 PPT criterion

According to Theorem 5 for each entangled state, there exists a map which can be used to certify the entanglement. The PPT criterion uses a specific map, namely the partial transposition.

Theorem 6 (PPT criterion)**.** *Any separable state $\rho_{AB} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ has a positive partial transposition:*

$$(id_A \otimes \vartheta)(\rho_{AB}) \geq 0.$$

Proof. Since the transposition is a positive map, Theorem 5 says that the partial transpose must be positive for all $\rho_{AB} \in \mathrm{SEP}(A:B)$. □

The PPT criterion can be used as a sufficient test for low dimensions. To show this we need the following theorem.

Theorem 7 (Woronowicz theorem [23] [20])**.** *Any positive map $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ for $d_A \cdot d_B \leq 6$ can be written as*

$$P = P_1 + \vartheta \circ P_2$$

where P_1, P_2 are completely positive maps.

Corollary 1 (Sufficiency of PPT condition for small dimensions [13])**.** *For $\dim(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}) \leq 6$ the PPT condition is a sufficient condition for separability.*

Proof. Assuming $\sigma \notin SEP(A:B)$ it follows from Theorem 5 that

$$(\mathrm{id} \otimes P)(\sigma) \ngeq 0 \tag{64}$$

for some positive map $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$. Using Theorem 7, for $d_A \cdot d_B \leq 6$, the map P can be written as $P = P_1 + \vartheta \circ P_2$, for P_1, P_2 completely positive maps. If we introduce a new completely positive map $\widetilde{P}_2 = \vartheta \circ P_2 \circ \vartheta$ we can write P as

$$P = P_1 + \vartheta \circ P_2 = P_1 + \vartheta \circ P_2 \circ \vartheta \circ \vartheta = P_1 + \widetilde{P}_2 \circ \vartheta. \tag{65}$$

To see that $\widetilde{P}_2$ is a completely positive map we need to prove that the Choi representation is positive. Since the transposition map is a positive map, we can also check whether $(C_{\widetilde{P}_2})^T$ is positive:

$$(C_{\widetilde{P}_2})^T = \sum_{ij} (|i\rangle \langle j|)^T \otimes \left(P_2(|j\rangle \langle i|)^T\right)^T = \sum_{ij} |j\rangle \langle i| \otimes P_2(|j\rangle \langle i|) = (\mathrm{id} \otimes P_2)(\omega) = C_{P_2} \tag{66}$$

where $C_{P_2} \geq 0$, since P_2 is completely positive. Thus $\tilde{P}_2$ is also a completely positive map. Equation (64) can now be written as

$$\left(\mathrm{id} \otimes (P_1 + \tilde{P}_2 \circ \vartheta)\right)(\sigma) = (\mathrm{id} \otimes P_1)(\sigma) + (\mathrm{id} \otimes (\tilde{P}_2 \circ \vartheta))(\sigma) = \underbrace{(\mathrm{id} \otimes P_1)}_{\geq 0} \underbrace{(\sigma)}_{\geq 0} + \underbrace{(\mathrm{id} \otimes \tilde{P}_2)}_{\geq 0} \left((id \otimes \vartheta)(\sigma)\right) \ngeq 0 \tag{67}$$

where $(id \otimes \vartheta)(\rho)$ is the partial transpose of σ. Since $P_1, \tilde{P}_2$ are completely positive, and σ is positive, this must imply that the partial transposition of σ is not positive. Since we choose σ arbitrarily, this is also true for any $\sigma \notin$ SEP(A:B). The PPT condition is therefore a sufficient condition for separability for dimensions $d_A \cdot d_B \leq 6$. □

4.2 Extendibility

Definition 25 (k-extendible states [6])**.** *A state $\rho_{AB} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ is called k-extendible if $\exists \sigma_{AB_1 \ldots B_k} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes (\mathbb{C}^{d_B})^{\otimes k})$ such that:*

$$\sigma_{AB_i} = \mathrm{tr}_{B_1 \ldots B_{i-1} B_{i+1} \ldots B_k}(\sigma_{AB_1 \ldots B_k}) = \rho_{AB} \tag{68}$$

That is, taking the trace over all subsystems in B, except for the i'th subsystem, gives the state ρ_{AB}.

We denote $\mathrm{tr}_{B_1 \ldots B_{i-1} B_{i+1} \ldots B_k}$ by $\mathrm{tr}_{\overline{B}_i}$.

Theorem 8. *If a state is separable then it is also k-extendible for all $k \in \mathbb{N}$.*

Proof. If ρ_{AB} is separable, then we can choose:

$$\sigma_{AB_1 \dots B_k} = \sum_i p_i \phi_i \otimes \tau_i^{\otimes k} \quad \text{where } \phi_i \in \mathcal{D}(\mathbb{C}^{d_A}), \tau_i \in \mathcal{D}(\mathbb{C}^{d_B}) \tag{69}$$

Which when plugged into the definition of extendibility gives:

$$\begin{aligned} \sigma_{AB_j} &= \text{tr}_{\overline{B}_j}(\sigma_{AB_1,\dots,B_k}) &(70)\\ &= \sum_i p_i \text{tr}_{\overline{B}_j}(\phi_i \otimes \tau_i^{\otimes k}) &(71)\\ &= \sum_i p_i \phi_i \otimes \tau_i &(72)\\ &= \rho_{AB} &(73) \end{aligned}$$

□

This means that if a state $\rho_{AB} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$, is not k-extendible, then it must be entangled.

The next section is devoted to showing how one checks extendibility in practice.

5 Semidefinite Programming

Semidefinite programming is a subfield of convex optimization. A semidefinite program (SDP) is a convex optimization with the constraint that the variables we optimize must be positive semidefinite. This means that an SDP consists of an objective function to be optimized, and one or more linear equalities or positive semidefinite conditions. We define it as in [21].

Definition 26 (SDP problem)**.** *An SDP problem is defined as*

$$\begin{aligned} \underset{X}{\textit{maximize}} \quad & \langle A, X \rangle \\ \textit{subject to} \quad & P(X) = B \\ & X \geq 0 \end{aligned} \tag{74}$$

where $A, X \in \mathcal{L}(\mathbb{C}^{d_A}), B \in \mathcal{L}(\mathbb{C}^{d_B})$ are Hermitian matrices, and $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ is a Hermiticity-preserving linear map.

A useful property of semidefinite programming is its ability to check feasibility. Instead of searching for an optimal value, we construct an SDP such that it checks if there exists a solution which satisfies the constraints. This can be done by choosing a *trivial* objective such as:

$$\begin{aligned} \underset{X}{\text{maximize}} \quad & \langle 0, X \rangle \\ \text{subject to} \quad & P(X) = B \\ & X \geq 0 \end{aligned} \tag{75}$$

Any feasible solution gives the optimal value.

Theorem 9 (Extendibility as an SDP)**.** *Extendibility can be formulated as an SDP by:*

$$\begin{aligned} \underset{\sigma_{AB_1 \dots B_k}}{\text{maximize}} \quad & \langle 0, \sigma_{AB_1 \dots B_k} \rangle \quad \text{for } \sigma_{AB_1 \dots B_k} \in \mathcal{L}(\mathbb{C}^{d_A} \otimes (\mathbb{C}^{d_B})^{\otimes k}) \\ \text{subject to} \quad & \text{tr}(\sigma_{AB_1 \dots B_k}) = 1 \\ & \text{tr}_{\overline{B}_i}(\sigma_{AB_1 \dots B_k}) = \rho_{AB}, \ \forall i \in [k] \\ & \sigma_{AB_1 \dots B_k} \geq 0 \end{aligned} \tag{76}$$

To solve the semidefinite program from Theorem 9 we use one of the solvers already available. Specifically, we use PICOS [9], which is a high level library that lets us define the objective function and the linear constraints. PICOS then setup the problem and calls the solver, which in our case is Mosek [16].

PICOS uses the matrix representation of maps described in Section 2.5, so we must reformulate the constraints of the SDP to match this notation

$$\begin{aligned} \text{maximize} \quad & 0 \quad \textit{for } \sigma_{AB_1\dots B_k} \in \mathcal{L}(\mathbb{C}^{d_A} \otimes (\mathbb{C}^{d_B})^{\otimes k}) \\ \text{subject to} \quad & \widehat{\text{tr}} \cdot \widehat{\sigma}_{AB_1\dots B_k} = 1 \\ & \widehat{\text{tr}_{\overline{B}_i}} \cdot \widehat{\sigma}_{AB_1\dots B_k} = \widehat{\rho}_{AB} \quad \forall i \in [k] \\ & \sigma_{AB_1\dots B_k} \geq 0 \end{aligned} \tag{77}$$

To write this SDP in the standard form, we need to concatenate the equality constraints into one. This can be done using block matrices

$$\begin{aligned} \text{maximize} \quad & 0 \quad \textit{for } \sigma_{AB_1\dots B_k} \in \mathcal{L}(\mathbb{C}^{d_A} \otimes (\mathbb{C}^{d_B})^{\otimes k}) \\ \text{subject to} \quad & \begin{bmatrix} \widehat{tr} & 0 & \dots & 0 \\ 0 & \widehat{\text{tr}_{\overline{B}_1}} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \widehat{\text{tr}_{\overline{B}_k}} \end{bmatrix} \cdot \begin{bmatrix} \widehat{\sigma}_{AB_1\dots B_k} \\ \widehat{\sigma}_{AB_1\dots B_k} \\ \vdots \\ \widehat{\sigma}_{AB_1\dots B_k} \end{bmatrix} = \begin{bmatrix} 1 \\ \widehat{\rho}_{AB} \\ \vdots \\ \widehat{\rho}_{AB} \end{bmatrix} \\ & \sigma_{AB_1\dots B_k} \geq 0 \end{aligned} \tag{78}$$

This SDP does not scale well with dimension, as the dimensions of our extended state is $d_A \cdot d_B^k$. That is, it scales exponentially with the number of extensions. As will be shown a solution to this problem is requiring that the extensions are symmetric.

6 Symmetric Subspace

This section follows the lines of [11].

Definition 27 (The permutation operator [11]). *Let S_n denote the symmetric group on [n]. Then we define the permutation operator on $(\mathbb{C}^d)^{\otimes n}$, as*

$$P_d(\pi) = \sum_{i_1\dots i_n \in [d]} |i_{\pi^{-1}(1)} \dots i_{\pi^{-1}(n)}\rangle \langle i_1 \dots i_n| \,. \tag{79}$$

For $\pi_1, \pi_2 \in S_n$, $P_d(\pi_1\pi_2) = P_d(\pi_1)P_d(\pi_2)$, which can be seen by

$$\begin{aligned} P_d(\pi_1) \cdot P_d(\pi_2) |i_1 i_2 \dots i_n\rangle &= P_d(\pi_1) |i_{\pi_2^{-1}(1)} \dots i_{\pi_2^{-1}(n)}\rangle \\ &= |i_{\pi_1^{-1}(\pi_2^{-1}(1))} \dots i_{\pi_1^{-1}(\pi_2^{-1}(n))}\rangle \\ &= P_d(\pi_1\pi_2) |i_1 i_2 \dots i_n\rangle \,. \end{aligned} \tag{80}$$

Definition 28 (The Symmetric Subspace [11]). *The symmetric subspace is the space of permutation symmetric vectors:*

$$\vee^n \mathbb{C}^d = \{|\psi\rangle \in (\mathbb{C}^d)^{\otimes n} : P_d(\pi) |\psi\rangle = |\psi\rangle \;\; \forall \pi \in S_n\}.$$

Definition 29 (The symmetric projector [11]). *The symmetric projector is defined as*

$$P_{sym}^{d,n} = \frac{1}{n!} \sum_{\pi \in S_n} P_d(\pi).$$

Theorem 10 (Symmetric projector as orthogonal projector [11]). *$P_{sym}^{d,n}$ is the orthogonal projector onto $\vee^n \mathbb{C}^d$*

Proof. A projector is orthogonal if it is Hermitian. We check:

$$\begin{aligned} (P_{sym}^{d,n})^\dagger &= \frac{1}{n!} \left(\sum_{\pi \in S_n} \sum_{i_1\dots i_n \in [d]} |i_{\pi^{-1}(1)} \dots i_{\pi^{-1}(n)}\rangle \langle i_1 \dots i_n| \right)^\dagger \\ &= \frac{1}{n!} \sum_{\pi \in S_n} \sum_{i_1\dots i_n \in [d]} |i_1 \dots i_n\rangle \langle i_{\pi^{-1}(1)} \dots i_{\pi^{-1}(n)}| \\ &= \frac{1}{n!} \sum_{\pi \in S_n} P_d(\pi^{-1}) \\ &= P_{sym}^{d,n}. \end{aligned} \tag{81}$$

Left to show is that $P_{sym}^{d,n}$ is a projection

$$(P_{sym}^{d,n})^2 = \frac{1}{n!}\sum_{\pi\in S_n} P_d(\pi)P_{sym}^{d,n}.$$

By

$$P_d(\pi)P_{sym}^{d,n} = P_d(\pi)\frac{1}{n!}\sum_{\pi'\in S_n} P_d(\pi') = \frac{1}{n!}\sum_{\pi'\in S_n} P_d(\pi\pi') = \frac{1}{n!}\sum_{\pi^{-1}\pi'\in S_n} P_d(\pi') = \frac{1}{n!}\sum_{\pi'\in S_n} P_d(\pi') = P_{sym}^{d,n}, \tag{82}$$

we find that

$$(P_{sym}^{d,n})P_{sym}^{d,n} = \frac{1}{n!}\sum_{\pi\in S_n} P_d(\pi)P_{sym}^{d,n} = \frac{1}{n!}\sum_{\pi\in S_n} P_{sym}^{d,n} = P_{sym}^{d,n}.$$

And thus the symmetric projector is orthogonal, and a projector.

To prove that $P_{sym}^{d,n}$ is the projector onto the symmetric subspace we must show that $\vee^n\mathbb{C}^d = \mathrm{Im}(P_{sym}^{d,n})$. We find that if $|\psi\rangle \in \vee^n\mathbb{C}^d$, then $|\psi\rangle = P_d(\pi)|\psi\rangle \;\; \forall\pi\in S_n$, and $P_d(\pi)P_{sym}^{d,n}|\psi\rangle = P_{sym}^{d,n}|\psi\rangle$ by Equation (82). Therefore we have $\mathrm{Im}(P_{sym}^{d,n}) \subseteq \vee^n\mathbb{C}^d$.

We also see that for $|\psi\rangle \in \vee^n\mathbb{C}^d$,

$$P_{sym}^{d,n}|\psi\rangle = \frac{1}{n!}\sum_{\pi\in S_n} P_d(\pi)|\psi\rangle = |\psi\rangle, \tag{83}$$

which shows that $\vee^n\mathbb{C}^d \subseteq \mathrm{Im}(P_{sym}^{d,n})$. □

We will now introduce an important identity of the symmetric subspace. First, we define space A by the span of symmetric product vectors in $\mathbb{C}^d$:

$$A = \mathrm{span}\{|\psi\rangle^{\otimes n} : |\psi\rangle \in \mathbb{C}^d\}. \tag{84}$$

Definition 30 (Type vector)**.** *The type of $\vec{i} \in (i_1,\ldots,i_n)$, $i_i \in [d]$, is a vector, $T(\vec{i})$, for which the j'th element counts how many times j appears in $\vec{i}$. The set of type vectors for $n,d\in\mathbb{N}$ is defined by:*

$$\mathcal{I}_{d,n} = \{(t_1,\ldots,t_d) : t_1,\ldots,t_d\in\mathbb{N}, t_1+\ldots+t_d = n\}.$$

By this definition we define another space by

$$B = \mathrm{span}\{|s_{\vec{t}}\rangle : \vec{t}\in\mathcal{I}_{d,n}\}, \tag{85}$$

where $|s_{\vec{t}}\rangle$ is defined by:

$$|s_{\vec{t}}\rangle = \sum_{\vec{i}:T(\vec{i})=\vec{t}} \frac{1}{\sqrt{\binom{n}{\vec{t}}}}|i_1\ldots i_n\rangle \tag{86}$$

Theorem 11 (The symmetric subspace [11])**.**

$$\vee^n\,\mathbb{C}^d = A = B. \tag{87}$$

Proof. The vectors which span A and B are permutation invariant. This means that $A\subseteq\vee^n\mathbb{C}^d$ and $B\subseteq\vee^n\mathbb{C}^d$. Now it remains to be proven that $\vee^n\mathbb{C}^d\subseteq A$ and $\vee^n\mathbb{C}^d\subseteq B$.

First, to prove that $\vee^n\mathbb{C}^d = B$ we note that $P_{sym}^{d,n}|i_1\ldots i_n\rangle = \binom{n}{T(\vec{i})}^{-\frac{1}{2}}|s_{T(\vec{i})}\rangle$, and as $P_{sym}^{d,n}$ projects into the symmetric subspace, we have

$$\vee^n\mathbb{C}^d = \mathrm{Im}(P_{sym}^{d,n}) = \mathrm{span}\{(P_{sym}^{d,n}|i_1\ldots i_n\rangle)\} = \mathrm{span}\{|s_{\vec{t}}\rangle : \vec{t}\in\mathcal{I}_{d,n}\} = B$$

To show that $\vee^n\mathbb{C}^d\subseteq A$ we imagine first a polynomial in some finite-dimensional vector space V, $p(x) = |v_0\rangle + x|v_1\rangle + x^2|v_2\rangle + \ldots + x^d|v_d\rangle \in V$, $|v_0\rangle\ldots|v_d\rangle\in V$. If W is a subspace of V such that $p(x)\in W\;\forall x\in\mathbb{C}$ then $|v_0\rangle\ldots|v_d\rangle\in W$ by the following argument, since finite-dimensional subspaces are closed

$$v_0 = p(0)\in W$$

$$v_1 = p'(0) = \lim_{h\to 0}\frac{\overbrace{p(h)}^{\in W} - \overbrace{p(0)}^{\in W}}{h}\in W.$$

This can be extended to a multivariate polynomial $p(x_1, x_2, \dots, x_d)$. If we let $|v_{k_1 k_2 \dots k_d}\rangle$ denote the coefficient of the term $x_1^{k_1} x_2^{k_2} \dots x_d^{k_d}$, then these coefficients can be written using partial derivatives. Iterating the same argument as the single variable polynomial, it follows that the coefficients of the multivariate polynomial also is in W.

$$|v_{k_1 \dots k_d}\rangle = \frac{1}{k_1! \dots k_d!} \frac{\partial^{k_1}}{\partial x_1^{k_1}} \frac{\partial^{k_2}}{\partial x_2^{k_2}} \cdots \frac{\partial^{k_d}}{\partial x_d^{k_d}} \, p(0, 0, \dots, 0) \in W \tag{88}$$

Now consider the polynomial

$$|p(x_1, \dots, x_d)\rangle = \left(\sum_{i=1}^{d} x_i \, |i\rangle \right)^{\otimes n} . \tag{89}$$

This is in A for all $x_1, \dots, x_d$ as it is a product state. Equation (89) can also be written using the vectors introduced in Equation (86)

$$|p(x_1, \dots, x_d)\rangle = \sum_{i_1, \dots, i_n} x_{i_1} \dots x_{i_n} c_{\vec{t}} |s_{\vec{t}}\rangle . \tag{90}$$

where $c_{\vec{t}}$ is some coefficient. We note that $|s_{\vec{t}}\rangle \in B$, and as previously shown $B = \vee^n \mathbb{C}^d$. If we let $V = A$ and $W = \vee^n \mathbb{C}^d$ the above argument proves that $\vee^n \mathbb{C}^d \subseteq A$. □

Theorem 12. [11] *Let* $L, M \in \mathcal{L}(\vee^n \mathbb{C}^d)$ *such that*

$$\langle \gamma^{\otimes n} | \, L \, | \gamma^{\otimes n} \rangle = \langle \gamma^{\otimes n} | \, M \, | \gamma^{\otimes n} \rangle \quad \forall \, |\gamma\rangle \in \mathbb{C}^d \tag{91}$$

then $L = M$.

Proof. As $\vee^n \mathbb{C}^d = \operatorname{span}\{|\phi\rangle^{\otimes n} : |\phi\rangle \in \mathbb{C}^d\}$ we have $L = M$ if

$$\langle \beta^{\otimes n} | \, L \, | \alpha^{\otimes n} \rangle = \langle \beta^{\otimes n} | \, M \, | \alpha^{\otimes n} \rangle \quad \forall \, |\alpha\rangle, |\beta\rangle \in \mathbb{C}^d. \tag{92}$$

For fixed $|\alpha\rangle, |\beta\rangle$ we define

$$|v_{x,y}\rangle = e^{ix} \, |\alpha\rangle + e^{iy} \, |\beta\rangle \quad \text{for } \ |\alpha\rangle, |\beta\rangle \in \mathbb{C}^d \tag{93}$$

We note that

$$|v_{x,y}\rangle^{\otimes n} = \sum_{k_1, \dots, k_n \in \{0,1\}^n} e^{i\left(\left(\sum_{s=1}^n k_s\right)x + \left(n - \sum_{s=1}^n k_s\right)y\right)} \, |\tau_{k_1} \tau_{k_2} \dots \tau_{k_n}\rangle \tag{94}$$

where $|\tau_0\rangle = |\alpha\rangle, |\tau_1\rangle = |\beta\rangle$. Using this, we can compute

$$\frac{1}{(2\pi)^2} \int_0^{2\pi} dx \int_0^{2\pi} dy \; e^{in(y-x)} \left(|v_{x,y}\rangle \langle v_{x,y}| \right)^{\otimes n} \tag{95}$$

$$= \frac{1}{(2\pi)^2} \int_0^{2\pi} dx \int_0^{2\pi} dy \; e^{in(y-x)} \sum_{\substack{k_1, \dots k_n \\ l_1, \dots, l_n}} e^{i\left(\left(\sum_{s=1}^n k_s - \sum_{s=1}^n l_s\right)x + \left(\sum_{s=1}^n l_s - \sum_{s=1}^n k_s\right)y\right)} \, |\tau_{k_1} \dots \tau_{k_n}\rangle \langle \tau_{l_1} \dots \tau_{l_n}| \tag{96}$$

$$= \sum_{\substack{k_1, \dots k_n \\ l_1, \dots, l_n}} |\tau_{k_1} \dots \tau_{k_n}\rangle \langle \tau_{l_1} \dots \tau_{l_n}| \, \frac{1}{(2\pi)^2} \int_0^{2\pi} dx \int_0^{2\pi} dy \; e^{i\left(\sum_{s=1}^n k_s - \sum_{s=1}^n l_s - n\right)x} \cdot e^{i\left(\sum_{s=1}^n l_s - \sum_{s=1}^n k_s + n\right)y}. \tag{97}$$

This is only non-zero when

$$\begin{aligned} \sum_{s=1}^n k_s - \sum_{s=1}^n l_s &= n \\ \sum_{s=1}^n l_s - \sum_{s=1}^n k_s &= -n. \end{aligned} \tag{98}$$

The only term that survives is therefore the one where

$$\begin{aligned} \sum_{s=1}^n k_s &= n \\ \sum_{s=1}^n l_s &= 0. \end{aligned} \tag{99}$$

This corresponds to the term where all $k_1, \ldots, k_n = 1$ and $l_1, \ldots, l_n = 0$. Using the definition of $|\tau_k\rangle$ we finally get

$$\frac{1}{(2\pi)^2} \int_0^{2\pi} dx \int_0^{2\pi} dy \; e^{in(y-x)} \left(|v_{x,y}\rangle \langle v_{x,y}| \right)^{\otimes n} = (|\alpha\rangle \langle\beta|)^{\otimes n}. \tag{100}$$

If $\langle \gamma^{\otimes n} | L | \gamma^{\otimes n} \rangle = \langle \gamma^{\otimes n} | M | \gamma^{\otimes n} \rangle \;\; \forall \, |\gamma\rangle \in \mathbb{C}^d$, then Equation (92) can be rewritten using Equation (100) as

$$\begin{aligned} & \langle \beta^{\otimes n} | L | \alpha^{\otimes n} \rangle && (101)\\ &= \mathrm{tr}(L \, |\alpha\rangle \langle\beta|^{\otimes n}) && (102)\\ &= \frac{1}{(2\pi)^2} \int_0^{2\pi} dx \int_0^{2\pi} dy \; e^{in(y-x)} \mathrm{tr}\Big(L \left(|v_{x,y}\rangle \langle v_{x,y}| \right)^{\otimes n} \Big) && (103)\\ &= \frac{1}{(2\pi)^2} \int_0^{2\pi} dx \int_0^{2\pi} dy \; e^{in(y-x)} \mathrm{tr}\Big(M \left(|v_{x,y}\rangle \langle v_{x,y}| \right)^{\otimes n} \Big) && (104)\\ &= \mathrm{tr}(M \, |\alpha\rangle \langle\beta|^{\otimes n}) && (105)\\ &= \langle \beta^{\otimes n} | M | \alpha^{\otimes n} \rangle . && (106) \end{aligned}$$

As $|\alpha\rangle, |\beta\rangle$ were arbitrary, this implies that $L = M$. □

Corollary 2. *The dimension of the symmetric subspace is*

$$\dim(\vee^n \mathbb{C}^d) = \binom{d+n-1}{n} \tag{107}$$

We will denote this by $d\,[n]$.

Proof. There are $\binom{d+n-1}{n}$ ways to choose n elements from a set of d elements if repetitions are allowed. This corresponds to the number of ways to choose $(t_1, \ldots, t_d)$ such that their sum is n. This means that there are $\binom{d+n-1}{n}$ different vectors $\vec{t} \in \mathcal{I}_{d,n}$, which corresponds to the number of basis vectors from equation (86). □

7 Symmetric Extensions

With some of the important properties of the symmetric subspace now introduced, we can define our extensions using symmetry.

Definition 31 (Bose-symmetric k-extendibility)**.** *A state $\rho_{AB} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ is called Bose-symmetric k-extendible if $\exists \widetilde{\sigma}_{AB_1 \ldots B_k} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \vee^k \mathbb{C}^{d_B})$ such that:*

$$\widetilde{\sigma}_{AB_1} = (\mathrm{id}_A \otimes \mathrm{tr}_{[k-1]})(\widetilde{\sigma}_{AB_1 \ldots B_k}) = \rho_{AB} \tag{108}$$

Since the B systems of our Bose-symmetric extensions are in the symmetric subspace, we can use Theorem 11 to rewrite the extensions using the basis $|s_{\vec{t}}\rangle$, from Equation (86). These new extensions have the advantage of being written in a more compact basis, causing the extensions to scale like $d_A \cdot \binom{d_B+k-1}{k}$, which for fixed dimension d_A, d_B, scales like $\mathcal{O}(k^{d_B-1})$ instead of $d_A \cdot d_B^k$, which is $\mathcal{O}(d_B^k)$. Without this polynomial scaling, one would not be able to check for more than a few extensions, since the dimensions of the problem quickly exceed the memory of most computers. This new basis, however, does not explicitly describe the individual systems, but rather only their combined system. This means that we have to redefine the partial trace over all but one system in this new basis in order to get this improvement.

Lemma 3 (Bose trace [19])**.** *Let $\{|s_{\vec{t_1}}\rangle\}$,$\{|s_{\vec{t_2}}\rangle\}$ be the basis of $\vee^n \mathbb{C}^d$ as defined in equation (86), and let $\{|i\rangle_B\}$,$\{|j\rangle_B\}$ be the computational basis of $\mathbb{C}^{d_B}$. Let $|s'_{\vec{t}}(i)\rangle$ denote the vector which arises by lowering the i'th number of $\vec{t}$: $\vec{t}'(i) = (t_1, ..., t_i - 1, ..., t_d)$. Then the map that traces out n-1 systems in the symmetric subspace $tr_{B^{[n-1]}} : \mathcal{D}(\vee^n \mathbb{C}^{d_B}) \to \mathcal{D}(\mathbb{C}^{d_B})$ is*

$$\mathrm{tr}_{B^{[n-1]}} |s_{\vec{t_1}}\rangle \langle s_{\vec{t_2}}| = \sum_{i,j=1}^{d} |i\rangle \langle j|_B \, c_{ij}(\vec{t_1}, \vec{t_2}) \tag{109}$$

Where $c_{ij}(\vec{t_1}, \vec{t_2})$ is defined as

$$\begin{aligned} c_{ij}(\vec{t_1}, \vec{t_2}) &= \mathrm{tr}(|i\rangle \langle j|_B \, \mathrm{tr}_{B^{[n-1]}} |s_{\vec{t_1}}\rangle \langle s_{\vec{t_2}}|) \\ &= \frac{\sqrt{t_{1_i} t_{2_j}}}{n} \langle s'_{\vec{t_1}}(j) | s'_{\vec{t_2}}(i) \rangle \end{aligned} \tag{110}$$

Corollary 3 (Bose-extensions as SDP)**.** *The Bose-symmetric extensions from Definition 31 can be formulated as the following SDP*

$$\begin{aligned} \underset{\widetilde{\sigma}_{AB_1\ldots B_k}}{\text{maximize}} \quad & \langle 0, \widetilde{\sigma}_{AB_1\ldots B_k}\rangle \quad \text{for } \sigma_{AB_1\ldots B_k} \in \mathcal{L}(\mathbb{C}^{d_A} \otimes \vee^k \mathbb{C}^{d_B}) \\ \text{subject to} \quad & \operatorname{tr}(\widetilde{\sigma}_{AB_1\ldots B_k}) = 1 \\ & \operatorname{tr}_{B^{[n-1]}}(\widetilde{\sigma}_{AB_1\ldots B_k}) = \rho_{AB} \\ & \widetilde{\sigma}_{AB_1\ldots B_k} \geq 0 \end{aligned} \tag{111}$$

To prove that Bose-k-extendibility for all k is a sufficient test for entanglement, we need to define some measure of distance between the set of separable states and the set of k-extendible states ρ_{AB}. That is, we look to prove that

$$\text{Dist}(\rho_{AB}, SEP(A:B)) \leq f(k) \underset{k\to\infty}{\longrightarrow} 0 \tag{112}$$

To prove this we will use the Schatten 1-norm.

Definition 32 (Schatten p-norm)**.** *For $X \in \mathcal{L}(\mathbb{C}^d)$ and $p \geq 1$ the Schatten p-norm is*

$$||X||_p = \sqrt[p]{tr(|X|^p)} \tag{113}$$

where $|X| = \sqrt{X^\dagger X}$.

We use two special cases of these norms:

1. Trace-norm: $||X||_1 = \sum_{i=1}^d S_i(X)$.
2. ∞-norm : $||X||_\infty = \max(S_i(X))$. The ∞-norm is techinally not a p-norm but the limit of the p-norm as p goes to infinity: $||X||_p \underset{p\to\infty}{\rightarrow} ||X||_\infty$.

Where $S_i(X)$ are the singular values of X. These two norms are dual.

Theorem 13. *For any $X \in \mathcal{L}(\mathbb{C}^d)$ we have*

$$\begin{aligned} ||X||_\infty &= \sup_{||Y||_1=1} |\langle Y, X\rangle| \\ ||X||_1 &= \sup_{||Y||_\infty=1} |\langle Y, X\rangle| \end{aligned} \tag{114}$$

Proof. Let $X = \sum_{i=1}^d S_i(X) |v_i\rangle \langle w_i|$ be the singular value composition of X. According to the Hölder inequality, $|\langle Y, X\rangle| \leq ||Y||_1 ||X||_\infty$. Therefore we have

$$\sup_{||Y||_1=1} |\langle Y, X\rangle| \leq ||X||_\infty. \tag{115}$$

If we assume that the first singular value is the largest, $S_1 = \max_i S_i(X) = ||X||_\infty$ then we can choose $\widetilde{Y} = |v_1\rangle \langle w_1|$ such that

$$\sup_{||Y||_1=1} |\langle Y, X\rangle| \geq \left| \operatorname{tr}\left(\sum_{i=1}^d S_i |w_1\rangle \langle v_1|v_i\rangle \langle w_i| \right) \right| = S_1 = ||X||_\infty. \tag{116}$$

A similar argument can be used to prove the second duality. Using Hölders inequality again, we have

$$\sup_{||Y||_\infty=1} |\langle Y, X\rangle \leq ||X||_1. \tag{117}$$

If we now choose $\widetilde{Y} = \sum_j |v_j\rangle \langle w_j|$, then we have

$$\begin{aligned} \sup_{||Y||_\infty=1} |\langle Y, X\rangle| &\geq \operatorname{tr}\left(\sum_{j=1}^d \sum_{i=1}^d S_i(X) |w_j\rangle \langle v_j|v_i\rangle \langle w_i| \right) \\ &= \sum_{j=1}^d \sum_{i=1}^d S_i(X) \langle v_i|v_j\rangle \langle w_j|w_i\rangle \\ &= \sum_{i=1}^d S_i(X) = ||X||_1. \end{aligned} \tag{118}$$

□

These two norms can then be used to define a set of operator norms for linear maps

Definition 33 (p → q norm for linear maps). *Let $L : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ be a linear map. Then*

$$||L||_{p\to q} = \sup_{||X||_p=1} ||L(X)||_q \tag{119}$$

Where we are going to need the two special cases

$$\begin{aligned} ||L||_{1\to 1} &= \sup_{||X||_1=1} ||L(X)||_1 \\ ||L||_{\infty\to\infty} &= \sup_{||X||_\infty=1} ||L(X)||_\infty \end{aligned} \tag{120}$$

These two norms are dual $||L||_{1\to1} = ||L^*||_{\infty\to\infty}$. This can be seen by Theorem 13

$$\begin{aligned} ||L||_{1\to1} = \sup_{||X||_1=1} ||L(X)||_1 &= \sup_{||X||_1=1} \sup_{||Y||_\infty=1} |\langle Y, L(X)\rangle \\ &= \sup_{||X||_1=1} \sup_{||Y||_\infty=1} |\langle L^*(Y), X\rangle \\ &= \sup_{||Y||_\infty=1} ||L^*(Y)||_\infty = ||L^*||_{\infty\to\infty}. \end{aligned} \tag{121}$$

We will need

Theorem 14 (Russo-Dye [18]). *Let $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ be a positive, unital map. then*

$$||P||_{\infty\to\infty} = ||P(\mathbb{1}_{d_A})||_\infty = ||\mathbb{1}_{d_B}||_\infty = 1 \tag{122}$$

We can now define the diamond norm and its dual, the CB-norm.

Definition 34 (Diamond norm). *For $L : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ we define*

$$\begin{aligned} ||L||_\diamond &= \sup_{n\in\mathbb{N}} ||id_n \otimes L||_{1\to1} \\ ||L||_{CB} &= \sup_{n\in\mathbb{N}} ||id_n \otimes L||_{\infty\to\infty} \end{aligned} \tag{123}$$

which are dual, i.e. $||L||_\diamond = ||L^*||_{CB}$.

These norms are finite, but the proof of this is beyond the scope of this thesis. We will need the following property of the diamond norm on quantum channels.

Theorem 15. *Let $P : \mathcal{L}(\mathbb{C}^{d_A}) \to \mathcal{L}(\mathbb{C}^{d_B})$ be a quantum channel. Then*

$$||P||_\diamond = 1. \tag{124}$$

Proof. Using the duality of the diamond norm we get

$$||P||_\diamond = ||P^*||_{CB} = \sup_{n\in\mathbb{N}} ||id_n \otimes P^*||_{\infty\to\infty}. \tag{125}$$

Since P is a quantum channel, the adjoint map P^* is unital and completely positive, which allows us to use Theorem 14

$$\sup_{n\in\mathbb{N}} ||id_n \otimes P^*||_{\infty\to\infty} = \sup_{n\in\mathbb{N}} ||(id_n \otimes P^*)(\mathbb{1}_n \otimes \mathbb{1}_{d_B})||_\infty = \sup_{n\in\mathbb{N}} ||(\mathbb{1}_n \otimes \mathbb{1}_{d_A})||_\infty = 1. \tag{126}$$

□

With our distance measure now defined, we are going to need the following property of the symmetric projector.

Theorem 16 (Partial trace of symmetric projector). *For $d, n \in \mathbb{N}$ we have*

$$\mathrm{tr}_{n+1}(P_{sym}^{d,n+1}) = \frac{n+d}{n+1} P_{sym}^{d,n}$$

where tr_{n+1} is the partial trace over the last system.

Proof. Since both sides of the equation are linear operators acting on $(\mathbb{C}^d)^{\otimes n}$, it is enough to show the equality when acting on a basis of $(\mathbb{C}^d)^{\otimes n}$.

$$\mathrm{tr}_{n+1}(P_{sym}^{d,n+1})\left|i_1...i_n\right\rangle = \frac{1}{(n+1)!}\sum_{\pi\in S_{n+1}}\sum_{i_{n+1}=1}^{d}\left\langle i_{\pi^{-1}(n+1)}|i_{n+1}\right\rangle\left|i_{\pi^{-1}(1)}...i_{\pi^{-1}(n)}\right\rangle. \tag{127}$$

Let $S^l_{n+1} := \{\pi \in S_{n+1} : \pi(l) = n+1\}$ be the set of permutations mapping l to $n+1$. This set is isomorphic to S_n where the isomorphism is given by :

$$f_l(\pi(i)) = \begin{cases}\pi(n+1) & \text{if } i = l\\ \pi(i) & \textit{else.}\end{cases} \tag{128}$$

For abbriviation we let $\widetilde{\pi}$ denote $f_l(\pi)$. In Equation (127) the bracket $\left\langle i_{\pi^{-1}(n+1)}|i_{n+1}\right\rangle$ is only 1 for $\pi \in S^l_{n+1}$ when $i_l = i_{n+1}$.

$$\mathrm{tr}_{n+1}(P_{sym}^{d,n+1})\left|i_1...i_n\right\rangle = \frac{1}{(n+1)!}\sum_{i_{n+1}=1}^{d}\sum_{\substack{l\in\{1,...,n+1\}\\ i_l=i_{n+1}}}\sum_{\pi\in S^l_{n+1}}\left|i_{\pi^{-1}(1)}...i_{\pi^{-1}(n)}\right\rangle. \tag{129}$$

Applying f_l we can write

$$\mathrm{tr}_{n+1}(P_{sym}^{d,n+1})\left|i_1...i_n\right\rangle = \frac{1}{(n+1)!}\sum_{i_{n+1}=1}^{d}\sum_{\substack{l\in\{1,...,n+1\}\\ i_l=i_{n+1}}}\sum_{\widetilde{\pi}\in S_n}\left|i_{\widetilde{\pi}^{-1}(1)}...i_{\widetilde{\pi}^{-1}(n)}\right\rangle. \tag{130}$$

Where we used that $(i_{\pi^{-1}(1)}...i_{\pi^{-1}(n)}) = (i_{\widetilde{\pi}^{-1}(1)}...i_{\widetilde{\pi}^{-1}(n)})$, by the definition of f_l. The first two sums correspond to how many of the $(i_1...i_{n+1})$ have the same value as i_{n+1}. Renaming $i_{n+1} = k$ this can be written as $t_k + 1$ where t denotes the type of $(i_1...i_n)$ we get

$$\begin{aligned}\mathrm{tr}_{n+1}(P_{sym}^{d,n+1})\left|i_1...i_n\right\rangle &= \frac{1}{(n+1)!}\sum_{k=1}^{d}(t_k+1)\sum_{\widetilde{\pi}\in S_n}\left|i_{\widetilde{\pi}^{-1}(1)}...i_{\widetilde{\pi}^{-1}(n)}\right\rangle\\ &= \frac{1}{(n+1)!}(n+d)\sum_{\widetilde{\pi}\in S_n}\left|i_{\widetilde{\pi}^{-1}(1)}...i_{\widetilde{\pi}^{-1}(n)}\right\rangle\\ &= \frac{n+d}{n+1}\frac{1}{n!}\sum_{\widetilde{\pi}\in S_n}\left|i_{\widetilde{\pi}^{-1}(1)}...i_{\widetilde{\pi}^{-1}(n)}\right\rangle\\ &= \frac{n+d}{n+1}P_{sym}^{d,n}\left|i_1...i_n\right\rangle\end{aligned} \tag{131}$$

□

Theorem 17 (Symmetric projector as convex set [11, Proposition 6.] [3])**.** *The symmetric projector can be written as a convex combination, i.e.* $P_{sym}^{d,n} \in conv\{\left|\phi\right\rangle\left\langle\phi\right|^{\otimes n} : \left|\phi\right\rangle \in \mathbb{C}^d\}$. *This means that there exist positive numbers* $\{q_i^{d,n}\}_{i=1}^{N_{d,n}}$ *and vectors* $\{\left|\phi_i\right\rangle \in \mathbb{C}^d\}_{i=1}^{N_{d,n}}$ *such that*

$$\sum_{i=1}^{N_{d,n}} q_i^{d,n} = 1, \tag{132}$$

$$P_{sym}^{d,n} = \sum_{i=1}^{N_{d,n}} q_i^{d,n}\left|\phi_i\right\rangle\left\langle\phi_i\right|^{\otimes n}. \tag{133}$$

By [11, Proposition 6.] $P_{sym}^{d,n}$ is in the convex hull of $\left|\phi\right\rangle\left\langle\phi\right|^{\otimes n}$. Using Carathéodory's convex hull theorem [3], the finite convex combination is obtained. The proof of this is out of the scope of this thesis, and is therefore omitted.

Definition 35 (Bose-measurement-prepare map)**.** *The Bose-measurement-prepare map,* $\mathrm{MP}_{n\to k} : \mathcal{L}(\vee^n\mathbb{C}^d) \to \mathcal{L}(\vee^k\mathbb{C}^d)$, *is defined as*

$$MP_{n\to k}(\rho) = \frac{d[n]}{d[n+k]}\mathrm{tr}_{[n]}\big(P_{sym}^{d,n+k}(\rho\otimes\mathbb{1}^{\otimes k})\big), \tag{134}$$

where $\mathrm{tr}_{[n]} = \mathrm{tr}_{1...n}$.

We will show how this is a measurement-prepare map from Definition 23.

Lemma 4. *The Bose-measurement-prepare map has the following properties:*

1. *Entanglement breaking*
2. *Trace-preserving*

Proof. To prove the first property, we rewrite Equation (134) to

$$\begin{aligned}\mathrm{MP}_{n\to k}(\rho) &= \frac{d[n]}{d[n+k]}\mathrm{tr}_{[n]}\left(\sum_{i=1}^{N_{d,n+k}} q_i^{d,n+k}\,|\phi_i\rangle\langle\phi_i|^{\otimes(n+k)}\,(\rho\otimes\mathbb{1}^{\otimes k})\right)\\ &= \frac{d[n]}{d[n+k]}\left(\sum_{i=1}^{N_{d,n+k}} q_i^{d,n+k}\,\langle\phi_i^{\otimes n}|\,\rho\,|\phi_i^{\otimes n}\rangle\,|\phi_i\rangle\langle\phi_i|^{\otimes k}\right).\end{aligned} \tag{135}$$

If we let $P_i = q_i^{d,k+n}\,|\phi_i\rangle\langle\phi_i|^{\otimes n}$, this is a measurement-prepare map from Definition 23 and is therefore entanglement breaking by Theorem 2. The trace-preserving property can be proved by applying the map to a state $\rho\in\mathcal{D}(\vee^n\mathbb{C}^d)$ and taking the trace. Using Equation (134) this can be written as

$$\mathrm{tr}(\mathrm{MP}_{n\to k}(\rho)) = \frac{d[n]}{d[n+k]}\mathrm{tr}_{[n]}\left(\rho\,\mathrm{tr}_{n+1\ldots n+k}(P_{sym}^{d,n+k})\right) \tag{136}$$

We now need to calculate $\mathrm{tr}_{n+1,\ldots,n+k}(P_{sym}^{d,n+k})$ which can be done using Theorem 16.

$$\begin{aligned}\mathrm{tr}_{n+1,\ldots,n+k}(P_{sym}^{d,n+k}) &= \frac{d+n+k-1}{n+k}\mathrm{tr}_{n+1,\ldots,n+k-1}(P_{sym}^{d,n+k-1})\\ &= \frac{(n+d)(n+d+1)\ldots(d+n+k-1)}{(n+1)(n+2)\ldots(n+k)}P_{sym}^{d,n}\\ &= \frac{d[n+k]}{d[n]}\;P_{sym}^{d,n}.\end{aligned} \tag{137}$$

Since ρ is in the symmetric subspace, we get

$$\mathrm{tr}(\mathrm{MP}_{n\to k}(\rho)) = \frac{d[n]}{d[n+k]}\frac{d[n+k]}{d[n]}\mathrm{tr}(\rho\cdot P_{sym}^{d,n}) = \mathrm{tr}(\rho) \tag{138}$$

□

Definition 36 (CL map). *The CL map,* $\mathrm{CL}_{n\to n+k}:\mathcal{L}((\mathbb{C}^d)^{\otimes n})\to\mathcal{L}((\mathbb{C}^d)^{\otimes(n+k)})$, *is defined as*

$$\mathrm{CL}_{n\to n+k}(\rho) = \frac{d[n]}{d[n+k]}P_{sym}^{d,n+k}(\rho\otimes\mathbb{1}^{\otimes k})P_{sym}^{d,n+k}. \tag{139}$$

Theorem 18 (Chiribella identity [4]). *For* $\rho\in\mathcal{L}(\vee^n\mathbb{C}^d)$ *the Bose-measure-prepare map can be written as*

$$\mathrm{MP}_{n\to k}(\rho) = \sum_{s=0}^{k}\frac{\binom{n}{s}\binom{d+k-1}{k-s}}{\binom{d+n+k-1}{k}}\mathrm{CL}_{s\to k}(\mathrm{tr}_{(s+1)\ldots n}(\rho)), \tag{140}$$

where $\mathrm{tr}_{(s+1)\ldots n}$ *traces out systems s+1 to n.*

Proof. It is enough to check

$$\mathrm{tr}\left(|\beta\rangle\langle\beta|^{\otimes k}\,\mathrm{MP}_{n\to k}(|\alpha\rangle\langle\alpha|^{\otimes n})\right) \overset{?}{=} \mathrm{tr}\left(|\beta\rangle\langle\beta|^{\otimes k}\sum_{s=0}^{k}\frac{\binom{n}{s}\binom{d+k-1}{k-s}}{\binom{d+n+k-1}{k}}\mathrm{Cl}_{s\to k}(\mathrm{tr}_{(s+1)\ldots n}(|\alpha\rangle\langle\alpha|^{\otimes n}))\right) \tag{141}$$

$\forall\,|\alpha\rangle,|\beta\rangle\in\mathbb{C}^d$ with norm 1.

To show that this is enough we use Theorem 12. For maps P and T on $\mathcal{L}(\vee^n\mathbb{C}^d)$ and fixed $|\alpha\rangle\in\mathbb{C}^d$ with

$$\langle\beta^{\otimes k}|\,P(|\alpha\rangle\langle\alpha|^{\otimes n})\,|\beta^{\otimes k}\rangle = \langle\beta^{\otimes k}|\,T(|\alpha\rangle\langle\alpha|^{\otimes n})\,|\beta^{\otimes k}\rangle\,,\ \forall\,|\alpha\rangle,|\beta\rangle\in\mathbb{C}^d. \tag{142}$$

Theorem 12 implies that

$$P(|\alpha\rangle\langle\alpha|^{\otimes n}) = T(|\alpha\rangle\langle\alpha|^{\otimes n})\ \forall\,|\alpha\rangle\in\mathbb{C}^d. \tag{143}$$

Then for $X \in \mathcal{L}(\vee^n\mathbb{C}^d)$ we have that

$$\begin{aligned}
&\operatorname{tr}\Big(P^*(X)^\dagger \left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes n}\Big)\\
&= \operatorname{tr}\Big(X^\dagger P(\left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes n})\Big)\\
&= \operatorname{tr}\Big(X^\dagger T(\left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes n})\Big)\\
&= \operatorname{tr}\Big(T^*(X)^\dagger \left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes n}\Big),
\end{aligned}$$

for which Theorem 12 implies that

$$P^*(X)^\dagger = T^*(X)^\dagger \Rightarrow P(X) = T(X). \tag{144}$$

To check equation (141), we start by looking at the RHS term-wise

$$\begin{aligned}
&\operatorname{tr}\Bigg(\left|\beta\right\rangle \left\langle\beta\right|^{\otimes k} \mathrm{CL}_{s\to k}(\operatorname{tr}_{(s+1)\dots n}(\left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes n})\Bigg)\\
&= \operatorname{tr}\Bigg(\left|\beta\right\rangle \left\langle\beta\right|^{\otimes k} \mathrm{CL}_{s\to k}(\left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes s}))\Bigg)\\
&= \operatorname{tr}\Bigg(\left|\beta\right\rangle \left\langle\beta\right|^{\otimes k} \frac{d[s]}{d[k]} P^{d,k}_{sym}\big(\left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes s} \otimes \mathbb{1}^{\otimes k-s}\big)P^{d,k}_{sym}\Bigg)\\
&= \operatorname{tr}\Bigg(P^{d,k}_{sym} \left|\beta\right\rangle \left\langle\beta\right|^{\otimes k} P^{d,k}_{sym}\big(\left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes s} \otimes \mathbb{1}^{\otimes k-s}\big)\Bigg)\frac{d[s]}{d[k]}.
\end{aligned} \tag{145}$$

Since $\left|\beta\right\rangle \left\langle\beta\right|^{\otimes k}$ is symmetric, the symmetric projector acts as an identity on this state.

$$\begin{aligned}
&\operatorname{tr}\Bigg(P^{d,k}_{sym} \left|\beta\right\rangle \left\langle\beta\right|^{\otimes k} P^{d,k}_{sym}\big(\left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes s} \otimes \mathbb{1}^{\otimes k-s}\big)\Bigg)\frac{d[s]}{d[k]}\\
&= \operatorname{tr}\Bigg(\left|\beta\right\rangle \left\langle\beta\right|^{\otimes k}\big(\left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes s} \otimes \mathbb{1}^{\otimes k-s}\big)\Bigg)\frac{d[s]}{d[k]}\\
&= \operatorname{tr}\big(\left|\beta\right\rangle \left\langle\beta\right|^{\otimes s} \left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes s}\big)\operatorname{tr}\big(\left|\beta\right\rangle \left\langle\beta\right|^{\otimes k-s} \mathbb{1}^{\otimes k-s}\big)\frac{d[s]}{d[k]}\\
&= |\left\langle\alpha|\beta\right\rangle|^{2s}\frac{d[s]}{d[k]}.
\end{aligned} \tag{146}$$

We denote $|\left\langle\beta|\alpha\right\rangle|^{2s} = x^s$. The entire RHS of Equation (141) is now

$$\begin{aligned}
&\operatorname{tr}\Bigg(\left|\beta\right\rangle \left\langle\beta\right|^{\otimes k} \sum_{s=0}^{k} \frac{\binom{n}{s}\binom{d+k-1}{k-s}}{\binom{d+n+k-1}{k}} \mathrm{CL}_{s\to k}(\operatorname{tr}_{(s+1)\dots n}(\left|\alpha\right\rangle \left\langle\alpha\right|^{\otimes n}))\Bigg)\\
&= \sum_{s=0}^{k} \frac{\binom{n}{s}\binom{d+k-1}{k-s}}{\binom{d+n+k-1}{k}} \frac{d[s]}{d[k]} x^s\\
&= \sum_{s=0}^{k} \frac{\binom{n}{s}\binom{d+k-1}{k-s}}{\binom{d+n+k-1}{k}} \frac{\binom{d+s-1}{s}}{\binom{d+k-1}{k}} x^s.
\end{aligned} \tag{147}$$

The binomial coefficients can be written out

$$\begin{aligned}
&\sum_{s=0}^{k} \frac{\binom{n}{s}\binom{d+k-1}{k-s}}{\binom{d+n+k-1}{k}} \frac{\binom{d+s-1}{s}}{\binom{d+k-1}{k}} x^s\\
&= \sum_{s=0}^{k} \binom{n}{s} \frac{(d+k-1)!(d+s-1)!k!(d+n-1)!k!(d-1)!}{(k-s)!(d+s-1)!s!(d-1)!(d+n+k-1)!(d+k-1)!} x^s\\
&= \sum_{s=0}^{k} \binom{n}{s}\binom{k}{s} \frac{k!(d+n-1)!}{(d+n+k-1)!} x^s\\
&= \frac{d[n]}{d[n+k]} \sum_{s=0}^{k} \binom{k}{s}\binom{n}{s} \frac{k!(d+n-1)!n!(d-1)!(d+n+k-1)!}{(d+n+k-1)!(d+n-1)!(n+k)!(d-1)!} x^s\\
&= \frac{d[n]}{d[n+k]} \sum_{s=0}^{k} \frac{\binom{n}{s}\binom{k}{s}}{\binom{n+k}{k}} x^s.
\end{aligned} \tag{148}$$

We will now look at the LHS.

$$\begin{aligned}\mathrm{tr}(|\beta\rangle\langle\beta|^{\otimes k}\,\mathrm{MP}_{n\to k}(|\alpha\rangle\langle\alpha|^{\otimes n})) &= \frac{d[n]}{d[n+k]}\mathrm{tr}\Big(\,|\beta\rangle\langle\beta|^{\otimes k}\,\mathrm{tr}_{[n]}\big(P^{d,n+k}_{sym}(|\alpha\rangle\langle\alpha|^{\otimes n}\otimes \mathbb{1}^{\otimes k})\big)\Big)\\ &= \frac{d[n]}{d[n+k]}\mathrm{tr}\left(\left(\mathbb{1}^{\otimes n}\otimes|\beta\rangle\langle\beta|^{\otimes k}\right)P^{d,n+k}_{sym}\left(|\alpha\rangle\langle\alpha|^{\otimes n}\otimes\mathbb{1}^{\otimes k}\right)\right)\\ &= \frac{d[n]}{d[n+k]}\mathrm{tr}\left(P^{d,n+k}_{sym}\big(\,|\alpha\rangle\langle\alpha|^{\otimes n}\otimes|\beta\rangle\langle\beta|^{\otimes k}\,\big)\right)\\ &= \frac{d[n]}{d[n+k]}\Big(\big(\,\langle\alpha|^{\otimes n}\otimes\langle\beta|^{\otimes k}\,\big)P^{d,n+k}_{sym}\big(\,|\alpha\rangle^{\otimes n}\otimes|\beta\rangle^{\otimes k}\,\big)\Big)\,.\end{aligned} \tag{149}$$

Let us define

$$|\gamma_i\rangle = \begin{cases}|\alpha\rangle & \text{if } i=1,...,n\\ |\beta\rangle & \text{if } i=n+1,...,n+k\end{cases} \tag{150}$$

Then the LHS can be written as

$$\begin{aligned}&\frac{d[n]}{d[n+k]}\Big(\big(\,\langle\alpha|^{\otimes n}\otimes\langle\beta|^{\otimes k}\,\big)P^{d,n+k}_{sym}\big(\,|\alpha\rangle^{\otimes n}\otimes|\beta\rangle^{\otimes k}\,\big)\Big)\\ &=\frac{d[n]}{d[n+k]}\frac{1}{(n+k)!}\sum_{\pi\in S_{n+k}}\Big(\big(\,\langle\alpha|^{\otimes n}\otimes\langle\beta|^{\otimes k}\,\big)\,|\gamma_{\pi^{-1}(1)}\rangle\otimes|\gamma_{\pi^{-1}(2)}\rangle\otimes...\otimes|\gamma_{\pi^{-1}(n+k)}\rangle\Big)\\ &=\frac{d[n]}{d[n+k]}\frac{1}{(n+k)!}\sum_{s=0}^{k}c_s\cdot x^s,\end{aligned} \tag{151}$$

here the index corresponds to the number of vectors $\langle\alpha|$ being matched with $|\beta\rangle$ by the permutations π. Since the numbers of $|\alpha\rangle, |\beta\rangle$ are fixed, each time a $\langle\alpha|$ is matched with a $|\beta\rangle$ we also have a matching pair of $\langle\beta|\alpha\rangle$ from the permutation. The maximum number of times $\langle\alpha|$ and $|\beta\rangle$ can be matched is the number of times $|\beta\rangle$ appears, i.e. k. The sum therefore consists of powers of $\langle\alpha|\beta\rangle\langle\beta|\alpha\rangle$, which we earlier defined as x, multiplied by a constant, which describes how many of these permutations there exists.

To find c_s we determine the number of permutations that select s elements from positions {n+1,. . . ,n+k} of β's and map them into {1,. . . ,n} and $(n-s)$ elements from positions {1,. . . ,n} of α's and map them into positions $\{1,\dots,n\}$, corresponding to the rest of the elements. In addition, the order of $|\alpha\rangle$'s and $|\beta\rangle$'s does not matter, so we can permute these in $n!$ and $k!$ ways respectively.

$$c_s = \binom{k}{s}\binom{n}{s}n!k! \tag{152}$$

$$\begin{aligned}\mathrm{tr}(|\beta\rangle\langle\beta|^{\otimes k}\,\mathrm{MP}_{n\to k}(|\alpha\rangle\langle\alpha|^{\otimes n})) &= \frac{d[n]}{d[n+k]}\sum_{s=0}^{k}\frac{\binom{k}{s}\binom{n}{s}n!k!}{(n+k)!}x^s\\ &= \frac{d[n]}{d[n+k]}\sum_{s=0}^{k}\frac{\binom{k}{s}\binom{n}{s}}{\binom{n+k}{k}}x^s\end{aligned} \tag{153}$$

This is exactly what we got for the RHS in Equation (148). □

Theorem 19 (Distance between Bose-measurement-prepare and partial trace)**.** *Let $MP_{n\to k}:\mathcal{L}(\vee^n\mathbb{C}^d)\to\mathcal{L}(\vee^n\mathbb{C}^d)$ be the Bose-measurement-prepare map from Definition 134. Then $\forall n,k\in\mathbb{N}$ we have*

$$||\mathrm{MP}_{n\to k}-\mathrm{tr}_{(k+1)\dots n}||_\diamond \le 2\epsilon_{n,k}, \tag{154}$$

where $\epsilon_{n,k}=\left(1-\frac{\binom{n}{k}}{\binom{d+n+k-1}{k}}\right)$, and $tr_{(k+1)\dots n}$ traces out systems $k+1$ to n.

Proof. In the Chiribella identity we write out the last element in the sum

$$\begin{aligned}\mathrm{MP}_{n\to k}(\rho) &= \frac{\binom{n}{k}\binom{d+k-1}{k-k}}{\binom{d+n+k-1}{k}}\mathrm{CL}_{k\to k}(\mathrm{tr}_{(k+1)\dots n}(\rho))+\sum_{s=0}^{k-1}\frac{\binom{n}{s}\binom{d+k-1}{k-s}}{\binom{d+n+k-1}{k}}\mathrm{CL}_{s\to k}(\mathrm{tr}_{(k+1)\dots n}(\rho))\\ &= \frac{\binom{n}{k}}{\binom{d+n+k-1}{k}}(\mathrm{tr}_{(k+1)\dots n}(\rho))+\sum_{s=0}^{k-1}\frac{\binom{n}{s}\binom{d+k-1}{k-s}}{\binom{d+n+k-1}{k}}\mathrm{CL}_{s\to k}(\mathrm{tr}_{(k+1)\dots n}(\rho))\end{aligned} \tag{155}$$

$\mathrm{MP}_{n\to k}$ is trace-preserving, as is the trace, so the remaining sum must be trace preserving, too. The remaining sum is completely positive because $\mathrm{CL}_{s\to k}$ and tr are, and thus is a quantum channel. We denote this sum N, which gives us

$$\mathrm{MP}_{n\to k}(\rho) = \frac{\binom{n}{n}}{\binom{d+n+k-1}{k}}(\mathrm{tr}_{(k+1)\dots n}(\rho)) + \left(1 - \frac{\binom{n}{n}}{\binom{d+n+k-1}{k}}\right)N. \tag{156}$$

Defining

$$\epsilon_{n,k} = 1 - \frac{\binom{n}{k}}{\binom{d+n+k-1}{k}},$$

gives us

$$\mathrm{MP}_{n\to k}(\rho) = (1-\epsilon_{n,k})\mathrm{tr}_{(k+1)\dots n} + \epsilon_{n,k}N. \tag{157}$$

We can use this form of the measurement and prepare map in the diamond norm:

$$\begin{aligned}||\mathrm{MP}_{n\to k} - \mathrm{tr}_{(k+1)\dots n}||_\diamond &= ||(1-\epsilon_{n,k})\mathrm{tr}_{(k+1)\dots n} + \epsilon_{n,k}N - \mathrm{tr}_{(k+1)\dots n}||_\diamond \\ &= \epsilon_{n,k}||\mathrm{tr}_{(k+1)\dots n} + N||_\diamond \\ &\leq 2\epsilon_{n,k}.\end{aligned} \tag{158}$$

In the last step we use Theorem 15, since both the trace and N are quantum channels. Using a special case of the De-Finetti theorem, we can prove the convergence. □

Corollary 4. *(Convergence of the Bose-symmetric hierarchy) For $\rho_{AB_1\dots B_n} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \vee^n \mathbb{C}^{d_B})$ we have*

$$\inf_{\sigma_{AB}\in\mathrm{SEP}(A:B)} ||\sigma_{AB} - \rho_{AB}||_1 \leq 2\frac{d_B+1}{d_B+n+1} \xrightarrow[n\to\infty]{} 0 \tag{159}$$

Where $\rho_{AB} = \mathrm{tr}_{B[n-1]}(\rho_{AB_1\dots B_n})$.

Proof. Let $\widetilde{d_A} \in \mathbb{N}$ and $\widetilde{\rho}_{AB_1\dots B_n} \in \mathcal{D}(\mathbb{C}^{\widetilde{d_A}} \otimes \vee^n \mathbb{C}^{d_B})$. Then

$$\begin{aligned}||\mathrm{MP}_{n\to 1} - \mathrm{tr}_{B[n-1]}||_\diamond &= \sup_{\widetilde{d_A}} \sup_{\widetilde{\rho}_{AB_1\dots B_n}} ||\left(\mathrm{id}_A \otimes (\mathrm{MP}_{n\to 1} - \mathrm{tr}_{B[n-1]})\right)(\widetilde{\rho}_{AB_1\dots B_n})||_1 \\ &\geq ||\left(\mathrm{id}_A \otimes (\mathrm{MP}_{n\to 1} - \mathrm{tr}_{B[n-1]})\right)(\rho_{AB_1\dots B_n})||_1 \\ &= ||\left(\mathrm{id}_A \otimes \mathrm{MP}_{n\to 1}\right)(\rho_{AB_1\dots B_n}) - \rho_{AB}||_1.\end{aligned} \tag{160}$$

Since $\mathrm{MP}_{n\to 1}$ is an entanglement-breaking map, the left term inside the norm is some $\widetilde{\sigma}_{AB} \in \mathrm{SEP}(A:B)$ so that

$$||\mathrm{MP}_{n\to 1} - \mathrm{tr}_{B[n-1]}||_\diamond \geq ||\widetilde{\sigma}_{AB} - \rho_{AB}||_1. \tag{161}$$

Following Theorem 19, the smallest distance between a state in the space of separable states and the ρ_{AB} is

$$\inf_{\sigma_{AB}\in\mathrm{SEP}(A:B)} ||\sigma_{AB} - \rho_{AB}||_1 \leq 2\epsilon_{n,1} = 2\frac{d_B+1}{d_B+n+1}. \tag{162}$$

□

This shows that the further a state is Bose-symmetric k-extendible, the closer it is to the set of separable states, and thus extendibility on the Bose-symmetric subspace is a sufficient test for entanglement for a finite number of extensions.

8 Examples

This section is devoted to going through some of the important results, that can be shown using our implementation of the extendibility hierarchy.

8.1 Werner state

The Werner state, $\rho_w^\alpha \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$, $\alpha \in [0;1]$ is a mixture of projectors onto the symmetric- and antisymmetric subspace

$$\rho_w^\alpha = \alpha \frac{2}{d^2+d} P_{sym}^{d,2} + (1-\alpha) \frac{2}{d^2-d} P_{asym}^{d,2} \tag{163}$$

The symmetric projector is the one defined in Definition 10, and the antisymmetric projector is the projector into the antisymmetric subspace $\wedge^n \mathbb{C}^d = \text{span}\{|\psi\rangle \in (\mathbb{C}^d)^{\otimes n} : P_d(\pi)\,|\psi\rangle = (-1)^\pi\,|\psi\rangle \quad \forall \pi \in S_n\}$, where $(-1)^\pi$ is 1 if π is an even permutation, and -1 if π is odd. This antisymmetric projector is defined as [8]:

$$P_{asym}^{d,n} = \frac{1}{n!} \sum_{\pi \in S_n} (-1)^\pi P_d(\pi) \tag{164}$$

For $\alpha < 0.5$ the state ρ_w^α is entangled. This is detectable by the PPT criterion, but we will use it to test our extendibility test. If we choose $\alpha = 0$, then the state is entirely in the antisymmetric subspace. Using the non-symmetric Definition 25 , we get that for $d = 3$ and $d = 4$ the state is $d-1$ extendible, but our Bose-symmetric extensions from Definition 31 detect it as not even being 2-Bose symmetric extendible. This is because the Bose-symmetric extensions only searches the symmetric subspace, where as the other also include the antisymmetric subspace.

8.2 Horodecki state

The Horodecki state $\rho_h^\alpha \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^4)$ is defined as [14]

$$\rho_h = \begin{bmatrix} \alpha & 0 & 0 & 0 & 0 & \alpha & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 & 0 & \alpha & 0 \\ 0 & 0 & \alpha & 0 & 0 & 0 & 0 & \alpha \\ 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2}(1+\alpha) & 0 & 0 & \frac{1}{2}\sqrt{1-\alpha^2} \\ \alpha & 0 & 0 & 0 & 0 & \alpha & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 & 0 & \alpha & 0 \\ 0 & 0 & \alpha & 0 & \frac{1}{2}\sqrt{1-\alpha^2} & 0 & 0 & \frac{1}{2}(1+\alpha) \end{bmatrix} \tag{165}$$

This state is entangled for $\alpha \neq 0, 1$. Moreover, it has positive partial transpose. Setting $\alpha = 0.5$, the Bose-symmetric extensions on the first system, is able to detect the entanglement, by not being 12-extendible. If we extend the second system, we get that it is only 4-extendible. Being able to detect this entanglement shows the power of the symmetric subspace, since the dimensions of the Bose-symmetric extension if we extend the first system for $k = 12$, is $\binom{2+12-1}{12} \cdot 4 = 52$ compared to the dimensions of the two other extensions, $2^{12} \cdot 4 = 16384$, which is too large for the computer to handle.

8.3 PPT edge

The state $\rho^{\in}\mathcal{D}(\mathbb{C}^3 \otimes \mathbb{C}^3)$, $-\frac{\pi}{3} < \theta < \frac{\pi}{3}$, $b > 0$ is entangled defined as [15]

$$\rho = \begin{bmatrix} 2\cos(\theta) & 0 & 0 & 0 & -e^{i\theta} & 0 & 0 & 0 & -e^{-i\theta} \\ 0 & 1/b & 0 & -\cos(\theta) & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & -\cos(\theta) & 0 & 0 \\ 0 & -\cos(\theta) & 0 & b & 0 & 0 & 0 & 0 & 0 \\ -e^{-i\theta} & 0 & 0 & 0 & 2\cos(\theta) & 0 & 0 & 0 & -e^{i\theta} \\ 0 & 0 & 0 & 0 & 0 & 1/b & 0 & -\cos(\theta) & 0 \\ 0 & 0 & -\cos(\theta) & 0 & 0 & 0 & 1/b & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\cos(\theta) & 0 & b & 0 \\ -e^{i\theta} & 0 & 0 & 0 & -e^{-i\theta} & 0 & 0 & 0 & 2\cos(\theta) \end{bmatrix} \tag{166}$$

Choosing $\theta = \pi/6$, $b = 2$, we get that the state is not 8-extendible. For $b > 2$, the state gets less extendible. For $b = 25$ it is not 3-extendible. Similarly for $b < 1$, the state is also less extendible. For example we get that $b = 0.1$ is not 8-extendible. The closer to one we get, the more extendible the state is. For $b = 0.5$ and $b = 2$ we get that the state is not 8-extendible. We are, however, not able to go check for more than 8-extendibility, due to some limitations in PICOS.

9 Conclusion

We have discussed some of the fundamental principles, including two examples of how entanglement can be exploited in quantum information protocols. Two tests for detecting if a state is entangled have been discussed, namely the Peres-Horodecki criterion, and the hierarchy of extendibility. By the Woronowicz theorem the PPT criterion is a sufficient test for small dimensions ($d_1 d_2 \leq 6$).

We have also introduced the symmetric subspace, and how it can be utilised to define Bose-symmetric extension, which we have shown is a sufficient test and more efficient than the original extensions. Finally we have implemented the discussed tests in Python, and used this to detect entanglement of some examples. Our tests can, however, still be improved. Future work could include adding the PPT condition to the SDP of extendibility as a constraint or using SDPs to generate an entanglement witness.

References

[1] Charles H. Bennett et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Phys. Rev. Lett.* 70 (13 Mar. 1993), pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895. URL: https://link.aps.org/doi/10.1103/PhysRevLett.70.1895.

[2] Fernando GSL Brandão, Matthias Christandl, and Jon Yard. "A quasipolynomial-time algorithm for the quantum separability problem". In: *Proceedings of the forty-third annual ACM symposium on Theory of computing*. ACM. 2011, pp. 343–352.

[3] Constantin Carathéodory. "Über den Variabilitätsbereich der Fourier'schen Konstanten von positiven harmonischen Funktionen". In: *Rendiconti Del Circolo Matematico di Palermo (1884-1940)* 32.1 (1911), pp. 193–217.

[4] Giulio Chiribella. "On quantum estimation, quantum cloning and finite quantum de Finetti theorems". In: *Conference on Quantum Computation, Communication, and Cryptography*. Springer. 2010, pp. 9–25.

[5] Matthias Christandl et al. "One-and-a-half quantum de Finetti theorems." In: *Communications in Mathematical Physics* 273.2 (2007).

[6] Andrew C Doherty, Pablo A Parrilo, and Federico M Spedalieri. "Complete family of separability criteria". In: *Physical Review A* 69.2 (2004), p. 022308.

[7] RE Edwards. "Functional analysis: Theory and applications, Holt, Rinehart and Winston, New York, 1965". In: *MR* 36 (1994), p. 4308.

[8] Robert B. Griffiths. *Lecture notes on Systems of Identical Particles*. http://quantum.phys.cmu.edu/qm2/qmc161.pdf. Mar. 2011.

[9] Guillaume Sagnol. *PICOS*. Version 1.1.2. URL: http://picos.zib.de/.

[10] Leonid Gurvits. "Classical deterministic complexity of Edmonds' problem and quantum entanglement". In: *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*. ACM. 2003, pp. 10–19.

[11] Aram W Harrow. "The church of the symmetric subspace". In: *arXiv preprint arXiv:1308.6595* (2013).

[12] Michael Horodecki, Peter W. Shor, and Mary Beth Ruskai. "Entanglement breaking channels". In: *Reviews in Mathematical Physics* 15.06 (2003), pp. 629–641.

[13] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Separability of mixed states: necessary and sufficient conditions". In: *Physics Letters A* 223.1 (1996), pp. 1–8.

[14] Pawel Horodecki. "Separability criterion and inseparable mixed states with positive partial transposition". In: *Physics Letters A* 232.5 (1997), pp. 333–339.

[15] Seung-Hyeok Kye and Hiroyuki Osaka. "Classification of bi-qutrit positive partial transpose entangled edge states by their ranks". In: *Journal of Mathematical Physics* 53.5 (2012), p. 052201.

[16] MOSEK ApS. *MOSEK*. Version 8.0.60. URL: https://mosek.com/.

[17] Nielsen and Chuang. *Quantum Computation and Quantum Informatics*. Cambridge University Press, 2000. ISBN: 0521635039.

[18] B Russo, HA Dye, et al. "A note on unitary operators in C^*-algebras". In: *Duke Mathematical Journal* 33.2 (1966), pp. 413–416.

[19] Sebastian Seehars. "Symmetric extensions in entanglement theory and quantum cryptography". MA thesis. Ludwigs-Maximillians-Universität München, Sept. 2011.

[20] Erling Størmer. "Positive linear maps of operator algebras". In: *Acta Mathematica* 110.1 (1963), pp. 233–278. ISSN: 1871-2509. DOI: 10.1007/BF02391860. URL: http://dx.doi.org/10.1007/BF02391860.

[21] John Watrous. *Lecture notes on Semidefinite programming.* https://cs.uwaterloo.ca/~watrous/CS766/LectureNotes/07.pdf. Fall 2011.

[22] Michael M. Wolf. *Quantum Channels and Operations, A Guided Tour.* https://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf. 2012.

[23] Stanisław L. Woronowicz. "Positive maps of low dimensional matrix algebras". In: *Reports on Mathematical Physics* 10.2 (1976), pp. 165–183.

10 Appendix

All code is available at https://github.com/jeppe742/QuantBoxPy