Entanglement Breaking Channels in Quantum Information

by
Katrina L. Olfert

A Thesis
presented to
The University of Guelph

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

Guelph, Ontario, Canada

ABSTRACT

ENTAGELMENT BREAKING CHANNELS IN QUANTUM INFORMATION

Katrina L. Olfert
University of Guelph

Advisors:
Dr. Rajesh Pereira
Dr. David Kribs

Quantum channels are central objects of study in quantum information, of which entanglement breaking channels are an interesting subset. Entanglement is considered a fundamental resource and property of quantum mechanics that we can use as a driving force for new theories and to continue research in this area. We exhibit the connection between stochastic matrix theory and the iterative behaviour of entanglement breaking channels and relate the Jordan forms of the entanglement breaking channels and stochastic matrices. We build on this perspective to study the fixed point theory for such channels. We further consider the nullspace structure of entanglement breaking channels, in particular proving that every operator space of trace zero matrices is the nullspace of such a channel. We connect the nullspace of entanglement breaking channels with private subspaces and present examples and discuss connections between quantum privacy and trace zero matrices. Finally, we draw a connection between random unitary channels and entanglement breaking channels.

Dedication

To my mum, grandpa, and Riley. Thank you for everything.

Acknowledgements

Firstly I would like to thank my advisors, Dr. David Kribs and Dr. Rajesh Pereira, thank you for giving me the opportunity to study quantum information. The patience, expertise and willingness to help you exhibited made abstract concepts seem accessible. I am extremely grateful for all the time and effort you both put into my education.

I would also like to thank my friends and office mates for being an excellent, encouraging group of people. I'll miss you!

Contents

Chapter 1

Introduction

The efforts to formalize quantum mechanics were highly influential on several branches of mathematics such as Functional Analysis and Operator Algebras. The mathematical background provides the rules and structure needed to begin to describe physical quantum systems. Although some of the mathematical background seems fairly elementary, as it is abstract it makes some essential facts seem obvious and allows a clearer picture of the underlying algebraic structure of quantum mechanics. This can make concepts and questions easier to understand and allow solutions to be more varied in their application. This thesis uses those mathematical formalisms to make statements specifically about entanglement breaking channels. Schrödinger and Einstein, Podolsky, and Rosen were the first people to mention entanglement in the 1930s, it was discovered in an attempt to paint a complete picture of quantum mechanics. Entanglement is considered a fundamental resource and property of quantum mechanics. A state of a composite system that cannot be written as a product of states of its component systems is an entangled state. Considering these states, we can use entanglement as a driving force for new theories and to continue research in this area. The non-classical nature of entanglement is a major part of why quantum systems behave how they do and what makes quantum mechanics interesting.

Entanglement is a key resource in quantum communication and computation. We measure capacity for communication by how much information can be sent through an error-prone channel using multiple independent transmissions. We know that the capacity of a classical channel is a unique scalar value whereas the capacity of a quantum channel cannot be defined by a single value [44]. The quantum capacity of a channel connects quantum entanglement and the transfer of quantum information. The applications of quantum capacity include quantum communication, quantum error correction and quantum computing-related research. A logical step when solving a large problem is to look at special cases. When considering how to completely understand entanglement from a communication point of view, we can look at when there is a quantum capacity of zero. The work [26] applied this strategy, and the results were a class of channel called entanglement breaking channels (EB channels). Their discovery by Holevo in [22], and the additional articles in [23] and [25] spurred more research on this topic in [26] where equivalences were discovered that broadened the area of study for EB channels and motivated this thesis. As entanglement is a key facet of quantum communication, we want to better understand operations on states where entanglement is destroyed.

In chapter 2 we will present the necessary mathematical background and introduce key definitions from quantum information. Chapter 3 will provide an in-depth introduction to entanglement breaking channels. Chapter 4 will demonstrate how to get a stochastic matrix from the Holevo form and describe the iterative behaviour of entanglement breaking channels and stochastic matrices. We will also study the fixed point theory for such channels and conduct an analysis of the fixed point theory for these maps. We will consider the nullspace structure of entanglement breaking channels and connect the nullspace of entanglement breaking channels with private subspaces, as well as drawing a connection with random unitary channels.

Chapter 2

Background and Preliminaries

2.1 Functional Analysis

We begin by introducing basic notions from functional analysis which will become the basis of the results in Chapter 4.

Definition 2.1.1 (Metric Space)**.** [10, 34] A metric space is a set X and a metric $d : X \times X \to \mathbb{R}$ on X that forms an ordered pair (X,d) with the following properties:

- $d(x, y) \geq 0$;
- $d(x, y) = 0$ if and only if $x = y$ for all $x, y \in X$;
- $d(x, y) = d(y, x)$ for all $x, y \in X$;
- $d(x, y) \leq d(x, z) + d(z, y)$ for all $x, y, z \in X$.

Maps that preserve the metric play an important role in quantum information.

Definition 2.1.2 (Isometry)**.** [4] For metric spaces X and Y a map $f : X \to Y$ is called an isometry if for all $a, b \in X$ we have

$$d_Y(f(a), f(b)) = d_X(a, b).$$

Isometries preserve the distance between elements. This allows us to "move" objects between metrics without changing how they relate to each other.

Definition 2.1.3 (Norm)**.** [18, 37] Let V be a vector space over $\mathbb{R}$ or $\mathbb{C}$. A function $||\cdot|| : V \to \mathbb{R}$ is called a norm if it has the following properties:

- $||v|| > 0$, if $v \neq 0$, and $||0|| = 0$;
- $||cv|| = |c| \cdot ||v||$ for any $v \in V$ and scalar c;
- $||v + w|| \leq ||v|| + ||w||$ for any $v, w \in V$.

Definition 2.1.4 (Complete)**.** [28, 2] A normed space is complete if every Cauchy sequence is convergent.

Definition 2.1.5 (Linear Functional)**.** [17, 39] A linear functional on a vector space V over F ($\mathbb{R}$ or $\mathbb{C}$) is a linear transformation from V into F.

Definition 2.1.6 (Dual Space)**.** [40] The dual space, V^*, is defined as the set of all bounded linear functionals from V into F. We also denote the space of bounded linear operators $\mathcal{L}(V, \mathbb{C})$.

Definition 2.1.7 (Banach Space)**.** [1, 15] A Banach space is a complete normed space.

Definition 2.1.8 (Inner Product Space)**.** An inner product space is a vector space V over the field F with an inner product $\langle \cdot, \cdot \rangle : V \times V \to F$, that satisfies the following properties:

- $\langle x, y \rangle = \overline{\langle y, x \rangle}$;

- $\langle ax, y\rangle = a\langle x, y\rangle$ and $\langle x+y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$;

- $\langle x, x\rangle > 0$, $x \in V\backslash\{0\}$.

Definition 2.1.9 (Hilbert Space)**.** [20, 47] A Hilbert Space, $\mathcal{H}$, is a complete inner product space which is endowed with the induced norm; $||x|| = \sqrt{\langle x, x\rangle}$ for $\mathcal{H}$.

We now introduced bra-ket notation. Suppose we have a inner product $\langle \psi, \phi\rangle$ which we will now denote as $\langle \psi|\phi\rangle$. The ket, $|\phi\rangle$, is a vector in some Hilbert space $\mathcal{H}$ and the bra, $\langle\psi|$, is a linear functional in the dual space $\mathcal{H}^*$. By the Riesz representation Theorem, the dual of a Hilbert space is isometric to the Hilbert space itself. Hilbert space extends some properties of Euclidean space from finite to infinite dimensions. We can now represent the states of a quantum system as unit vectors in the Hilbert space. A vector $\psi \in \mathcal{H}$ can be written as $|\psi\rangle$ while the linear functional on $\mathcal{H}$ it determines is denoted by $\langle\psi|$.

Definition 2.1.10 (Fixed Point)**.** [29] Let X be a set and $T : X \to X$, then $x \in X$ is said to be a fixed point if $Tx = x$.

Note that although x is a fixed point, it may not be unique.

Definition 2.1.11 (Attractive Fixed Point)**.** Let X be a set and $T : X \to X$. A fixed point of T, $x \in X$ is said to be attractive if there exists a neighbourhood N of x such that $\lim_{n\to\infty} T^n y = x$ for all $y \in N$.

Fixed points are not affected by the function T, they remain unchanged. There exists a special class of fixed points called attractive fixed points where for any value close enough to the fixed point x the iterated function converges to x [15]. Not all fixed points are attractive, they may be repulsive or neither attractive nor repulsive. Later in this chapter, we will introduce Brouwer's theorem which guarantees the existence of a fixed point for certain maps.

2.2 Matrix Theory

Definition 2.2.1 (Basis)**.** [15] A basis is a set of vectors in a vector space V that are linearly independent and that spans V.

A basis is used to determine the dimension of a vector space. Note that a vector space with no finite basis is infinite-dimensional.

We now discuss special types of matrices that are important to our results, denoting the set of complex $n \times n$ matrices M_n. Given a Hilbert space $\mathcal{H}$ we can let $\mathcal{L}(\mathcal{H})$ be the set of liner operators that act on $\mathcal{H}$. When $dim(\mathcal{H}) = n$, if we fix an orthonormal basis we can identify elements of $\mathcal{L}(\mathcal{H})$ with elements of M_n with corresponding matrix representations.

Definition 2.2.2 (Hermitian)**.** [19, 46] An $n \times n$ matrix A is Hermitian if

$$A = A^*,$$

where $A^* = \bar{A}^t$ is the conjugate transpose.

Definition 2.2.3 (Trace)**.** [49, 21] The trace of an $n \times n$ matrix, $A = (a_{ij})$ is the sum of its diagonal entries

$$Tr(A) = a_{11} + a_{22} + \ldots + a_{nn} = \sum_{i=1}^{n} a_{ii}.$$

We can show $\langle A, B \rangle = Tr(B^*A)$ is an inner product on the space of matrices. To prove the first property of inner product spaces

$$Tr(A^*A) = \sum_i \sum_j |a_{ij}|^2 \geq 0$$

and hence the only way the sum can equal zero is if each $a_{ij} = 0$. Now we show trace of a matrix is a linear map :

$$\begin{aligned} Tr(cA+B) &= \sum_{i=1}^{n}(ca_{ii}+b_{ii}) \\ &= c\sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} \\ &= c(Tr(A)) + Tr(B). \end{aligned}$$

Finally we prove the final property of inner product spaces:

$$\begin{aligned} \langle A, B\rangle &= Tr(B^*A) \\ &= \overline{Tr((B^*A)^*)} \\ &= \overline{Tr(A^*B)} \\ &= \overline{\langle B, A\rangle}. \end{aligned}$$

Definition 2.2.4 (Unitary Matrix)**.** [32, 21] An $n \times n$ matrix U is unitary if

$$U^*U = UU^* = I.$$

Here we have written I for the n-dimensional identity operator, also viewing it when necessary as the $n \times n$ identity matrix. Unitary matrices are always invertible and their inverse is also always unitary, this makes unitary matrices especially useful in transforming data. In fact, unitary operators are central to quantum information as they describe the time evolution of quantum systems.

Unitary operators are linear operators on complex vector spaces and are analogous to orthogonal operators in real vector spaces. A unitary operator on an inner product space is an isomorphism of the space onto itself. Unitary operators can act on a Hilbert space or between Hilbert spaces, they preserve the structure of the space they work in and the inner product thus preserving the topology.

Definition 2.2.5 (Positive Definite Matrix)**.** [15] An $n \times n$ Hermitian matrix A is positive if and only if

$$v^* A v > 0 ,$$

for all $v \in M_n \backslash \{0\}$.

Definition 2.2.6 (Positive Semidefinite)**.** [36] An $n \times n$ Hermitian matrix A is positive semidefinite if and only if

$$v^* A v \geq 0 ,$$

for all $v \in M_n$.

A positive semi-definite matrix will only have non-negative eigenvalues, this leads to some nice equivalences.

Definition 2.2.7 (Operator Norm)**.** [8] Any B, $A \in M_{mn}$ where M_{mn} is a set of $m \times n$ matrices, induces a linear operator from A to B, with respect to the standard basis. The corresponding operator norm on the space M_{mn} is

$$||M|| = \sup\{||Mx|| : x \in F^n \text{ with } ||x|| = 1\}.$$

Theorem 2.2.8. *For a Hermitian matrix A, the following are equivalent:*

- $v^* A v \geq 0$*, for all* $v \in \mathbb{C}$*;*
- *All eigenvalues of A are non-negative;*
- $A = M^* M$ *for some matrix* M*.*

Definition 2.2.9 (Probability Vector)**.** A probability vector is a vector (row or column) in which all elements are non-negative and all elements add up to one.

Definition 2.2.10 (Stochastic Matrix)**.** [45] A matrix A is column stochastic if it is a non-negative real square matrix where each column sums to 1.

The entries of a stochastic matrix are real numbers in the interval [0,1]. A stochastic matrix has the following properties as proved below:

- 1 is an eigenvalue of A;
- if λ is a ($\mathbb{R}$ or $\mathbb{C}$) eigenvalue of A then $|\lambda| \leq 1$.

It is easy to see that $\lambda = 1$ is an eigenvalue of A, now we will show the spectral radius of $A \leq 1$. Starting with λ,

$$|\lambda| = \frac{||xA||}{||x||} \leq max_{||x||=1}||xA|| = ||A||.$$

Since we have a column stochastic matrix we know $||A||_1 = 1$ and therefore $|\lambda| \leq 1$.

Example 2.2.1. Suppose we have a stochastic matrix

$$M = \begin{pmatrix} .3 & .5 & .2 \\ .3 & .4 & .3 \\ .4 & .1 & .5 \end{pmatrix}.$$

It is clear all entries of the matrix are real, the matrix is square and each column sums to one. If we were to solve for the eigenvalues we would get $\lambda = 1$ and $\lambda = \frac{1}{10}$ with multiplicity of two.

Now consider a general stochastic matrix

$$M = \begin{pmatrix} M_{1,1} & M_{1,2} & \dots & M_{1,n} \\ M_{2,1} & M_{2,2} & \dots & M_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ M_{n,1} & M_{n,2} & \dots & M_{n,n} \end{pmatrix}.$$

M_{ji} represents the probability of moving from j to i in one time step; since we are dealing with probabilities, the sum of each column must equal one. The probability of going from j to i in k steps is the probability M^k_{ji}.

Example 2.2.2. Let us start with the stochastic matrix from example 2.2.1.,

$$M = \begin{pmatrix} .3 & .5 & .2 \\ .3 & .4 & .3 \\ .4 & .1 & .5 \end{pmatrix}.$$

Let each M_{ji} represent the probability of a soccer player passing the ball from player j to player i. $M_{1,1} = .3$ means there is a 30% chance player 1 will keep the ball whereas $M_{2,1} = .3$ means there is a 30% chance player 1 will pass to player 2, $M_{3,2} = .1$ means there is a 10% chance player 2 will pass to player 3 etc.

Theorem 2.2.11 (Brouwer's Fixed Point Theorem)**.** *[6] For any continuous function f mapping a compact convex set K to itself there exists an $x \in K$ such that $f(x) = x$.*

We call x a fixed point, while Brouwer's theorem guarantees the existence of a fixed point it does not guarantee uniqueness of the fixed point.

Proposition 2.2.12. *Let S be a stochastic matrix. Then there exists a probability vector which is the fixed point of the mapping $x \to Sx$.*

Proof. We will show that every stochastic matrix has a fixed point by applying Brouwer's theorem. Stochastic matrices map probability vectors to probability vectors. We begin with the set of probability vectors, $P_n = \{\vec{p} = (p_1, p_2, ..., p_n)$ where $p_n \geq 0\ \forall n$ and $\sum_n p_n = 1\}$. To show the probability vectors are convex note that if $0 \leq \lambda \leq 1$ and $\vec{p}, \vec{q} \in P_n$, then $\lambda\vec{p} + (1-\lambda)\vec{q} = (\lambda p_1 + (1-\lambda)q_1, \ldots, \lambda p_n + (1-\lambda)q_n)$ is a probability vector as well. It is also clear that the set of probability vectors is compact since each p_n must be between 0 and 1 and therefore P_n is bounded and in finite dimensions bounded sets are compact. Now we show that a stochastic matrix maps probability vectors to probability vectors. Let $M = M_{ij}$ be stochastic matrices and let $\vec{p} = (p_1, p_2, \ldots, p_n) \in P_n$. Then the vector $M\vec{p}$ is a probability vector since:

$$\begin{aligned}
\sum_{i=1}^{n}\sum_{j=1}^{n} M_{ij}p_j &= \sum_{j=1}^{n}\left(\sum_{i=1}^{n} M_{ij}\right)p_j \\
&= \sum_{j=1}(1)p_j \\
&= 1.
\end{aligned}$$

From this we can conclude that because stochastic matrices map probability vectors to probability vectors, which are compact and convex, by Brouwer's Fixed Point Theorem every Stochastic matrix has a fixed point. However, we note that the fixed point is not necessarily an attractive fixed point. □

Definition 2.2.13 (Orthogonal Complement)**.** [16] If S is a subset of a Hilbert space $\mathcal{H}$ then the orthogonal complement of S is defined as

$$S^{\perp} = \{x \in \mathcal{H} : \langle x, s\rangle = 0,\ \forall s \in S\}.$$

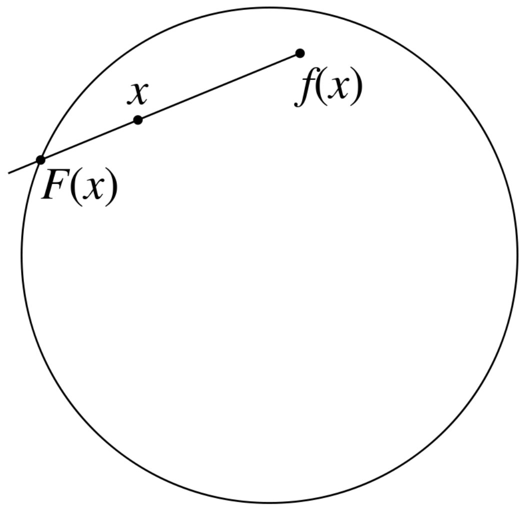


Figure 2.1: Visualization of application of Brouwer's theorem [3].

There are many useful properties of orthogonal complements such as

$$S \cap S^{\perp} = 0$$

and in finite dimensions

$$(S^{\perp})^{\perp} = S.$$

Definition 2.2.14 (Primitive Matrix)**.** [45] A non-negative square matrix P is primitive if there exists a k such that, where every element of P is non-negative. The smallest $k \in \mathbb{N}$ which accomplishes this is called the index of primitivity of k.

Theorem 2.2.15 (Perron-Frobenius)**.** *[35, 11] Let $F = (f_{ij})$ be an $n \times n$ primitive matrix. Then the following is true:*

- *There is a positive eigenvalue λ_{max} of F such that all other eigenvalues of F satisfy $|\lambda| < \lambda_{max}$;*

- *The eigenspace associated with λ_{max} is one-dimensional;*

- *The eigenvector v of F corresponding to the eigenvalue λ_{max} has all positive entries;*

- *Any non-negative eigenvector of F is a multiple of v.*

If our stochastic matrix is primitive then its fixed point is attractive. A stochastic matrix map has one eigenvalue $\lambda_{max} = 1$ while the rest of the eigenvalues are less than or equal to one. Additionally, since our matrix is primitive we know that all other λ are simply less that one. We have a dominant eigenvalue, therefore, using power iteration [5] we know our fixed point will be attractive.

Motivated by primitive non-negative matrices the concept of a primitive quantum channel has been developed in [42, 38].

Definition 2.2.16 (Steady State)**.** A steady state of a stochastic matrix F is an eigenvector v with eigenvalue 1 such that the entries are positive and sum to 1.

The steady-state is a vector that describes the eventual behaviour of a system when a long enough period of time has passed such that we have converged to the fixed point.

2.3 Operator Algebras and Completely Positive Maps

Definition 2.3.1 (Projection)**.** [15, 24] A projection P on a Hilbert space $\mathcal{H}$, is a Hermitian operator P such that $P^2 = P$.

Projections are idempotent operators and they can be used to describe the direct sum decomposition of a space V. The direct sum decomposition of a vector space V is $V = R \oplus N$ where R is the range of the projection and N is the null space of the projection. When our vector space V is a Hilbert space we can also consider how orthogonal projections behave on inner products: $\langle x, Py \rangle = \langle Px, y \rangle$.

Definition 2.3.2 (Banach Algebra)**.** A Banach algebra, $\mathcal{B}$, over some field ($\mathbb{R}$ or $\mathbb{C}$) is a Banach space that also has a multiplication operation such that

$$||xy|| \leq ||x||\,||y||,\ \forall x, y \in \mathcal{B}.$$

Definition 2.3.3 (Commutant)**.** [46] The Commutant of a subset $\mathcal{A}$ of operators or matrices where $\mathcal{A} \subseteq \mathcal{L}(\mathcal{H})$ is defined as $\mathcal{A}^{'} = \{T \in \mathcal{L}(\mathcal{H}) : TA = AT,\ \forall A \in \mathcal{A}\}$.

Definition 2.3.4 (C^{*}-algebra)**.** [12] A C^{*}-algebra, $\mathcal{C}$, is a Banach algebra over $\mathbb{C}$ with an operation $X \to X^{*}$ that satisfies the following properties:

- $(X^{*})^{*} = X$;
- $X^{*}Y^{*} = (YX)^{*}$;
- $(X^{*} + Y^{*}) = (X + Y)^{*}$;
- $(cX)^{*} = \bar{c}X^{*}$;
- $||X^{*}X|| = ||X||^{2}$;

for all $X, Y \in \mathcal{C}$ and $c \in \mathbb{C}$.

C^{*}-algebras are the building blocks of the formalisms of quantum mechanics. They were created to model the physical observables of quantum systems. Given a set of operators or matrices, we can also consider the following important algebra.

Definition 2.3.5 (Von Neumann Algebra)**.** [46] A Von Neumann Algebra $\mathcal{M}$ is a special type of C^{*}-subalgebra of $\mathcal{L}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$ with the additional property that

$$\mathcal{M} = \mathcal{M}^{''}.$$

Von Neumann algebras are important in quantum mechanics.

Definition 2.3.6 (Tensor Product)**.** A tensor product, also called a Kronecker product, is defined as

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nm}B \end{pmatrix},$$

where A and B are both matrices.

Tensor products describe composite quantum systems. From the example above A acts on an n dimensional vector space, B acts on an m dimensional vector space and $A \otimes B$ acts on an nm dimensional vector space.

Definition 2.3.7 (Positive Map)**.** A map $\Phi : \mathcal{A} \to \mathcal{B}$ between two $C^* - algebras$ $\mathcal{A}$ and $\mathcal{B}$ is positive if $a \geq 0$ implies $\Phi(a) \geq 0$, for $a \in \mathcal{A}$.

Definition 2.3.8 (n-Positive)**.** A map $\Phi : M_m \to M_p$ is n-positive if for all positive integers n $id_n \otimes \Phi$ is positive.

Definition 2.3.9 (Completely Positive Map)**.** The map Φ is completely positive if $id_k \otimes \Phi$ is a positive map for all k, where $id_k : M_k \to M_k$ is the identity map.

An example of a map that is positive but not completely positive is the transpose map, $T : X \to X^\top$. While it is obvious T maps positive semi-definite operators to semi-definite operators, we must show $(id_k \otimes T)$ does not. Let us give a counter example using bra-ket notation.

Example 2.3.1. Let us define an operator

$$\rho = \frac{1}{2}(|00\rangle + \langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|),$$

which we can rewrite as

$$\frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|).$$

Now we use it as input for our map $(id \otimes T)\rho$ and get

$$\begin{aligned}(id \otimes T)\rho &= \frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|) \\ &= \frac{1}{2}(|00\rangle + \langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|).\end{aligned}$$

If we were to calculate the eigenvalues for the resulting matrix we get $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2})$, thus making the transpose map positive but not completely positive.

As quantum channels are required to be completely positive, it is important to have a characterization of complete positivity for linear maps.

Theorem 2.3.10 (Choi's Theorem on Completely Positive Linear Maps)**.** *[7] Let $\Phi : M_n \to M_n$ be a linear map. The following are equivalent:*

- *Φ_n is n-positive;*
- *The matrix with operator entries*

$$C_\Phi = (id_n \otimes \Phi)(\sum_{ij} E_{ij} \otimes E_{ij}) = \sum_{ij} E_{ij} \otimes \Phi(E_{ij}) \in M_n,$$

  is positive, where $E_{ij} \in M_n$ is the matrix with 1 in the ij-th entry and 0 elsewhere;
- *Φ is completely positive.*

Definition 2.3.11 (Choi Matrix)**.** [7] The Choi matrix of a linear map $\Phi : M_n \to M_n$ is defined as $C_\Phi = \sum_{ij} E_{ij} \otimes \Phi(E_{ij})$, where E_{ij} is the matrix with 1 in the (i, j)th spot and 0's elsewhere.

Choi's theorem on completely positive linear maps is useful when proving positivity, while the Choi Matrix gives us the set of Kraus Operators as we will see below.

2.4 Quantum Information Theory

Now we can begin to describe quantum events and information using previously defined operations and theorems. Any quantum information or physical observable we wish to model or encrypt will be represented as qubits that have a probability distribution given by a quantum state which is represented as a vector or matrix.

Definition 2.4.1 (Qubit)**.** A qubit is a unit vector in $\mathbb{C}^2$.

A qubit is the standard basic unit of quantum information, where we have

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

We will use $\{|k\rangle\}_{k=0}^{n-1}$ to denote the standard basis of $\mathbb{C}^n$. Mathematically we represent a qubit that has not been measured, in the standard basis in $\mathbb{C}^2$ as

$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where $|\alpha|^2 + |\beta|^2 = 1$. After measurement in the standard basis the qubit collapses to either $|0\rangle$ with probability of $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$, $|0\rangle$ and $|1\rangle$ form an orthonormal basis. As $|\alpha|^2$ and $|\beta|^2$ are probabilities they sum to 1, this means the length is normalized to 1 and the state is a unit vector. We can combine qubits to form product basis states for example

$$|0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Definition 2.4.2 (Density Operator)**.** [24] A quantum state is described by a density operator ρ, which is defined by the following conditions:

- $\rho \geq 0$;
- $Tr(\rho) = 1$.

Density operators are one of many ways of describing quantum states. A density matrix ρ describes the probability distributions of qubit states. Suppose for instance $\rho = |\Phi\rangle\langle\Phi| \in M_2$ with $|\Phi\rangle$ defined as above, then we get

$$\rho = |\Phi\rangle\langle\Phi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \bar{\alpha} & \bar{\beta} \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\beta}\alpha & |\beta|^2 \end{pmatrix},$$

from there it is easy to see the condition $Tr(\rho) = |\alpha|^2 + |\beta|^2 = 1$.

Definition 2.4.3 (Trace Preserving Map)**.** A map $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$, where $\mathcal{H}$ is some Hilbert space, is trace preserving if $Tr(\Phi(\rho)) = Tr(\rho)\ \forall \rho$.

Definition 2.4.4 (Quantum Channel)**.** [26] A quantum channel Φ is a completely positive trace-preserving map.

Proposition 2.4.5. *Every quantum channel has at least one fixed point,* $\Phi(B) = B$.

Proof. Quantum channels are continuous and map density matrices to density matrices. The set of density matrices is compact and convex therefore by Brouwer's fixed point theorem every quantum channel has a fixed point. □

We can see that this result and the result in Proposition 2.2.12 are almost identical.

Definition 2.4.6 (Dual Map)**.** [24] For every positive trace preserving linear map Φ, the dual map Φ^* is defined by $Tr(\Phi(\rho)X) = Tr(\rho\Phi^*(X))$.

Φ and Φ^* both describe the evolution of quantum systems however Φ does so using quantum states and Φ^* does so in terms of observables.

Definition 2.4.7 (Positive Operator Valued Measure)**.** [33] $\{F_k\}$ is a POVM if it is a set of Hermitian positive semidefinite operators satisfying $\sum_k F_k = I$.

The measurement of quantum states is probabilistic, as each possible outcome has an associated probability of occurring. In quantum measurement we do not always care about the post-measurement state, instead, we are more interested in the probabilities of different outcomes. A set of F_k's can identify probabilities of the different measurement outcomes. Measurement of a state causes the superposition to collapse, POVMs define a probability $p_i = \langle\psi_i|F_i|\psi_i\rangle$ when measuring the state ψ_i, and so p_i is the probability the measurement outcome is F_i.

The following is a basic structural results on quantum channels that comes out of Choi's work.

Theorem 2.4.8. *Let Φ be a quantum channel on Hilbert space $\mathcal{H}$ with dimension equal to n. Then there are $n \times n$ matrices B_i mapping matrices B_i on $\mathcal{H}$ such that for any ρ, $\Phi(\rho) = \sum_i B_i\rho B_i^*$ and $\sum B_i^* B_i = I$.*

The matrices B_i are referred to as the Kraus operators of Φ. The full proof of this theorem is beyond the scope of this thesis but let us show that the last condition is equivalent to the map being trace preserving. In other words for some density matrix ρ, $\Phi(\rho) = \sum_i B_i\rho B_i^*$ is trace preserving if and only if $\sum B_i^* B_i = I$.

Proof. Suppose first that $\sum_i B_i^* B_i = I$ then for all ρ we have have our trace preserving quantum channel in operator-sum representation $\Phi(\rho) = \sum_{k=1}^n B_k \rho B_k^*$. Then

$$\begin{aligned}
Tr(\Phi(\rho)) &= Tr(\sum_{k=1}^n B_k \rho B_k^*) \\
&= \sum_{k=1}^n Tr(B_k \rho B_k^*) \\
&= \sum_{k=1}^n Tr(\rho B_k^* B_k) \\
&= Tr(\sum_{k=1}^n \rho B_k^* B_k) \\
&= Tr(\rho(\sum_{k=1}^n B_k^* B_k)) \\
&= Tr(\rho).
\end{aligned}$$

Now assuming $\Phi(\rho)$ is trace preserving we can reverse the previous argument.

$$\begin{aligned}
Tr(\rho) &= Tr(\Phi(\rho)) \\
&= Tr(\sum_{k=1}^n B_k \rho B_k^*) \\
&= Tr(\sum_{k=1}^n \rho B_k^* B_k) \\
&= Tr(\rho(\sum_{k=1}^n B_k^* B_k)),
\end{aligned}$$

the only way this is true for all ρ is if $\sum_{k=1}^n B_k^* B_k = I$. □

Definition 2.4.9 (vec Operator)**.** [48] A linear map $vec : \mathcal{L}(Y, X) \to X \otimes Y$ is defined by $vec(E_{i,j}) = |i\rangle \otimes |j\rangle$.

We denote the inverse vectorization operation as $vec^{-1} : \mathcal{H}_2 \otimes \mathcal{H}_1 \to \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$. The vec operator takes the columns of a matrix and stacks them as a single column vector, starting with the leftmost column of a matrix and continuing rightward. The inverse vec operation takes a vector and divides it into the columns of a matrix. Below we give an example for a 2×2 matrix.

Example 2.4.1. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$vec(A) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a \\ c \\ b \\ d \end{pmatrix}, \text{ and } vec^{-1}(\vec{a}) : \begin{pmatrix} a \\ c \\ b \\ d \end{pmatrix} \to \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Definition 2.4.10 (Partial Trace)**.** The partial trace, tr_B of a matrix, is the linear mapping from $\mathcal{H}_A \otimes \mathcal{H}_B$ to $\mathcal{H}_A$ such that,

$$tr_B(X \otimes Y) = Tr(Y)X,$$

where X is a matrix on $\mathcal{H}_A$ and Y is on $\mathcal{H}_B$.

Definition 2.4.11 (Separable map)**.** A completely positive linear map, Φ is said to be separable if it can be written in the form $\Phi(\rho) = \sum_{i=1}^{n}(A_i \otimes B_i)\rho(A_i \otimes B_i)^*$, for some operators A_i, B_i on $\mathcal{H}_A$ and $\mathcal{H}_B$.

Chapter 3

Entanglement Breaking Channels

An important class of channels are those that break all entanglement when acting on a composite system with the identity channel of the same size, $\Phi \otimes \mathrm{id}$. There are numerous equivalent characterizations of entanglement breaking channels, including a physically motivated description as the composition of so-called quantum-classical and classical-quantum channels in the same orthonormal basis.

3.1 Entanglement Breaking Channels

Entanglement is a complex physical resource in quantum systems. As such it appears in different areas of quantum information such as quantum communication, quantum cryptography, and quantum teleportation [27]. If a qubit interacts with its environment any effect the environment has on that qubit will also affect any entangled system the qubit is a part of. These things make entanglement difficult to study but if these concerns were removed we would have a more accurate mathematical explanation. We can do this by destroying entanglement with entanglement breaking channels. Let us begin with the basic definition of entanglement.

Definition 3.1.1 (Separable and Entangled States)**.** A density operator ρ acting on the tensor product of two Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable if it can be represented as $\rho = \sum_i p_i \rho_A \otimes \rho_B$, where p_i are probabilities and ρ_A and ρ_B are density matrices on $\mathcal{H}_A$ and $\mathcal{H}_B$. If ρ is not separable it is called entangled.

An entangled system cannot be separated or described by its individual subsystems. Conceptually it is helpful to see what an entangled state looks like for vector states. A vector $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if it can be written as $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ with $|\phi_1\rangle \in \mathcal{H}_A$ and $|\phi_2\rangle \in \mathcal{H}_B$. Otherwise $|\psi\rangle$ is entangled.

Example 3.1.1. Let us show that the well-known 2-qubit Bell basis states are entangled.

We recall there are four Bell states:

- $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $|\Psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- $|\Psi_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- $|\Psi_4\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

In order for them to be entangled they must not be separable. If $|\Psi_n\rangle$ is separable $|\Psi_n\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ for some vector states $|\psi_1\rangle$ and $|\psi_2\rangle$. Let us look at $|\Psi_1\rangle$, let

$$\begin{aligned}|\Psi_1\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\lambda|0\rangle + \gamma|1\rangle)\\ &= \alpha\lambda|00\rangle + \alpha\gamma|01\rangle + \beta\lambda|10\rangle + \beta\gamma|11\rangle.\end{aligned}$$

We know $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, therefore either α or γ must equal zero in order to get rid of $|01\rangle$ and either β or λ must be zero to get rid of $|10\rangle$. However, if either of those statements are true either $|00\rangle$ or $|11\rangle$ would also be zero and $|\Psi_1\rangle \neq |\Psi_1\rangle$. Therefore $|\Psi_1\rangle$ is not a separable state. The proof for $|\Psi_2\rangle, |\Psi_3\rangle$, and $|\Psi_4\rangle$ follow the same pattern.

3.1.1 Entanglement Breaking Channels

Definition 3.1.2 (Entanglement Breaking Channel)**.** [26] A quantum channel $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is called an entanglement breaking channel (EBC) if $(id \otimes \Phi)(\rho)$ is always separable, whenever ρ is a density matrix on $\mathcal{H} \otimes \mathcal{H}$.

When an EBC is applied to an entangled state on its larger composite system the output is a separable state. Entanglement breaking channels are additionally useful in that, when entangled states become separate we can look at each system in its own vector space. It is useful to study entanglement in noisy channels because the more noise there is the less entanglement you have; entanglement breaking channels excel in this area of application as they are particularly noisy [50].

Definition 3.1.3 (Holevo Form)**.** An entanglement breaking channel, Φ is written in Holevo form if it is of the form,

$$\Phi(\rho) = \sum_{k=1}^{m} R_k Tr(F_k \rho),$$

where R_k's are density matricies and $\{F_k\}_{k=1}^{m}$ forms a POVM; that is each $F_k \geq 0$ and $\sum_k F_k = I$.

The Holevo form of a channel is not unique, it depends upon the choice of R_k and F_k. The choice of R_k and F_k leads to interesting sub-types of entanglement breaking channels. Examples of subtypes of entanglement breaking channels include classical-quantum channels (c-q), Gaussian channels, and quantum-classical channels (q-c) [26].

Definition 3.1.4 (Classical-Quantum Channel)**.** [26] Classical-quantum (c-q) channels transform classical information into quantum information. For c-q channels we have F_k where $F_k = |k\rangle\langle k|$ is a one-dimensional projection which gives us an EBC:

$$\Phi(\rho) = \sum_k R_k Tr(F_k \rho) = \sum_k R_k \langle k|\rho|k\rangle.$$

Definition 3.1.5 (Quantum-Classical Channel)**.** [26] A channel is quantum-classical (q-c) if it satisfies Definition 3.1.3 and each density operator $R_k = |k\rangle\langle k|$ is a one dimensional projection with the set $\{|k\rangle\}$ forming an orthonormal basis which gives us an EBC:

$$\Phi(\rho) = \sum_k |k\rangle\langle k| Tr(F_k \rho).$$

Channels that are q-c transform quantum information into classical information whereas c-q channels transform classical information into quantum information.

The following theorem of Holevo's gives the main characteristics of EBC's.

Theorem 3.1.6. *[26] The following are equivalent:*

1. *Φ has Holevo form with F_k positive semi-definite forming a POVM and R_k density operators;*

2. *Φ is entanglement breaking;*

3. *$(id \otimes \Phi)(|\beta\rangle\langle\beta|)$ is separable for $|\beta\rangle = d^{\frac{-1}{2}} \sum_j |j\rangle \otimes |j\rangle$ a maximally entangled state;*

4. *Φ can be written in operator sum form using only Kraus operators of rank one;*

5. *$\gamma \circ \Phi$ is completely positive for all positivity preserving maps γ;*

6. *$\Phi \circ \gamma$ is completely positive for all positivity preserving maps γ.*

Proof. We begin by showing $1 \Rightarrow 2$, a channel in Holevo form, $\Phi(\rho) = \sum_k R_k Tr(F_k \rho)$. We must consider our channel Φ as $(id \otimes \Phi)(\Gamma)$, for any density operator Γ on $\mathcal{H} \otimes \mathcal{H}$. If

$dim(\mathcal{H}) = n$, then Γ has a block decomposition.

$$\begin{pmatrix} \Gamma_{11} & \Gamma_{12} & \dots & \Gamma_{1n} \\ \Gamma_{21} & \Gamma_{22} & \ddots & \Gamma_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ \Gamma_{n1} & \dots & \dots & \Gamma_{nn} \end{pmatrix},$$

where each Γ_{ij} is an operator on $\mathcal{H}$ so that

$$\begin{aligned} (id \otimes \Phi)(\Gamma) &= \begin{pmatrix} \Phi(\Gamma_{11}) & \dots & \Phi(\Gamma_{1n}) \\ \dots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \Phi(\Gamma_{n1}) & \dots & \Phi(\Gamma_{nn}) \end{pmatrix} \\ &= \sum_k \begin{pmatrix} R_k Tr(F_k\Gamma_{11}) & \dots & R_k Tr(F_k\Gamma_{1n}) \\ \vdots & \ddots & \vdots \\ R_k Tr(F_k\Gamma_{n1}) & \dots & R_k Tr(F_k\Gamma_{nn}) \end{pmatrix} \\ &= \sum_k \begin{pmatrix} Tr(F_k\Gamma_{11}) & \dots & Tr(F_k\Gamma_{1n}) \\ \vdots & \ddots & \vdots \\ Tr(F_k\Gamma_{n1}) & \dots & Tr(F_k\Gamma_{nn}) \end{pmatrix} \otimes R_k. \end{aligned}$$

We find that $(id \otimes \Phi)(\Gamma)$ is separable and therefore the entanglement breaking channel Φ is as well.

Showing 2 ⇒ 3 is trivial. We have our entanglement breaking channel

$$(id \otimes \Phi)(|\beta\rangle\langle\beta|) = (id \otimes \Phi)d^{-1}\sum_j |j\rangle\langle j| \otimes |j\rangle\langle j|$$
$$= d^{-1}\sum_j |j\rangle\langle j| \otimes \Phi(|j\rangle\langle j|),$$

which is clearly separable.

For 3 ⇒ 4 the Choi matrix of Φ is $(id \otimes \Phi)(|\beta\rangle\langle\beta|) = d^{-1}\sum_j |j\rangle\langle j| \otimes \Phi(|j\rangle\langle j|) = C_\Phi$. Since the Choi matrix is separable, C_Φ can be written as a convex combination of product states $C_\Phi = \sum_i^m K_i K_i^*$ where K_i is a product state. Since we want rank one Kraus operators we use the vec^{-1} operation, which takes matrices and transforms them to vectors, $vec^{-1}(K_i)$ is rank one if and only if K_i is a product state. Therefore our channel $\Phi(X) = \sum_{i=1}^m vec^{-1}(K_i)Xvec^{-1}(K_i)^*$, where the $\{vec^{-1}(K_i)\}$'s are our rank one Kraus operators.

To show 4 ⇒ 1 we start with $\Phi(X) = \sum_i K_i X K_i^*$ where the $\{K_i\}$'s are rank one Kraus operators. Since the K_i's are rank one we can let $K_i = v_i w_i^*$ where v_i and w_i are column vectors. Our channel becomes

$$\Phi(X) = \sum_i v_i w_i^* X w_i v_i^*$$
$$= \sum_i (w_i^* X w_i) v_i v_i^*$$
$$= \sum_i Tr(X w_i w_i^*) v_i v_i^*,$$

now let $F_i = w_i w_i^*$ and $R_i = v_i v_i^*$. It is easy to see that $\sum_i F_i = \sum_i w_i w_i^* = I$ and that $R_i = v_i v_i^*$ is a density matrix.

To prove the equivalence of 2 and 5 we start by proving that $\gamma \circ \Phi(\rho)$ is completely positive for a positivity preserving map γ when Φ is an entanglement breaking channel. Now we take the tensor product of the identity and $\gamma \circ \Phi(\rho)$ we get,

$$
\begin{aligned}
(id \otimes (\gamma \circ \Phi))(\rho) &= (id \otimes \gamma)(id \otimes \Phi)(\rho) \\
&= (id \otimes \gamma)(\sum_i \sigma_i \otimes \tau_i) \\
&= \sum_i \sigma_i \otimes \gamma(\tau_i).
\end{aligned}
$$

As the composition is still separable $\gamma \circ \Phi$ must be completely positive. To show the other direction suppose Φ is not entaglement breaking. Then there exists a density matrix rho such that $(id \otimes \Phi(\rho))$ is entangled; hence there exists a positivity preserving map gamma such that $\gamma \circ \Phi$ is completely positve. Now we take the tensor product of the identity and our map,

$$(id \otimes (\gamma \circ \Phi))(\rho) \geq 0.$$

If ρ is entangled there is a positive map $\gamma \circ \Phi$ such that $(id \otimes (\gamma \circ \Phi))(\rho)$ is not positive. We know $(id \otimes (\gamma \circ \Phi))(\rho)$ is positive and so ρ must be separable.
To show the equivalence of 5 and 6 consider that the dual of a positivity preserving map is positivity preserving. We know that $\gamma \circ \Phi$ is CP therefore we know $\gamma^* \circ \Phi^*$ is CP. We then take the dual of $\gamma \circ \Phi$,

$$\gamma^* \circ \Phi^* = (\Phi \circ \gamma)^*.$$

$(\Phi \circ \gamma)^*$ is completely positive therefore $\Phi \circ \gamma$ is as well. □

We can also add further equivalent conditions which prove a more information theoretic description of EB channels.

Theorem 3.1.7. *[24] The following conditions are equivalent:*

1. *Φ is Entanglement Breaking.*

2. *The Choi matrix of Φ is separable.*

3. *Φ is a quantum-classical-quantum channel.*

Proof. $1 \Rightarrow 2$ is trivial.

$2 \Rightarrow 3$ If the Choi matrix of Φ is separable then the output state is defined as $S_{BR} = \sum_j p_j S_B^j \otimes S_R^j$ where p_j is a probability. A Q-C-Q channel is defined as $\Phi(S) = \sum_j S_j TrSM_j$, where M_j is the measurement of the Q-C channel, S_j is a density matrix both with a classical system between their input and output and where S is a density matrix. We start by substituting S_{BR} into an entanglement breaking channel Φ,

$$\begin{aligned}
\Phi(S) &= dTr_R S_{BR}(I_B \otimes S_R^{\perp}) \\
&= dTr_R(\sum_j p_j S_B^j \otimes S_R^j)(I_B \otimes S_R^{\perp}) \\
&= dTr_R(\sum_j p_j S_B^j \otimes S_R^j S_R^{\perp}) \\
&= \sum_j p_j d S_B^j Tr(S_R^j S_R^{\perp}) \\
&= \sum_j S_B^j Tr(S_R^j p_j d S_R^{\perp}).
\end{aligned}$$

Now let $S_B^j = S_j$, $S_R^j = S$, and $p_j d S_R^{\perp} = M_j$ and we get $\Phi(S) = \sum_j S_j Tr(M_j S)$.

The proof for $3 \Rightarrow 1$ is as follows:

$$\Phi(S) = \begin{pmatrix} \Phi(S_{11}) & \Phi(S_{12}) & \dots & \Phi(S_{1n}) \\ \dots & \ddots & \ddots & \Phi(S_{2n}) \\ \vdots & \ddots & \ddots & \vdots \\ \Phi(S_{n1}) & \dots & \dots & \Phi(S_{nn}) \end{pmatrix}$$

$$= \sum_k \begin{pmatrix} S_k Tr(M_k S_{11}) & \dots & S_k Tr(M_k S_{1n}) \\ \vdots & \ddots & \vdots \\ S_k Tr(M_k S_{n1}) & \dots & S_k Tr(M_k S_{nn}) \end{pmatrix}$$

$$= \sum_k \begin{pmatrix} Tr(M_k S_{11}) & \dots & Tr(M_k S_{1n}) \\ \vdots & \ddots & \vdots \\ Tr(M_k S_{n1}) & \dots & Tr(M_k S_{nn}) \end{pmatrix} \otimes S_k.$$

Since $\Phi(S)$ is separable it is entanglement breaking. □

We finish this section with a note on a related class of channels: positive partial transpose channels.

Definition 3.1.8 (Partial Transpose)**.** The partial transpose of a density matrix ρ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}$ is the Hilbert space of system A and B respectively, is $\rho^{T_B} = (id \otimes T)(\rho)$, where T is the transpose map.

Definition 3.1.9 (PPT)**.** [24] A channel Φ from A to B is positive partial transpose (PPT) if, for an arbitrary input state S_{AR} the channel $\Phi \otimes id$, the output state $S_B R$ of the channel Phi tensor id has a postive partial transpose in the space $\mathcal{H}_R$.

Every entanglement-breaking channel is PPT, but not all PPT maps are entanglement breaking. If a map is PPT but not entanglement breaking we say it is an entanglement-binding map.

Conjecture 1 (PPT Squared Conjecture). *[41] Suppose we have two PPT quantum channels $\Phi : T_j \to T_k$ and $\Psi : T_k \to T_i$, then $\Phi \circ \Psi$ is an entanglement breaking channel.*

3.1.2 Schur Product Channels

Below we show that the following class of channels is closely related to EBC's.

Definition 3.1.10 (Schur Product Channel). $\Phi : M_n \to M_n$ is said to be a Schur product channel if we have a matrix A satisfying

$$\Phi(\rho) = A \odot \rho.$$

A and ρ are matrices of the same dimension and $\odot$ performs elementwise multiplication.

Proposition 3.1.11. *A Schur product channel, $\Phi(\rho_1) = A \odot \rho_1$, is completely positive if and only if $A \geq 0$.*

Proof. Suppose Φ is completely positive, by the result on page 286 of [7] we know $(id_k \otimes \Phi)$ is positive for all k. Now let

$$(id_k \otimes \Phi) = \begin{pmatrix} \Phi(\rho_{11}) & \dots & \Phi(\rho_{1n}) \\ \vdots & \ddots & \vdots \\ \Phi(\rho_{n1}) & \dots & \Phi(\rho_{nn}) \end{pmatrix} = \rho_2 \odot \begin{pmatrix} A & \dots & A \\ \vdots & \ddots & \vdots \\ A & \vdots & A \end{pmatrix},$$

where $\rho_1 \in M_n$ and $\rho_2 \in M_n \otimes M_n$. Since we are taking the tensor product of two spaces the dimension of the resulting matrix is larger than either or the original martices. Let J be the all one's matrix, J is positive semidefinite and $\Phi(A)$ is positive therefore by the Schur product theorem [43], $A \geq 0$. Now suppose if $A \geq 0$ then Φ is completely positive, let ρ_2 be positive semi definite matrix now we have a Schur product channel $\rho_2 \odot (J \otimes A) = (I_k \otimes \Phi)(\rho_1)$ which is the Choi matrix of Φ. By Schur product theorem $(I_k \otimes \Phi)(\rho_1)$ is positive semi definite and since it is the Choi matrix by [7] Φ is completely positive. $\square$

3.1.3 Complementary Channels

Definition 3.1.12 (Complementary Channel)**.** [22] Two channels Φ_B and Φ_C are said to be complementary if there exists two completely positive maps Φ_B: $\mathcal{H}_A \to \mathcal{H}_B$, Φ_C: $\mathcal{H}_A \to \mathcal{H}_C$ where $\mathcal{H}_{A,B,C}$ are the spaces of quantum systems A, B or C respectively and $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_C$ is a linear operator such that $\Phi_A[S] = Tr_B VSV^*, \Phi_B[S] = Tr_A VSV^*, S \in \mathcal{H}_A$

Complementary channels map an input space to a different output space using transformations. If v is an isometry, both maps are trace-preserving and therefore are also channels. Every CP map has a complementary channel, complementary channels can be thought of as unique as there exists a partial isometry $\mathcal{H}_C \to \mathcal{H}_{C'}$ between two maps Φ_C and $\Phi_{C'}$ both of which are complementary to Φ_B.

Proposition 3.1.13. *If we have a CP map Φ with Kraus representation*

$$\Phi(\rho) = \sum_{k=1}^{\tilde{d}} V_k \rho V_k^*,$$

the complementary map $\tilde{\Phi}$ is given by

$$\tilde{\Phi}(\rho) = \sum_{k,l=1}^{\tilde{d}} (Tr \rho V_l^* V_k)|e_k\rangle\langle e_l|,$$

where $\{e_k\}$ is the canonical basis for the coordinate space.

Example 3.1.2. Suppose we have an entanglement breaking channel Φ and want to find the complementary channel. By the equivalent conditions in Theorem 3.1.6 we know it can be written using only Kraus operators of rank one:

$$\Phi(\rho) = \sum_{k=1}^{\tilde{d}} |\phi_k\rangle\langle\psi_k|\rho|\psi_k\rangle\langle\phi_k|$$

where

$$\sum_{k=1}^{\tilde{d}} |\psi_k\rangle\langle\phi_k|\phi_k\rangle\langle\psi_k| = I.$$

From above we can now define the complementary channel as

$$\tilde{\Phi}(\rho) = \sum_{k,l=1}^{\tilde{d}} c_{kl}|e_k\rangle\langle\psi_k|\rho|\psi_l\rangle\langle e_l|$$

which we can write as

$$\tilde{\Psi}(\rho) = C \odot S,$$

which is a Schur product channel. We can conclude that the complementary map of entanglement breaking channels are Schur product channels.

3.1.4 Random Unitary Channels

Random unitary channels are a class of quantum channel that can be corrected using measurement performed on the environment. They are useful and therefore are an important class of channel.

Definition 3.1.14. A channel $\Phi : M_n \to M_n$ is said to be random unitary if it can be written in the form

$$\Phi(X) = \sum_{i=1}^{d} p_i U_i X U_i^*$$

where p_i form a probability distribution and $U_i \in U(n)$ are unitaries.

Definition 3.1.15. Let $\Phi : M_n \to M_n$ be a quantum channel with a minimal set of Kraus operators $\{K_i\}_{i=1}^{d}$. The canonical complement of Φ is the channel $\Phi^C : M_n \to M_d$ defined by

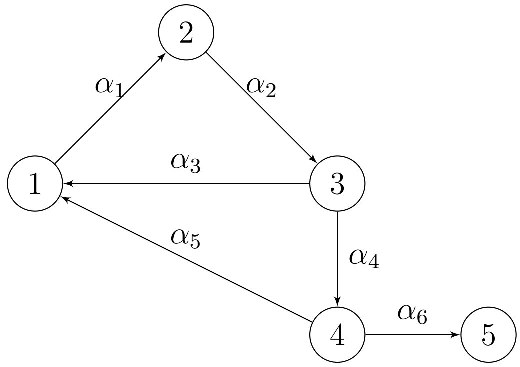
$$\Phi^C(X) = \sum_{i,j=1}^{d} \mathrm{Tr}(K_j^* K_i X) E_{ij}.$$

Ψ is a complementary channel for Φ if and only if there exists an isometry V such that

$$\Psi(X) = V\Phi^C(X)V^*.$$

3.2 PageRank

PageRank is an algorithm used to order webpages so that the most important and relevant webpages appear first. It is assumed that the more important or useful a page is the more other pages will link to that page. Pagerank considers the number of incoming links to a webpage and calculates an associated probability that a user would randomly click a link leading to that page. Once information has been collected we can create a column stochastic matrix S where each s_{ji} represents the probability of a user moving from page j to page i. When many users go from page j to page i S_{ji} in the stochastic matrix increases, telling PageRank that link i is important and should be one of the first links users see. You can represent the path a user could take to different webpages with a directed graph where each node is a webpage and the connecting lines are links between pages where each user has probability α_n of picking a link.



The column stochastic matrix S of the directed graph would be:

$$\begin{bmatrix} 0 & 0 & \alpha_3 & \alpha_4 & 0 \\ \alpha_1 & 0 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 & 0 \\ 0 & 0 & \alpha_4 & 0 & 0 \\ 0 & 0 & 0 & \alpha_6 & 0 \end{bmatrix}.$$

The last column in the matrix corresponds to node 5 which has no outgoing links, this is called a dangling node. Now we must adjust our algorithm to accommodate for dangling nodes. Suppose if there are no outgoing links a user is "teleported" to a new webpage, like typing in a new URL. Let α represent the probability a user can click on an outgoing link and $(1-\alpha)$ represent the probability a user must be "teleported" to a new page which is modelled by a uniform distribution W. After we perform many iterations to obtain our $\alpha' s$, we can represent the PageRank algorithm as $(I - \alpha S)x = (1-\alpha)W$. S is a matrix of probabilities of a user going from page j to page i in one timestep while W is some vector of probabilities that is used when a dangling node occures. The vector x is the steady state of whatever we are ranking, it is what we will converge to.

Definition 3.2.1 (PageRank)**.** [14] Let S be a column stochastic matrix where all entries are nonegative and the sum of entries in each column is 1. Let v be a column stochastic vector, and let $0 < \alpha < 1$ be a teleportation parameter. Then the PageRank problem is to find the solution, x or the PageRank vector, of the linear system

$$(I - \alpha S)x = (1 - \alpha)W.$$

The results in the next chapter use and are in part motivated by PageRank. We will show how a stochastic matrix associated to an entanglement breaking channel can be used to predict the long-term behaviour of the channel.

Chapter 4

New Structural Results on Entanglement Breaking Channels

4.1 Introduction

In this chapter, we first observe that every Holevo form of an entanglement breaking channel yields a stochastic matrix, and in turn, we note that every stochastic matrix naturally defines a quantum-classical channel. We show how a stochastic matrix obtained from an entanglement breaking channel in this way can be used to study the iterative long-term behaviour of the channel, and we use this perspective to study the fixed point theory for such channels. We further consider nullspaces of entanglement breaking channels, in particular, proving that every operator space of trace zero matrices is the nullspace of such a channel. We also present examples and discuss connections with quantum privacy. The contents of this chapter are drawn from the paper [30].

4.2 Stochastic Matrices and Entanglement Breaking Channels

Quantum channels are central objects of study in quantum information. They are represented mathematically by completely positive, trace preserving maps as discussed in detail above. In this section, we will show how to represent an entanglement breaking channel using stochastic matrices.

4.2.1 Stochastic Matrix from the Holevo Form

Let us consider more closely the action of a map in the form of Definition 3.1.3. When an entanglement breaking channel is applied to a density matrix ρ_0 the result is $\rho = \Phi(\rho_0)$, which is a density matrix in the range of Φ. As such, it belongs to the convex hull of the R_k's since $\Phi(\rho_0) = \sum_k Tr(F_k \rho_0) R_k$, and so $\rho = \sum_m c_m R_m$ where the $c_m = Tr(F_m \rho_0)$ are positive real numbers summing to one since

$$\begin{aligned}\sum_m c_m &= \sum_m Tr(F_m \rho_0) \\ &= Tr(\sum_m F_m \rho_0) \\ &= Tr(\rho_0) \\ &= 1.\end{aligned}$$

Using this decomposition of ρ, observe

$$\begin{aligned}\Phi(\rho) &= \sum_k Tr(F_k\rho)R_k \\ &= \sum_k \sum_m (c_m Tr(F_k R_m)R_k) \\ &= \sum_k \Big(\sum_m c_m Tr(F_k R_m)\Big) R_k,\end{aligned}$$

and hence $\Phi(\rho) = \sum_k a_k R_k$ where $a_k = \sum_m Tr(F_k R_m)c_m$ is some real number.

The transformation of the vector $\vec{c} = (c_1\, c_2\, \ldots)$ to the vector $\vec{a} = (a_k)$ can thus be described by a matrix multiplication $S\vec{c} = \vec{a}$ in which the (i, j) entry of the matrix S is $Tr(F_i R_j)$ giving us our result. All entries of S are nonnegative, as F_i and R_j are nonnegative and so $Tr(F_i R_j) = Tr((\sqrt{F_i}\sqrt{R_j})^*(\sqrt{F_i}\sqrt{R_j})) \geq 0$, therefore, all entries of S are nonnegative. The sum of all the entries in any column of S is one since $\{F_i\}$ forms a POVM and R_j is a density matrix; indeed, for each j, we have $\sum_i Tr(F_i R_j) = Tr(\sum_i F_i R_j) = Tr(R_j) = 1$. Therefore, we have observed that attached to any representation of an entanglement breaking channel in the Holevo form is a (column) stochastic matrix

$$S = \begin{pmatrix} s_{11} & s_{12} & \ldots & s_{1j} \\ s_{21} & s_{22} & \ddots & s_{2j} \\ \vdots & \ddots & \ddots & \vdots \\ s_{i1} & s_{i2} & \ldots & s_{ij} \end{pmatrix},$$

where $s_{ij} = Tr(F_i R_j)$ for all i, j. From the above notation for $\Phi(\rho)$ with $\rho \in Range(\Phi)$ in Holevo form we have $\Phi(\rho) = \sum_k (\vec{s}_k \cdot \vec{c})R_k$, where $\vec{s}_k = (s_{kj})$ is the kth row vector of S.

There are different combinations of F_k and R_k's that satisfy the requirements of Holevo form for an entanglement breaking channel Φ. Therefore the representation of a channel

Φ depends upon the choice of F_k and R_k and is not unique. The stochastic matrix S also depends on our choice of the Holevo form and as the channel is not unique S is not uniquely determined by the channel. This leads to our first question: what properties of the stochastic matrix are invariant under the choice of Holevo form? The following result shows how the structure of any such stochastic matrix representation is closely related to the structure of the channel itself.

Theorem 4.2.1. *Let Φ be an entanglement breaking channel on M_n. Suppose S is a stochastic matrix defined by operators F_k, R_k that define a Holevo form for Φ. Then the Jordan canonical forms of Φ and S are the same, except possibly on blocks that correspond to zero eigenvalues.*

Proof. Suppose we have the Holevo representation $\Phi(\rho) = \sum_{k=1}^{m} Tr(F_k\rho)R_k$. We begin by looking at Φ as an linear operator on M_n. Consider a matrix representation $[\Phi]$ of Φ in a fixed orthonormal basis for $\mathbb{C}^n$, and for $X \in M_n$ then $\text{vec}(X)$ is an n^2 column vector. Then one can verify that this matrix can be decomposed as the product $[\Phi] = AB$ where A is the $n^2 \times m$ matrix whose kth column is $\text{vec}(R_k)$ for all k and B is the $m \times n^2$ matrix whose kth row is the transposed column matrix $\text{vec}(F_k)^T$. On the other hand, one can verify that the stochastic matrix S defined by the operators F_k, R_k is equal to BA.

Thus we have $[\Phi] = AB$ and $S = BA$, and we can now apply the classical Flanders Theorem [9] that relates the Jordan forms of matrix products AB and BA as claimed in the theorem statement. □

Example 4.2.1. The extreme case given by the completely depolarizing channel on M_n satisfies $\Phi_{\text{CD}}(\rho) = \frac{Tr(\rho)}{n}I$ for all ρ. So in this case we have Holevo operators $F_1 = I$ and $R_1 = \frac{1}{n}I$. In this trivial case, with the notation of the theorem, A is the $n^2 \times 1$ matrix with n entries of $\frac{1}{n}$ corresponding to the diagonal matrix units and 0's elsewhere, and B is the $1 \times n^2$ matrix with n entries of 1 in the same coordinate positions and 0's elsewhere.

Here $S = BA = (1)$ and $[\Phi] = AB$ is the corresponding rank-1 matrix representation of the channel.

Example 4.2.2. Another simple example is given by the map-to-diagonal channel on M_n, which replaces off-diagonal entries of a matrix with zeros, $\Lambda(\rho) = \mathrm{diag}(\rho)$. As a map on operators, this is a special type of q-c channel (see below) with Holevo form given by $F_k = |k\rangle\langle k| = R_k$ for a fixed orthonormal basis $\{|k\rangle\}_{k=1}^n$. In this case the factored matrices are related as $B = A^*$, and the stochastic matrix construction yields the $n \times n$ identity matrix $S = BA = I$.

The result above shows that the non-zero spectrum of Φ and that of any of its stochastic matrix representations S are the same, including multiplicities. More than that, as the long term behaviour of repeated applications of a finite-dimensional linear operator is determined by its Jordan Canonical form, it also shows that iterations of Φ can be modelled by repeated applications of any choice of S.

In the next section, we will discuss how to model repeated iterations of Φ. First, we note how the relationship between the channel and stochastic matrix is tighter in a special case, and we also present a converse in a sense of the connection with stochastic matrices uncovered above, by showing that every stochastic matrix naturally defines a special type of entanglement breaking channel.

4.2.2 Quantum-Classical Channels from Stochastic Matrices

A special class of entanglement breaking channels produce (classical) probability distributions from input quantum states via expectation values from a POVM [26].

Let $S = (s_{ij})$ be an $n \times n$ stochastic matrix, with each $s_{ij} \geq 0$ and $\sum_{i=1}^n s_{ij} = 1$ for all $1 \leq j \leq n$. Let $\{|k\rangle\}_{k=1}^n$ be a fixed orthonormal basis for $\mathbb{C}^n$. For each k, let F_k be the diagonal operator on $\mathbb{C}^n$ with $n \times n$ diagonal matrix representation in the fixed basis and whose diagonal entries form the kth row of S. That is,

$$S = \begin{pmatrix} — & F_1 & — \\ — & F_2 & — \\ & \vdots & \\ — & F_k & — \end{pmatrix},$$

and explicitly, $F_k = \sum_{j=1}^{n} s_{kj} |j\rangle\langle j|$ for each k. Observe that every F_k is a positive operator and $\sum_{k=1}^{n} F_k = I$ by construction.

Now let $R_k = |k\rangle\langle k|$ for $1 \leq k \leq n$ and define a q-c channel on M_n by $\Phi_S(\rho) = \sum_{k=1}^{n} Tr(F_k \rho) R_k$. Finally, observe that if we apply our stochastic matrix construction above to the entanglement breaking channel Φ_S, we get the matrix S back again as follows: for $1 \leq i, j \leq n$, we have

$$Tr(F_i R_j) = \sum_{k=1}^{n} s_{ik} Tr(|k\rangle\langle k||j\rangle\langle j|) = s_{ij}.$$

4.3 Fixed Point Theory for Entanglement Breaking Channels

We note that a quantum channel from $M_n \to M_n$ maps the compact convex set of density matrices to itself. Therefore Brouwer's theorem guarantees that every such quantum channel must have a fixed point. This fixed point may or may not be globally attractive; for entanglement breaking channels, we can use the theory of stochastic matrices and the connections developed above to study this question.

There is a very well known sufficient condition for a stochastic matrix to have a unique globally attractive fixed point among the probability vectors.

The corollary of Theorem 2.2.15 is that if the associated stochastic matrix of an entanglement breaking channel is primitive then its fixed point is globally attractive. We note the following equivalent condition for a nonnegative matrix to be primitive.

Proposition 4.3.1. *Let A be an n by n nonnegative matrix. Then A is primitive if and only if for every nonnegative nonzero $x \in \mathbb{R}^n$, there exists $k > 0$ such that $A^k x$ has all of its entries strictly positive.*

Motivated by this, the concept of a primitive quantum channel has been developed in [42, 38].

Definition 4.3.2. [42] Let Φ be a quantum channel, then Φ is said to be primitive if there exists $k > 0$ such that $\Phi^k(\rho)$ is positive definite for all density matrices ρ.

We note the following result connecting these two notions of primitivity. In the following proposition, we make the assumption that none of the F_i's in the POVM in the Holevo form are zero. This assumption is always followed in practice.

Proposition 4.3.3. *Let Φ be an entanglement breaking channel and S be an associated stochastic matrix. Then Φ is primitive if and only if $\sum_k R_k$ is positive definite and S is primitive.*

Proof. Suppose S is primitive and $\sum_k R_k$ is positive definite, then let v be the Perron-Frobenius eigenvector of S normalized so that its entries sum to one. Then for any density matrix ρ, $\lim_{k\to\infty} \Phi^k(\rho) = \sum_k v_k R_k$. Since $\sum_k v_k R_k \geq (\min_k v_k) \sum_k R_k > 0$, it follows that Φ is a primitive quantum channel. Now suppose Φ is primitive. Then for any j, there exists an m such that $\Phi^m(R_j)$ is positive definite. Let $w = S^m e_j$, then $\Phi^m(R_j) = \sum_k w_k R_k$. Since $(\max_k w_k) \sum_k R_k \geq \sum_k w_k R_k > 0$, it follows that $\sum_k R_k$ is positive definite. Now let $x = Sw = S^{m+1} e_j$. Then $x_i = \sum_k Tr(F_i R_k) w_k = Tr(F_i(\sum_k w_k R_k))$. Since $\sum_k w_k R_k = \Phi^m(R_j)$ is positive definite and F_i is nonzero positive semidefinite, $x_i > 0$ and $S^{m+1} e_j$ has all positive entries. Since j was arbitrary, S is primitive. □

4.3.1 The Special Case of Unital Channels

In the case that a channel is unital ($\Phi(I) = I$), there is often more structure that can be identified. The following result makes use of the fixed point theory for such channels [31] to give a tight description of the fixed point set when it is entanglement breaking.

We introduce the fixed point set of Φ denoted $\text{Fix}(\Phi) = \{X \in M_n : \Phi(X) = X\}$, and recall the standard notation $\{A_k\}'$ for the commutant of a set of operators A_k; the set of all operators that commute with all A_k.

Proposition 4.3.4. *If Φ is a unital entanglement breaking channel, then the fixed point set* $\text{Fix}(\Phi)$ *is a commutative $*$-algebra.*

Proof. As Φ is entanglement breaking recall we can assume from the last chapter that, it has an operator-sum representation $\Phi(\rho) = \sum_k A_k \rho A_k^*$ comprised of rank one operators $A_k = |\psi_k\rangle\langle\phi_k|$, where we will assume with no loss of generality that each $|\phi_k\rangle$ is a unit vector. The unital condition on Φ thus give us $I = \sum_k |\psi_k\rangle\langle\psi_k|$.

We now apply the fixed point theory for unital channels from [31] to conclude that $\text{Fix}(\Phi) = \{A_k\}' = \{A_k, A_k^*\}'$, and moreover that this set is a $*$-algebra (a finite-dimensional C*-algebra). As such, the set is spanned by its projections P, and $\Phi(P) = P$ if and only if $PA_k = A_k P$ for all k. So given a projection $P \in \text{Fix}(\Phi)$, its range is a reducing subspace for the range of each A_k (i.e., invariant for both the range of A_k and its orthogonal complement). But the range of A_k is $\text{span}\{|\psi_k\rangle\}$, and hence $|\psi_k\rangle$ must be an eigenvector for P.

Bringing these facts together, let P_1, P_2 be projections inside $\text{Fix}(\Phi)$ and let a_k, b_k be scalars such that $P_1|\psi_k\rangle = a_k|\psi_k\rangle$ and $P_2|\psi_k\rangle = b_k|\psi_k\rangle$ for each k. Then we have the following:

$$\begin{aligned} P_1P_2 = P_1P_2(I) &= P_1P_2\big(\sum_k |\psi_k\rangle\langle\psi_k|\big) = \sum_k P_1(b_k|\psi_k\rangle\langle\psi_k|) \\ &= \sum_k b_k a_k |\psi_k\rangle\langle\psi_k| = \sum_k a_k P_2 |\psi_k\rangle\langle\psi_k| \\ &= P_2\big(\sum_k P_1|\psi_k\rangle\langle\psi_k|\big) = P_2P_1. \end{aligned}$$

Given an arbitrary pair of self-adjoint operators inside $\mathrm{Fix}(\Phi)$, which form a spanning set for the algebra, all the spectral projections of the operators belong to the set and are mutually commuting by the above argument, and it follows the fixed point set is commutative as claimed. □

As a finite-dimensional, unital, and commutative $*$-algebra, there is necessarily a family of projections $P_1, \ldots, P_d$ with mutually orthogonal ranges inside $\mathrm{Fix}(\Phi)$, such that $\sum_j \mathrm{rank}(P_j) = n$ and the following orthogonal decomposition satisfied: $\mathrm{Fix}(\Phi) = \mathbb{C}P_1 \oplus \ldots \oplus \mathbb{C}P_d$.

4.4 Nullspaces of Entanglement Breaking Channels

Partly motivated by the work above, in addition to operator theoretic considerations, in this section, we consider the nullspace structure for entanglement breaking channels.

We give constructions of channels that annihilate subspaces of trace zero matrices, and discuss a connection with quantum privacy. Note that the nullspace of any quantum channel, in particular as a trace-preserving map, is contained inside the operator subspace of trace zero matrices.

4.4.1 Private Subspaces and Nullspaces

One motivation for considering nullspaces for quantum channels comes from quantum privacy, as the new observation below explains.

Recall the basic definition of a private subspace.

Definition 4.4.1. Given a channel Φ on $\mathcal{H}$ and a subspace $\mathcal{C}$, we say $\mathcal{C}$ is *private for* Φ if there is a density operator ρ_0 such that $\Phi(\rho) = \rho_0$ for all ρ supported on $\mathcal{C}$; that is, for all ρ on $\mathcal{H}$ with $\rho = P_{\mathcal{C}}\rho P_{\mathcal{C}}$ and where $P_{\mathcal{C}}$ is the projection onto $\mathcal{C}$.

Proposition 4.4.2. *Let Φ be a quantum channel on $\mathcal{H}$ and let $\mathcal{C} \subseteq \mathcal{H}$ be a subspace. Then $\mathcal{C}$ is private for Φ if and only if the set of trace zero operators supported on $\mathcal{C}$ is contained inside the nullspace of Φ; that is, $\mathcal{L}(\mathcal{C})_0 \subseteq \text{nullspace}(\Phi)$.*

Proof. Let $\mathcal{N} = \text{nullspace}(\Phi)$ and note that by considering the Cartesian decomposition of an operator, showing $\mathcal{L}(\mathcal{C})_0 \subseteq \mathcal{N}$ is equivalent to showing the Hermitian operators inside $\mathcal{L}(\mathcal{C})_0$ belong to $\mathcal{N}$.

So suppose $\mathcal{C}$ is private for Φ. Given a trace zero Hermitian operator H supported on $\mathcal{C}$, we can write it in the standard way as a difference of positive operators supported on $\mathcal{C}$: $H = \lambda_1\rho_1 - \lambda_2\rho_2$ where ρ_i are density operators and λ_i are real scalars. But actually $\lambda := \lambda_1 = \lambda_2$ as $Tr(H) = 0$. Hence, $\Phi(H) = \lambda(\Phi(\rho_1) - \Phi(\rho_2)) = \lambda(\rho_0 - \rho_0) = 0$ and $H \in \mathcal{N}$.

On the other hand, given any two density operators ρ_1, ρ_2 supported on $\mathcal{C}$, their difference is a trace zero operator supported on $\mathcal{C}$. Thus, if $\mathcal{L}(\mathcal{C})_0 \subseteq \mathcal{N}$, we have $0 = \Phi(\rho_1 - \rho_2) = \Phi(\rho_1) - \Phi(\rho_2)$ and it follows that $\mathcal{C}$ is a private subspace for Φ. $\square$

4.4.2 Channel Vanishing of Prescribed Operator Spaces

We now show how to explicitly construct entanglement breaking channels that include specific subspaces of trace zero Hermitian matrices in their nullspace.

Proposition 4.4.3. *Let $\mathcal{N}$ be a subspace of the trace zero Hermitian matrices inside M_n. Then there is an entanglement breaking channel $\Phi : M_n \to M_n$ such that* $\text{nullspace}(\Phi) = \mathcal{N}$.

Proof. Let M_n^0 be the space of trace zero matrices inside M_n. Further let $\{H_k\}_{k=1}^m$ be an orthonormal basis (in the trace inner product) of Hermitian operators for $\mathcal{N}^\perp \cap M_n^0$, and let $H_{m+1} = -\sum_{k=1}^m H_k$. For $1 \le k \le m+1$, define scalars $\lambda_k = \lambda_{k,min}$ when H_k has negative eigenvalues and where $\lambda_{k,\text{min}}$ is the minimal eigenvalue of H_k, and put $\lambda_k = -1$ when $H_k \ge 0$. Let $\lambda = -\sum_k \lambda_k$ and define positive operators $F_k = \lambda^{-1}(H_k - \lambda_k I)$. Observe that $\{F_k\}_{k=1}^{m+1}$ forms a POVM as $\sum_k F_k = I$.

Now let $\{R_k\}_{k=1}^{m+1}$ be a set of linearly independent density operators inside M_n, and define an entanglement breaking channel $\Phi(\rho) = \sum_k Tr(\rho F_k) R_k$. We then have the following string of equivalencies,

$$\begin{aligned} A \in \text{nullspace}(\Phi) &\Leftrightarrow Tr(AF_k) = 0 \ \ \forall 1 \le k \le m+1 \\ &\Leftrightarrow A \in (\text{span}\{F_k\}_{k=1}^{m+1})^\perp \\ &\Leftrightarrow A \in (\text{span}\{H_k\}_{k=1}^{m+1} \cup \{I\})^\perp \\ &\Leftrightarrow A \in (\text{span}\{H_k\}_{k=1}^{m+1})^\perp \cap \{I\}^\perp \\ &\Leftrightarrow A \in (\mathcal{N}^\perp \cap M_n^0)^\perp \cap M_n^0 \\ &\Leftrightarrow A \in \mathcal{N}, \end{aligned}$$

and the result follows. □

4.4.3 An Addition on Constructing Channels that Annihilate Prescribed Subspaces

Inspired by the above, we look more generally at constructions of channels. Let $\mathcal{N}$ be a self-adjoint subspace of trace zero matrices inside M_n; so $\mathcal{N} \subseteq M_n^0$. A note on constructing channels that annihilate prescribed subspaces: let $\mathcal{S} := \text{span}\{S_i\}_{i=1}^m \subseteq M_n$ be a subspace of matrices; since we hope that we can find a channel Φ such that $\Phi(S_i) = 0$ for each i, we should insist at least that $\text{Tr}(S_i) = 0$ for all i. The attempt to construct a Φ can be framed as follows: Let $\{Z_i\}$ be an orthonormal basis for the orthogonal complement $\mathcal{N}^\perp$, and so $Tr(AZ_i) = 0$ for all i and $A \in \mathcal{N}$. We claim that every channel Φ that annihilates $\mathcal{N}$ corresponds to a solution of the following *Linear Matrix Inequality* (LMI):

$$L_Z(\mathbf{A}) = I_n \otimes A_0 + \sum_{i=1}^{r} \overline{Z_i} \otimes A_i \geq 0; \tag{4.1}$$

that is, each channel Φ corresponds to a tuple of $n \times n$ matrices $\mathbf{A} := (A_0, A_1, \ldots, A_r)$, such that A_0 is a density matrix, $Tr(A_i) = 0$ for $i \neq 0$, and the A_i when tensored with the complex conjugates $\overline{Z_i}$ and summed up as above, yields a positive semidefinite matrix. To see why this is so, we will define Φ by making it the map whose Choi matrix is $L_Z(A)$. Recall that the Choi matrix is defined by

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

where we write the matrix units $E_{ij} = |i\rangle\langle j|$ in a fixed basis $\{|i\rangle\}$. Hence for $X = \sum_{i,j} x_{ij} E_{ij}$, we have

$$\Phi(X) = \sum_{i,j} x_{ij} \Phi(E_{ij}) = (Tr \otimes \text{id})\Big((X^T \otimes I) C_\Phi \Big).$$

But Φ is completely positive if and only if C_Φ is positive semidefinite. Suppose then that $L_Z(\mathbf{A}) \geq 0$, and define a completely positive map Φ via the identification $C_\Phi = L_Z(\mathbf{A})$. Next we show that Φ is trace-preserving. Observe we have:

$$\begin{aligned}\Phi(X) &= (Tr \otimes \mathrm{id})\Big((X^T \otimes I)C_\Phi\Big)\\ &= (Tr \otimes \mathrm{id})\Big((X^T \otimes I)L_Z(A)\Big)\\ &= Tr(X^T)\rho + \sum_i Tr(X^T\overline{Z_i})A_i\\ &= Tr(X)\rho + \sum_i Tr(XZ_i^*)A_i.\end{aligned}$$

Taking the trace, and recalling that A_0 has trace 1 and the other A_i have trace 0, we get $\mathrm{Tr}(\Phi(X)) = \mathrm{Tr}(X)$ for all X. Thus, Φ is a quantum channel. Finally, we show that $\Phi(A) = 0$ for all $A \in \mathcal{N}$. This follows from

$$\Phi(A) = Tr(A)\rho + \sum_i Tr(AZ_i^*)A_i,$$

and the fact that $Tr(A) = 0 = Tr(AZ_i^*) = 0$, for all i. The proof in the previous section goes further, and constructs a Φ that is entanglement breaking; this requires that $C_\Phi = \sum_i \rho_i \otimes \sigma_i$ where all ρ_i, σ_j are (scaled) density matrices. In general though, we are trying to understand the form various solutions to $L_Z(\mathbf{A}) \geq 0$ can take. This point of view might be a way to generalize the construction above further.

In the spirit of these channel nullspace investigations, we can also consider the class of bi-unitary channels. Such channels are described by scenarios in which a system is potentially exposed to unitary noise with some fixed probability $0 < p < 1$; as a completely positive map, this is given by a map of the form $\Phi(\rho) = (1-p)\rho + p\,U\rho U^*$ for some fixed unitary operator U.

Suppose A is a Hermitian matrix in the nullspace of Φ. Then we will have

$$UAU^* = -\frac{1-p}{p}A$$

As UAU^* has the same spectrum as A, this can only happen when $p = \frac{1}{2}$, which gives us a further equation

$$UAU^* = -A,$$

which forces A and $-A$ to have the same eigenvalues. Next, we can diagonalize U as

$$U = \sum_{i=1} w_i |i\rangle\langle i|,$$

Expanding $A = (a_{ij})$ in this basis gives

$$UAU^* = \sum_{ij} w_i \bar{w}_j a_{ij} |i\rangle\langle j|,$$

and so $w_i \bar{w}_j a_{ij} = -a_{ij}$.

We thus end up with two options: $a_{ij} = 0$ or $w_i = -w_j$. This tells us that we have a non-trivial null space where U has eigenvalues that come in positive and negative pairs. This is reminiscent of the positive and negative spin of electrons and the eigenvalues of the Pauli matrices.

4.4.4 Nullspaces of Entanglement Breaking and Random Unitarity Channels

One useful application of the ideas above is to random unitary (or mixed unitary) channels. Throughout this section, we will connect random unitary channels and nullspaces of entanglement breaking channels.

Lemma 4.4.4. *A channel $\Phi : M_n \to M_n$ is random unitary if and only if there exists an isometry V such that, for all $X \in M_n$ such that* $\mathrm{Tr}(X) = 0$, *$V\Phi^C(X)V^*$ has all of its diagonal entries equal to* 0.

The result may be found as Theorem 1 in [13], but we will provide a short proof for completeness:

Proof. Suppose first that Φ is random unitary; then there exist unitaries $\{U_i\}_{i=1}^r$ and a probability distribution $\{p_i\}_{i=1}^r$ and an isometry V such that (i, j) entry of $V\Phi^C(X)V^*$ is equal to $\mathrm{Tr}(\sqrt{p_ip_j}U_j^*U_iX)$; setting $i = j$ we get $p_i\mathrm{Tr}(X)$ and so for all traceless X, the diagonal entries are 0.

For the converse, suppose an isometry V exists with the property that $V\Phi^C(X)V_{ii}^* = 0$ for all traceless X. Define $\widetilde{K_i} = \sum_{j=1}^d v_{ij}K_i$; then $\{\widetilde{K_i}\}$ are a set of Kraus operators for Φ, and $V\Phi^C(X)V_{ij}^* = \mathrm{Tr}(\widetilde{K_j}^*\widetilde{K_i}X)$. We have

$$\mathrm{Tr}(\widetilde{K_i}^*\widetilde{K_i}X) = 0$$

for all i, and for all traceless X; hence $\widetilde{K_i}^*\widetilde{K_i} \in \{I\}^{\perp\perp}$, and so $\widetilde{K_i}^*\widetilde{K_i}$ is a multiple of the identity: $\widetilde{K_i}^*\widetilde{K_i} = p_iI$. Thus, $U_i := \frac{1}{\sqrt{p_i}}\widetilde{K_i}$ is unitary, and $\widetilde{K_i} = \sqrt{p_i}U_i$. That the set $\{p_i\}_{i=1}^r$ form a probability distribution follow from the fact that Φ^C is trace-preserving and therefore so is $V\Phi^C(X)V^*$. □

Now we can connect random unitary channels to nullspaces of entanglement breaking channels with the following theorem.

Theorem 4.4.5. *Let Φ be a quantum channel from M_n to M_n with canonical complement $\Phi^C : M_n \to M_d$. Then Φ is random unitary if and only if there exists an entanglement* *breaking channel $E : M_d \to M_r$ of Choi rank r taking M_d into an r-dimensional commutative algebra Δ, such that $E(\Phi^C(X)) = \frac{1}{r}\mathrm{Tr}(X)I_r$ for $X \in M_n$.*

Proof. First, suppose Φ is random unitary; by Lemma 4.4.4 there must be an isometry $V : \mathbb{C}^d \to \mathbb{C}^r$ such that $V\Phi^C(X)V^*$ has 0 on its diagonals when X is traceless. Let v_i be the i^{th} column of V^*; then $v_i^*\Phi^C(X)v_i = 0$ for all traceless X, and the condition that V is an isometry may be phrased as

$$\sum_{i=1}^{r} v_i v_i^* = I_r.$$

Define $p_i = \frac{1}{n}v_i^*\Phi^C(I)v_i$; as Φ^C is trace-preserving and V an isometry, we have that $\sum_{i=1}^r p_i = \frac{1}{n}\mathrm{Tr}(I_n) = 1$.

Let $\{\widetilde{u}_i\}_{i=1}^r$ be any orthonormal basis for $\mathbb{C}^r$ scaled by $\frac{1}{\sqrt{r}}$, and rescale these again to form the vectors $\{u_i\}_{i=1}^r := \{\sqrt{p_i}^{-1}\widetilde{u}_i\}_{i=1}^r$ which still form an orthogonal basis for $\mathbb{C}^r$. Then define the entanglement breaking map E to have Kraus operators $\{u_i v_i^*\}_{i=1}^r$. It is clear that the Choi rank of E is r, from the fact that $\mathrm{range}(E) = \mathrm{span}\{u_i u_i^*\}_{i=1}^r$ and the fact that the $\{u_i\}$ form an orthogonal basis.

Then, for any X, write $X = n^{-1}\mathrm{Tr}(X)I + X_0$ where X_0 is traceless, and observe

$$\begin{aligned} E(\Phi^C(X_0)) &= \sum_{i=1}^{r} u_i v_i^* \Phi^C(X_0) v_i u_i^* \\ &= 0. \end{aligned}$$

That is, E annihilates the traceless part of $\mathrm{range}(\Phi^C)$. Thus it remains to see what E does to $\Phi^C(I)$. This is

$$E(\Phi^C(I)) = \sum_{i=1}^{r} \frac{1}{p_i} \widetilde{u_i} v_i^* \Phi^C(I) v_i \widetilde{u_i}^*$$
$$= n \sum_{i=1}^{r} \frac{p_i}{p_i} \widetilde{u_i} \widetilde{u_i}^*$$
$$= \frac{n}{r} I_r$$

following from the definition of p_i and the fact that $\widetilde{\sqrt{r} u_i}$ form an orthonormal basis for $\mathbb{C}^r$.

Observe that although the map E is not trace-preserving in the usual trace, the range of E, $\text{span}\{u_i u_i^*\}$, is unitarily equivalent to the r-dimensional diagonal algebra, Δ_r; suppose the unitary implementing this is W. Let $P = W^* \text{diag}(p_1, \cdots, p_r) W$, which is clearly a positive definite matrix in the commutant $\text{span}\{u_i u_i^*\}' = \text{span}\{u_i u_i^*\}$, and hence we may define the trace $\text{Tr}_P = \text{Tr}(DW^* PW)$ for $D \in W^* \Delta_r W$, and E is in fact trace-preserving with respect to this new trace. This is because

$$\text{Tr}(\Phi^C(I)) = \text{Tr}(\Phi^C(I) V^* V) = \sum_{i=1}^{r} v_i^* \Phi^C(I) v_i = n \sum_{i=1}^{r} p_i.$$

For the other direction, suppose $E : M_d \to M_r$ exists and has the required property of annihilating the traceless part of $\text{range}(\Phi^C)$ and mapping $\Phi^C(I)$ to a multiple of the identity.

As the range of E is a commutative algebra, Δ, the trace on Δ must have the form $\text{Tr}_\Delta(D) = \frac{1}{n} \text{Tr}(DP)$ for some $P \in \Delta' = \Delta$. Also, for any set of Kraus operators of the form $\{u_i v_i^*\}_{i=1}^m$ $(m \geq r)$ for E, we must have that $u_i u_i^* \in \Delta$, and hence $\{u_i\}$ must contain an orthogonal set of vectors from $\mathbb{C}^r$; though redundancy is possible, there is no loss of generality in assuming the rank-one projections $u_i u_i^*$ are unique; as we know the Choi rank of E is r, the the set $\{u_i\}_{i=1}^r$ is in fact an orthogonal basis.

Then, for any traceless X_0, we have that

$$E(\Phi^C(X_0)) = \sum_{i=1}^{r} \langle v_i, \Phi^C(X_0)v_i \rangle u_i u_i^* = 0$$

and since $\{u_i\}$ are orthogonal, $u_i u_i^*$ are linearly independent and so $v_i^* \Phi^C(X_0) v_i = 0$ for all v.

Finally, since E is trace-preserving between the regular trace on M_d and Tr_Δ, we have that

$$\sum_{i=1}^{r} v_i u_i^* u_i v_i^* = P;$$

hence the matrix V^* with columns $\frac{1}{\|u_i\|} v_i$ is an isometry from $\mathbb{C}^d$ into $\mathbb{C}^r$ with the inner product $\langle v, w \rangle_P = \langle v, Pw \rangle$ with the property that $V\Phi^C(X_0)V^*$ has zeroes on the diagonal. By Lemma 4.4.4, Φ must be random unitary. □

If we consider the statement $E(\Phi^C(X)) = \frac{1}{r}\mathrm{Tr}(X)I_r$, the right side of the equation looks like the complete depolarizing channel let us examine the left side.

Example 4.4.1. In the case of the complete depolarizing channel Φ_{CD}, one can check the channel is implemented as a random unitary channel with the Pauli matrices as follows.

Proof. We have the completely depolarizing channel $\Phi(\rho) : M_2 \to M_2$, and the Pauli matrices $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Our channel is defined as $\Phi(\rho) = \frac{1}{4}(\rho + X\rho X^* + Y\rho Y^* + Z\rho Z^*)$. As ϕ is a density matrix we know for all $\rho \in M_2$ where $\rho \geq 0$ and $Tr(\rho) = 1$. As a results we get

$$\Phi(\rho) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}I$$

and therefore Φ privatizes $\mathcal{H} = \mathbb{C}^2$. □

And one can verify the theorem is satisfied for this channel with Φ^C equal to the identity channel and $E = \Phi_{CD}$.

Chapter 5

Conclusions and Further Work

In this thesis, we show how to obtain a stochastic representation of the Holevo form of entanglement breaking channels. By using this result in concert with Perron-Frobenius theorem we can predict the long term behaviour of an entanglement breaking channel Φ given the stochastic matrix is primitive. If further work is done we may be able to find other conditions that enable the prediction of the behaviour of a channel. We also present examples and discuss connections with quantum privacy and examine the nullspace structure for entanglement breaking channels. When considering the use of quantum information in privacy we prove that every operator space of trace zero matrices is the nullspace of such a channel. This allows us to choose the size of the null space, having a larger null space equates to "more encoded" information. A potential real-world application is information being more difficult to decode and eavesdrop on. Finally, we gave constructions of channels that annihilate subspace of trace zero matrices and discuss a connection with quantum privacy.

This work may be extended by looking at any operator systems which may be useful in identifying different values in a noisy channel. From there we examine their error-correcting codes and identify any practical applications. Another direction of research is to generalize any results to different types of quantum channels if possible. One example is Schur product channels, which are the complement of entanglement breaking channels, where these results could then be applied to quantum error correction. The stochastic representation of Holevo form is an additional tool to use when approaching unsolved problems like the PPT squared conjecture. Potential quantum privacy applications may arise from looking at what the characterizations of quantum channels and their Kraus representation look like. While PageRank inspired the results on the eventual behaviour of a channel it may be interesting to look if different sub-types of entanglement breaking channels converge to the steady state faster and if other types of quantum channels will also converge to a steady state.

Bibliography

[1] Banach, S. Sur les opérations dans les ensembles abstraits et leur application aux équations intégrales. *Fundamenta Mathematicae 3*, 1 (1922), 133–181.

[2] Banach, S. *Théorie des opérations linéaires*. Chelsea Pub Co, 1932.

[3] Benutzer, G. Retraction used in the proof of the Brouwer fixed point theorem., 2006. [Online; accessed October 22, 2019].

[4] Birkhoff, G., and MacLane, S. *A survey of modern algebra*. AK Peters/CRC Press, 2017.

[5] Börm, S., and Mehl, C. *Numerical methods for eigenvalue problems*. Walter de Gruyter, 2012.

[6] Brouwer, L. E. J. Über eineindeutige, stetige Transformationen von Flächen in sich. *Mathematische Annalen 69*, 2 (1910), 176–180.

[7] Choi, M.-D. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications 10*, 3 (1975), 285–290.

[8] Conway, J. B. *A course in functional analysis*, vol. 96. Springer, 2010.

[9] Flanders, H. Elementary divisors of AB and BA. *Proceedings of the American Mathematical Society 2*, 6 (1951), 871–874.

[10] Fréchet, M. M. Sur quelques points du calcul fonctionnel. *Rendiconti del Circolo Matematico di Palermo (1884-1940) 22*, 1 (1906), 1–72.

[11] Frobenius, G. *Über Matrizen aus nicht negativen Elementen*. Königliche Akademie der Wissenschaften Sitzungsber, Kön, 1912.

[12] Gelfand, I., and Naimark, M. On the embedding of normed rings into the ring of operators in Hilbert space. *Annals of Mathematics 48* (1947), 930–948.

[13] Girard, M., Leung, D., Levick, J., Li, C.-K., Paulsen, V., Poon, Y. T., and Watrous, J. On the mixed-unitary rank of quantum channels. *arXiv preprint arXiv:2003.14405* (2020).

[14] Gleich, D. F. Pagerank beyond the web. *SIAM Review 57*, 3 (2015), 321–363.

[15] Griffel, D. H. *Applied functional analysis.* Courier Corporation, 2002.

[16] Halmos, P. R. *Finite-dimensional vector spaces.* Courier Dover Publications, 2017.

[17] Hartig, D. G. The Riesz representation theorem revisited. *The American Mathematical Monthly 90*, 4 (1983), 277–280.

[18] Helly, E. Über Systeme linearer Gleichungen mit unendlich vielen Unbekannten. *Monatshefte für Mathematik 31*, 1 (1921), 60–91.

[19] Hermite, C. Remarque sur un théorème de M. Cauchy. *Comptes rendus hebdomadaires des séances de l'Académie des sciences 41* (1855), 181–183.

[20] Hilbert, D., Neumann, J. v., and Nordheim, L. Über die grundlagen der quantenmechanik. *Mathematische Annalen 98*, 1 (1928), 1–30.

[21] Hoffman, K., and Kunze, R. Linear algebra. *Englewood Cliffs, New Jersey* (1971).

[22] Holevo, A. S. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii 9*, 3 (1973), 3–11.

[23] Holevo, A. S. Entanglement-breaking channels in infinite dimensions. *Problems of Information Transmission 44*, 3 (2008), 171–184.

[24] Holevo, A. S. *Quantum systems, channels, information: a mathematical introduction*, vol. 16. Walter de Gruyter, 2012.

[25] Holevo, A. S., and Shirokov, M. E. On classical capacities of infinite-dimensional quantum channels. *Problems of Information Transmission 49*, 1 (2013), 15–31.

[26] Horodecki, M., Shor, P. W., and Ruskai, M. B. Entanglement breaking channels. *Reviews in Mathematical Physics 15*, 06 (2003), 629–641.

[27] Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K. Quantum entanglement. *Reviews of Modern Physics 81*, 2 (2009), 865.

[28] Jung, C. F. On generalized complete metric spaces. *Bulletin of the American Mathematical Society 75*, 1 (1969), 113–116.

[29] Kreyszig, E. *Introductory functional analysis with applications*, vol. 1. Wiley New York, 1978.

[30] Kribs, D., Levick, J., Olfert, K., Pereira, R., and Rahaman, M. *In Preparation.*

[31] Kribs, D. W. Quantum channels, wavelets, dilations and representations of $\mathcal{O}_n$. *Proceedings of the Edinburgh Mathematical Society 46* (2003), 421–433.

[32] Loewy, A. Ueber Scharen reeller quadratischer und Hermitescher Formen. *Journal für die reine und angewandte Mathematik 122* (1900), 53–72.

[33] Nielsen, M. A., and Chuang, I. *Quantum Computation and Quantum Information.* Cambridge University Press, 2002.

[34] O'Searcoid, M. *Metric spaces.* Springer Science & Business Media, 2006.

[35] Perron, O. Zur Theorie der Matrizen. *Mathematische Annalen 64* (1907), 248.

[36] Pierpont, J. The theory of functions of real variables. *New York 560* (1905).

[37] Popiołek, J. Real normed space. *Formalized Mathematics 2*, 1 (1991), 111–115.

[38] Rahaman, M. A new bound on quantum Wielandt inequality. *IEEE Transactions on Information Theory 66*, 1 (2019), 147–154.

[39] Riesz, F. Sur les opérations fonctionnelles linéaires. *Comptes rendus de l'Académie des Sciences 149* (1909), 974–977.

[40] Rudin, W. *Functional Analysis, McGrawHill.* Inc, New York, 1991.

[41] Ruskai, M. B., Junge, M., Kribs, D., Hayden, P., and Winter, A. Operator structures in quantum information theory. *Final Report, Banff International Research Station* (2012).

[42] Sanz, M., Pérez-García, D., Wolf, M. M., and Cirac, J. I. A quantum version of Wielandt's inequality. *IEEE Transactions on Information Theory 56*, 9 (2010), 4668–4673.

[43] Schur, J. Bemerkungen zur theorie der beschränkten bilinearformen mit unendlich vielen veränderlichen. *Journal für die reine und Angewandte Mathematik 1911*, 140 (1911), 1–28.

[44] Shor, P. W. Capacities of quantum channels and how to find them. *arXiv preprint quant-ph/0304102* (2003).

[45] Varga, R. S. *Iterative analysis.* Springer, 1962.

[46] Von Neumann, J. *Collected works.* Pergamon, 1961.

[47] Von Neumann, J. *Mathematical Foundations of Quantum Mechanics: New Edition.* Princeton university press, 2018.

[48] Watrous, J. *The theory of quantum information.* Cambridge University Press, 2018.

[49] WEYL, H. *Raum, zeit, materie*, vol. 7. Springer, 1918.

[50] YANG, L.-M., LI, T., FEI, S.-M., AND WANG, Z.-X. Entanglement-breaking of quantum dynamical channels. *Quantum Information Processing 18*, 7 (2019), 231.