Operator Theory and Conditions for Quantum Local Operations and Classical Communication

by

Comfort Mintah

A Thesis
presented to
The University of Guelph

In partial fulfilment of requirements
for the degree of
Masters of Science
in
Mathematics and Statistics

Guelph, Ontario, Canada

ABSTRACT

OPERATOR THEORY AND CONDITIONS FOR QUANTUM LOCAL OPERATIONS AND CLASSICAL COMMUNICATION

Comfort Mintah
University of Guelph, 2016

Advisor:
Professor D.W. Kribs
Professor R. Pereira

We study the finite dimensional C^*-algebras and their representation theory. The physical description of quantum local operations and classical communication (LOCC) and its schematics are presented. Focusing on the mathematical description of one-way LOCC, we give detailed analysis of recently derived operator relations in quantum information theory. We also show how functional analytic tools such as operatorx systems, operator algebras, and Hilbert C^*-modules all naturally emerge in this setting. We make use of these structures to derive some key results in one-way LOCC. Perfect distinguishability of one-way LOCC versus arbitrary quantum operations is analyzed. It turns out that they are equivalent for several families of operators that appear jointly in matrix and operator theory and quantum information theory. The main results of this work are contained in the paper [13].

ACKNOWLEDGEMENTS

I am grateful to the almighty God for his sufficient grace and protection for a successful work done. I would like to express my sincere gratitude to my supervisor Professor David Kribs and my co-supervisor Professor Rajesh Pereira and collaborator Prof Michael Nathanson for their encouragement, time and suggestions for a successful achievement of this thesis.

To AIMS-Next Einstein Initiative and University of Guelph Mathematics and Statistics Department, I say thank for giving me the opportunity to accomplish my dreams.

Finally, I would like to thank my father Mr S.K Mintah, my brother Daniel Oduro-Mintah and my lovely sisters Rosina Mintah and Florence Mintah for their constant support and advice.

Contents

Chapter 1

Introduction

Local Operations and Classical Communication(LOCC) emerges naturally as a class of operations from quantum information theory. It examines the relation between locality and quantum entanglement, but its operational definition demonstrates the possibilities and limitations of distributed quantum algorithms. Local operations and classical communication (LOCC) is a protocol in quantum information theory in which a multipartite quantum system is distributed to various parties who are restricted to perform local operations on their respective subsystems. To enhance measurement the parties are allowed classical communication to help identify their state. From the point of view of quantum communication, LOCC is the most reliable way to distinguish between states perfectly, since the parties involved are physically separated from each other. This work will concern itself with LOCC between bipartite system.

The set up of the bipartite system is as follows: consider two different parties Alice and Bob, each of whom control a quantum system, represented on the finite

dimensional Hilbert space $\mathcal{H}_A$ and $\mathcal{H}_B$. Alice and Bob are separated from each other in a distance lab. Their joint system has been prepared in a pure state from a known set of entangled states $\mathcal{S} = \{|\psi_i\rangle\}$. Their task is to determine the value of i perfectly using local operations and classical communication(LOCC). The type of local operations allowed are operations of the form $\mathcal{E} = \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \cdots \otimes \mathcal{E}_k$ and measurements $\mathcal{M}_k = \{A_1 \otimes A_2 \otimes \cdots \otimes A_k\} \in \mathcal{H}$ (where $\mathcal{H} = H_1 \otimes H_2 \otimes \cdots \otimes H_k$) , $A_i \geq 0$ and $\sum_k A_i = I$ for all $i = 1, 2, \cdots, k$. Classical communication involves the transfer of bits of information.

Although LOCC is a very useful way of characterizing states between different parties that are distance apart, its mathematical structure is complex and difficult to characterize, and hence our restriction to one-way LOCC (one of the schemes of LOCC). In one-way LOCC the communication is limited to a predetermined direction. Thus, if Alice goes first, then Bob adapts his measurements based on the information he received from Alice. An example of one-way LOCC protocol is quantum teleportation [2] which we will see in more details later in this work. Also, there are known examples of tasks which require two-way communication in order to be accomplished with LOCC [1, 9, 18, 13].

A particularly instructive problem for LOCC operations is that of distinguishing pure quantum states. Thus given an unknown representative $|\psi\rangle$ from a set of states $\mathcal{S}$, $|\psi\rangle$ can always be identified using quantum operations if and only if the elements of $\mathcal{S}$ are mutually orthogonal. No such simple characterization has been found for general LOCC, although many results have been obtained for specific cases (such as [22, 8, 17])

The mathematical characterization of one-way LOCC and operator relations

was recently obtained by [18]. We use [18] as our motivation for most of the new results we will establish in this work.

The approach of this thesis is as follows: In Chapter 2, we give the mathematical preliminaries that will be relevant in the understanding of the body of the thesis. We describe the fundamentals of finite dimensional C^*-algebras and their representation theory. We see the importance of finite dimensional C^*-algebra representation theory in our discussions on operator systems and separating vectors. In Chapter 3, we define quantum local operations and classical communication (LOCC) in terms of quantum measurements and indicate the schemes of quantum LOCC. We discuss some recent established results for distinguishing states perfectly via LOCC. These results will be the fundamentals for most of the new results we will establish in the next chapter. In Chapter 4, we restrict ourselves to one of the types of quantum LOCC called one-way LOCC and give the mathematical structure of one-way LOCC . We establish some new results and conditions on how to distinguish set of states perfectly by one-way LOCC. We demonstrate the connection between arbitrary quantum operations and one-way LOCC. We see that for certain classes of states perfect distinguishability by one-way LOCC is equivalent to arbitrary quantum operations. We discuss operator systems, operator algebras and separating vectors and establish their connection with one-way LOCC. Finally, we show how the Hilbert C^*-module arises as a natural setting from one-way LOCC and establish new results for this case.

Chapter 2

Structure theory for finite dimensional operator algebras

This chapter discusses some preliminaries and definitions relevant to the understanding of the body of this thesis. We restrict ourselves primarily to operators on finite dimensional Hilbert space, but for depth of exposition we also include details on the general infinite dimensional case. The Hilbert space denoted by $\mathcal{H}$ is our space of interest and is defined as a complex vector space which is endowed with an inner product that is complete under the induced norm. The vector space is said to be complete if every Cauchy sequence converges to an element in the vector space. Notice that every convergent sequence is Cauchy. The set of bounded operators or all continuous linear operators on the Hilbert space $\mathcal{H}$ is denoted by $B(\mathcal{H})$.

This chapter is arranged as follows. In Section 2.1 we discuss the basic definitions and properties of C^*-algebras. In Section 2.2 we prove the von Neumann double

commutant theorem. In Section 2.3 we describe the representation theory and the structure of finite dimensional C^*-algebra. We look at the structure of von Neumann algebras which we will see form the fundamentals to the understanding of operator systems and separating vectors. In Section 2.4 we discuss quantum operations with some examples needed for the body of this thesis. Finally, in section 2.5 we discuss operator structure such as operator systems, and separating vectors and give examples of matrices that have separating vectors. We will see the connection between these and one-way local operations and classical communication later in Chapter 4 of our work.

2.1 The basics of C^*-algebras

A Banach algebra $\mathcal{A}$ is a Banach space that satisfies associative and distributive multiplication such that

$$\lambda(AB) = (\lambda A)B = A(\lambda B)$$

and

$$\|AB\| \leq \|A\|\|B\|$$

for all A, B in the Banach space and $\lambda \in \mathbb{C}$. The algebra $\mathcal{A}$ with a conjugate linear involution $*$ (adjoint) is said to be a $*$- algebra if it satisfies the following conditions, for all A, B in $\mathcal{A}$ and λ in $\mathbb{C}$,

1. $(A + B)^* = A^* + B^*$
2. $(\lambda A)^* = \overline{\lambda} A^*$

3. $A^{**} = A$

4. $(AB)^* = B^*A^*$

The algebra is said to be a C^*-algebra if its satisfies the above conditions, thus it is a $*$-algebra and has the additional norm condition

$$\|A^*A\| = \|A\|^2 .$$

In quantum computing, the algebra $\mathcal{A}$ is known as the "interaction algebra" for the channel. We will see that it is $*$-closed and hence a finite dimensional C^*-algebra. Let us consider some examples of C^*-algebras.

Example 2.1.1. *The algebra of all bounded operators on the Hilbert space $B(\mathcal{H})$ with the usual adjoint is a C^*-algebra.*

Definition 2.1.1 (Concrete algebra)**.** *A concrete algebra is a normed closed self-adjoint subalgera of $B(\mathcal{H})$*

Every finite dimensional C^*-algebra we will see can be identified as a subalgebra of complex matrices.

Definition 2.1.2. *Let A be an element or operator in the C^*-algebra $\mathcal{A}$ then*

1. *A is self-adjoint if $A^* = A$.*

2. *A is normal if $AA^* = A^*A$.*

3. *A is unitary if $AA^* = I = A^*A$.*

Definition 2.1.3 (Spectrum)**.** *The spectrum of an element A of $\mathcal{A}$ is the set*

$$\sigma(A) := \{\lambda \in \mathbb{C} : \ det(\lambda I - A\}) = 0\}.$$

The complement of the spectrum is called the resolvent set.

In the finite dimensional case, the spectrum of A is its set of eigenvalues. With the definition of the spectrum in mind we define positive element or operators as follows:

Definition 2.1.4 (positive elements)**.** *An element A is positive if it is self-adjoint and the spectrum of A is a subset of the positive real line.*

Note that if $A \leq B$ on the set of self-adjoint operators then $B - A$ is positive. Thus, positive elements are used to determine the order on the self-adjoint element of the C^*-algebra. Next, we define the spectral radius of an element in the algebra.

Definition 2.1.5. *The spectral radius A is defined as*

$$spr(A) = sup_{\lambda \in \sigma(A)} |\lambda| \, .$$

Notice that for every element in the Banach algebra the spectral radius is determined by

$$\mathrm{spr}(A) = \lim_{n \mapsto \infty} \|A^n\|^{\frac{1}{n}} \, .$$

2.2 The von Neumann double commutant theorem

A von Neumann algebra is a C^*-subalgebra which contains the identity operator and is closed under the weak operator topology.

Definition 2.2.1 (Weak operator topology)**.** *The weak operator topology denoted by WOT on $B(\mathcal{H})$ is the topology on $B(\mathcal{H})$ for which the sets*

$$W(T, x, y) := \{A \in B(\mathcal{H}) : |\langle (T - A)x|y\rangle| < 1\},$$

for all $T \in B(\mathcal{H})$ and $x, y \in \mathcal{H}$ form a topological base. Note that the set

$$W(T_i, x_i, y_i, 1 \leq i \leq n) := \cap_{i=1}^{n} W(T_i, x_i, y_i).$$

That is $T_\alpha \xrightarrow{WOT} T$ if and only if $\lim_\alpha \langle T_\alpha x|y\rangle = \langle Tx|y\rangle$ for all $x, y \in \mathcal{H}$.

Definition 2.2.2 (Strong operator topology)**.** *The strong operator topology denoted by SOT is defined as the topology defined by open sets of the form*

$$S(T, x) := \{A \in B(\mathcal{H}) : \|(T - A)x\| < 1\},$$

for all $T \in B(\mathcal{H})$ and $x \in \mathcal{H}$.

Thus $T_\alpha \xrightarrow{SOT} T$ if and only if $\lim_\alpha T_\alpha x = Tx$, for all $x \in \mathcal{H}$.

Next, we discuss the relation between strong operator topology(SOT) and weak operator topology(WOT).

Proposition 2.2.1. *Let f be a linear functional on $B(\mathcal{H})$. The following are equivalent*

1. *f is WOT-continuous.*

2. *f is SOT-continuous.*

3. *There exists $x_1, \cdots, x_n, y_1, \cdots, y_n \in \mathcal{H}$ such that*

$$f(T) = \sum_{i=1}^{n} \langle Tx_i | y_i \rangle .$$

Proof. (1) $\implies$ (2) is straightforward from definition and Cauchy Schwarz inequality. Every linear functional that is WOT-continuous is also SOT-continuous.

(2) $\implies$ (3) The set $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ is open in $\mathbb{C}$ so that $f^{-1}(\mathbb{D})$ is open in SOT. Clearly, the zero operator lies in $f^{-1}(\mathbb{D})$ and hence there is a neighborhood of $0 \in f^{-1}(\mathbb{D})$. Hence there exists $v_1, v_2, \cdots, v_k \in V$ such that for $A \in B(V)$, if $\|Av_j\| < 1$ for all j then $|f(A)| < 1$. Let us consider vector space $V^k = \underbrace{V \times V \times \cdots \times V}_{\text{k times}}$ and the subspace $S \subseteq V^k$ such that

$$S = \{(Av_1, Av_2, \cdots, Av_k) : A \in B(V)\}$$

and let $g : S \mapsto \mathbb{C}$ with

$$g\left(Av_1, Av_2, \cdots, Av_k\right) = f(A) ,$$

well defined. Notice that $\|g\| < 1$. By the Hahn-Banach theorem there exists $h : V^k \mapsto \mathbb{C}$ such that $\|h\| < 1$ and $h|S = g$. Since h is a bounded linear map, by the Riesz

representation theorem there exists $y_1, y_2, \cdots, y_k \in V$ such that

$$h\left((w_1, \cdots, w_k)\right) = \sum_{j=1}^{k} \langle y_j | w_j \rangle ,$$

then

$$\begin{aligned} f(A) &= g\left(Av_1, \cdots, Av_k\right) \\ &= h\left(Av_1, \cdots, Av_k\right) \\ &= \sum_{j=1}^{k} \langle y_j | Av_j \rangle \end{aligned}$$

(3) $\implies$ (1) Want to show that $f(T) = \langle Tx|y\rangle$ is WOT continuous.

Let $W(0, x, y) = f^{-1}(\mathbb{D})$ and $a \in \mathbb{C}$ such that for $r > 0$, let $T \in B(\mathcal{H})$ with $f(T) = a$ then $f^{-1}\left(B_r(a)\right) = W(T, x, y)$ which is open.

□

Definition 2.2.3. *(Commutant) Let $\mathcal{S}$ be any subset of $B(\mathcal{H})$, then the commutant of $\mathcal{S}$ denoted by $\mathcal{S}'$ is defined as*

$$\mathcal{S}' = \{T \in B(\mathcal{H}) : ST = TS, \forall\, S \in \mathcal{S}\}$$

Corollary 2.2.1. *If $\mathcal{S}$ is a self-adjoint unital C^*-subalgebra of $B(\mathcal{H})$ then the commutant $\mathcal{S}'$ is also self-adjoint.*

Proof. Let $\mathcal{S} \subseteq B(\mathcal{H})$ be self-adjoint, then for all $A \in \mathcal{S}$ implies $A^* \in \mathcal{S}$. Let $T \in \mathcal{S}^{'}$,

want to show that $T^* \in S^{'}$. Let $A \in \mathcal{S}$ then $A^* \in \mathcal{S}$ as well by definition of the commutant

$$A^*T = TA^* . \tag{2.2.1}$$

Taking the adjoint of both sides of Equation (2.2.1) gives

$$\begin{aligned} (A^*T)^* &= (TA^*)^* \\ T^*A &= AT^* . \end{aligned}$$

We see that T^* commutes with every element of $\mathcal{S}$, that is for all $A \in \mathcal{S}$

$$T^*A = AT^* .$$

Therefore, T^* is in $\mathcal{S}^{'}$ and hence the commutant $\mathcal{S}'$ is self-adjoint.

□

It is important to notice that the commutant of the C^*-algebra is always a von Neumann algebra, since the commutant $\mathcal{S}'$ is a self-adjoint unital C^*-subalgebra and WOT-closed. Thus, if $T_\alpha \in \mathcal{S}'$ and $T_\alpha \xrightarrow{WOT} T$, then for every $A \in \mathcal{S}$

$$AT = \text{WOT-lim}_\alpha AT_\alpha = \text{WOT-lim}_\alpha T_\alpha A = TA .$$

Definition 2.2.4 (Double Commutant)**.** *The double commutant is defined as the commutant of the commutant and is denoted by* $\mathcal{S}'' = (\mathcal{S}')'$.

Theorem 2.2.1 (von Neumann double commutant [4]). *Let $\mathcal{S}$ be a C^*-subalgebra of $B(\mathcal{H})$ with the trivial null space. Then*

$$\mathcal{S}'' = \overline{\mathcal{S}}^{WOT} = \overline{\mathcal{S}}^{SOT}.$$

Proof. Notice that since SOT is stronger than WOT and the double commutant $\mathcal{S}''$ is WOT-closed and contains the subalgebra $\mathcal{S}$, we have

$$\overline{\mathcal{S}}^{\mathrm{SOT}} \subset \overline{\mathcal{S}}^{\mathrm{WOT}} \subset \mathcal{S}''.$$

Let T be a fixed operator in $\mathcal{S}''$ and vectors $v_1, v_2, \cdots, v_n$. We find $A \in \mathcal{S}$ such that

$$\sum_{i=1}^{n} \|(T-A)v_i\|^2 < 1$$

as this represents a basic SOT open neighborhood of T. Let us consider when $n = 1$ and let P be a projection onto the space $\overline{\mathcal{S}v_1}$. Then clearly the projection belongs to $\mathcal{S}'$. Particularly $\mathcal{S}P\mathcal{H} \subset P\mathcal{H}$ and thus $PAP = AP$ for every A in the subalgebra $\mathcal{S}$. Therefore

$$PA = (A^*P)^* = (PA^*P)^* = PAP = AP.$$

If $u = P^{\perp}v_1$, then $\mathcal{S}u = \mathcal{S}P^{\perp}v_1 = 0$. Also, since $\mathcal{S}$ has a trivial null space, $u = 0$ implies v_1 lies in $\overline{\mathcal{S}v_1}$. So $PT = TP$, and Tv_1 belong to $\overline{\mathcal{S}v_1}$. Therefore there is an operator

$A \in \mathcal{S}$ such that

$$\|(T - A)v_1\| < 1\,.$$

Next, we consider $n > 2$. The Hilbert space is of the form $\mathcal{H}^{(n)}$, which represents the direct sum of n copies of $\mathcal{H}^{(n)}$. Let $A^{(n)}$ be the operators in $\mathcal{H}^{(n)}$ denoted by

$$A^{(n)}\,(\lambda_1, \lambda_2, \cdots, \lambda_n) = (A\lambda_1, A\lambda_2, \cdots, A\lambda_n)\ .$$

Let $\mathcal{S}^{(n)} := \{A^{(n)} : A \in \mathcal{S}\}$ and an operator $U \in B(\mathcal{H}^{(n)})$ is an $n \times n$ matrix with coefficient $u_{ij} \in B(\mathcal{H})$.

Our task is to compute $\mathcal{S}^{(n)''}$. It is easy to observe that an operator $U = [u_{ij}]$ lies in $\mathcal{S}^{(n)'}$ if and only if each of the matrix entry u_{ij} belongs to $\mathcal{S}^{'}$. Hence an operator $T = [t_{ij}] \in \mathcal{S}^{(n)''}$ must commute with each matrix unit e_{ij}. Thus, the operator with (i, j) coefficient is equal to I while all the other entries is zero. A sequence of calculation shows that T is forced to a diagonal matrix with $t_{ii} = T_{11}$ for all $1 \leq i \leq n$. That is $T = T_{11}^{(n)}$. In addition, T commutes with $U^{(n)}$ for each $U \in \mathcal{S}'$. This implies that T_{11} belongs to $\mathcal{S}^{''}$. Therefore

$$\mathcal{S}^{(n)''} = (\mathcal{S}^{''})^{(n)}\,.$$

Now, if we apply $n = 1$, we see that $T^{(n)} \in (\mathcal{S}^{''})^{(n)}$ and $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ leads to an operator $A \in \mathcal{S}$ such that

$$1 > \|(T^{(n)} - A^{(n)})\mathbf{v}\|^2 = \sum_{i=1}^{n} \|(T - A)\,v_i\|^2\,.$$

Therefore A lies in the SOT neighborhood of T. $\square$

Next, we discuss some basic properties of C^*-algebra representations.

2.3 Representations of C^*-algebras

A representation π of a C^*-algebra $\mathcal{A}$ on the Hilbert space $\mathcal{H}$ is a $*$- homomorphism of π into $B(\mathcal{H})$.

Definition 2.3.1 ($*$-homomorphism)**.** *The map $\pi : \mathcal{A} \mapsto B(\mathcal{H})$ is a $*$-homomorphism if it satisfies the following conditions*

1. *linearity; for $\lambda \in \mathbb{C}$ and $A, B \in \mathcal{A}$*

$$\pi(\lambda A + B) = \lambda\pi(A) + \pi(B).$$

2. *homomorphism; $\pi(AB) = \pi(A)\pi(B)$.*

3. *$*$-property; $\pi(A^*) = \pi(A)^*$.*

We note that every $*$-homomorphism is positive : Let $A \in \mathcal{A}$ and $A \geq 0$ then $A = B^*B$ for some $B \in \mathcal{A}$. This implies that for all $|\psi\rangle \in \mathcal{H}$,

$$\begin{aligned}
\langle \pi(A)\psi|\psi\rangle &= \langle \pi(B^*B)\psi|\psi\rangle \\
&= \langle \pi(B)^*\pi(B)\psi \,|\, \psi \,\rangle \quad \text{by } *\text{-homomorphism property} \\
&= \langle \pi(B)\psi|\pi(B)\psi\rangle \\
&= \|\pi(B)\,|\psi\rangle\|^2 \geq 0\,.
\end{aligned}$$

Therefore for all $|\psi\rangle \in \mathcal{H}$,

$$\langle \pi(A)\psi|\psi\rangle \geq 0\,.$$

The representation π is said to be ***irreducible*** if $\pi(\mathcal{A})$ has no proper closed invariant space. The subspace S of $\mathcal{H}$ is said to be invariant for the C^*-algebra $\mathcal{A}$ if $A(S) \subseteq S$ for all $A \in \mathcal{A}$.

Definition 2.3.2 (Positive linear functional)**.** *A positive linear functional on a C^*-algebra $\mathcal{A}$ is a linear map $f : \mathcal{A} \mapsto \mathbb{C}$ such that $f(A) \geq 0$ whenever $A \geq 0$. It is called a state if it is norm* 1.

Now, let π be a representation of the algebra $\mathcal{A}$ on a Hilbert space $\mathcal{H}$ and $|\psi\rangle$ a vector in $\mathcal{H}$, then

$$f(A) = \langle \pi(A)\psi|\psi\rangle$$

is positive since π is a positive map and $|\psi\rangle \geq 0$. The key idea of representing C^*-algebras is to build from the representation of states. This procedure was determined by Gelfand, Naimark and Segal which is known as the GNS construction. Below is the theorem of the GNS construction as discussed by [4], its proof is beyond the scope of this thesis. Let us first recall the definition of a *cyclic vector*: A vector $|\psi\rangle \in \mathcal{H}$ is a *cyclic vector* if

$$\text{span}\overline{\{A\,|\psi\rangle : A \in \mathcal{A}\}} = \mathcal{H}\,.$$

Theorem 2.3.1 (GNS construction)**.** *Let f be a positive linear functional on the C^*-algebra $\mathcal{A}$. Then there is a representation π_f of $\mathcal{A}$ on $\mathcal{H}$ and a vector $|\psi_f\rangle$ in $\mathcal{H}$ which*

is a cyclic vector of $\pi(\mathcal{A})$ *such that* $\||\psi_f\rangle\| = \|f\|$ *and*

$$f(A) = \langle \pi_f(A)\psi_f|\psi_f\rangle$$

for all $A \in \mathcal{A}$.

2.3.1 Finite dimensional C^*-algebras

We recall that the set of all compact operators on the Hilbert space $\mathcal{H}$ is a concrete C^*-algebra. Let us denote the set of compact operator on the Hilbert space $\mathcal{H}$ as $\mathcal{K}(\mathcal{H})$.

Definition 2.3.3 (Compact Operators)**.** *The linear map* $K : X \mapsto Y$*, where* X *and* Y *are Banach spaces, is compact if the image closed unit ball* $C_1(0)$ *under* K *is relatively compact(the closure of* X *are compact).*

Since all relatively compact sets are bounded, a compact operator maps the closed unit ball into a bounded set and hence is continuous. Note that any bounded operator that has finite rank is compact. Therefore all finite dimensional operators on the Hilbert space $\mathcal{H}$ are compact.

Theorem 2.3.2. *The only irreducible* C^**-subalgebra of* $\mathcal{K}(H)$ *is itself.*

To prove the above theorem, let us consider the technical lemma below. The proof of the lemma can be found in [4].

Lemma 2.3.1. *If $\mathcal{A}$ is a non-zero C^*-algebra of compact operators, then it contains a minimal projection P of $\mathcal{A}$ such that $P\mathcal{A}P = \mathbb{C}P$.*

Furthermore, if π is a non-zero representation of $\mathcal{A}$ then there is a minimal projection P of $\mathcal{A}$ such that $\pi(P) \neq 0$. When π is irreducible the projection is rank one.

Now, we prove Theorem 2.3.2.

Proof. Let $\mathcal{A}$ be a non-zero irreducible subalgebra of $\mathcal{K}(\mathcal{H})$. Let P be a minimal projection in $\mathcal{A}$, then P is rank 1 from Lemma 2.3.1. Then there is a unit vector e such that $P = ee^*$. Since $\mathcal{A}$ is irreducible, if we let x and y be vectors in $\mathcal{H}$, then we can choose elements A and B in $\mathcal{A}$ such that $Ae = x$ and $Be = y$. Then $\mathcal{A}$ contains

$$APB^* = Aee^*B^* = (Ae)(Be)^* = xy^* .$$

Thus, $\mathcal{A}$ contains every rank one operator which span $\mathcal{K}(\mathcal{H})$ and therefore we obtain $\mathcal{A} = \mathcal{K}(\mathcal{H})$. □

Lemma 2.3.2. *Every non-zero representation of a C^*-algebra $\mathcal{A}$ of compact operators has an irreducible subrepresentation which is unitary equivalent to the restriction of $\mathcal{A}$ to a (minimal) reducing subspace.*

Proof. Let π be non-zero representation of $\mathcal{A}$. By Lemma 2.3.1, there is a minimal projection E such that $P = \pi(E)$ is non-zero. Let f be the unit vector in the range of P and let $\mathcal{H}_f^\pi = \overline{\pi(\mathcal{A})f}$. Also, if we let e be the unit vector in the range of E and let $\mathcal{H}_e = \overline{\mathcal{A}e}$. Then the subspaces $\mathcal{H}_e$ and $\mathcal{H}_f^\pi$ are invariant for $\mathcal{A}$ and $\pi(\mathcal{A})$ respectively.

From Lemma 2.3.1, since $E\mathcal{A}E = \mathbb{C}E$, the state on $\mathcal{A}$ given by $\varphi(A) = \langle Ae|e\rangle$ satisfies

$$EAE = \varphi(A)E \tag{2.3.1}$$

for all $A \in \mathcal{A}$.

Now, let us define a linear map U from $\mathcal{H}_e$ to $\mathcal{H}_f^\pi$ by the formula

$$U(Ae) := \pi(A)f = \pi(AE)f\,. \tag{2.3.2}$$

A simple computation shows that for $A, B \in \mathcal{A}$

$$\begin{aligned}
\langle UAe|UBe\rangle &= \langle \pi(AE)f|\pi(BE)f\rangle \\
&= \langle \pi(EB^*AE)f|f\rangle \\
&= \langle \pi(\varphi(B^*AE))f|f\rangle \quad \text{from Equation 2.3.1} \\
&= \langle \varphi(B^*A)\pi(E)f \,|\, f\rangle \\
&= \varphi(B^*A)\langle Pf|f\rangle \quad \text{since } \pi(E) = P \\
&= \langle B^*Ae|e\rangle\langle f|f\rangle \quad Pf = f \\
&= \langle B^*Ae \,|\, e\rangle \quad \text{using } \langle f|f\rangle = 1 \\
\langle UAe|UBe\rangle &= \langle Ae|Be\rangle
\end{aligned}$$

Consequently, U is an isometry from $\mathcal{H}_e$ to $\mathcal{H}_f^\pi$. In particular, U is well defined. For

$A, B \in \mathcal{A}$, we have

$$\begin{aligned}
\pi(A)\left(U(Be)\right) &= \pi(A)\pi(B)f \\
&= \pi(AB)f \quad \text{homomorphism of } \pi \\
&= U(ABe) \quad \text{from Equation (2.3.2)} \\
\pi(A)\left(U(Be)\right) &= UAU^*\left(U(Be)\right) .
\end{aligned}$$

Thus, $\pi(A)|_{\mathcal{H}_f^\pi} = UA|_{\mathcal{H}_e}U^*$ for every $A \in \mathcal{A}$. So $\pi|\mathcal{H}_f^\pi$ is unitarily equivalent to the restriction of $\mathcal{A}$ to $\mathcal{H}_e$.

Also, let π_e denote the restriction map of $\mathcal{A}$ to $\mathcal{H}_e$. Notice that $\pi_e(E) = ee^*$ is rank one. Indeed, $EAe = EAEe$ belongs to $\mathbb{C}e$ for every $A \in \mathcal{A}$, and thus $\mathbb{C}e$ is the range of $\pi_e(E)$. Suppose that P is a projection in $B(\mathcal{H}_e)$ which commutes with $\pi_e(\mathcal{A})$. Then

$$Pe = P\pi_e(E)e = \pi_e(E)Pe$$

is a multiple of e. As $Pe = P^2e$, this multiple is 0 or 1. Considering $I - P$ instead of P if necessary, we may suppose $Pe = 0$. But then

$$PAe = P\pi_e(A)e = \pi_e(A)Pe = 0$$

for all $A \in \mathcal{A}$; whence $P = 0$. Therefore $\pi_e(\mathcal{A})' = \mathbb{C}I$; and so π_e is irreducible. Hence the subspace $\mathcal{H}_e$ is minimal. □

Let $\mathcal{M}_n$ be the algebra of $n \times n$ complex matrices.

Corollary 2.3.1. *Every irreducible representation of $\mathcal{M}_n$ or $\mathcal{K}$ is unitarily equivalent to the identity representation.*

Proof. From Theorem 2.3.2, we have that the only invariant subspace for $\mathcal{M}_n$ or $\mathcal{K}$ is the whole space itself. □

Next, we show that the representation of the algebra $\mathcal{A}$ is the direct sum of irreducible ones.

Theorem 2.3.3. *Let $\mathcal{A}$ be a non-zero C^*-subalgebra of compact operators. Then every representation of π of $\mathcal{A}$ is the direct sum of irreducible representations which are unitary equivalent to the identity representation.*

Proof. By Lemma 2.3.2, we notice $\mathcal{H}_\pi$ contains a subspace $\mathcal{H}_f^\pi$ such that the restriction of $\pi(\mathcal{A})$ to $\mathcal{H}_f^\pi$ is an irreducible representation which is unitarily equivalent to a subrepresentation π_e of the identity representation. Let us choose the maximal family $\{\mathcal{H}_n^\pi\}$ of pairwise orthogonal reducing subspaces with this property. Then $\mathcal{H}_\pi$ is spanned by $\mathcal{H}_n^\pi$'s. For otherwise, the complement $(\sum_n \mathcal{H}_n^\pi)^\perp$ would dominate another such subspace $\mathcal{H}_f^\pi$ by Lemma 2.3.2 again. This would contradict the maximality of the original family. Let π_n be the restriction of π to $\mathcal{H}_n^\pi$. Then we obtain the decomposition $\pi = \sum_n \oplus \pi_n$, and each π_n is equivalent to an irreducible subrepresentation of the identity. □

Note that Theorem 2.3.3 is an expansion of Corollary 2.3.1, which simply means that for every irreducible representation π, we can always find a unitary operator U such that $U^*\pi(\cdot)U = id$, where id is the identity representation.

Theorem 2.3.4. *Let $\mathcal{A}$ be a C^*-subalgebra of the compact operators $\mathcal{K}(\mathcal{H})$. Then there are Hilbert spaces $\mathcal{H}_k$ of dimension n_k, for $k \geq 0$ and non-zero integers m_k such that*

$$\mathcal{H} \simeq \mathcal{H}_0 \oplus \sum_{k\geq 1} \oplus \mathcal{H}_k^{m_k}$$

and

$$\mathcal{A} \simeq 0 \oplus \sum_{k\geq 1} \oplus \mathcal{K}(\mathcal{H}_k)^{m_k}\,.$$

Proof. Let $\mathcal{H}_0 = \ker\mathcal{A}$. Then by Theorem 2.3.3, the Hilbert space $\mathcal{H}_0^{\perp}$ may be decomposed as a direct sum of reducing K_j such that the restriction of π_j of $\mathcal{A}$ to K_j is irreducible. Also, from Theorem 2.3.2, we have that $\pi_j(\mathcal{A}) = \mathcal{K}(K_j)$. Let us collect together all the equivalent representations into classes $\{\pi_j : j \in \mathcal{S}_k\}$. Let $\mathcal{H}_k$ be the Hilbert space of dimension $n_k = \dim K_j$ for $j \in S_k$, let m_k be the cardinality of $\mathcal{S}_k$, and let π_k be the identity representation of $\mathcal{K}(\mathcal{H}_k)$. Then it is evident that

$$\mathcal{H} \simeq \mathcal{H}_0 \oplus \sum_{k\geq 1} \oplus \mathcal{H}_k^{m_k}$$

and

$$\mathcal{A} \simeq 0 \oplus \sum_{k\geq 1} \oplus \mathcal{K}(\mathcal{H}_k)^{m_k}\,.$$

Finally, notice that the rank one projection $P_k \in \mathcal{K}(\mathcal{H}_k)$ is mapped onto the projection of rank m_k As the projection is compact, it follows that m_k is finite for all k. □

Now we may apply the structure theory of compact operators as seen in Theorem 2.3.4 to the finite dimensional C^*-algebras. Note that every finite dimensional C^*-algebra can be represented $*$-isomorphically as a C^*-algebra acting on the Hilbert space $\mathcal{H}$ by the GNS construction.

Theorem 2.3.5. *Every finite dimensional C^*-algebra $\mathcal{A}$ is $*$-isomorphic to the direct sum of full matrix algebras*

$$\mathcal{A} \cong \mathcal{M}_{n_1} \oplus \mathcal{M}_{n_2} \oplus \cdots \oplus \mathcal{M}_{n_k}$$

.

Proof. The proof of this theorem follows immediately from Theorem 2.3.4. Thus the number of summands must be finite and also the dimensions m_k must be finite for every k in order to get the direct sum to be finite dimensional. The direct sum of each unit on each summand is the identity element. □

Next we give the representation theory of the finite dimensional C^*-algebra as a direct consequence of Theorem 2.3.3.

Corollary 2.3.2. *If π is a non-zero $*$-representation of a finite dimensional C^*-algebra $\mathcal{A}$, then there exists cardinal numbers $\alpha_1, \cdots, \alpha_m$ such that π is unitary equivalent to*

$$id_i^{(\alpha_1)} \oplus \cdots \oplus id_n^{(\alpha_m)}$$

where id_k is the identity representation of $\mathcal{M}_{n_k}$.

2.3.2 Structure of von Neumann algebras

A finite dimensional representation of a von Neumann algebra is a C^*-algebra. Let $\mathcal{A}$ be a concrete finite dimensional $*$-algebra represented by matrices. By Corollary 2.3.2, $*$-subalgebras on the finite dimensional Hilbert space $\mathcal{H}$ are unitary equivalent to $*$-algebras of the form

$$\mathcal{A} \cong \oplus_{k=1}^{N} \left(\mathcal{M}_{n_k} \otimes I_{m_k}\right) , \tag{2.3.3}$$

where I_{m_k} is the identity of size m_k and $\mathcal{M}_{n_k}$ is a full matrix square of size n_k . Notice that the tensoring of a matrix algebra with the identity on another algebra denotes considering matrices which are block diagonal with as many blocks as there are elements on the diagonal of the identity matrix. The blocks of the diagonal matrices are identical in size and in their content.

The block diagonal matrix is determined by the form of its center denoted by $\mathcal{Z}(A) = \{A \in \mathcal{A} : [A, B] = 0, \text{for}\, B \in \mathcal{A}\}$ (operator in the algebra that commutes with any other element of the algebra). The center can also be defined as the intersection of the algebra $\mathcal{A}$ and the commutant $\mathcal{A}'$. Thus,

$$\mathcal{Z}(A) = (\mathcal{M}_{n_k} \otimes I_{m_k}) \cap (I_{n_k} \otimes \mathcal{M}_{m_k}) \simeq \mathbb{C}.$$

The commutant of the algebra $\mathcal{A}$ denoted by $\mathcal{A}'$ satisfies

$$\mathcal{A}' = \oplus_{k=1}^{N} (I_{n_k} \otimes \mathcal{M}_{m_k}) .$$

Notice that Equation (2.3.3) is a special case of Theorem 2.3.4. Thus, Theorem 2.3.4 represents the structure of the C^*-algebra in the infinite dimensional case.

2.4 Quantum operations

In this section, we discuss operations in quantum information which will help in understanding the body of this thesis. The Dirac's notation for vectors will be used throughout this thesis. We denote the column vector as $|\,\rangle$ and its dual the row vector is denoted by $\langle\,|$. The product of the 'bra' and 'ket' gives $\langle\,|\,\rangle : \mathcal{H} \times H \mapsto \mathbb{C}$ called the inner product and satisfies the following properties,

1. linearity; $\langle u + v|w\rangle = \langle u|w\rangle + \langle v|w\rangle$, for all $u, v \in \mathcal{H}$ and $w \in \mathcal{H}$.

2. conjugacy; $\langle u|w\rangle = \overline{\langle u|w\rangle}$, for all $u, w \in \mathcal{H}$.

3. scalar multiplication; $\langle ku|w\rangle = k\langle u|w\rangle$, for all $k \in \mathbb{C}$ and $u, w \in \mathcal{H}$. Note that the scalar k is conjugate on the second argument.

4. positivity; $\langle u|u\rangle \geq 0$ with equality if and only if $u = 0$.

The rank one projection $P = |\phi\rangle\langle\phi|$ also known as the 'outer product' for $|\phi\rangle \in \mathcal{H}$ satisfies the property that

$$P|\psi\rangle = (|\phi\rangle\langle\phi|)|\psi\rangle = \langle\phi|\psi\rangle|\phi\rangle \ ,$$

where $\langle\phi|\psi\rangle$ is equal to some scalar $\lambda \in \mathbb{C}$. For the purpose of our work we choose elements in $B(\mathcal{H})$ as positive and trace one elements (density operators).

The matrix representation of the direct sum of an algebra mentioned in Section 2.4 above is given by

$$\mathcal{A} := \oplus_i^n \mathcal{A}_i = \left\{ \begin{pmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & A_n \end{pmatrix} : A_i \in \mathcal{A}_i \right\},$$

where each $\mathcal{A}_i$ is unitary equivalent to an algebra of the form $I_{m_i} \otimes \mathcal{M}_{n_i}$.

Example 2.4.1. $\mathcal{M}_2 \oplus \mathcal{M}_2 = \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} : A, B \in \mathcal{M}_2 \right\}$, *which is of dimension of the Hilbert space is* $(2+2) = 4$.

The tensor product is defined as follows; let $|\phi_1\rangle, \cdots, |\phi_n\rangle$ and $|\psi_1\rangle, \cdots, |\psi_m\rangle$ be the basis elements of $\mathcal{H}$ and H respectively. Then $\mathcal{H} \otimes H = \text{span}\{|\phi_i\rangle \otimes |\psi_j\rangle \text{ for } 0 \leq i \leq n,\ 0 \leq j \leq m\}$. The dimension of $\mathcal{H} \otimes H$ is nm. In general the matrix representation of the tensor product is given by

$$A = \begin{pmatrix} \phi_{11} & \phi_{12} & \phi_{13} & \dots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \phi_{23} & \dots & \phi_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \phi_{n1} & \phi_{n2} & \phi_{n3} & \dots & \phi_{nn} \end{pmatrix}, \quad B = \begin{pmatrix} \psi_{11} & \psi_{12} & \psi_{13} & \dots & \psi_{1m} \\ \psi_{21} & \psi_{22} & \psi_{23} & \dots & \psi_{2m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \psi_{m1} & \psi_{m2} & \psi_{m3} & \dots & \psi_{mm} \end{pmatrix}$$

for $A \in B(\mathcal{H})$ and $B \in B(H)$. Then

$$A \otimes B = \begin{pmatrix} \phi_{11} \cdot B & \phi_{12} \cdot B & \phi_{13} \cdot B & \dots & \phi_{1n} \cdot B \\ \phi_{21} \cdot B & \phi_{22} \cdot B & \phi_{23} \cdot B & \dots & \phi_{2n} \cdot B \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \phi_{n1} \cdot B & \phi_{n2} \cdot B & \phi_{n3} \cdot B & \dots & \phi_{nn} \cdot B \end{pmatrix}.$$

Let us consider an example from the above representation

Example 2.4.2.

$$I_2 \otimes \mathcal{M}_3 = \left\{ \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} ; \textit{for}\, A \in \mathcal{M}_3 \right\}$$

and the dimension of the Hilbert space is $(2 \times 3) = 6$.

Example 2.4.3.

$$\mathcal{M}_3 \oplus \mathcal{M}_3 = \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} ; \textit{for}\, A, B \in \mathcal{M}_3 \right\}$$

and the Hilbert space is dimension $(3 + 3) = 6$.

Consider the example $(I_2 \otimes \mathcal{M}_3) \oplus \mathcal{M}_5$ with the Hilbert space of dimension 11. The matrix representation gives

$$(I_2 \otimes \mathcal{M}_3) \oplus \mathcal{M}_5 = \left\{ \begin{pmatrix} A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & B \end{pmatrix} : A \in \mathcal{M}_3 \,\text{and}\, B \in \mathcal{M}_5 \right\}.$$

In general, we have $\oplus_{i=1}^{d} I_{m_i} \otimes \mathcal{M}_{n_i}$ is the matrix of dimension $\sum_{i=1}^{d} m_i n_i$.

Another important operation to take note of is the partial trace. Let $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ such that $\rho^A \in \mathcal{H}^A$ and $\rho^B \in \mathcal{H}^B$, for $\rho = \rho^A \otimes \rho^B$. Then the partial trace with respect to A is given by

$$\mathrm{Tr}_A(\rho) = \mathrm{Tr}_A(\rho^A \otimes \rho^B) = \rho^B \mathrm{Tr}(\rho^A)\,. \tag{2.4.1}$$

As seen from above, we know that ρ^A is a density operator and hence is of trace 1. Therefore, from Equation (2.4.1), we have

$$\mathrm{Tr}_A(\rho) = \rho^B\,.$$

Similar arguments hold for the partial trace with respect to the B. The unitary operators we will be using often in the thesis will be the Pauli operators denoted by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and I_n is the $n \times n$ identity matrix on the Hilbert space $\mathcal{H}$.

A quantum channel is another quantum operation we will be meeting as we go further this thesis.

Definition 2.4.1. *A quantum channel is defined as a completely positive (CP) and trace preserving (TP) map. Normally denoted as CPTP maps.*

Next, we consider definitions of completely positive (CP) and trace preserving(TP) maps.

Definition 2.4.2 (Trace-preserving map)**.** *A map* $\Phi : B(\mathcal{H}) \mapsto B(\mathcal{H})$ *is said to be trace preserving if for all* $\rho \in B(\mathcal{H})$*,*

$$Tr(\Phi(\rho)) = Tr(\rho)\,.$$

We next give the operator definition for completely positive(CP) maps derived by Choi [19] instead of the more abstract definition.

Definition 2.4.3 (Completely positive map)**.** *Let* $\mathcal{H}$ *be a finite dimensional Hilbert space and* $B(\mathcal{H})$ *the bounded operator on the Hilbert space. Let* $\Phi : B(\mathcal{H}) \mapsto B(\mathcal{H})$*, where* $\mathcal{H}$ *is of dimension* n*. The map* Φ *is said to be completely positive if it has an 'operator sum representation' for all* $\rho \in B(\mathcal{H})$ *. That is there are operators* $E_i \in B(\mathcal{H})$

$$\Phi(\rho) = \sum_{i=1}^{n} E_i^* \rho E_i\,, \tag{2.4.2}$$

where the operators E_i are called the Kraus operators.

The decomposition in Equation (2.4.2) above is not unique and is linearly related to

$$\Phi(\rho) = \sum_{j} F_j^* \rho F_j\,, \tag{2.4.3}$$

for all μ_{ji} such that $F_j = \sum_i \mu_{ji} E_i$. We also note that Φ is TP if and only if

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

2.5 Operator systems and separating vectors

Recall the structure of the finite dimensional C^*-algebras; Let $\mathcal{A}$ be an algebra which is $*$-isomorphic to the orthogonal direct sum of full matrix algebras M_n. Then from the representation theory the algebra $\mathcal{A}$ is unitary equivalent to the direct sum of matrices of the form $\oplus_i (I_{k_i} \otimes M_{n_i})$, where k_i corresponds to the multiplicities of n_i-dimensional irreducible representations that determine the structure of the algebra $\mathcal{A}$.

Definition 2.5.1 (operator system)**.** *Let $\mathcal{A}$ be a unital C^*-algebra. An operator system is any linear subspace $\mathfrak{C}$ of $\mathcal{A}$ which contains the identity and is closed under taking adjoints.*

To see the difference between operator systems and operator algebras, consider the following two simple examples.

Example 2.5.1. *The set of hermitian matrices* $A = \begin{pmatrix} a & c \\ \overline{c} & b \end{pmatrix}$ *, for $a, b \in \mathbb{R}$ and $c \in \mathbb{C}$ is an operator system but not an algebra.*

Example 2.5.2. *The 2×2 diagonal matrix* $B = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ *, for $a, b \in \mathbb{R}$ is an operator algebra.*

Example 2.5.2 satisfies all the conditions of an operator algebra. The beauty about Example 2.5.2 is that it is also an operator system. In the case of Example 2.5.1 the multiplication condition for an operator algebra fails. Hence the 2×2 hermitian matrices given in Example 2.5.1 above is not an operator algebra. Therefore, every operator algebra is an operator system but the converse is not true.

Next, we discuss separating vectors.

Definition 2.5.2. *Let $\mathcal{H}$ be a Hilbert space and let $\mathfrak{C} \subseteq B(\mathcal{H})$ be a set of operators on $\mathcal{H}$ that form an operator system. A vector $|\psi\rangle \in \mathcal{H}$ is said to be a separating vector of $\mathfrak{C}$ if $A|\psi\rangle \neq 0$ whenever A is a nonzero element of $\mathfrak{C}$.*

If $\mathcal{H}$ is finite dimensional and $\mathfrak{C}$ is in fact C^*-subalgebra, then we can use the aforementioned representation theory for such algebras to determine the existence of a separating vector as follows. (See [20] for more in-depth investigations on this topic.)

Proposition 2.5.1. *A C^*-algebra $\oplus_i (I_{k_i} \otimes \mathcal{M}_{n_i})$ has a separating vector if and only if $k_i \geq n_i$ for all i.*

Proof. Let us consider first the case $I_k \otimes \mathcal{M}_n$. Suppose $k \geq n$ and let $\{|\psi_1\rangle, \cdots, |\psi_k\rangle\}$ span the space $\mathbb{C}^n$. Let $|\psi\rangle = (|\psi_1\rangle, \cdots, |\psi_k\rangle)^T$ where T is the transpose of $|\psi\rangle$. We observe that for $A \in \mathcal{M}_n$ with $(I_k \otimes A)|\psi\rangle = 0$ implies $A|\psi_i\rangle = 0$ for all i and hence $A = 0$. Therefore, $|\psi\rangle$ is a separating vector.

Conversely. Suppose $k < n$ and P be a non-zero projection onto the orthogonal complement of the space $\{|\psi_i\rangle\}$ for any $(|\psi_1\rangle, \cdots, |\psi_k\rangle)^T$ with $|\psi_i\rangle \in \mathbb{C}^n$. It follows that $(I_k \otimes P)|\psi\rangle = 0$ but $P \neq 0$, and hence $(I_k \otimes M_n)$ has no separating vector. Therefore,

for the general case $\oplus_i (I_{k_i} \otimes \mathcal{M}_{n_i})$, a similar argument holds for $k_i \geq n_i$ for all i. $\square$

Example 2.5.3. *$I_3 \otimes \mathcal{M}_2$ has a separating vector.*

Solution. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2$, then $\begin{pmatrix} A & 0 & 0 \\ \vdots & A & \vdots \\ 0 & \cdots & A \end{pmatrix} \in I_3 \otimes \mathcal{M}_2$. Let $|\psi\rangle = \{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ span the space $\mathbb{C}^2$. Let $|\psi\rangle = \begin{pmatrix} |\psi_1\rangle \\ |\psi_2\rangle \\ |\psi_3\rangle \end{pmatrix}$ and choose $|\psi_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|\psi_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. We see clearly that $A|\psi_1\rangle = 0 \implies a = c = 0$ and $A|\psi_2\rangle = 0 \implies b = d = 0$. Therefore $A|\psi\rangle = 0 \implies A = 0$. Hence $I_3 \otimes \mathcal{M}_2$ has a separating vector.

Now, using the same argument as above for $I_2 \otimes \mathcal{M}_3$.

Example 2.5.4. *$I_2 \otimes \mathcal{M}_3$ has no separating vector.*

Let $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in \mathcal{M}_3$, then clearly $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \in I_2 \otimes \mathcal{M}_3$. Let $|\psi\rangle =$

$\begin{pmatrix} |\psi_1\rangle \\ |\psi_2\rangle \end{pmatrix}$ such that $|\psi_1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and $|\psi_2\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ span $\mathbb{C}^3$, then $A|\psi_1\rangle$ is

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

which implies that $a = d = g = 0$.

Also $A|\psi_2\rangle$ gives

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

which implies $b = e = h = 0$.

Therefore

$$\begin{pmatrix} 0 & 0 & c \\ 0 & 0 & f \\ 0 & 0 & i \end{pmatrix} |\psi\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Thus $A|\psi\rangle = 0$ for $A \neq 0$. Hence $|\psi\rangle$ has no separating vector.

Chapter 3

Quantum local operations and classical communication (LOCC)

A basic scenerio of quantum information is when two different parties Alice and Bob, each of whom controls a quantum system, represented on the finite dimensional Hilbert spaces denoted by $\mathcal{H}_A$ and $\mathcal{H}_B$ are restricted to perform local operations and classical communication. Their joint system $\mathcal{H}_A \otimes \mathcal{H}_B$ has been prepared in a pure state from a known set of entangled states $\mathcal{S} = \{|\psi_i\rangle\}_{i=0,1,\cdots n-1}$. Their task is to distinguish the set of states perfectly using LOCC.

The type of LOCC depends on the classical communication allowed between the different parties. Recall that for the bipartite state, local operations are of the form $\mathcal{E} = \mathcal{E}_A \otimes \mathcal{E}_B$ and von Neumann measurement $\{\mathcal{M}_k = A_0 \otimes A_1\} \in \mathcal{H}$, $A_i \geq 0$ and $\sum_i A_i = I_i$ on the joint subsystem. Classical communications involves the transfer of bits of information. Let us consider an example in the two dimensional case where Alice

and Bob need to distinguish between the pair of Bell states.

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B \right) \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B \right) \end{aligned} \tag{3.0.1}$$

Suppose Alice's local operations are $A_1 = |0\rangle\langle 0| \otimes I_B$ and $A_2 = |1\rangle\langle 1| \otimes I_B$. Alice after measurement has a 50% chance of getting either a $|0\rangle$ or a $|1\rangle$. If Alice obtains a $|0\rangle$ after measurement, she communicates her result to Bob who also applies his local operations $B_1 = I_A \otimes |0\rangle\langle 0|$ and $B_2 = I_A \otimes |1\rangle\langle 1|$ on his subsystem. An outcome of $|0\rangle$ tells us the state $|\psi_i\rangle$ is $|\psi_0\rangle$ and $|\psi_1\rangle$ if the measurement outcome is $|1\rangle$. The protocol is especially simple in this example since Bob does not depend on Alice's measurement outcome. In general, we will allow Bob to adapt his measurement depending on Alice's measurement outcome.

3.1 Early significant results for LOCC

A lot of progress has been made in the study of local operations and classical communication in terms of reliably distinguishing states. The first exploration started with Peres and Wootters in [21], who demonstrated that two different unentangled nonorthogonal states cannot be distinguished using LOCC. An example to demonstrate this is to consider three linear polarized states: $0°, 60°$ and $120°$. These states are clearly not orthogonal to each other. Alice's and Bob's task is to determine which

of these states they have in their possession using separate measurements followed by classical communication. Here they are not allowed any joint measurement, to share entanglement, or to exchange quantum information. Peres-Wootters concluded that because the states are non-orthogonal they cannot be distinguished perfectly by local operations and classical communication. They established that local operation and classical communication on the states gives no information about the states. Also, by numerical calculation they showed that a joint measurement on the states yielded more information about the states.

By choosing the same polarized states as mentioned above, Massar and Popescu [15] analytically demonstrated that if Alice and Bob are restricted to a finite number of ensembles of identically prepared particles, they cannot distinguish between the states perfectly by LOCC. Thus, their LOCC ability to reliably identify the states will be less than a joint measurement on their states. An example is seen in quantum data hiding [5, 16] where some classical data is encoded into a bipartite state such that Alice and Bob have access to very little information when restricted to local operations and classical communication.

In [1] (building up from Peres-Wootters), Bennett *et al* in 1999 showed that there exists orthogonal product states that cannot be distinguished using local operations and classical communication (LOCC). It is important to notice that the product states are orthogonal in this case. Let us consider a set of states which are orthonormal, and have the form $|\alpha\rangle \otimes |\beta\rangle$ on $\mathbb{C}^3 \otimes \mathbb{C}^3$ as in [1].

$$
\begin{aligned}
|\psi_1\rangle &= |1\rangle \otimes |1\rangle \\
|\psi_2\rangle &= |0\rangle \otimes \frac{|0+1\rangle}{\sqrt{2}} \\
|\psi_3\rangle &= |0\rangle \otimes \frac{|0-1\rangle}{\sqrt{2}} \\
|\psi_4\rangle &= |2\rangle \otimes |1+2\rangle \\
|\psi_5\rangle &= |2\rangle \otimes |1-2\rangle \\
|\psi_6\rangle &= |1+2\rangle \otimes |0\rangle \\
|\psi_7\rangle &= |1-2\rangle \otimes |0\rangle \\
|\psi_8\rangle &= \frac{|0+1\rangle}{\sqrt{2}} \otimes |2\rangle \\
|\psi_9\rangle &= \frac{|0-1\rangle}{\sqrt{2}} \otimes |2\rangle
\end{aligned}
$$

Alice's and Bob's task is to distinguish these states perfectly by LOCC. Suppose Alice's measurement outcome is $|0\rangle$; then the possibilities are $|\psi_2\rangle, |\psi_3\rangle, |\psi_8\rangle$ or $|\psi_9\rangle$. These states are nonorthogonal to each other and hence Bob will not be able to perfectly distinguish between the states. Suppose Bob's measurement outcome is $|2\rangle$; then he will neither be able to reliably distinguish between the states $|\psi_8\rangle$ and $|\psi_9\rangle$. A similar argument holds if we allow Bob to go first.

Note that an elimination of any two of the so-called 'domino states' will allow perfect distinguishability via LOCC. Suppose we eliminate $|\psi_6\rangle$ and $|\psi_8\rangle$ and allow Alice to go first, then Bob will be able to perfectly distinguish between the states using LOCC.

Also, if we eliminate $|\psi_2\rangle$ or $|\psi_4\rangle$ and allow Bob to go first the same applies. Although the product states mentioned above cannot be distinguished perfectly by LOCC they can be reliably distinguished by arbitrary quantum operations. Thus, elements of the set can be distinguished perfectly by separable operations (SEP)(an example of an arbitrary quantum operation). In terms of nested measurement classes,

$$\text{LOCC} \subset \text{SEP}.$$

Mathematically, separable operations are defined as follows: A measurement $\mathbb{M} = \{\mathcal{M}_k\}$ is separable if each $\mathcal{M}_k$ can be written as $\sum_{k,l} A_{k,l} \otimes B_{k,l}$ with $A_{k,l} \otimes B_{k,l} \geq 0$ for each k, l. Separable operations have nicer structure than local operations and classical communication.

One of the most important results in the study of LOCC was established by Jonathan Walgate and his group in 2000 [23], who argued that if the states $|\phi\rangle$ and $|\psi\rangle$ are orthogonal;

$$\langle\phi|\psi\rangle = 0\,,$$

then they can be distinguished perfectly by one-way LOCC. They established this by considering two orthogonal states $|\phi\rangle$ and $|\psi\rangle$. Alice and Bob need to distinguish between these states, but they are restricted to local operations and classical communication. To accomplish this task, Alice chooses any basis that represents the states given by

$$|\phi\rangle = |1\rangle_A |\eta_1\rangle_B + \cdots + |l\rangle_A |\eta_n\rangle_B \tag{3.1.1}$$

$$|\psi\rangle = |1\rangle_A |\nu_1\rangle_B + \cdots + |l\rangle_A |\nu_n\rangle_B \tag{3.1.2}$$

where $\{|1\rangle_A, \cdots, |l\rangle_A\}$ are the basis for Alice's subsystem and $|\eta_i\rangle$ and $|\nu_i\rangle$ are unnormalised and not necessarily orthogonal states. Alice does a measurement to determine the actual i and communicates it to Bob. Bob then does a local measurement on his subsystem to determine the shared state between them. To do this, let us express the basis $|\eta_i\rangle$ and $|\nu_i\rangle$ in terms of Bob's subsystem such that

$$|\eta_i\rangle = \sum_i F_{ij} |j\rangle_B \quad \text{and} \quad |\nu_i\rangle = \sum_i G_{ij} |j\rangle_B \tag{3.1.3}$$

where F_{ij} and G_{ij} form $n \times m$ matrix F and G constructed in the form

$$FG^* = \begin{pmatrix} \langle\eta_1|\nu_1\rangle & \langle\eta_1|\nu_2\rangle & \cdots & \cdots & \langle\eta_1|\nu_m\rangle \\ \langle\eta_2|\nu_1\rangle & \langle\eta_2|\nu_2\rangle & \cdots & \cdots & \langle\eta_2|\nu_m\rangle \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \langle\eta_n|\nu_1\rangle & \langle\eta_n|\nu_2\rangle & \langle\eta_n|\nu_3\rangle & \cdots & \langle\eta_n|\nu_m\rangle \end{pmatrix},$$

such that all the information about the states $|\phi\rangle$ and $|\psi\rangle$ are preserved during the construction. Also, since $\langle\phi|\psi\rangle = 0$, it follows that

$$\sum_{i=1}^{n} \langle\eta_i|\nu_i\rangle = \mathrm{Tr}(FG^*) = 0\,.$$

Notice that the matrix FG^* holds more information apart from the fact that the states

are orthogonal. Thus it encodes the key to distinguishing between these two possible states. Let us recall that Alice's plan is to distinguish the states $|\phi\rangle$ and $|\phi\rangle$ by finding some basis(any basis) in which she can represent her states restricted to the form

$$\begin{aligned} |\phi\rangle &= |1\rangle_A |\eta_1\rangle_B + \cdots + |l\rangle_A |\eta_n\rangle_B \\ |\psi\rangle &= |1\rangle_A \left|\eta_1^{\perp}\right\rangle_B + \cdots + |l\rangle_A \left|\eta_n^{\perp}\right\rangle_B . \end{aligned}$$

Alice must choose her basis carefully such that no matter what result of $|i\rangle_A$ she obtains, Bob is guaranteed of being able to distinguish between his possible states. This implies that, for all i, $|\nu_i\rangle$ must be orthogonal to $|\eta_i\rangle$. Therefore

$$\langle \eta_i | \nu_i \rangle = 0 . \tag{3.1.4}$$

We note that the matrix FG^* has all of its diagonal equal to zero. Equation (3.1.4) is what we call the distinguishability criterion. Thus, Bob will be able to distinguish between the two possible state only if the unnormalized basis $|\eta_i\rangle$ and $|\nu_i\rangle$ are orthogonal.

Theorem 3.1.1. *[23] Two orthogonal* 2×2 *states can always be distinguished perfectly by one-way LOCC.*

Proof. The proof of this theorem is immediate from the construction of the distinguishability criterion. That is, Alice can always find a basis of the form

$$|\psi_i\rangle = |0\rangle_A \left|\eta_0^i\right\rangle_B + |1\rangle_A \left|\eta_1^i\right\rangle_B ,$$

where $\langle \eta_0^i | \eta_0^j \rangle = \langle \eta_1^i | \eta_1^j \rangle = 0$ whenever $i \neq j$ and for $i, j = 0, 1$, in which two states of any dimension can be distinguished perfectly by LOCC. □

In general, let us consider a unitary transformation of Alice's measurement basis map to a conjugate unitary transformations upon the matrix FG^*.

Theorem 3.1.2. *A unitary transformation U_A upon Alice's measurement will transform FG^* to $U'_A(FG^*)U'^*_A$.*

Proof. From the representation of the orthogonal states in Equations (3.1.1) and (3.1.2) above, we have that

$$|\psi\rangle = \sum_i |i\rangle_A |\eta_i\rangle_B \ . \tag{3.1.5}$$

Then Alice's unitary transformation is given by

$$|i\rangle_A = \sum_j (U_{ij})^*_A \left|\tilde{j}\right\rangle_A \ .$$

From Equation (3.1.3), Alice's measurement becomes

$$|\psi\rangle = \sum_{ijk} (U_{ij})^*_A \left|\tilde{j}\right\rangle_A F_{ik} |k\rangle_B \ .$$

Notice that Bob might assist Alice by unitarily rotating his basis by U_B such that

$$|k\rangle_B = \sum_l (U_{kl})^*_B \left|\tilde{l}\right\rangle_B \ ,$$

which gives

$$|\psi\rangle = \sum_{ijkl} \left|\tilde{j}\right\rangle_A \left|\tilde{l}\right\rangle_B (U_{ji})^*_A F_{ik} (U_{kl})^*_B \,.$$

Choose $U^*_{ij} = U'_{ji}$, let us describe our new basis for our new matrix F' such that

$$F'_{lk} = \sum_{jl} (U_{jl})'_A F_{ik} (U_{kl})^*_B \,.$$

Therefore we have our matrix F and G under the following transformation

$$\begin{aligned} F' &= U'_A F U^*_B \\ G' &= U'_A G U^*_B \end{aligned}$$

Hence the matrix FG^* will be transformed as

$$\begin{aligned} F'G'^* &= \left(U'_A F U^*_B\right)\left(U'_A G U^*_B\right)^* \\ &= \left(U'_A F U^*_B\right)\left(U_B G^* U'^*_A\right) \\ &= U'_A (FG^*) U'^*_A \end{aligned}$$

□

We see that Bob's unitary transformation has dropped out and hence the rotation in his basis will not affect the entries $\langle \nu_i | \eta_i \rangle$ that make up FG^*. In summary, Alice can find a basis in the form (3.1.1) and (3.1.2) satisfying the distinguishability criterion if and only if there exists a unitary $U = U_A$ such that $U\left(FG^*\right)U^*$ has all of

its diagonal elements as zero.

Theorem 3.1.3. *[22] Three orthogonal 2×2 states cannot be perfectly distinguished by LOCC if and only if two of the states are product states.*

Proof. From Equation (3.1.5), the three orthogonal 2×2 state is given by

$$\begin{aligned} |\psi_1\rangle &= |0\rangle_A |\eta_0\rangle_B + |1\rangle_A |\eta_1\rangle_B \\ |\psi_2\rangle &= |0\rangle_A \left|\eta_0^{\perp}\right\rangle_B + |1\rangle_A \left|\eta_1^{\perp}\right\rangle_B \\ |\psi_3\rangle &= |0\rangle_A \left|\eta_0'\right\rangle_B + |1\rangle_A \left|\eta_1'\right\rangle_B \end{aligned}$$

If the states are distinguishable then there must be a choice $\{|0\rangle_A, |1\rangle_A\}$ such that $\langle\eta_0|\eta_0'\rangle = \langle\eta_0^{\perp}|\eta_0'\rangle = 0$ and $\langle\eta_1|\eta_1'\rangle = \langle\eta_1^{\perp}|\eta_1'\rangle = 0$. Suppose Alice's measurement outcome is $|0\rangle$, then in one of the two case states forming the inner product must have a magnitude of zero. Hence for Bob to be able to distinguish between the states then at least two of the states must be a product state. That is

$$\begin{aligned} |\psi_1\rangle &= |0\rangle_A |\eta_0\rangle_B + |1\rangle_A |\eta_1\rangle_B \\ |\psi_2\rangle &= |0\rangle_A \left|\eta_0^{\perp}\right\rangle_B \\ |\psi_2\rangle &= |1\rangle_A \left|\eta_1^{\perp}\right\rangle_B \end{aligned}$$

□

Similar argument holds for the four orthogonal 2×2 states, except in this case all four states must be product state in order for perfect distinguishability via LOCC.

Another important result is that of H. Fan [6], he demonstrated that any three generalized Pauli states of dimension d, where d is a prime number greater than two can be distinguished perfectly by LOCC. This fact is backed by [18], which states that any three mutually orthogonal maximally entangled in $\mathbb{C}^d \otimes \mathbb{C}^d$ for d even, cannot be distinguished perfectly by one-way LOCC.

A special case of Fan's result is discussed in Nathanson's 2005 paper [17], where he showed that any three orthogonal maximally entangled states in $\mathbb{C}^3 \otimes \mathbb{C}^3$ can be distinguished perfectly by LOCC and in [18], he gave examples of three maximally entangled states that can be distinguished with full LOCC but not with one-way LOCC.

3.2 Schemes of LOCC

The notion of LOCC is determined by the type of classical communication used in the protocol. Here we briefly describe the different schemes, giving extra attention to the one-way version, which is the focus of the next chapter.

Local operations(LO)

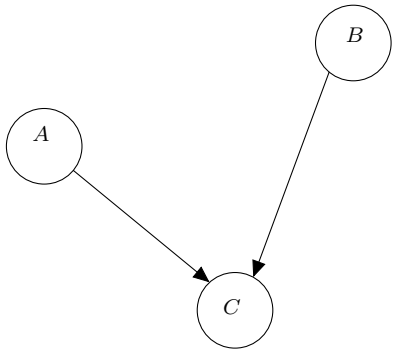

Figure 3.1: Local product measurement

In this scheme, Alice and Bob perform separate measurement in the same basis. Note that Bob does not need to know Alice's measurement outcome. They separately send their measurement outcome to a third party Chris who identifies the state that they started with. Thus they only communicate after the fact to compare their results.

Two-way local operation and classical communication(LOCC)

Figure 3.2: LOCC

This scheme allows Alice and Bob to communicate classically as much as they like and to iteratively adapt their measurement as they go.

One-way local operation and classical communication (LOCC-1)

Figure 3.3: LOCC-1

In this scheme, Bob adapts his measurement based on classical information he receives from Alice but the other way around is not allowed. For the rest of the thesis we restrict ourselves to one-way LOCC. This is the scheme that includes the key protocols in quantum information, such as quantum teleportation. In the protocol of quantum teleportation Alice and Bob initially share an entangled state $|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice has an unknown state $|\phi\rangle$ she wishes to transmit to Bob. Alice does her measurement and communicates her result to Bob. Based on the information Bob receives from Alice, he applies the appropriate operation to to get the exact unknown state $|\phi\rangle$, which is precisely what Alice want. Thus suppose the qubit in Bob's possession is in the state $|\beta\rangle$, then:

- If Alice measures $|00\rangle$, then $|\phi\rangle = |\beta\rangle$.
- If Alice measures $|01\rangle$, then Bob applies the Pauli X, $|\phi\rangle = X|\beta\rangle$.

- If Alice measures $|10\rangle$, then $|\phi\rangle = Z\,|\beta\rangle$.
- If Alice measures $|11\rangle$, then $|\phi\rangle = XZ\,|\beta\rangle$.

In general, as shown by Nathanson [18] one-way LOCC is described mathematically as the measurement outcome $\mathcal{M}_k = \{A_k \otimes B_{k,j}\}$ for some fixed j and for any k, where $A_k, B_{k,j} \geq 0$ and $\sum_k A_k = I_A$ and $\sum_k B_{k,j} = I_B$.

Recall the example for distinguishing between the Bells basis given at the start of this chapter. Alice's local operations by definition are $A_1 = |0\rangle\langle 0|$ and $A_2 = |1\rangle\langle 1|$. Similarly, Bob has $B_{1,1} = B_{2,1} = |0\rangle\langle 0|$ and $B_{1,2} = B_{2,2} = |1\rangle\langle 1|$. Also, in the case of quantum teleportation, one can view Alice's measurements as von Neumann measurements of the form

$$\begin{aligned} A_1 &= |00\rangle\langle 00| \\ A_2 &= |01\rangle\langle 01| \\ A_3 &= |10\rangle\langle 10| \\ A_4 &= |11\rangle\langle 11| \end{aligned}$$

and Bob's measurements given by $B_{1,1} = B_{2,1} = B_{3,1} = B_{4,1} = I_B$.

Note that this rule for one-way LOCC allows for perfect distinguishability for the states $\{|\psi_i\rangle\}$ if

$$\langle\psi_i|\, A_k \otimes B_{k,j}\, |\psi_i\rangle = 0\,,$$

for all k and $i \neq j$.

In many of the cases we are interested in, $\{|\psi_i\rangle = (I \otimes U_i)|\psi_0\rangle\}$ where U_i is a unitary operator on $\mathbb{C}^d$ and $|\psi_0\rangle$ is the d dimensional standard maximally entangled state on $\mathbb{C}^d \otimes \mathbb{C}^d$

$$|\psi_0\rangle = \frac{1}{\sqrt{d}}\left(|00\rangle + |11\rangle + \cdots + |d-1 d-1\rangle\right) .$$

In fact, we note that any maximally entangled state can be written as $(I \otimes U_i)|\psi_0\rangle$ for the same d-dimensional unitary. Thus in the two dimensional case given in Equation (3.0.1) above,

$$\begin{aligned} |\psi_0\rangle &= (I \otimes U_1)\left(\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)\right) \\ |\psi_1\rangle &= (I \otimes U_2)\left(\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)\right) , \end{aligned}$$

where U_1 is the identity and U_2 is the Pauli X. We see that after Alice's measurement, Bob will only be able to distinguish between the states perfectly by one-way LOCC if the states are orthogonal. The fundamental mathematical description of one-way LOCC is given as follows [18].

Proposition 3.2.1. *For any set of orthogonal states $\mathcal{S}$ in $\mathbb{C}^d \otimes \mathbb{C}^d$ such that $\mathcal{S} = \{|\psi_i\rangle = (I \otimes U_i)|\psi_0\rangle\} \in \mathbb{C}^d \otimes \mathbb{C}^d$, where $|\psi_0\rangle$ is the standard maximally entangled state. The following are equivalent.*

1. The elements $\mathcal{S}$ can be perfectly distinguished by one-way LOCC.

2. There exists a set of states $\{|\phi_k\rangle\}_{k=1}^r \subseteq \mathbb{C}^d$ and positive numbers m_k such that

$\sum_k m_k |\phi_k\rangle \langle\phi_k| = I$ *for all* k *and* $i \neq j$

$$\langle\phi_k|U_j^* U_i |\phi_k\rangle = 0 \tag{3.2.1}$$

3. *There is a* $d \times r$ *partial isometry matrix* W *such that* $WW^* = I_d$*, and for all* $i \neq j$*, every diagonal entry of the* $r \times r$ *matrix* $W^* U_j^* U_i W$ *is equal to zero.*

Proof. The vectorization of the matrix $|\psi_0\rangle = \dfrac{\mathrm{vec}(I_d)}{\sqrt{d}}$. Similarly, the vectorization of $(I \otimes U_i)|\psi_0\rangle = \dfrac{\mathrm{vec}(U_i)}{d}$. Now suppose condition (1) holds and that Alice's measurement outcome $A_k = |\alpha_k\rangle\langle\alpha_k| \otimes I$, then

$$|\psi_k\rangle = \frac{(|\alpha_k\rangle\langle\alpha_k| \otimes I)\,\mathrm{vec}(U_i)}{\sqrt{d} m_k}\,. \tag{3.2.2}$$

Notice that m_k is the trace of the rank one matrix A_k. Now recall the $(C \otimes A)\,\mathrm{vec}(B) = \mathrm{vec}\left(ABC^T\right)$, where T is the transpose of the matrix C. From Equation (3.2.2) we have

$$|\psi_k\rangle = \frac{\mathrm{vec}\left(U_i |\overline{\alpha_k}\rangle \langle\overline{\alpha_k}|\right)}{\sqrt{d} m_k}\,.$$

Bob's state after Alice's measurement is

$$\begin{aligned} B_k &= \frac{\mathrm{Tr}_A\left(\mathrm{vec}(U_i |\overline{\alpha_k}\rangle \langle\overline{\alpha_k}|)\mathrm{vec}(U_i |\overline{\alpha_k}\rangle \langle\overline{\alpha_k}|)^*\right)}{d m_k^2} \\ &= \frac{U_i |\overline{\alpha_k}\rangle \langle\overline{\alpha_k}| U_j^*}{d m_k^2} \end{aligned}$$

For Bob to be able to distinguish between the states perfectly then the following condi-

tion must be satisfied,

$$\langle\overline{\alpha_k}|U_j^* U_i|\overline{\alpha_k}\rangle = 0\,, \tag{3.2.3}$$

whenever $i \neq j$.

In other words the algebraic relations of Equation (3.2.1) are satisfied with $|\phi_k\rangle = |\overline{\alpha_k}\rangle$ for all k. Suppose Equation (3.2.3) of condition holds and Alice's positive operator value measure is $\sum_k m_k \left|\phi_k\right\rangle \left\langle\phi_k\right|$ then Bob's measurement outcome gives

$$B_k = \frac{U_i \left|\overline{\alpha_k}\right\rangle \left\langle\overline{\alpha_k}\right| U_j^*}{d m_k^2}\,.$$

Hence Bob will be able to distinguish between the states $|\phi_k\rangle$ perfectly by one-way LOCC.

When condition (2) holds we can define a partial isometry $W^* : \mathbb{C}^d \longrightarrow \mathbb{C}^r$ as the sum of outer products

$$W = \sum_{k=1}^{r} \sqrt{m_k}\left|\phi_k\right\rangle \left\langle k-1\right|\,.$$

Let us verify that $WW^* = I_d$. Consider

$$\begin{aligned} WW^* &= \sum_{k=1}^{r}\sum_{k'=1} \sqrt{m_k m_{k'}}\,|\phi_k\rangle\,\langle k-1|\,\big|k'-1\big\rangle\,\langle\phi_{k'}| \\ &= \sum_{k=1}^{r} m_k\,|\phi_k\rangle\,\langle k-1|\,|k-1\rangle\,\langle\phi_k| \quad \text{for } k=k' \\ &= \sum_{k=1}^{r} m_k\,|\phi_k\rangle\,\langle\phi_k| \\ \therefore WW^* &= I_d \end{aligned}$$

Moreover, for all $1 \leq k \leq r$, the kth diagonal entry satisfies:

$$\begin{aligned} \langle k-1|\,W^*U_j^*U_iW\,|k-1\rangle &= \sum_{k_1=1}^{r}\sum_{k_2=1}^{r} \sqrt{m_{k_1}m_{k_2}}\,\langle k-1|\,|k_1-1\rangle\,\langle\phi_{k_1}|\,U_j^*U_i\,|\phi_{k_2}\rangle\,\langle k_2-1|\,|k-1\rangle \\ &= m_k\,\langle\phi_{k-1}|\,U_j^*U_i\,|\phi_{k-1}\rangle \end{aligned}$$

for $k_1 = k_2 = k-1$. Therefore

$$\langle k-1|\,W^*U_j^*U_iW\,|k-1\rangle = 0 \tag{3.2.4}$$

wherever $i \neq j$.

Hence from Equation (3.2.4) the matrix $W^*U_j^*U_iW$ has all the diagonal elements equal to zero whenever $i \neq j$.

Conversly, given a matrix representation of a partial isometry $W : \mathbb{C}^r \longrightarrow \mathbb{C}^d$ with diagonal entries satisfying condition (3), we can use the corresponding outer product representation to define $\{\phi_k\}$ that satisfy condition (2). □

The standard nested measurement classes of the above schematics for LO, LOCC-1 and LOCC is as follows

$$\text{LO} \subset \text{LOCC} - 1 \subset \text{ LOCC}.$$

Note that there are examples of states that can be distinguished by full LOCC but cannot be distinguished by a one-way LOCC.

Example 3.2.1. *From [1], the basis of a nine pure product state also known as the 'Domino states' in* $\mathbb{C}^3 \otimes \mathbb{C}^3$ *cannot be distinguished using one-way LOCC. A subset of seven of these nine states can be distinguished using full LOCC.*

Example 3.2.2. *Consider the following states,*

$$\begin{aligned} |\psi_1\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |\psi_2\rangle &= |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ |\psi_3\rangle &= |1\rangle \otimes |0\rangle \\ |\psi_4\rangle &= |1\rangle \otimes |1\rangle \ . \end{aligned}$$

Can these states be distinguished perfectly by only local operations without any classical communication?

We observe that the states above can be distinguished perfectly by one-way LOCC. That is, if Alice measures a state $|0\rangle$ *or* $|1\rangle$*, Bob is left with the states* $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), |0\rangle$ *or* $|1\rangle$*. If Bob measurement outcome is* $|0\rangle$*, then Bob is left to distin-*

guish perfectly between the states $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$, *and* $|0\rangle$. *We see clearly that these states are not orthogonal to each other. Thus without any form of classical communication allowed between Alice and Bob, Bob is stuck and will not be able to distinguish between his set of states perfectly by his local operations. Therefore the states above cannot be distinguished perfectly by only local operations (LO).*

Chapter 4

Operator and matrix theory techniques applied to one-way LOCC

In this chapter, we establish new results for distinguishing states perfectly under one-way LOCC and under arbitrary quantum operations. We discuss related operator structures such us operator systems, operator algebras and Hilbert C^*-modules. We finally establish the connection between these structures and one-way LOCC. The contents of this chapter are based on the paper [13].

4.1 Perfect distinguishability under one-way LOCC vs arbitrary operations

Perfect distinguishability by one-way local operations and classical communication (LOCC-1) for a general class of states is a much more stronger condition than perfect distinguishability using arbitrary operations. Recall that arbitrary pure states

can be perfectly distinguished if and only if the states are orthonormal to each other. It follows specifically that a collection of states $\{(I \otimes M_i)\,|\psi_0\rangle\}_i$ is distinguished under arbitrary operations if and only if

$$\mathrm{Tr}\left(M_j^* M_i\right) = 0$$

whenever $i \neq j$.

In this section, we show the theoretic implication for one-way LOCC and arbitrary quantum operations. We establish that perfect distinguishability under arbitrary quantum operations is equivalent to perfect distinguishability under one-way LOCC for certain classes of pure states.

An example of set of states which are perfectly distinguished by arbitrary quantum operations but not with one-way LOCC is the set of three orthogonal states given in [18, 1]. These states are of the form $\{(I \otimes M_i)\,|\psi_0\rangle\}_i$ where all of the M_i are generalized permutation matrices. Generalized permutation matrices are matrices which have exactly one non-zero entry in every row and every column.

Example 4.1.1. *The* 3×3 *matrices* $P_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ $P_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $P_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ *are permutation matrices.*

We observe that each row and column contains exactly one non-zero element. That is the 3×3 *permutation matrices above is row equivalent to the* 3×3 *identity matrix. Also*

$$P_1 P_2 = P_1 P_3 = P_2 P_3 = 0\,,$$

implies P_1, P_2 *and* P_3 *are orthogonal .*

For the example mentioned in [18], we see that permutation matrices contain two parameters. There are some allowed choices of parameters. The first makes all but one of the nonzero entries of the three matrices one and the other two into permutation matrices. The second differ from a permutation matrix in only one entry. This raises the question of whether there is an example of states that can be distinguishable reliably by arbitrary quantum operations but not by one-way LOCC, where all the $\{M_i\}$ are permutation matrices. Our next proposition shows this possibility.

Let $\triangle$ be the map which zeros out all the off diagonal entries of a square matrix but leaves its diagonal entries the same. Thus, as a map, there is a basis $\{|k\rangle\}$ such that $\triangle(\rho) = \sum_k |k\rangle \langle k| \rho |k\rangle \langle k|$ is the von Neumann measurement map defined on the basis. Next, we recall the definition of a Latin square and the theory of the pigeonhole principle.

Definition 4.1.1 (Latin square)**.** *The* $d \times d$ *matrix* $\mathcal{L}$ *with entries* $\{1, 2, \cdots, d\}$ *is a Latin square if it satisfies the property that no two entries in any fixed row or column are the same.*

Pigeonhole Principle: If n items are put in m boxes with $n > m$, then at least one of

the boxes must contain more than one item.

We will see the relevance of the Pigeonhole principle in the proposition that follows.

Proposition 4.1.1. *Let $\{P_k\}_{k=1}^n$ be a set of $d \times d$ permutation matrices and let $\mathcal{S} = \{(I \otimes P_i)\,|\psi_0\rangle\}_i$ where $|\psi_0\rangle$ is the standard maximally entangled state. Then the following are equivalent*

1. The states in $\mathcal{S}$ are perfectly distinguishable by one-way LOCC.

2. The states in $\mathcal{S}$ are perfectly distinguishable by arbitrary operations.

3. $\triangle(P_j^* P_i) = 0$ whenever $i \neq j$.

Moreover, if these conditions hold and $n = d$, then there exists a $d \times d$ Latin square $\mathcal{L}$ with the property that $\forall i, j, k \in \{1, 2, \cdots, d\}$ the (i, j) entry of P_k is one if and only if the (i, j) entry of $\mathcal{L}$ is k.

Proof. (1) $\implies$ (2) is evidently by virtue of the type of operations used, but we can also see this through the equations by choosing a W from Proposition 3.2.1 and observing

$$\mathrm{Tr}\left(P_j^* P_i\right) = \mathrm{Tr}\left(P_j^* P_i W W^*\right) = \mathrm{Tr}\left(W^* P_j^* P_i W\right) = 0$$

for all $i \neq j$.

To see (2) $\implies$ (3), we note that for all $i \neq j$, if $\mathrm{Tr}(P_j^* P_i) = 0$, then $\triangle(P_j^* P_i) = 0$ as well since the $P_j^* P_i$ are permutation matrices.

For (3) $\implies$ (1), let us simply take $r = d$ and W to be the identity. We see that Proposition 3.2.1 is satisfied.

Finally, suppose these equivalent conditions hold and that $n = d$. If both P_i and P_j have a one in their (k, l) entry, then $P_j^* P_i$ would have its (l, l) entry strictly positive, which would contradict $\mathrm{Tr}(P_j^* P_i) = 0$. Thus we can let $\mathcal{L}$ be the $d \times d$ matrix whose (i, j) entry is one: $\mathcal{L} = \sum_{k=1}^{d} kP_k$, which is evidently a Latin square.

□

Next, we introduce the concept of the simultaneous Schmidt decomposition. Consider the bipartite composite system $\mathcal{H}_A \otimes \mathcal{H}_B \simeq \mathbb{C}^d \otimes \mathbb{C}^d$.

Definition 4.1.2 (Simultaneous Schmidt Decomposition)**.** *We say the set* $\{(I \otimes M_k) |\psi_0\rangle\}_{k=1}^{n}$ *have a simultaneous Schmidt decomposition if there exists unitary matrices* U *and* V *and a complex* n *diagonal matrix such that*

$$M_k = U D_k V \, .$$

Observe that because we are not imposing any requirement that the diagonal entries of D_k be nonnegative, we see from [12] that the decompositions are not Schmidt decompositions but instead are called the "Weak Schmidt Decomposition". It was noted in [10] that the generalized Bell states, possessing a simultaneous Schmidt decomposition is a sufficient condition for distinguishing states reliably by LOCC.

Next, we generalize and strengthen their results by showing that for any set of states which have simultaneous Schmidt decomposition, distinguishability by arbitrary

quantum operations is equivalent to distinguishability by one-way LOCC.

Proposition 4.1.2. *Let* $\mathcal{S} = \{(I \otimes M_k)\,|\psi_0\rangle\}_{k=1}^{n} \in \mathbb{C}^d \otimes \mathbb{C}^d$ *have a simultaneous Schmidt decomposition. Then the following statements are equivalent.*

1. *The states in* $\mathcal{S}$ *are perfectly distinguishable by one-way LOCC.*

2. *The states in* $\mathcal{S}$ *are perfectly distinguishable by arbitrary operations.*

3. *There exists a* $d \times d$ *unitary matrix* A *such that*

$$\triangle\left(A^* M_j^* M_i A\right) = 0$$

whenever $i \neq j$.

Proof. The proof of (1) $\implies$ (2) is straightforward as above, and (3) $\implies$ (1) follows from Proposition 3.2.1.

For (2) $\implies$ (3), suppose (2) holds, thus $\mathrm{Tr}(M_j^* M_i) = 0$ whenever $i \neq j$. Let U and V be unitary matrices and diagonal matrix D_k such that $M_k = U D_k V$ for all k. Then $V M_j^* M_i V^*$ is diagonal for all i, j. Let F be a $d \times d$ Fourier matrix. Then $F^* V M_j^* M_i V^* F$ is a trace zero circulant matrix when $i \neq j$. Hence condition (3) is satisfied for a choice of $A = V^* F$ (In fact we can let $A = V^* F D$ for any diagonal unitary matrix D, so the solution is far from unique). □

Consider the following physically motivated class of examples to which this result applies. Let us recall the relation between commuting operators and operators that possesses simultaneous Schmidt decompositions.

Lemma 4.1.1. *Let $\{A_i\}_{i=1}^n$ be normal operators. The matrices A_i commute if and only if the operators A_i have simultaneous Schmidt decomposition.*

This implies that the result for the class of permutation matrices in Proposition 4.1.1 is equivalent to Proposition 4.1.2 if all the P_i's are normal and commute with each other.

Definition 4.1.3. *Let $\mathcal{H} = \mathbb{C}^d$ be a d-dimensional complex Hilbert space with orthonormal basis $\{|k\rangle\}_{k=0}^{d-1}$. Let $\omega = e^{\frac{2\pi i}{d}}$. We define two unitary operators X and Z on $\mathcal{H}$ as follows: $X|k\rangle = |k+1(mod\, d)\rangle$ and $Z|k\rangle = \omega|k\rangle$. Then the Generalized Pauli operators are the set $\{X^a Z^b\}_{a,b=0}^{d-1}$.*

The sets $\{X^k\}_{k=0}^{d-1}$ and $\{Z^k\}_{k=0}^{d-1}$ are both Abelian groups. It is easy to see they satisfy the hypothesis and the second equivalent condition of Proposition 4.1.2(with these operators playing the role of operators in M_i); hence they satisfy all the equivalent conditions of the proposition. A more general result along these lines can be found in [10].

We next prove one more result of this type, giving an alternate proof of a known result. We first need the following result of Fillmore [7].

Lemma 4.1.2. *Let M be any trace zero matrix, then there exists a unitary matrix V such that*

$$\triangle(V^*MV) = 0\,.$$

We can use the lemma to prove our result for pairs of states arising from two matrices (which need not be unitary). For clarity we simply refer to the operators that

define the corresponding states in the matrix form. We quickly recall the definition of a co-isometry. An element ϕ in a unital C^*-algebra $\mathcal{A}$ is said to be a ***co-isometry*** if $\phi\phi^* = 1$.

Proposition 4.1.3. *Let M_1 and M_2 be two $d \times d$ complex matrices. The following are equivalent.*

1. *There exists a $d \times d$ unitary matrix V such that $\triangle(V^* M_2^* M_1 V) = 0$.*

2. *There exists an integer $r \geq d$, and a co-isometry $W : \mathbb{C}^r \mapsto \mathbb{C}^d$ such that*

$$\triangle(W^* M_2^* M_1 W) = 0$$

   whenever $i \neq j$.

3. *$Tr(M_2^* M_1) = 0$.*

Thus we have recovered the remarkable result of Walgate, et al. [23], that any two orthogonal pure states can be distinguished by one-way LOCC. We note that (3) no longer implies either (1) or (2) when the number of general unitary matrices increases. This does not hold for a specific set of three generalized permutation matrices given in [18].

Next, we discuss the connection between operator algebras, operator systems and separating vectors with one-way LOCC.

4.2 Implications of one-way LOCC in operator systems, operator algebras and separating vectors

In the context of one-way LOCC, we are interested in operator systems, operator algebras and separating vectors that arise naturally through equations of Proposition 3.2.1. We exhibit a connection between perfect distinguishability with one-way LOCC and separating vectors of operator algebras and operator systems.

The next remark makes use Section 2.5. Before we state the following remark, let us recall that $\mathfrak{C}$ is a C^*-subalgebra of the algebra $\mathcal{A}$.

Remark 4.2.1. *Suppose $|\psi\rangle$ is a separating vector of $\mathfrak{C}$ and that $\mathfrak{C}$ is an algebra. Then a simple dimension bound may be obtained as a consequence of this result on the size of $\mathfrak{C}$ by observing that $A \mapsto A|\psi\rangle$ is an injective linear map from $\mathfrak{C}$ to $\mathcal{H}$, and hence $dim(\mathfrak{C}) \leq dim(\mathcal{H})$. This in particular applies to operator systems defined by families of one-way LOCC unitaries, as noted in Corollary 4.2.1 below.*

Recall from Section 2.5 that any C^*-subalgebra of such an operator system must has a separating vector. Let $\triangle$ be the map which zeros out all the off diagonals and leaves the main diagonal unchanged.

Theorem 4.2.1. *Let $W : \mathbb{C}^r \mapsto \mathbb{C}^d$ be an operator and let $\triangle$ be the diagonal map on $\mathbb{C}^r$ in a fixed basis $|\psi\rangle = \{|\psi_1\rangle, \cdots, |\psi_k\rangle\}$. Consider the operator system $\mathfrak{C}$ on $\mathbb{C}^d$ defined as the set of all operators X which satisfy:*

$$\triangle(W^*XW) = \frac{Tr(X)}{d} \triangle(W^*W) \ . \tag{4.2.1}$$

If $\mathfrak{A}$ is a C^*-subalgebra of $\mathfrak{C}$, then $\mathfrak{A}$ has a separating vector.

Proof. There exists $k : 1 \leq k \leq r$ such that the (k,k) entry of $\triangle(W^*W)$ is a strictly positive real number. Let us call the number c. Let $|\psi\rangle$ be the k-th column of W, then

$$\|A|\psi\rangle\|^2 = \langle k| W^*A^*AW |k\rangle = \frac{c}{d} tr(A^*A) \neq 0$$

when A (and hence A^*A) is a nonzero element of $\mathfrak{A}$. It follows that $|\psi\rangle$ is a separating vector for $\mathfrak{A}$. □

It is well known in the context of LOCC that no more than d maximally entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$ can be distinguished perfectly with LOCC. In the case of such a maximal set, we state a corollary to the above result.

Corollary 4.2.1. *Let $\mathcal{S} = \{|\psi_i\rangle = (I \otimes U_i)|\psi_0\rangle\}_{i=1}^d \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$ be the set of d orthogonal maximally entangled states which are perfectly distinguishable with one-way LOCC, and let $\mathfrak{C}$ be the operator system spanned by the set $\{U_j^*U_i\}$. Then $\mathfrak{C}$ has a separating vector if and only if $dim\mathfrak{C} = d$, and in this case $\mathfrak{C}$ forms a C^*-algebra.*

Before we proof the above, let us recall the Cayley-Hamilton Theorem: It states that every square matrix over the complex field (any commutative ring) satisfies it own characteristic equation.

Now we prove Corollary 4.2.1.

Proof. Since the states $|\psi_i\rangle$ are mutually orthogonal, the matrices $\{U_i\}$ are linearly independent and hence $dim\mathfrak{C} \geq d$. If dim $\mathfrak{C} > d$, then by Remark 4.2.1, $\mathfrak{C}$ does not have

a separating vector.

Also, if we assume that $\dim\mathfrak{C} = d$ then $\mathfrak{C} = \text{span}\{U_k\}$ and $U_j^* U_i \in \text{span}\{U_k\}$ for all i, j. By the Cayley- Hamilton theorem, we can find a complex polynomial $p_i(z)$ such that $U_i = p_i(U_i^*)$ for all i. Applying these facts and the invertibility of each U_i, it follows that $U_i U_j = p_i(U_i^*)U_j \in \mathfrak{C}$ for each pair i, j. Therefore, $\mathfrak{C}$ is a C^*-algebra. Since the $|\psi_i\rangle$ are distinguishable with one-way LOCC, there exists an isometry W such that Equation (4.2.1) hold for all $X \in \{U_j^* U_i\}$ and thus for all $X \in \mathfrak{C}$. Hence $\mathfrak{C}$ is a separating vector by Theorem 4.2.1. □

Note that this corollary does not actually require the $|\psi_i\rangle$ to be maximally entangled; it is sufficient for each of the U_i to be invertible. Also, we note that there are cases in which a set of d maximally entangled states can be distinguished with one-way LOCC but $dim\mathfrak{C} > d$. For instance, using the generalized Pauli matrices, if we look at the set $\mathcal{S} = \{U_i\}_{i=1}^d$ with $U_i = X^i$ for $1 \leq i \leq d-1$ and $U_d = Z$. If $|\phi\rangle$ is standard basis vector, then $\langle\phi| X^i Z |\phi\rangle = \langle\phi| X^i |\phi\rangle = 0$, if $i \neq 0$, implying that these states are LOCC-distinguishable. However, if $d > 2$ then $\mathfrak{C} = \text{span}\{U_j^* U_i\}$ has dimension $2d-1$, which implies that it does not have a separating vector.

We can also state the partial converse of Theorem 4.2.1. Firstly, recall that a set of quantum states $\{|\psi_i\rangle\}$ is **unambiguously distinguishable** if and only if they are linearly independent. A set of code words $\{X_i\}$ is unambiguously distinguishable if there exists a protocol with $(n+1)$ outcomes $\{Y_i\}$ such that for each $i \leq n$, the outcome Y_i occurs with positive probability and implies that X_i was sent. The outcome Y_{n+1} is

the error probability and provides no conclusive information about the identity of X_i. Also, a sufficient condition for unambiguously discrimination with one-way LOCC is the existence of the vector such that $\{M_k |\phi\rangle\}$ are linearly independent. This give us the following theorem.

Theorem 4.2.2. *Let $\mathfrak{C}$ be an operator in $\mathbb{C}^d$ spanned by the pairwise products $\{M_j^* M_i\}$, $i, j \in \{1, 2, \cdots, n\}$. If $\mathfrak{C}$ has a separating vector, then the bipartite states $\mathcal{S} = \{|\psi_i\rangle = (I \otimes M_i) |\psi_0\rangle\} \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$ can be unambiguously distinguished using one-way LOCC.*

Proof. If $\mathfrak{C}$ has a separating vector $|\phi\rangle$, then for any j, $\{M_j^* M_i |\phi\rangle\}_{i=1}^n$ is linearly independent which means that $\{M_i |\phi\rangle\}$ are linearly independent. If Alice performs a measurement and gets the outcome $|\overline{\phi}\rangle \langle\overline{\phi}|$, then Bob's system will be in the state $M_i |\phi\rangle$ for some i. Since the options are linearly independent, Bob can unambiguously distinguish them.

□

4.3 Hilbert module structure from LOCC

In this section, we discuss the Hilbert C^*-module structure which arises as a special case of our analysis of local operations and classical communication. In the case of one-way LOCC for which the states is to be distinguished is equal to the dimension d of the qudit base system; In other words the isometry W is unitary map or equivalently $r = d$ in the notion of Proposition 3.2.1. Though a unitary change of basis induced by W acting on the basis that defines the operation $\triangle$, we may assume $W = I$.

Let $\mathcal{A}$ be a C^*-algebra of operators on $\mathbb{C}^d$ with diagonal matrix representations in the basis that defines $\triangle$. Then $\mathfrak{C}$ defined above as the span of the operators $U_j^* U_i$ is a right (or left) $\mathcal{A}$-module. Let us define the map $\langle \cdot | \cdot \rangle : \mathfrak{C} \otimes \mathfrak{C} \mapsto \mathcal{A}$ such that

$$\langle X | Y \rangle = \triangle \left(Y^* X \right) .$$

One can check that this endows $\mathfrak{C}$ with the structure of the Hilbert $\mathcal{A}$-module, for which the unitary operators U_i form an orthogonal basis in this $\mathcal{A}$-valued inner product.

Given the elements $U, V \in \mathfrak{C}$, we say that $U \sim V$ if there exists an invertible diagonal matrix D such that $U = VD$. This is immediately seen to be an equaivalence relation, one which respects orthogonality.

Lemma 4.3.1. *Using the inner product defined above, the orthogonal complement is invariant under this equivalence relation: If $U \sim V$, then $\langle U | X \rangle = 0$ if and only if $\langle V | X \rangle = 0$.*

Proof. Consider the following calculation:

$$\langle U | X \rangle = \triangle(X^* U) = \triangle(X^* V D) = \triangle(X^* V) D = \langle V | X \rangle D \, ,$$

from which the proof follows. □

This implies that any orthogonal set with respect to $\langle \cdot | \cdot \rangle$ can contain at most one representative of each equivalence class, putting a significant bound on the size of any orthogonal set. In particular, we immediately recover the standard bound on the number

of LOCC-distinguishable maximally entangled states.

Proposition 4.3.1. *Let $\{U_k\}_{k=1}^n$ be a set of $d \times d$ unitary matrices which are mutually orthogonal under the inner product $\langle \cdot | \cdot \rangle$. Then $n \leq d$.*

Proof. If $\langle U_i | U_j \rangle = 0$, then $\mathrm{Tr}\left(U_j^* U_i\right) = \mathrm{Tr}\left(\triangle(U_j^* U_i)\right) = 0$. That is: Orthogonality under $\langle \cdot | \cdot \rangle$ implies orthogonality under Hilbert-Schmidt inner product. Let $\{D_1, D_2, \cdots, D_d\}$ be the set of diagonal unitary matrices with $\mathrm{Tr}\left(D_j^* D_i\right) = d\delta_{i,j}$. We look at the set $\mathcal{B} = \{U_k D_i\}$ for $k \in \{1, 2, \cdots, n\}$ and $i \in \{1, 2, \cdots, d\}$. From the Lemma 4.3.1,

$$\langle U_k D_i | U_l D_j \rangle = \langle U_k | U_l \rangle = 0$$

if $k \neq l$, which means that

$$\mathrm{Tr}\left((U_l D_j)^* U_k D_i\right) = 0\,.$$

Also,

$$\mathrm{Tr}\left((U_k D_j)^* U_k D_i\right) = \mathrm{Tr}\left(D_j^* D_i\right) = d\delta_{i,j}.$$

This implies that $\mathcal{B}$ is a set of nd matrices which are orthogonal in the Hilbert-Schmidt inner product, giving us $|\mathcal{B}| = nd \leq d^2$ and $n \leq d$. □

We can generalize this to a stronger statement which appears not to be as well known. Here we define

$$\langle X | Y \rangle_W = \triangle\left(W^* Y^* X W\right)$$

for any $r \times d$ matrix W with $r \geq d$. We say that a set of vectors in $\mathbb{C}^d$ is generic if any

d of them are linearly independent.

Proposition 4.3.2. *Let $\{M_k\}_{k=1}^n$ be a set of $d \times d$ matrices which are mutually orthogonal under the inner product $\langle\cdot|\cdot\rangle_W$. If for each M_k, we have rank $\{M_k\} = r_k$, then*

$$\sum_k r_k \leq d^2$$

as long as the columns of W are generic.

Proof. We first note that since each $r_k \leq d$, we have $\sum_k r_k \leq dn \leq d^2$ as long as $n \leq d$. So we need only to consider the case when $n > d$. As before, orthogonality under $\langle\cdot|\cdot\rangle_W$ implies the set $\{M_k W\}$ is mutually orthogonal in the Hilbert-Schmidt inner product. For each k, if

$$(W^* M_k^* M_k W)_{ii} = 0$$

then $W_i \in \ker(M_k)$. Since the columns of W are generic, the number of zeros is bounded by the dimension of the kernel of M_k. Hence, the matrix $\triangle\,(W^* M_k^* M_k W)$ has at least $r - (d - r_k)$ non-zero entries.

Define Q_k be the diagonal matrix such that

$$(Q_k)_{i,i} = \begin{cases} \frac{1}{\sqrt{(W^* M_k^* M_k W)_{i,i}}} & \text{if} \quad (W^* M_k^* M_k W)_{i,i} \neq 0 \\ 0 & \text{if} \quad (W^* M_k^* M_k W)_{i,i} = 0 \end{cases}$$

This means that all the diagonal elements of $Q_k^* M_k^* M_k Q_k$ are either zero or one. We

can then find a set of $r - d + r_k$ diagonal matrices $\{D_{ki}\}$ such that

$$\text{Tr } \left(D_{kj}^*(Q_k^* W^* M_k^* M_k W Q_k) D_{ki}\right) = \delta_{i,j} \text{Tr}\left(Q_k^* W^* M_k^* M_k W Q_k\right) .$$

These are orthogonal to each other and hence must be linearly independent.

This implies that $\mathcal{B} = \{M_k W Q_k D_{k,j}\}$ is a set of

$$n(r-d) + \sum_k r_k$$

matrices which are orthogonal in the Hilbert-Schmidt norm on $r \times d$ matrices, giving us

$$|\mathcal{B}| = n(r-d) + \sum_k r_k \leq rd$$

and

$$\sum_k r_k \leq (d-r)n + rd = d^2 + (r-d)(d-n) \leq d^2$$

since $n > d$ and $r \geq d$, and this completes the proof.

□

Chapter 5

Conclusion

We discussed the fundamentals and representation theory of finite dimensional C^*-algebras. We saw the physical description and schemes of quantum local operations and classical communication(LOCC) between two different parties. We considered some early significant results of LOCC which acted as a motivation for most of our new results we established. We noticed that the set of LOCC operations on a bipartite system is notoriously difficult to characterize mathematically, and we sometimes restrict ourselves to one-way LOCC. We established the equivalence between one-way LOCC and arbitrary quantum operations for certain classes of matrices.

We discussed detailed analysis in quantum information of recently derived operator relations for one-way. This investigation was initially motivated by an attempt to better understand the mathematical foundation that underlies the operator relations that characterize one-way LOCC. We were amazed by the operator structures we found in the background; specifically, operator algebras, operator systems, and Hilbert C^*-

modules. In addition to this perspective some tools from matrix theory, were able to establish some new results of perfect distinguishability of quantum states under different communication schemes, and we discovered new derivation for some established results and dimension bounds in the field. The content of these new results are contained in the paper [13].

Bibliography

[1] Charles H Bennett, David P DiVincenzo, Christopher A Fuchs, Tal Mor, Eric Rains, Peter W Shor, John A Smolin, and William K Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070, 1999.

[2] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Communications in Mathematical Physics*, 328(1):303–326, 2014.

[3] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10(3):285–290, 1975.

[4] Kenneth R. Davidson. *C*-algebras by example*, volume 6. American Mathematical Soc., 1996.

[5] David P DiVincenzo, Debbie W Leung, and Barbara M Terhal. Quantum data hiding. *IEEE Transactions on Information Theory*, 48(3):580–598, 2002.

[6] Heng Fan. Distinguishability and indistinguishability by local operations and classical communication. *Physical Review Letters*, 92(17):177905, 2004.

[7] PA Fillmore. On similarity and the diagonal of a matrix. *American Mathematical Monthly*, pages 167–169, 1969.

[8] Sibasish Ghosh, Guruprasad Kar, Anirban Roy, Aditi Sen, and Ujjwal Sen. Distinguishability of bell states. *Physical review letters*, 87(27):277902, 2001.

[9] Daniel Gottesman and Hoi-Kwong Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457–475, 2003.

[10] Tohya Hiroshima and Masahito Hayashi. Finding a maximally correlated state: Simultaneous schmidt decomposition of bipartite pure states. *Physical Review A*, 70(3):030302, 2004.

[11] Alexander S Holevo. *Quantum systems, channels, information: a mathematical introduction*, volume 16. Walter de Gruyter, 2013.

[12] Bobo Hua, Shaoming Fei, Jürgen Jost, and Xianqing Li-Jost. Schmidt-correlated states, weak schmidt decomposition and generalized bell bases related to hadamard matrices. *Reports on Mathematical Physics*, 74(1):89–103, 2014.

[13] David W. Kribs, Comfort Mintah, Michael Nathanson, and Rajesh Pereira. Operator structures and quantum one-way LOCC conditions. *Submitted*, 2016.

[14] Ruskai Mary Beth. LOCC in operator algebra language. *Tufts University and IQC, Waterloo*, 2012.

[15] Serge Massar and Sandu Popescu. Optimal extraction of information from finite quantum ensembles. *Physical Review Letters*, 74(8):1259, 1995.

[16] William Matthews, Stephanie Wehner, and Andreas Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Communications in Mathematical Physics*, 291(3):813–843, 2009.

[17] Michael Nathanson. Distinguishing bipartitite orthogonal states using LOCC: Best and worst cases. *Journal of Mathematical Physics*, 46(6):062103, 2005.

[18] Michael Nathanson. Three maximally entangled states can require two-way local operations and classical communication for local discrimination. *Physical Review A*, 88(6):062316, 2013.

[19] Vern Paulsen. *Completely bounded maps and operator algebras*, volume 78. Cambridge University Press, 2002.

[20] Rajesh Pereira. Trace vectprs in matrix analysis. *PhD thesis, University of Toronto*, 2003.

[21] Asher Peres and William K Wootters. Optimal detection of quantum information. *Physical Review Letters*, 66(9):1119, 1991.

[22] Jonathan Walgate and Lucien Hardy. Nonlocality, asymmetry, and distinguishing bipartite states. *Physical Review Letters*, 89(14):147901, 2002.

[23] Jonathan Walgate, Anthony J Short, Lucien Hardy, and Vlatko Vedral. Local distinguishability of multipartite orthogonal quantum states. *Physical Review Letters*, 85(23):4972, 2000.