2020

Conditions for the existence of quantum error correction codes

Daniel Mark Lucas
Iowa State University

Conditions for the existence of quantum error correction codes

by

Daniel Mark Lucas

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Mathematics

Program of Study Committee:

Yiu Tung Poon, Major Professor
Domenico D'Alessandro
Leslie Hogben
Sung Yell Song
Eric Weber

The student author, whose presentation of the scholarship herein was approved by the program of study committee, is solely responsible for the content of this dissertation. The Graduate College will ensure this dissertation is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2020

TABLE OF CONTENTS

ABSTRACT

In this dissertation, we consider quantum errors, represented by quantum channels defined on the space of $n \times n$ complex matrices, M_n. We begin with a quantum channel T defined on M_n. The Kraus operators of this channel can be used to generate an operator system S, which is guaranteed to have a basis of Hermitian matrices $A_1, ..., A_m$ in M_n. Given $k, m \geq 1$, we find a lower bound on n above which there is always an $n \times k$ matrix U with orthonormal columns such that $U^*A_1U, ..., U^*A_mU$ are diagonal $k \times k$ matrices. We then extend this to a lower bound on n above which there is always a k-dimensional quantum error correction code for any quantum channel T on M_n with an associated operator system S with $\dim(S) \leq m + 1$. Such a bound is equivalent to a lower bound on n above which the joint rank-k numerical range of any m Hermitian matrices in M_n is non-empty. So, we further extend our result to a lower bound on n above which the rank-k numerical range of any m Hermitian matrices in M_n is star-shaped.

CHAPTER 1. INTRODUCTION

The latter half of the 20th century saw both the invention and the explosive growth of computer technology. This had such a profound impact on the world that the period from then to the present has been dubbed the Information Age. Electronic computers were first invented in the 1940's, and at the time were incredibly expensive, took up rooms full of space, and had barely a fraction of the computing power of today's scientific calculators. They were also very prone to errors, and were widely considered nothing more than an interesting theoretical idea. However, the invention of the integrated circuit in 1959 and then the microprocessor in 1971 allowed computers to develop from slow, expensive behemoths only owned by government agencies, major universities and research companies to comparatively fast, cheap, personal computers the size of a briefcase.

Even then, computers likely wouldn't have had the impact they've had if not for the invention of the internet in the 60's and 70's. The development of secure, widely accessible and reliably error-free electronic communication changed computers from an information storage and processing device to one of our primary means of communication and a method of engaging in instantaneous transactions. While the idea of packing a transmission with additional data to allow for the detection and correction of errors is initially simple, the discovery of more efficient ways of achieving this have drastically improved transmission rates. Even in the last few years, there has been a leap forward in transmission rates that was only possible because of the application of drastically more efficient error correction algorithms.

As we developed faster and more efficient computing technology and algorithms, we began to discover more and more problems that classical computers are incapable of solving efficiently. A well-known example of one of these problems is the problem of factoring the product of large primes. For two large enough primes a, b, the product ab can take months

to factor, even for some of the most powerful supercomputers in existence. Through the use of a quantum principle called *superposition*, quantum computers can test multiple inputs simultaneously, which allows us to solve some problems like this in a matter minutes or even seconds. However, just as in the early development of classical computers, error correction is a serious hurdle that must be crossed. Quantum states are very sensitive to errors in the hardware, and are particularly vulnerable to interference from outside the system.

In addition, the development of quantum computing will actually give rise to new problems. The reason the example problem of factoring the product of large primes is so well-known is that much of our internet security depends on the difficulty of this problem. The development of privately available quantum or hybrid quantum-classical computers will necessitate a restructuring of security protocols for online interactions. While there are quantum-proof security protocols in classical computing, there is also a phenomenon in quantum mechanics called the wave function collapse that allows for the creation of relatively simple protocols that are theoretically unbreakable. This makes the development of reliable quantum communication an important endeavor, and so there is a looming need for more efficient and robust quantum error correction algorithms. However, some of the same properties of quantum mechanics that make quantum computing such a promising technology also give rise to serious difficulties when it comes to correcting quantum communication errors. The wave function collapse means we have to be able to correct any errors without directly measuring the state that was sent through the communication channel, and because of the superposition principle, errors are continuous linear functions on a vector space, rather than discrete functions on a finite field. While these are difficult problems to overcome, there have been exciting developments in this field over the last several decades.

In this dissertation, we will discuss the development of the field of quantum mechanics from the late 20th century to the present. We start with a description of classical error

correction, then give a brief description of the basic principles of quantum mechanics. One of these principles, called quantum entanglement, allows us obtain some information about a quantum state without directly measuring it. We describe how this fact allows us to import some of the algorithms from classical error correction and adjust them for use in quantum error correction. We describe a method of quantum error correction that can be done without measurement at all, provided we know what errors might occur in transmission and the probability of each error occurring. Finally, we describe the theoretical work that has been done to determine general conditions on a quantum communication channel under which the existence of an error correction algorithm is guaranteed.

CHAPTER 2. BACKGROUND

2.1 Basics of Linear Algebra

There are a variety of ways that quantum information theory can be represented. This dissertation approaches the topic primarily through the lens of linear algebra, and we introduce here some of the basic definitions and concepts that we will use later.

An *inner product space* $\mathcal{V}$ is an n-dimensional vector space over a field F equipped with a function $\langle \cdot, \cdot \rangle : \mathcal{V} \times \mathcal{V} \to F$ s.t.

1. For $x, y \in \mathcal{V}$, $\langle x, y \rangle = \overline{\langle y, x \rangle}$
2. For $x, y, z \in \mathcal{V}$, $a \in F$, $a(\langle x, z \rangle + \langle y, z \rangle) = \langle a(x + y), z \rangle$
3. For all $x \in \mathcal{V}$, $\langle x, x \rangle \geq 0$ and $\langle x, x \rangle = 0$ iff. $x = 0$

Such a functional is called an *inner product* on $\mathcal{V}$. For $\mathcal{H} = \mathbb{C}^n$, we define the inner product as $\langle v, w \rangle = w^* v = \sum_{i=1}^{n} \overline{w}_i v_i$. The inner product induces a metric on $\mathcal{V}$ defined as $||\cdot|| = \sqrt{\langle \cdot, \cdot \rangle}$. If $\mathcal{V}$ is complete with respect to this metric, it is called a *Hilbert space*. For a Hilbert space $\mathcal{H}$, we denote by $M(\mathcal{H})$ the space of linear functions $A : \mathcal{H} \to \mathcal{H}$. When $\mathcal{H} = \mathbb{C}^n$, we may write M_n, instead. For $A \in M(\mathcal{H})$, the *Hermitian adjoint* of A is the function $A^* \in M(\mathcal{H})$ s.t. $\langle Av, w \rangle = \langle v, A^* w \rangle$ for all $v, w \in \mathcal{H}$. For $\mathcal{H} = \mathbb{C}^n$, this can be explicitly defined as the conjugate transpose of A.

Let $A \in M_n$. We call A *normal* if $A^* A = A A^*$. We call A *Hermitian* if $A^* = A$, and we denote the space of all $n \times n$ Hermitian matrices as $\mathcal{H}_n$. We call A *positive semidefinite*, denoted $A \geq 0$, if $\langle Av, v \rangle \geq 0$ for all $v \in \mathbb{C}^n$. We call A *unitary* if $A^* A = I$, where I denotes the identity function on $\mathbb{C}^n$, and we denote the set of all unitary $n \times n$ matrices $\mathcal{U}_n$. We call A *scalar* if $A = \lambda I$ for some $\lambda \in \mathbb{C}$ and *diagonal* if $a_{i,j} = 0$ whenever $i \neq j$, where $a_{i,j}$ is the (i, j)-th entry of A. If A is diagonal, we often describe it using the entries of its main

diagonal as $A = \text{diag}(a_{1,1}, ..., a_{n,n})$. We denote the space of all $n \times n$ diagonal matrices as $\mathcal{D}_n$. The following is a well-known and very useful theorem about Hermitian and positive semidefinite matrices called the Spectral Decomposition Theorem:

Theorem 2.1. *Let $A \in M_n$. Then A is normal if and only if there is a unitary matrix $U \in M_n$ such that*

$$U^*AU = diag(d_{1,1}, ..., d_{n,n}) \text{ for some } d_{1,1}, ..., d_{n,n} \in \mathbb{C}$$

A is Hermitian if and only if it is normal and $d_{1,1}, ..., d_{n,n} \in \mathbb{R}$, and A is positive semidefinite if and only if it is Hermitian and $d_{i,i} \geq 0$ for $1 \leq i \leq n$.

More generally, we can define a matrix space $\mathbb{C}^{m\times n}$ of linear maps $A : \mathbb{C}^n \to \mathbb{C}^m$. This space is itself a Hilbert space, but to define the inner product, we need to define the *trace* of a square matrix $A \in M_n$.

Definition 2.2. Let $A \in M_n$. Then $\text{tr}(A) = \sum_{i=1}^{n} a_{i,i}$.

We can then define the inner product of the matrix space $\mathbb{C}^{m\times n}$ as $\langle A, B\rangle = \text{tr}(B^*A)$ for $A, B \in \mathbb{C}^{m\times n}$. The trace also has several useful properties that may come into play later.

- For $A, B \in M_n$, $a \in \mathbb{C}$, $\text{tr}(aB + C) = a \cdot \text{tr}(B) + \text{tr}(C)$.
- For two matrices A, B s.t. $AB \in M_n$, $\text{tr}(AB) = \text{tr}(BA)$.
- For $A \in M_n$, $\text{tr}(A^*) = \overline{\text{tr}(A)}$.

Let $P \in \mathcal{H}_n$ be s.t. $P^2 = P$. Then P is called an *orthogonal projection*, and there is a $k \leq n$ and a $U \in \mathbb{C}^{n\times k}$ such that $U^*U = I_k$, where I_k is the identity function on $\mathbb{C}^k$, and $P = UU^*$. Conversely, given any k-dimensinoal subspace $\mathcal{K} \subset \mathbb{C}^n$, there is an orthogonal

projection $P \in M_n$ such that $Pv \in \mathcal{K}$ for every $v \in \mathbb{C}^n$ and for every $w \in \mathcal{K}$, there is a $v \in \mathbb{C}^n$ such that $Pv = w$.

For two matrices $A \in \mathbb{C}^{m\times n}, B \in \mathbb{C}^{p\times q}$, the *tensor product* of A and B is the block matrix $A \otimes B = (a_{i,j}B)_{i,j}$. We can then define the tensor product of two matrix spaces, $\mathbb{C}^{m\times n} \otimes \mathbb{C}^{p\times q}$, as the space of all linear combinations of elements of the form $A \otimes B$ for $A \in \mathbb{C}^{m\times n}, B \in \mathbb{C}^{p\times q}$. It is common practice to call the Kronecker product the tensor product for the sake of simplicity, rather than maintaining the distinction. This product has some very useful properties:

- For $A, B \in \mathbb{C}^{m\times n}, C \in \mathbb{C}^{p\times q}$,

$$(A \otimes C) + (B \otimes C) = (A + B) \otimes C \text{ and } (C \otimes A) + (C \otimes B) = C \otimes (A + B).$$

- For $A \in \mathbb{C}^{m\times n}, B \in \mathbb{C}^{p\times q}, c \in \mathbb{C}$, $c(A \otimes B) = (cA) \otimes B = A \otimes (cB)$.
- For $A \in \mathbb{C}^{m\times n}, B \in \mathbb{C}^{n\times m}, C \in \mathbb{C}^{p\times q}, D \in \mathbb{C}^{q\times p}$, $(A \otimes C)(B \otimes D) = (AB) \otimes (CD)$.
- For $A \in \mathbb{C}^{m\times n}, B \in \mathbb{C}^{p\times q}$, $(A \otimes B)^* = (A^*) \otimes (B^*)$.

2.2 Algebraic Geometry

For our main result, we use some theorems from the field of algebraic geometry and so we introduce some of the basic concepts and theorems here. All of these definitions and theorems come from [13].

Definition 2.3. Let V be a vector space of dimension $n+1$ over $\mathbb{C}$. The set of 1-dimensional subspaces of V is called the *n-dimensional projective space* over $\mathbb{C}$, and is denoted $\mathbb{P}^n$.

An element of $\mathbb{P}^n$ can be described using any non-zero vector in the subspace. As such, for $v \in \mathbb{P}^n$, $\lambda \in \mathbb{C} \setminus \{0\}$, $\lambda \cdot v = v$. Because of this particular quirk of the projective plane, *homogeneous* functions play a very important role in algebraic geometry, as we will see soon.

Definition 2.4. Let V be an n-dimensional vector space over a field $\mathbb{F}$. A function f defined on V is *homogeneous* if there is a $d \in \mathbb{N}$ such that for every $a \in \mathbb{F}$,

$$f(ax_1, ax_2, ..., ax_n) = a^d f(x_1, ..., x_n)$$

Then d is called the *degree* of f.

We call a homogeneous polynomial $f : \mathbb{C}^{n+1} \to \mathbb{C}$ of degree d a *form* on $\mathbb{P}^n$. This is equivalent to the condition that every term of f has total degree d. We can now define a *projective variety*.

Definition 2.5. A subset $X \subset \mathbb{P}^n$ is a *projective variety* if there is a finite set of forms $f_1, ..., f_k$ on $\mathbb{P}^n$ such that

$$X = \{v \in \mathbb{P}^n : f_1(v) = \cdots = f_k(v) = 0\}$$

These definitions extend intuitively to the direct product of two projective planes $\mathcal{P}^m \times \mathcal{P}^n$. A polynomial $f : \mathbb{C}^{m+1} \times \mathbb{C}^{n+1} \to \mathbb{C}$ is a form on $\mathbb{P}^n \times \mathbb{P}^m$ if there is some $p, q \in \mathbb{N}$ s.t. for any $(u, v) \in \mathbb{C}^{n+1} \times \mathbb{C}^{m+1}$ and $\mu, \lambda \in \mathbb{C}$, $f(\lambda u, \mu v) = \lambda^p \mu^q f(u, v)$. That is, f is homogeneous in each set of indeterminates independently. Then a subset $X \subset \mathbb{P}^m \times \mathbb{P}^n$ is a projective variety if there is some set of forms $\{f_1, ..., f_k\}$ on $\mathbb{P}^m \times \mathbb{P}^n$ s.t.

$$X = \{(v, w) \in \mathbb{P}^m \times \mathbb{P}^n : f_1(v, w) = \cdots = f_k(v, w) = 0\}$$

For any $m, n \in \mathbb{N}$, there is an embedding called the *Segre embedding* that maps $\mathbb{P}^n \times \mathbb{P}^m$ isomorphically to a projective variety in $\mathbb{P}^{(m+1)(n+1)-1}$. The proof that this embedding is an isomorphism of projective varieties is on page 55 of [13], and relies on a lot of groundwork that is laid earlier in the book, and so we will not include it here. However, we will describe the map itself.

Let $N = (m+1)(n+1)-1$. For $w \in \mathbb{P}^N$, index the entries of w as $w_{i,j}$, where $i = 0, ..., m$ and $j = 0, ..., n$. Then the Segre embedding is defined by the map $\varphi : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^N$, where $\varphi(u, v) = (u_i v_j)_{i,j}$. So, $\mathbb{P}^m \times \mathbb{P}^n$ can be thought of as a projective variety of $\mathbb{P}^{(m+1)(n+1)-1}$. Now, for the main result we use in this dissertation, we will need a definition of the dimension of a projective variety, which requires some setup.

Definition 2.6. Given a projective variety $X \subset \mathbb{P}^n$, a subset $Y \subset X$ is a *subvariety* of X if it is a projective variety.

Definition 2.7. A projective variety $X \subset \mathbb{P}^n$ is *reducible* if there are two subvarieties $X_1, X_2 \subsetneq X$ such that $X_1 \cup X_2 = X$. It is *irreducible* otherwise.

Definition 2.8. The *dimension* of a projective variety $X \subset \mathbb{P}^n$ is the largest integer n such that there is a strictly decreasing chain $Y_0 \supsetneq \cdots \supsetneq Y_n \supsetneq \varnothing$ of length n of irreducible projective subvarieties of X.

It is quite straightforward to build this sequence of projective subvarieties for $\mathbb{P}^m \times \mathbb{P}^n$. Let $Y_0 = \mathbb{P}^m \times \mathbb{P}^n$, for $1 \leq k \leq m$, let $Y_k = \{(v, w) \in \mathbb{P}^m \times \mathbb{P}^n : v_1 = \cdots = v_k = 0\}$, and for $m + 1 \leq k \leq m + n$, let $Y_k = \{(v, w) \in \mathbb{P}^m \times \mathbb{P}^n : v_1 = \cdots = v_m = w_1 = \cdots = w_{k-m} = 0\}$. So, the dimension of $\mathbb{P}^m \times \mathbb{P}^n$ is $m + n$.

This last proposition from [13] is the goal of this section. As with the Segre embedding, the proof of this proposition relies on the groundwork that is laid earlier in the book, and so we do not include it. However, this is a specific application of a very well-known theorem from algebraic geometry called Bezout's Theorem.

Proposition 2.9. *If $r \leq n$, then r forms have a common zero on an n-dimensional projective variety.*

2.3 Classical Error Correction

The basic problem of classical error correction is fairly straightforward. One party, commonly referred to as Alice, transmits a package of n bits to another party, commonly referred to as Bob. Somewhere along the communication line, which is called a *noisy channel*, one or more errors occur, and as a result, the package Bob receives is not the same as the package Alice sent. In this scenario, we then have two *alphabets*, or sets. One of possible n-bit packages Alice could send, $\{x_1, ..., x_N\} = X$, and one of possible packages Bob could receive, $\{y_1, ..., y_M\} = Y$. We can then describe the noisy channel using the column stochastic matrix $\mathcal{N} = \big(p(y_i|x_j)\big)_{i,j}$, where $p(y_i|x_j)$ is the probability that Alice sent x_j, given that Bob received y_i. The problem of error correction is to find some subset $S \subset X$ such that if Alice sends some $x_i \in S$, Bob can determine with an acceptably low probability of error which x_i Alice sent.

To achieve this, we need to construct the *confusability graph* of the channel. A *graph* (V, E) is defined as a set of vertices V connected by a set of edges $E \subseteq V \times V$ such that $(v, v) \notin E$ for all $v \in V$ and if $(v, w) \in E$, $(w, v) \in E$. We can construct the confusability graph of $\mathcal{N}$, $G_{\mathcal{N}}$, by letting X be the set of vertices and defining the edge set as

$$E := \big\{(x_i, x_j) \in X \times X : i \neq j,\ \exists\ \ell \in \{1, ..., M\} \text{ s.t. } p(y_\ell|x_i) \cdot p(y_\ell|x_j) > 0\big\}$$

While we define the edge set this way to allow for a more concise explanation, in practical application, there are sometimes errors that are possible, but exceedingly unlikely, so it can be more practical to begin by artificially setting $p(y_\ell|x_i) = 0$ if $p(y_\ell|x_i) < r$ for some probability threshold $r \geq 0$. We then define the edge set using the simpler matrix. Then clearly, if $(x_i, x_j) \notin E$ and Bob receives some $y_\ell \in Y$ such that $p(y_\ell|x_i) > 0$, then Bob can assume that Alice did not send x_j. If $S \subset X$ is such that $E \cap (S \times S) = \varnothing$, we call S an *independent set*. Then, if Alice sends some $x_i \in S$, Bob can determine without error which x_i Alice sent. One useful tool in finding such independent sets is the *adjacency matrix* of the confusability graph, which is defined as

$$(M_{\mathcal{N}})_{i,j} = \begin{cases} 1 & \text{if} \quad (i,j) \in E \\ 0 & \text{if} \quad (i,j) \notin E \end{cases}$$

Then, for a set $S = \{x_i \in X : i \in \alpha\}$, $\alpha \subset \{1, ..., |X|\}$, S is independent if and only if the submatrix $B[\alpha] = (M_{\mathcal{N}})_{i,j \in \alpha}$ is a zero matrix.

Example. A simple, though admittedly inefficient, example of an error correcting algorithm involves a 3-bit noisy channel in which it is assumed that at most one bit will be corrupted. The vertex set is $X = \{x_0, x_1, ..., x_7\}$, where x_i represents the number i for $0 \leq i \leq 7$. Since at most one error can occur, two numbers can be confused if they differ by two or fewer bits. For example, 000 and 011, after being sent through the noisy channel, both have a chance of becoming the numbers 010 or 001. We call the number of bits that differ between two numbers the *Hamming distance*, denoted $d_H(x, y)$. So, the confusability graph of this noisy channel is $G_{\mathcal{N}} = (X, E)$, where $E = \{(x, y) \in X \times X : d_H(x, y) \leq 2, x \neq y\}$.

We then have the adjacency matrix

$$M_{\mathcal{N}} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Clearly, the only independent sets are $\{x_0, x_7\}, \{x_1, x_6\}, \{x_2, x_5\}, \{x_3, x_4\}$. Any of these sets can be used to design an error correcting algorithm, but the most intuitive method is to use x_0 and x_7, which represent the numbers 000 and 111. Then, whatever bit Alice wants to send, she simply triples it and sends it through the noisy channel. Whatever Bob receives, he chooses the value that is in the majority, and if the assumption that at most one bit is corrupted holds true, that is the value that Alice wanted to send.

Of course, as soon as such an algorithm is found, the question of optimization immediately arises. Given two finite sets X and Y and a noisy channel $\mathcal{N} : X \to Y$, what is the largest cardinality we can achieve for an independent set $S \subset X$? This value is called the *zero error capacity.*

Definition 2.10. Let $\mathcal{N} : X \to Y$ be a noisy channel between two finite alphabets X and Y, and let $G_{\mathcal{N}} = (X, E)$ be the confusability graph of $\mathcal{N}$. Then the *zero error capacity* of $\mathcal{N}$ is

$$\alpha(\mathcal{N}) = \max\{|S| : S \subset X, E \cap (S \times S) = \varnothing\}$$

This value is certainly important, but note that part of the definition of a noisy channel involves a specific number of bits being transmitted, and only some of those bits can actually contain meaningful information. If Alice needs to transmit more bits than the channel can reliably support in a single transmission, she will need to send more than one package. This changes the way we mathematically represent the channel. Let $\mathcal{N}$ be a noisy channel through which Alice sends n-bit numbers from an alphabet X and Bob receives numbers from an alphabet Y, and let $G_{\mathcal{N}} = (X, E)$ be the confusability graph of the channel. Suppose Alice sends two n-bit numbers through the channel. Assuming the channel is the same when Alice transmits each number and that errors occur independently, we have a new channel $\mathcal{N} \times \mathcal{N} : X \times X \to Y \times Y$. There are then three ways that two elements $(x_1, x_2), (x_1', x_2') \in X$ could be confused. Either $(x_1, x_1'), (x_2, x_2') \in E$, $(x_1, x_1') \in E$ and $x_2 = x_2'$ or $x_1 = x_1'$ and $(x_2, x_2') \in E$.

To describe the confusability graph of $\mathcal{N} \times \mathcal{N}$, we will need a few more tools from graph theory. First, let $G = (V, E)$ be a graph, and let $x, y \in V$. We write $x \simeq y$ if $(x, y) \in E$ or $x = y$. We can now define the *strong product* of two graphs.

Definition 2.11. Let $G = (V_1, E_1), H = (V_2, E_2)$ be graphs. Let $V = V_1 \times V_2$ and define $E \subset V \times V$ as

$$E := \{(a, b, c, d) \in V \times V : a \simeq c, b \simeq d, (a, b) \neq (c, d)\}$$

Then the *strong product* of G and H is $G \boxtimes H = (V, E)$.

Clearly, $G_{\mathcal{N} \times \mathcal{N}} = G_{\mathcal{N}} \boxtimes G_{\mathcal{N}}$. In a similar way, we can extend this to k uses of the noisy channel, and then the channel is $\mathcal{N}^k$ with the confusability graph $G_{\mathcal{N}}^{\boxtimes k}$.

2.4 Postulates of Quantum Mechanics

In order to describe error correction in quantum communication, we need a basic description of quantum mechanics, how information is encoded in quantum states, and how to represent an error in quantum communication. The field of quantum mechanics is based on a set of axiomatic postulates. These are described in a variety of different ways, each of which represents a particular interpretation of the physical facts that have been observed through experimentation. The following postulates are taken from [2], and they represent one interpretation of quantum mechanics that is particularly convenient for use in the field of quantum information theory.

Since we are introducing this in the context of quantum information theory, we will use what is called *Bra-ket notation* in this section. In this notation, standard basis vectors in $\mathbb{C}^n$ are written as $|0\rangle, ..., |n-1\rangle$, the conjugate transpose of a vector $|x\rangle \in \mathbb{C}^n$ is written as $\langle x|$, and for two vectors $|x\rangle, |y\rangle \in \mathbb{C}^n$, the inner product is written $\langle y|x\rangle$ and the tensor product can either be written $|x\rangle|y\rangle$ or $|xy\rangle$.

Postulate 2.1. *Associated to any isolated physical system is a Hilbert space $\mathcal{H}$ known as the* state space *of the system. The system is completely described by its state vector $|v\rangle \in \mathcal{H}$ such that $||v|| = 1$.*

The simplest quantum mechanical system, and the system which we will be most concerned with, is the qubit. A qubit has a two-dimensional state space. Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for that state space. Then an arbitrary state vector in the state space can be written

$$|\psi\rangle = a|0\rangle + b|1\rangle \text{ for some } a, b \in \mathbb{C} \text{ such that } |a|^2 + |b|^2 = 1$$

In quantum information theory, we usually work using qubits for a variety of reasons, one of which is that it allows us to import many of the algorithms from classical computing with fewer adjustments. Intuitively, the states $|0\rangle$ and $|1\rangle$ are analogous to the two values 0 and 1 which a bit may take. The way a qubit differs from a bit is that *superpositions* of these two states, of the form $a|0\rangle + b|1\rangle$, can also exist, in which it is not possible to say that the qubit is definitely in the state $|0\rangle$, or definitely in the state $|1\rangle$.

For example, when a photon hits a half-silvered mirror, it can either be reflected or pass through, and we can represent these two states using the standard basis vectors of $\mathbb{C}^2$, e_1 and e_2, respectively. Then the principle of superposition states that any unit vector in $\mathbb{C}^2$ also describes a possible state of the photon. In other words, it is possible that the photon passes through and is reflected, and therefore occupies two different physical locations at the same time.

Postulate 2.2. *The evolution of a closed quantum system (a system that is protected from uncontrolled outside forces) is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,*

$$|\psi'\rangle = U|\psi\rangle$$

One of the more mysterious aspects of quantum mechanics is the fact that simply measuring a quantum state actually changes it. This effect is called the *wave function collapse*, and it is described in the next postulate.

Postulate 2.3. *Quantum measurements are described by a collection $A_m \in M_n$ of* measurement operators*, called a* measurement system*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is*

$$p(m) = \langle\psi|A_m^* A_m|\psi\rangle,$$

and the state of the system after the measurement is

$$\frac{A_m|\psi\rangle}{\sqrt{\langle\psi|A_m^* A_m|\psi\rangle}}$$

The measurement operators satisfy the completeness equation*,*

$$\sum_m A_m^* A_m = I$$

A simple example of a measurement system is $M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|$. Then, given a state $|\psi\rangle = a|0\rangle + |1\rangle$, the probability that the measurement outcome is 0 is $|a|^2$, and the probability that it is 1 is $|b|^2$.

This brings us to another interesting problem in quantum mechanics, that of distinguishing between different quantum states. A set of states $\{|x_1\rangle, ..., |x_k\rangle\}$ is *perfectly distinguishable* if there is a measurement system $\{A_1, ..., A_k\}$ such that $\langle x_i|A_j^* A_j|x_i\rangle = \delta_{i,j}$. The following well-known result is proved in [12], and gives a much simpler equivalent condition to this definition:

Theorem 2.12. *A set $\{|x_1\rangle, ..., |x_k\rangle\} \in \mathbb{C}^n$ is perfectly distinguishable if and only if it is orthonormal.*

Proof. Suppose $\{|x_1\rangle, ..., |x_k\rangle\} \subset \mathbb{C}^n$ is orthonormal, and define $A_i = |x_i\rangle\langle x_i|$. Then

$$\langle x_i|A_j^* A_j|x_i\rangle = |\langle x_i|x_j\rangle|^2 = \delta_{i,j}$$

So $\{|x_1\rangle, ..., |x_k\rangle\}$ is perfectly distinguishable.

Suppose $\{|x_1\rangle, ..., |x_k\rangle\} \subset \mathbb{C}^n$ is perfectly distinguishable. Then for some measurement system $\{A_1, ..., A_k\}$ such that $\langle x_i|A_j^* A_j|x_i\rangle = \delta_{i,j}$. For $|x_i\rangle, |x_j\rangle$, there are some $|y\rangle \in \mathbb{C}^n$ s.t. $||y|| = 1$, $\langle x_j|r\rangle = 0$ and $|x_i\rangle = a|x_j\rangle + b|y\rangle$, where $|a|^2 + |b|^2 = 1$. Then, since $\langle x_j|A_i^* A_i|x_j\rangle = 0$,

$$1 = \langle x_i|A_i^* A_i|x_i\rangle = \langle ax_j + by|A_i^* A_i|ax_j + by\rangle = |b|^2$$

So, $a = 0$. Then $\langle x_i|x_j\rangle = 0$, and therefore $\{|x_1\rangle, ..., |x_k\rangle\}$ is orthonormal. □

The next postulate deals with composite quantum systems made up of two or more quantum systems.

Postulate 2.4. *The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is*

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle.$$

This allows us to describe one of the most interesting features of quantum mechanics, *entanglement*. Consider the two qubit state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

There are no $|x\rangle, |y\rangle \in \mathbb{C}^2$ such that $|\psi\rangle = |x\rangle|y\rangle$, since that would require the existence of $x_1, x_2, y_1, y_2 \in \mathbb{C}$ s.t. $x_1 y_1 = x_2 y_2 = \frac{1}{\sqrt{2}}$, which implies x_1, x_2, y_1, y_2 are all nonzero, and

$x_1y_2 = x_2y_1 = 0$, which requires at least two of x_1, x_2, y_1, y_2 to be zero. This illustrates what it means for a quantum state to be *entangled*.

Definition 2.13. Let $|v\rangle \in \mathbb{C}^m \otimes \mathbb{C}^n$. We call $|v\rangle$ *separable* if there are $|x\rangle \in \mathbb{C}^m, |y\rangle \in \mathbb{C}^n$ such that $|v\rangle = |x\rangle|y\rangle$. We call $|v\rangle$ *entangled* otherwise.

Entanglement is one of the most incredible and mysterious aspects of quantum mechanics, because when two particles are entangled, operations performed on one particle affect the other particle *regardless of the distance between them*. For example, consider the state $|\psi\rangle$ defined earlier. If the second qubit is measured and gives the state $|0\rangle$, that change can be represented by the measurement operator $U = I_2 \otimes (|0\rangle\langle 0|)$, and the resulting state of the entire system is

$$\frac{U|\psi\rangle}{\sqrt{\langle\psi|U^*U|\psi\rangle}} = |00\rangle$$

So both qubits underwent a wave function collapse, not just the second qubit.

Now that we have a way of representing any given quantum state, we can describe how numbers are encoded in quantum states. If we have a number $a \in \mathbb{N}$ such that $a \leq 2^n$, we can write a as an n-bit binary number, and then represent it using n qubits as the state $|a\rangle$. For example, if we want to represent the number 3 using a system of 5 qubits, we use the state $|00011\rangle \in \mathbb{C}^{32}$.

We cannot always determine uniquely the state of a quantum system, and so we consider the collection of possible states $|x_1\rangle, ..., |x_r\rangle$ that the system may be in and the probabilities $p_1, ..., p_r$, where $\sum_{i=1}^{r} p_i = 1$, that each state is the actual state of the system. We then describe the state of the system using the matrix $\rho = \sum_{i=1}^{r} p_i|x_i\rangle\langle x_i|$. If $r > 1$, we call ρ a *mixed state*, otherwise it is called a *pure state*. We call such a matrix a *density matrix*.

Let $\rho = \sum_{i=1}^{r} p_i |x_i\rangle\langle x_i|$ for some $|x_1\rangle, ..., |x_r\rangle \in \mathbb{C}^n$, $p_1, ..., p_r \in [0,1]$ s.t. $\sum_{i=1}^{r} p_i = 1$, and let $|v\rangle \in \mathbb{C}^n$. Then

$$\langle v|\rho|v\rangle = \sum_{i=1}^{r} p_i \langle v|x_i\rangle\langle x_i|v\rangle = \sum_{i=1}^{r} p_i |\langle v|x_i\rangle|^2 \geq 0,$$

so $\rho \geq 0$. Furthermore, $\mathrm{tr}(\rho) = \sum_{i=1}^{r} p_i \cdot \mathrm{tr}(|x_i\rangle\langle x_i|) = \sum_{i=1}^{r} p_i \cdot \mathrm{tr}(\langle x_i|x_i\rangle) = 1$.

With this new representation of quantum states, we need an equivalent representation of measurement for density matrices. We maintain the same definition of measurement system. Let $\{A_i : 1 \leq i \leq r\}$ be a measurement system. Then for a pure state $\rho = |x\rangle\langle x|$, we have

$$\mathrm{tr}(A_i \rho A_i^*) = \mathrm{tr}(A_i |x\rangle\langle x| A_i^*) = \langle x|A_i^* A_i|x\rangle = p(i),$$

so, the probability that measuring the mixed state ρ will result in outcome i is $p_i = \mathrm{tr}(A_i \rho A_i^*)$.

Definition 2.14. The mixed states $\rho_1, ..., \rho_d \in M_n$ are *perfectly distinguishable* if there is a measurement system $\{A_1, ..., A_k\}$, $k \geq d$, such that $\mathrm{tr}(A_i \rho_j A_i^*) = \delta_{i,j}$ for $1 \leq i, j \leq d$.

There is, again, a well-known and simple equivalent condition in [12].

Theorem 2.15. *A collection of density matrices $\{\rho_1, ..., \rho_d\} \subset M_n$ is perfectly distinguishable if and only if $\rho_i \rho_j = 0$ for $i \neq j$.*

Proof. Suppose $\{\rho_1, ..., \rho_d\} \subset M_n$ are density matrices such that $\rho_i \rho_j = 0$ for $i \neq j$. For $1 \leq i \leq d-1$, let P_i be the orthogonal projection onto the subspace $\mathrm{ran}(\rho_i) = \{\rho_i v : v \in \mathbb{C}^n\}$. Then $\sum_{i=1}^{d-1} P_i$ is an orthognal projection, so $P_d = I - \sum_{i=1}^{d-1} P_i$ is an orthogonal projection. Then we have $\sum_{i=1}^{d} P_i = I$, so $\{P_1, ..., P_d\}$ is a measurement system.

Since $\text{ran}(\rho_d) \subset \text{ran}(P_d)$ and $\text{ran}(\rho_i) = \text{ran}(P_i)$ for $1 \leq i \leq d-1$,

$$\text{tr}(P_i \rho_j P_i^*) = \text{tr}(P_i \rho_j) = \text{tr}(\delta_{i,j} \rho_j) = \delta_{i,j}$$

Now suppose $\{\rho_1, ..., \rho_d\} \subset M_n$ is perfectly distinguishable. Then there is a measurement system $\{A_1, ..., A_d\}$ such that $\text{tr}(A_i \rho_j A_i^*) = \delta_{i,j}$. First of all, note that for any $A \geq 0$, there is a $U \in \mathcal{U}_n$ and a diagonal $D \geq 0$ s.t. $A = U^* D U$. Then $\text{tr}(A) = \text{tr}(U^* D U) = \text{tr}(D) = \sum_{i=1}^{n} d_{i,i}$, so $\text{tr}(A) = 0$ if and only if $A = 0$. We will use this fact later in the proof.

Now, we want to show that $\text{tr}(A_i \rho_j A_i^*) = \text{tr}(\rho_j A_i^* A_i) = 0$ if and only if $\rho_j A_i^* A_i = 0$. One direction is obvious, so we only need to prove that $\rho_j A_i^* A_i = 0$ if $\text{tr}(\rho_j A_i^* A_i) = 0$. For ease of reference let $P = \rho_j$ and $Q = A_i^* A_i$, and suppose $\text{tr}(PQ) = 0$. Then $P, Q \geq 0$, so there is a unitary U such that $U^* P U = D = \text{diag}(d_1, ..., d_k, 0, ..., 0) \geq 0$. Let $\tilde{Q} = U^* Q U$. Then

$$\sum_{i=1}^{k} d_i \tilde{q}_{i,i} = \text{tr}(D\tilde{Q}) = \text{tr}((U^* P U)(U^* Q U)) = \text{tr}(PQ) = 0,$$

so $\tilde{q}_{i,i} = 0$ for $1 \leq i \leq k$. We can write $\tilde{Q}$ as the block matrix $\tilde{Q} = \begin{bmatrix} \tilde{Q}_{1,1} & \tilde{Q}_{1,2} \\ \tilde{Q}_{1,2}^* & \tilde{Q}_{2,2} \end{bmatrix}$, where $\tilde{Q}_{1,1} \in M_k$. Since $\tilde{Q} \geq 0$, $\tilde{Q}_{1,1} \geq 0$, and therefore $\tilde{Q}_{1,1} = 0$. Then for $v \in \mathbb{C}^k$ and $h \in \mathbb{C}^{n-k}$,

$$\left\langle \begin{bmatrix} v \\ h \end{bmatrix}, \tilde{Q} \begin{bmatrix} v \\ h \end{bmatrix} \right\rangle = \langle v, \tilde{Q}_{1,2} h \rangle + \langle h, \tilde{Q}_{1,2}^* v + \tilde{Q}_{2,2} h \rangle$$

For some $r > 0$, let $v = -r\tilde{Q}_{1,2} h$. Then the inner product becomes

$$-2r||\tilde{Q}_{1,2} h||^2 + \langle h, \tilde{Q}_{2,2} h \rangle$$

Let $r \to \infty$. Since $\tilde{Q} \geq 0$, this inner product must always be positive, so $||\tilde{Q}_{1,2} h||^2 = 0$.

Since h was an arbitrary vector, $\tilde{Q}_{1,2} = 0$. So, $\tilde{Q} = \begin{bmatrix} 0 & 0 \\ 0 & \tilde{Q}_{2,2} \end{bmatrix}$. Then for all $v, w \in \mathbb{C}^n$, $Dv \in \text{span}(e_1, ..., e_k)$ and $\tilde{Q}w \in \text{span}(e_{k+1}, ..., e_n)$, so

$$0 = v^* D\tilde{Q}w = v^* U^* PUU^* QUw = v^* U^* PQUw$$

Since $U \in \mathcal{U}_n$, this is equivalent to $v^* PQw = 0$ for all $v, w \in \mathbb{C}^n$. Then $PQ = 0$. Note that this proof is still valid for any $P, Q \geq 0$, $P, Q \in M_n$.

So, $\text{tr}(\rho_j A_i^* A_i) = 0$ if and only if $\rho_j A_i^* A_i = 0$. We also have $\text{tr}(\rho_i A_i^* A_i) = 1 = \text{tr}(\rho_i)$, since ρ_i is a density matrix. Then $\text{tr}(\rho_i(I - A_i^* A_i)) = 0$. Since $I - A_i A_i^* = \sum_{j \neq i} A_j A_j^* \geq 0$ and $\rho_i \geq 0$, $\rho_i(I - A_i^* A_i) = 0$, and therefore $\rho_i = \rho_i A_i^* A_i$. Then, for $i \neq j$, we have

$$\rho_i \rho_j = \rho_i A_i^* A_i \rho_j = \rho_i \cdot 0 = 0,$$

since $\text{tr}(A_i^* A_i \rho_j) = \text{tr}(A_i \rho_j A_i^*) = 0$. □

CHAPTER 3. QUANTUM ERROR CORRECTION

3.1 Quantum Confusability Graph and Zero Error Capacity

Since quantum communication sends information encoded in quantum states, any error that occurs during transmission would be a physical event that transforms the original quantum state into a new quantum state. We call such an operation a *quantum channel*, and we represent it using a linear map $\Phi : M(\mathcal{H}) \to M(\mathcal{K})$, where $M(\mathcal{H})$ is the space of endomorphisms on $\mathcal{H}$. Since Φ must map quantum states to quantum states, we must have $\Phi(\rho) \geq 0$ if $\rho \geq 0$ and $\text{tr}(\Phi(\rho)) = \text{tr}(\rho)$ for all $\rho \in M(\mathcal{H})$. We call such maps *positive* and *trace preserving*. Furthermore, since we can take a physical operation and apply it to every particle in a multipartite state simultaneously, Φ must also be *completely positive*.

Definition 3.1. Let $\Phi : M(\mathcal{H}) \to M(\mathcal{K})$ be linear. Then Φ is *completely positive* if $(I_n \otimes \Phi)(\rho) \geq 0$ for all positive semidefinite $\rho \in M(\mathcal{H}^{\otimes n})$ for all $n \geq 1$.

We have a very convenient representation for completely positive maps in the following well-known theorem proven by Choi in [1], usually referred to as Choi's Theorem:

Theorem 3.2. *Let $\Phi : M_n \to M_d$ be linear. Then the following are equivalent:*
(1) Φ is completely positive.
(2) $C_\Phi = [\Phi(e_i e_j^*)]_{i,j=1}^n \geq 0$, where $e_1, ..., e_n$ are the standard basis vectors for $\mathbb{C}^n$.
(3) There are some $F_1, ..., F_r \in \mathbb{C}^{d \times n}$ s.t. $\Phi(X) = \sum_{i=1}^{r} F_i X F_i^*$ for all $X \in M_n$.

Proof. We begin by proving that (1)⇒(2). Let $\Phi : M_n \to M_d$ be completely positive, and let $Q = (e_i e_j^*)_{i,j=1}^n$, where $e_1, ..., e_n$ are the standard basis vectors for $\mathbb{C}^n$. Then

$$Q^* = \left((e_i e_j^*)_{i,j=1}^n\right)^* = ((e_j e_i)^*)_{i,j=1}^n = (e_i e_j^*)_{i,j=1}^n = Q$$

and

$$Q^2 = \left(\sum_{k=1}^{n}(e_i e_k^*)(e_k e_j^*)\right)_{i,j=1}^{n} = \left(\sum_{k=1}^{n} e_i e_j^*\right)_{i,j=1}^{n} = nQ$$

Then for any eigenvector v of Q, if λ is its corresponding eigenvector, we have

$$\lambda^2 x = Q^2 x = nQx = n\lambda x,$$

so $\lambda = 0$ or n, and therefore $Q \geq 0$. Then, since Φ is completely positive,

$$(I_n \otimes \Phi)(Q) = \left(\Phi(e_i e_j^*)\right)_{i,j=1}^{n} \geq 0$$

Now we prove (2)⇒(3). Let $\Phi : M_n \to M_d$ be linear such that $C_\Phi \geq 0$, and let $v_1, ..., v_K \in \mathbb{C}^{nd}$ be unit eigenvectors of C_Φ with norms equal to the square root of their associated eigenvalues. Then

$$C_\Phi = \sum_{i=1}^{K} v_i v_i^*$$

Then for $1 \leq i \leq K$, there is a set of n vectors $h_1^{(i)}, ..., h_n^{(i)} \in \mathbb{C}^d$ such that $v_i = \begin{bmatrix} h_1^{(i)} \\ \vdots \\ h_n^{(i)} \end{bmatrix}$.

Then for $1 \leq i \leq K$, define $B_i = \begin{bmatrix} h_1^{(i)} & \cdots & h_n^{(i)} \end{bmatrix}$. Then $B_i \in \mathbb{C}^{d \times n}$, so if we define

$$\Psi(X) = \sum_{i=1}^{K} B_i X B_i^*,$$

Ψ is a linear map from M_n to M_d. Since $\Psi(e_i e_j^*) = \sum_{\ell=1}^{K} h_i^{(\ell)} (h_j^{(\ell)})^*$ is equal to the (i,j)-th $d \times d$ block submatrix of C_Φ, we have $\Psi(e_i e_j^*) = \Phi(e_i e_j^*)$ for $1 \leq i, j \leq n$.

Since the set $\{e_i e_j^* : 1 \leq i, j \leq n\}$ is a basis for M_n and Φ, Ψ are both linear maps,

$$\Phi(X) = \Psi(X) = \sum_{i=1}^{K} B_i X B_i^* \text{ for all } X \in M_n.$$

Finally, we prove (3)→(1). Let $Q = (X_{i,j})_{i,j=1}^{p} \in M_p(M_n)$ be positive semidefinite. Then

$$(I_p \otimes \Phi)(Q) = (\Phi(X_{i,j}))_{i,j} = \left(\sum_{i=1}^{r} F_i X_{i,j} F_i^* \right)_{i,j} = \sum_{i=1}^{r} (B_k X_{i,j} B_k^*)_{i,j} \geq 0,$$

since the sum of positive semidefinite matrices is positive semidefinite. Then $(I_p \otimes \Phi)$ is positive for arbitrary p, and therefore Φ is completely positive. □

Then, if $\Phi : M_n \to M_d$ is completely positive, we have

$$\text{tr}(\Phi(X)) = \text{tr}\left(\sum_{i=1}^{r} F_i X F_i^* \right) = \text{tr}\left(\sum_{i=1}^{r} F_i^* F_i X \right)$$

This is equal to $\text{tr}(X)$ for all $X \in M_n$ iff. $\sum_{i=1}^{r} F_i^* F_i = I_n$.

Now that we have a way to describe errors, we turn to the theory of correcting them. The most obvious method is to take our inspiration from classical error correction. We want to find a set $\{x_1, ..., x_k\}$ of perfectly distinguishable states such that $\{\Phi(x_1 x_1^*), ..., \Phi(x_k x_k^*)\}$ are perfectly distinguishable. The existence of such a set would allow Bob to determine without error which state Alice sent, although it would not necessarily allow Bob to actually recover that state.

Given a quantum channel $\Phi : M_n \to M_d$, what is the largest perfectly distinguishable subset $\{x_1, ..., x_k\} \subset \mathbb{C}^n$ s.t. $\{\Phi(x_1 x_1^*), ..., \Phi(x_k x_k^*)\}$ is perfectly distinguishable? By analogy to classical error correction, we define the zero error capacity of a quantum channel as follows:

Definition 3.3. Let $\Phi : M_n \to M_d$ be a quantum channel. Then the *zero error capacity* of Φ is

$$\alpha(\Phi) = \max\left\{k \in \mathbb{N} : \exists\, \{x_1, ..., x_k\} \subset \mathbb{C}^n \text{ s.t. for } i, j \in [k], i \neq j, x_i^* x_j = \Phi(x_i x_i^*)\Phi(x_j x_j^*) = 0\right\}$$

The following theorem from [12] gives a useful equivalent condition to the existence of such a subset:

Theorem 3.4. *Let $\Phi : M_n \to M_d$ be a TPCP map defined as $\Phi(X) = \sum_{i=1}^{r} F_i X F_i^*$ for all $X \in M_n$, and let $\{x_1, ..., x_k\} \subset \mathbb{C}^n$ be orthonormal. Then for $i \neq j$, $1 \leq i, j \leq k$, $\Phi(x_i x_i^*)\Phi(x_j x_j^*) = 0$ if and only if $x_i^* F_\ell^* F_m x_j = 0$ for $1 \leq \ell, m \leq r$.*

Proof. Suppose $\Phi(x_i x_i^*) \cdot \Phi(x_j x_j^*) = 0$ for $i \neq j$. Recall from the proof of 2.15 that since $\Phi(x_i x_i^*) \geq 0$ for $1 \leq i \leq k$, $\Phi(x_i x_i^*)\Phi(x_j x_j^*) = 0$ if and only if $\operatorname{tr}(\Phi(x_i x_i^*)\Phi(x_j x_j^*)) = 0$. We have

$$\begin{aligned}
\operatorname{tr}\left(\left(\sum_{\ell=1}^{r} F_\ell x_i x_i^* F_\ell^*\right)\left(\sum_{m=1}^{r} F_m x_j x_j^* F_m^*\right)\right) &= \sum_{\ell,m=1}^{r} \operatorname{tr}(F_\ell x_i x_i^* F_\ell^* F_m x_j x_j^* F_m^*) \\
&= \sum_{\ell,m=1}^{r} \langle F_m x_j, F_\ell x_i\rangle \cdot \operatorname{tr}(F_\ell x_i x_j^* F_m^*) \\
&= \sum_{\ell,m=1}^{r} \langle F_m x_j, F_\ell x_i\rangle \cdot \langle F_\ell x_i, F_m x_j\rangle \\
&= \sum_{\ell,m=1}^{r} |\langle F_m x_j, F_\ell x_i\rangle|^2
\end{aligned}$$

So, $\operatorname{tr}(\Phi(x_i x_i^*)\Phi(x_j x_j^*)) = 0$ if and only if $|\langle F_m x_j, F_\ell x_i\rangle| = 0$ for $1 \leq \ell, m \leq r$. Then $\Phi(x_i x_i^*)\Phi(x_j x_j^*) = 0$ if and only if $F_\ell x_i \perp F_m x_j$ for $1 \leq i, j \leq m$. □

This equivalent condition leads us to the concept of *operator systems*, which are defined as follows:

Definition 3.5. Let $S \subset M_n$ be a subspace of M_n. Then S is an *operator system* if:

(1) $I \in S$

(2) If $A \in S$, $A^* \in S$.

Let $\Phi : M_n \to M_d$ be a TPCP channel defined as $\Phi(X) = \sum_{i=1}^{r} F_i X F_i^*$, and define

$$S_\Phi = \text{span}(F_i^* F_j : 1 \leq i, j \leq r)$$

Clearly, if $F_i^* F_j \in S_\Phi$, then $(F_i^* F_j)^* = F_j^* F_i \in S_\Phi$, and since Φ is trace-preserving, $\sum_{i=1}^{r} F_i^* F_i = I$, so S_Φ is an operator system. For an operator system S, an orthonormal set $\{x_1, ..., x_k\} \subset \mathbb{C}^n$ s.t.

$$\text{tr}(A x_i x_j^*) = x_j^* A x_i = 0$$

for all $i \neq j$, $1 \leq i, j \leq k$ and all $A \in S_\Phi$ is called a *S-independent set* of size k. Then the condition given in Theorem 3.4 is equivalent to the condition $\{x_1, ..., x_k\}$ is an S_Φ-independent set.

Note that, while a quantum channel Φ defines an operator system S_Φ, different quantum channels can have the same operator system. A trivial example would be $\Phi(X) = I_n X I_n$ and $\Psi(X) = \begin{bmatrix} I_n \\ 0 \end{bmatrix} X \begin{bmatrix} I_n & 0 \end{bmatrix}$. So, when we find a S_Φ-independent set of size k, the we can use the same set to design an error correcting algorithm for any quantum channel that shares an operator system with Φ.

Operator systems are also sometimes called *noncommutative graphs* in the context of error correction because they can be seen as a generalization of the confusability graph of a noisy channel, which we considered in classical error correction. We can illustrate this fact by constructing the operator system of a classical noisy channel. Let $\mathcal{N} : X \to Y$ be a classical noisy channel, and for $1 \leq i \leq |X|, 1 \leq j \leq |Y|$, define $F_{i,j} = \sqrt{p(y_j|x_i)} \hat{e}_j e_i^*$, where

$e_1, ..., e_{|X|}$ and $\hat{e}_1, ..., \hat{e}_{|Y|}$ are the standard basis vectors of $\mathbb{C}^{|X|}$ and $\mathbb{C}^{|Y|}$, respectively. Define $\Phi_{\mathcal{N}} : M_{|X|} \to M_{|Y|}$ as

$$\Phi_{\mathcal{N}}(\rho) = \sum_{i=1}^{|X|} \sum_{j=1}^{|Y|} F_{i,j} \rho F_{i,j}^* \text{ for } \rho \in M_{|X|}$$

By construction, $\Phi_{\mathcal{N}}$ is completely positive, and

$$\sum_{i,j} F_{i,j}^* F_{i,j} = \sum_i \left(\sum_j p(y_j|x_i) \right) e_i e_i^* = \sum_i e_i e_i^* = I$$

So, $\Phi_{\mathcal{N}}$ is also trace-preserving, and is therefore a quantum channel. We can then define the operator system of $\mathcal{N}$ as

$$S_{\mathcal{N}} = \text{span}(F_{h,i}^* F_{j,\ell} : 1 \leq h, j \leq |X|, 1 \leq i, \ell \leq |Y|)$$

If we represent $x_i \in X$ with $e_i e_i^*$ for $1 \leq i \leq |X|$, we have

$$\Phi_{\mathcal{N}}(e_i e_i^*) = \sum_{j=1}^{|Y|} p(y_j|x_i) \hat{e}_j \hat{e}_j^*$$

So, for $1 \leq h < i \leq |X|$,

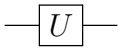
$$\Phi_{\mathcal{N}}(e_h e_h^*) \Phi_{\mathcal{N}}(e_i e_i^*) = \left(\sum_{j=1}^{|Y|} p(y_j|x_h) \hat{e}_j \hat{e}_j^* \right) \left(\sum_{j=1}^{|Y|} p(y_j|x_i) \hat{e}_j \hat{e}_j^* \right) = \sum_{j=1}^{|Y|} p(y_j|x_h) \cdot p(y_j|x_i) \hat{e}_j \hat{e}_j^*$$

This is zero if and only if $p(y_j|x_h) \cdot p(y_j|x_i) = 0$ for $1 \leq j \leq |Y|$, so if $G_{\mathcal{N}}$ is the confusability graph of $\mathcal{N}$, by Theorem 3.4, a set $T = \{x_{i_1}, ..., x_{i_k}\} \subset X$ is independent if and only if $\{e_{i_1}, ..., e_{i_k}\}$ is a $S_{\mathcal{N}}$-independent set. So we see that in the field of error correction, $S_{\mathcal{N}}$ acts as a generalization of $G_{\mathcal{N}}$.

3.2 Quantum Error Correcting Codes

We now come to the problem of quantum error correction. When describing quantum error correction algorithms, it is common practice to return to representing quantum states as vectors, written in bra-ket notation, since it makes descriptions of these algorithms more clear.

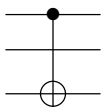
Operations performed on quantum states are called quantum *gates* in this context, and are represented using unitary matrices. It is also convenient to represent these gates graphically, particularly the CNOT gate that we will use repeatedly in this section. A gate U that is only applied to a single qubit is depicted as



When a quantum gate U has dimension 2^n for some $n > 1$, we use a similar graphical representation, simply extending it to cover all of the affected qubits. We can also abuse this notation somewhat and use the same graphical representation to represent the state undergoing a quantum channel. The gates are applied from left to right, and we will now describe the CNOT gate, which is used several times in this section. The CNOT gate has a control bit and a target bit. If the control bit is 0, the gate does nothing. If the control bit is 1, the gate changes the value of the target bit from 1 to 0 or vice versa. In the simple example of a CNOT gate on two qubits, this is represented by the matrix

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Of course, it becomes much more difficult to describe this matrix when dealing with more than two qubits, particularly if there are intervening bits between the control bit and the target bit. This is where the graphical representation becomes much more convenient. The following is a CNOT gate applied on a system of three qubits, with the first bit as the control and the third as the target:

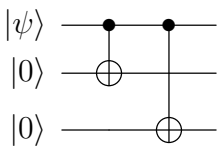


We use the $\bullet$ to indicate the control bit and the $\oplus$ to represent the target. We to indicate the initial state of a qubit, we write its quantum state as a bra vector at the beginning of the line that represents it. For example, if the qubit is in the state $|\psi\rangle$, we would write

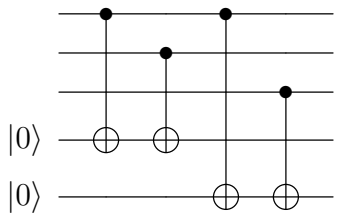
$$|\psi\rangle \ —$$

We can now give an example of a simple quantum error correction algorithm which draws its inspiration from the example of classical error correction that we discussed earlier. Just as the classical example uses a 3-bit channel, this algorithm involves a quantum channel $\Phi : M_8 \to M_8$ that has a low probability of "flipping" one of the qubits in the standard basis vectors $|000\rangle, |001\rangle, ..., |111\rangle$. For example, if it flips the second bit, it would map $|i0j\rangle$ to $|i1j\rangle$ and vice versa for $i, j \in \{0, 1\}$.

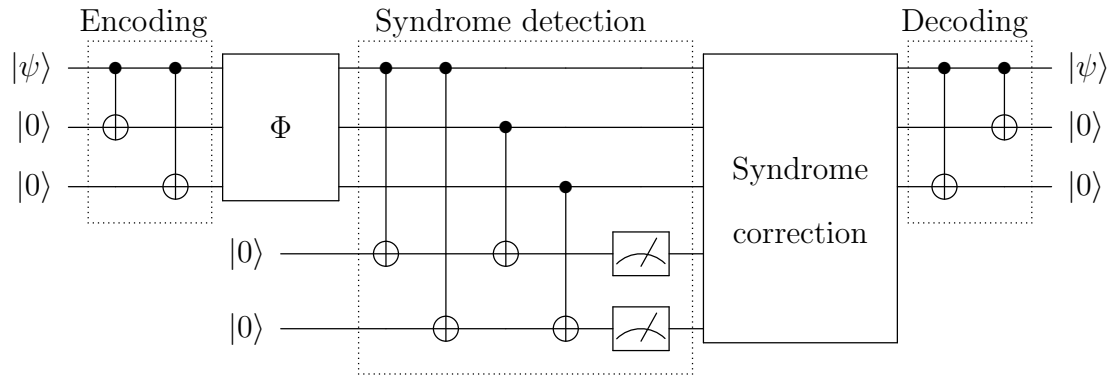
By analogy to the classical case, Alice can transmit a single qubit, $|\psi\rangle = a|0\rangle + b|1\rangle \in \mathbb{C}^2$, without error by encoding it with two qubits in the state $|0\rangle$ using the following algorithm:



This results in the entangled state $a|000\rangle + b|111\rangle$, which Alice then sends to Bob. It is at this point that we see one of the difficulties of designing quantum error correction algorithms based on analogous algorithms from classical error correction. In the classical case, Bob can simply inspect the number he received and, based on the majority rule, determine the original value. However, in the quantum case, measuring the quantum state would cause a wave function collapse, changing the state Bob received. To avoid this, Bob must add two qubits in the state $|0\rangle$ to the system and perform some operations to entangle them with the state he has received using the following algorithm:



Bob then measures the last two qubits. The value he gets is called the *error syndrome*, and it is used to determine what, if any, error occurred. If he gets $|00\rangle$, then no error occurred, so he has the state $a|000\rangle + b|111\rangle$. If he gets $|01\rangle$, then the last qubit was flipped, so he has the state $a|001\rangle + b|110\rangle$. If he gets $|10\rangle$, then the second qubit was flipped, and if he gets $|11\rangle$, then the first qubit was flipped. He can then apply a simple quantum channel to flip the affected qubit back. Finally, he applies the same algorithm that Alice used in reverse to get the state $(a|0\rangle + |1\rangle)|00\rangle$, which will allow him to independently manipulate the state with which Alice started. All together, this algorithm is represented as follows, with the symbol  representing measurement:



At its foundation, this algorithm works as a continuous extension of the discrete classical error correction algorithm. Here, Alice maps her single qubit onto a subspace of a larger state space which can be protected from the errors that might occur during transmission through Φ. In general, if the dimension of such a subspace is k, we call it a k-dimensional *quantum error correction code*. Knill and Laflamme give a very useful equivalent condition in [4].

Theorem 3.6. *Let $\mathcal{K} \subset \mathbb{C}^n$ be a nonzero subspace and let $P : \mathbb{C}^n \to \mathcal{K}$ be the orthogonal projection onto $\mathcal{K}$. Let $\Phi : M_n \to M_n$ be a TPCP map given by $\Phi(X) = \sum_{i=1}^{r} F_i X F_i^*$ for all $X \in M_n$. Then there is a TPCP map $\Psi : M_n \to M_n$ such that $\Psi(\Phi(vv^*)) = vv^*$ for all $v \in \mathcal{K}$ iff. there is some $\Lambda \in M_r$ such that $PF_i^*F_jP = \lambda_{i,j}P$ for $1 \leq i, j \leq r$.*

We will prove one direction of this statement below. The other direction will be proved in Theorem 3.8.

Proof. Suppose there is a quantum channel $\Psi : M_d \to M_n$ s.t. $\Psi(\Phi(vv^*)) = vv^*$ for all $v \in \mathcal{K}$. Then Ψ admits the form $\Psi(\rho) = \sum_{i=1}^{q} E_i \rho E_i^*$, with $\sum_{i=1}^{q} E_i^* E_i = I$. We can define a

quantum channel $\eta : M_n \to M_n$ as

$$\eta(\rho) = P\rho P = \Psi(\Phi(P\rho P)) = \sum_{i=1}^{q}\sum_{j=1}^{r}(E_iF_jP)\rho(E_iF_jP)^*$$

Since the operator system of a quantum channel is determined by the quantum channel, $S_\eta = \text{span}(PF_i^*E_h^*E_jF_\ell P : 1 \leq h, j \leq r, 1 \leq i, \ell \leq q) = \text{span}(P)$. Then there is some

$$\{\alpha_{h,i,j,\ell} : 1 \leq h, j \leq r, 1 \leq i, \ell \leq q\} \subset \mathbb{C}$$

s.t. $PF_i^*E_h^*E_jF_\ell P = \alpha_{h,i,j,\ell}P$ for $1 \leq h, j \leq r, 1 \leq i, \ell \leq q$. Then for $1 \leq i, j \leq r$, since Ψ is trace-preserving by assumption,

$$PF_i^*F_jP = PF_i^*\left(\sum_{h=1}^{q}E_h^*E_h\right)F_jP = \sum_{h=1}^{q}PF_iE_h^*E_hF_jP = \left(\sum_{h=1}^{q}\alpha_{h,i,h,j}\right)P$$

Then, if we define $\Lambda \in M_r$ s.t. $\lambda_{i,j} = \sum_{h=1}^{q}\alpha_{h,i,h,j}$, one direction is proved. □

While this kind of algorithm works well in theory, it requires both an encoding and decoding operation and an algorithm for determining the communication error without measuring the state that was actually transmitted. This leaves the process open to human error, particularly in the operation of measuring to get the syndrome. Much of this human error can be avoided if we can design a quantum channel that can recover the correct quantum state without measurement. In [6], Li, Nakahara, Poon, Sze and Tomita found that whenever there is a recovery channel that can correct Φ *with* a syndrome measurement, we can also construct a recovery channel that can correct Φ *without* a syndrome measurement. This construction utilizes the *partial trace*, which is defined as follows:

Definition 3.7. Let $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_r$, let $A : \mathcal{H} \to \mathcal{H}$ be linear and for some $i \in \{1, ..., r\}$, let $e_1, ..., e_n$ be the standard basis vectors for $\mathcal{H}_i$. Then the i-th *partial trace* is

$$\mathrm{tr}_i(A) = \sum_{j=1}^{n} (I_{\mathcal{H}_1} \otimes \cdots \otimes e_j^* \otimes \cdots \otimes I_{\mathcal{H}_r}) A (I_{\mathcal{H}_1} \otimes \cdots \otimes e_j \otimes \cdots \otimes I_{\mathcal{H}_n})$$

In particular, this construction from [6] uses the first partial trace, and for the sake of clarity, we can describe its action more simply. Let $A \in M_n, B \in M_m$. Then

$$\mathrm{tr}_1(A \otimes B) = \mathrm{tr}(A) \cdot B.$$

Theorem 3.8. *Let $\Phi : M_n \to M_n$ be a quantum channel defined as $\Phi(\rho) = \sum_{i=1}^{r} F_i \rho F_i^*$. Suppose $\mathcal{K} \subset \mathbb{C}$ is an error correcting code of dimension k, and let $P \in M_n$ be on orthogonal projection on $\mathcal{K}$. Let $W \in \mathbb{C}^{n \times k}$ be s.t. $W^*W = I_k$ and $P = WW^*$, so that any $\rho \in M_n$ s.t. $P\rho P = \rho$ has the form $W\tilde{\rho}W^*$ for some $\tilde{\rho} \in M_k$. The there is a unitary $R \in M_n$ and a positive definite matrix $D \in M_q$ with $q \leq \min\{r, n/k\}$ such that for any density matrix $\tilde{\rho} \in M_k$,*

$$R^* \Phi(W\tilde{\rho}W^*) R = (D \otimes \tilde{\rho}) \oplus 0_{n-qk}$$

In particular, if n is a multiple of k so that M_n can be regarded as $M_{n/k} \otimes M_k$, then

$$R^* \Phi(W\tilde{\rho}W^*) R = \tilde{D} \otimes \tilde{\rho} \text{ with } \tilde{D} = D \oplus 0_{n/k-q}$$

and a recovery quantum channel can be constructed as the map $\Psi : M_n \to M_n$ defined by

$$\Psi(\rho) = W(tr_1(R\rho R^*))W^*$$

Proof. Suppose $\mathcal{K} \subset \mathbb{C}^n$ is an error correcting code of dimension k, and let P be an orthogonal projection onto $\mathcal{K}$. Then by Theorem 3.6, there is a $\Lambda \in M_r$ s.t. $PF_i^*F_jP = \lambda_{i,j}P$ for

$1 \leq i, j \leq r$. Then we have

$$\Lambda \otimes P = (\lambda_{i,j}P)_{i,j=1}^{r} = (PF_i^*F_jP)_{i,j=1}^{r}$$

$$= \begin{bmatrix} PF_1^* \\ \vdots \\ PF_r^* \end{bmatrix} \begin{bmatrix} F_1P & \cdots & F_rP \end{bmatrix}$$

Since any matrix of the form BB^* is positive semidefinite, $\Lambda \otimes P \geq 0$, so $\Lambda \geq 0$. Suppose Λ has rank q. Then there is a unitary $U \in M_r$ such that $U^*\Lambda U = D \oplus 0_{r-q}$ for some diagonal matrix $D \geq 0$. Define

$$E_j = \sum_{i=1}^{r} u_{i,j}F_i \text{ for } j = 1, ..., r$$

Let $F = \begin{bmatrix} F_1 & \cdots & F_r \end{bmatrix}$, and let $E = \begin{bmatrix} E_1 & \cdots & E_r \end{bmatrix}$. Then $E = F(U \otimes I_n)$ and for any $\rho \in M_n$,

$$\begin{aligned} \Phi(\rho) &= \sum_{j=1}^{r} F_j\rho F_j^* = F(I_r \otimes \rho)F^* \\ &= F(U \otimes I_n)(I_r \otimes \rho)(U \otimes I_n)^*F^* \\ &= E(I_r \otimes \rho)E^* = \sum_{j=1}^{r} E_j\rho E_j^* \end{aligned}$$

So $\Phi(\rho) = \sum_{j=1}^{r} E_j\rho E_j^*$. Futhermore,

$$PE_i^*E_jP = \sum_{\ell,m=1}^{r} \overline{u}_{\ell,i}u_{m,j}PF_\ell^*F_mP = \sum_{\ell,m=1}^{r} \overline{u}_{\ell_i}u_{m,j}\lambda_{\ell,m}P = (U^*\Lambda U)_{i,j}P = d_{i,j}P \text{ for } 1 \leq i, j \leq r$$

We can assume without loss of generality that $E_j = F_j$, and so $PF_i^*F_jP = d_{i,j}P$ for $1 \leq i, j \leq r$. Then we can replace the matrix F with $F = \begin{bmatrix} F_1 & \cdots & F_q \end{bmatrix}$. Since $P = WW^*$ with $W^*W = I_k$, it follows that

$$W^*F_i^*F_jW = d_{i,j}I_k \text{ and } (I_q \otimes W)^*F^*F(I_q \otimes W) = D \otimes I_k$$

Define an $n \times qk$ matrix $R_1 = F(I_q \otimes W)(D^{-1/2} \otimes I_k)$, where $D^{-1/2} = \text{diag}\left(\frac{1}{\sqrt{d_{1,1}}}, ..., \frac{1}{\sqrt{d_{q,q}}}\right)$. Then $R^*R = I_{qk}$. Let R_2 be an $n \times (n - qk)$ matrix s.t. $R = \begin{bmatrix} R_1 & R_2 \end{bmatrix}$ is unitary. Now for any $\rho \in M_n$ with $P\rho P = \rho$, $\rho = W\tilde{\rho}W^*$ for some $\tilde{\rho} \in M_k$. For $j > q$, $W^*F_j^*F_jW = d_{j,j}I_k = 0$, so $F_jW = 0$. Then

$$\Phi(\rho) = \sum_{j=1}^{r} F_j(W\tilde{\rho}W^*)F^* = \sum_{j=1}^{q} F_j(W\tilde{\rho}W^*)F_j^* = F(I_q \otimes (W\tilde{\rho}W^*))F^* \tag{1}$$

It follows that

$$\begin{aligned} R^*\Phi(\rho)R &= R^*F(I_q \otimes W)(I_q \otimes \tilde{\rho})(I_q \otimes W)^*F^*R \\ &= R^*R_1(D^{1/2} \otimes I_k)(I_q \otimes \tilde{\rho})(D^{1/2} \otimes I_k)R_1^*R \\ &= \begin{bmatrix} D^{1/2} \otimes I_k \\ 0 \end{bmatrix} (I_q \otimes \tilde{\rho}) \begin{bmatrix} D^{1/2} \otimes I_k & 0 \end{bmatrix} = (D \otimes \tilde{\rho}) \oplus 0_{r-qk} \end{aligned}$$

Finally, since $P = P\left(\sum_{i=1}^{r} F_i^*F_i\right)P = \left(\sum_{i=1}^{r} d_{i,i}\right)P$, $\sum_{i=1}^{r} d_{i,i} = 1$. Then

$$\text{tr}_1(R^*\Phi(W\tilde{\rho}W^*)R) = \left(\sum_{i=1}^{r} d_{i,i}\right)\tilde{\rho} = \tilde{\rho},$$

so if we define $\Psi(\rho) = W(\text{tr}_1(R^*\rho R))W^*$, $\Psi(\Phi(W\tilde{\rho}W^*)) = W\tilde{\rho}W^*$ for all $\tilde{\rho} \in M_k$. □

For an example of this type of error correction algorithm, recall the noisy channel described in the quantum error correction algorithm above. If we explicitly describe this channel, we can construct a recovery channel without a syndrome measurement. Let

$$\begin{aligned} F_0 &= \sqrt{p_0}I_8, & F_1 &= \sqrt{p_1}\sigma_x \otimes I_2 \otimes I_2, \\ F_2 &= \sqrt{p_2}I_2 \otimes \sigma_x \otimes I_2, & F_3 &= \sqrt{p_3}I_2 \otimes I_2 \otimes \sigma_x, \end{aligned}$$

where $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $p_0 + p_1 + p_2 + p_3 = 1$. Then for a 3-qubit state ρ, the action of the noisy channel on ρ is defined as $\Phi(\rho) = \sum_{i=0}^{3} F_i \rho F_i^*$. As in the first error correction method, Alice takes the state $a|0\rangle + b|1\rangle$ and encodes it in the state $a|000\rangle + b|111\rangle$. Then if ρ is the density matrix she is sending through Φ, we have

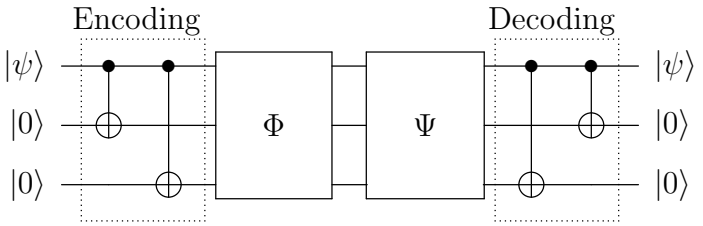
$$\rho = \begin{bmatrix} a & 0 & \cdots & 0 & b \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ c & 0 & \cdots & 0 & 0 \end{bmatrix} \text{ and } \Phi(\rho) = \begin{bmatrix} p_0 a & 0 & 0 & 0 & 0 & 0 & 0 & p_0 b \\ 0 & p_3 a & 0 & 0 & 0 & 0 & p_3 b & 0 \\ 0 & 0 & p_2 a & 0 & 0 & p_2 b & 0 & 0 \\ 0 & 0 & 0 & p_1 d & p_1 c & 0 & 0 & 0 \\ 0 & 0 & 0 & p_1 b & p_1 a & 0 & 0 & 0 \\ 0 & 0 & p_2 c & 0 & 0 & p_2 d & 0 & 0 \\ 0 & p_3 c & 0 & 0 & 0 & 0 & p_3 d & 0 \\ p_0 c & 0 & 0 & 0 & 0 & 0 & 0 & p_0 d \end{bmatrix}$$

We now construct a quantum recovery channel that is inverse to Φ on the subspace $\mathcal{K} = \text{span}(|000\rangle, |111\rangle)$. Let $P = \begin{bmatrix} e_1 & 0 & \cdots & 0 & e_8 \end{bmatrix}$, and define

$$G_1 = P, \qquad G_2 = P \begin{bmatrix} e_2 & e_1 & 0 & 0 & 0 & 0 & e_8 & e_7 \end{bmatrix}$$

$$G_3 = P \begin{bmatrix} e_3 & 0 & e_1 & 0 & 0 & e_8 & 0 & e_6 \end{bmatrix}, \quad G_4 = P \begin{bmatrix} e_5 & 0 & 0 & e_8 & e_1 & 0 & 0 & e_4 \end{bmatrix}$$

Then we have $\sum_{i=1}^{4} G_i^* G_i = I_8$, so if we define $\Psi : M_8 \to M_8$ as $\Psi(\rho) = \sum_{i=1}^{4} G_i \rho G_i^*$, then Ψ is a trace-preserving, completely positive (TPCP) map. Furthermore, for any density matrix $\rho \in \text{span}(vv^* : v \in \mathcal{K}, ||v|| = 1)$, $\Psi(\Phi(\rho)) = \rho$. Putting all of this together, we have the following quantum algorithm:



Just as with the first error correcting method, Alice begins by encoding the state she wishes to send onto a subspace of $\mathbb{C}^8$ which can be protected from error. However, after the state has gone through the channel, instead of needing to entangle additional qubits and measure to get a syndrome, then correct the error, then finally decode the result to get the original state, Bob can simply apply Ψ, then decode the result. This is far more efficient and less prone to human error.

In both methods, the subspace $\mathcal{K}$ that can be protected against the error channel Φ depends entirely on S_Φ, and not directly on Φ itself. However, the actual recovery quantum channel that Knill and Laflamme construct in their proof does depend on the specific $F_1, ..., F_r$, not just S_Φ. The construction given by Li, Nakahara, Poon, Sze and Tomita in Theorem 3.8 is simpler and far more flexible, as it corrects not just Φ, but also any $\Psi : M_n \to M_n$ s.t. $S_\Psi \subset S_\Phi$. The following theorem, also from [6], states this more precisely:

Theorem 3.9. *Let $R, W, F_1, ..., F_r$ be as described in Theorem 3.8. If $\tilde{\Phi}$ is another quantum channel $\tilde{\Phi}(\rho) = \sum_{j=1}^{s} \tilde{F}_j \rho \tilde{F}_j^*$, where the operators $\tilde{F}_j$ are linear combinations of $F_1, ..., F_r$, then there is a $\tilde{D} \geq 0$ such that for any density matrix $\tilde{\rho} \in M_k$ and $\rho = W\tilde{\rho}W^*$, we have*

$$R^* \tilde{\Phi}(\rho) R = (\tilde{D} \otimes \tilde{\rho}) \oplus 0$$

Proof. Using the same notations as in Theorem 3.8, for $j = 1, ..., s$, let

$$\tilde{F}_j = \sum_{i=1}^{r} t_{i,j} F_i \text{ for some } t_{1,j}, ..., t_{r,j} \in \mathbb{C}$$

Recall that $F_j W = 0$ for $j > q$. Then $\tilde{F}_j W = \sum_{i=1}^{q} t_{i,j} F_i W$ for $j = 1, ..., s$. Define a $q \times s$ matrix $T = (t_{i,j})_{i,j}$. For any density matrix $\rho = W\hat{\rho}W^* \in M_n$,

$$\begin{aligned}
\tilde{\Phi}(\rho) &= \sum_{j=1}^{s} \tilde{F}_j W \hat{\rho} W^* \tilde{F}_j^* \\
&= \sum_{j=1}^{s} \left(\sum_{i=1}^{q} t_{i,j} F_i \right) W \hat{\rho} W^* \left(\sum_{h=1}^{q} \bar{t}_{h,j} F_h^* \right) \\
&= \sum_{h,i=1}^{q} F_i \left(\sum_{j=1}^{s} t_{i,j} \bar{t}_{h,j} W \hat{\rho} W^* \right) F_h^* \\
&= F(TT^* \otimes W\hat{\rho}W^*)F^*
\end{aligned}$$

Note that this is the same as equation 1 from the proof of Theorem 3.8, but with TT^* replacing I_q. Then, letting $\tilde{D} = D^{1/2} TT^* D^{1/2} \geq 0$,

$$R^* \tilde{\Phi}(\rho) R = (\tilde{D} \otimes \hat{\rho}) \oplus 0$$

□

CHAPTER 4. NUMERICAL RANGE GENERALIZATIONS

The equivalent conditions from Theorems 1.12 and 1.14 are closely related to a particular generalization of the *numerical range* of a matrix $A \in M_n$, defined as

$$W(A) = \{v^*Av : v \in \mathbb{C}^n, ||v|| = 1\}$$

First, for $A_1, ..., A_m \in M_n$, we define the *joint numerical range* as

$$W(A_1, ..., A_m) = \{x \in \mathbb{C}^m : \exists\ v \in \mathbb{C}^n \text{ s.t. } v^*v = 1 \text{ and } v^*A_iv = x_i \text{ for } 1 \leq i \leq m\}$$

Let $\mathcal{P}_k(n)$ be the set of all orthogonal projections $P : \mathbb{C}^n \to \mathcal{K}$ s.t. $\dim(\mathcal{K}) = k$. Then, define the *rank-k numerical range* of A as

$$\Lambda_k(A) = \{\lambda \in \mathbb{C} : \exists\ P \in \mathcal{P}_k(n) \text{ s.t. } PAP = \lambda P\}$$

We then further generalize this to the *rank-k joint numerical range* of a set of matrices.

Definition 4.1. Let $A_1, ..., A_m \in M_n$. Then the *rank-k joint numerical range* of $A_1, ..., A_m$ is defined as

$$\Lambda_k(A_1, ..., A_m) = \{u \in \mathbb{C}^m : \exists\ P \in \mathcal{P}_k(n) \text{ s.t. } PA_iP = u_iP \text{ for } 1 \leq i \leq m\}$$

Then by Theorem 1.14, the existence of a k-dimensional code for a quantum channel $\Phi : M_n \to M_d$, defined as $\Phi(\rho) = \sum_{i=1}^{r} F_i\rho F_i^*$, is equivalent to the condition

$$\Lambda_k(F_i^*F_j : 1 \leq i, j \leq r) \neq \varnothing$$

Suppose $A \in M_n, P \in \mathcal{P}_k(n)$ s.t. $PF_i^*F_jP = a_{i,j}P$ for $1 \leq i,j \leq r$. Then, by the linearity of matrix operations, for any $B \in S_\Phi$, $PBP = \lambda P$ for some $\lambda \in \mathbb{C}$. So, if $\dim(S_\Phi) = m+1$ and $\{I, B_1, ..., B_m\}$ is a basis for S_Φ, $\Lambda_k(F_i^*F_j : 1 \leq i,j \leq r) \neq \varnothing$ if and only if $\Lambda_k(B_1, ..., B_m) \neq \varnothing$. Furthermore, since $B \in S_\Phi$ if and only if $B^* \in S_\Phi$, we can assume that any basis of S_Φ is composed of Hermitian matrices, which simplifies the calculations involved in determining whether $\Lambda_k(B_1, ..., B_m) \neq \varnothing$.

The equivalent condition from Theorem 3.4 is related to a further generalization of the rank-k joint numerical range. Let $\mathcal{D}_k$ be the space of diagonal matrices in M_k. Then, for $A \in M_n$, define $D_k(A)$ as

$$D_k(A) = \{D \in \mathcal{D}_k : \exists\, U \in \mathbb{C}^{n\times k} \text{ s.t. } U^*U = I_k, U^*AU = D\}$$

Then, for $A_1, ..., A_m \in M_n$, define $D_k(A_1, ..., A_m)$ as

$$D_k(A_1, ..., A_m) = \{(D_1, ..., D_m) \in (\mathcal{D}_k)^m : \ \exists\, U \in \mathbb{C}^{n\times k} \text{ s.t. } U^*U = I_k, \\ U^*A_iU = D_i \text{ for } 1 \leq i \leq m\}$$

Then, by Theorem 3.4, there exists a set of perfectly distinguishable quantum states $\{x_1, ..., x_k\} \subset \mathbb{C}^n$ such that $\{\Phi(x_1x_1^*), ..., \Phi(x_kx_k^*)\}$ are perfectly distinguishable if and only if $D_k(F_i^*F_j : 1 \leq i,j \leq r) \neq \varnothing$. We can again turn to the operator system of Φ, S_Φ, and find a basis of Hermitian matrices $\{I, B_1, ..., B_m\} \subset S_\Phi$. Then $D_k(F_i^*F_j : 1 \leq i,j \leq r) \neq \varnothing$ if and only if $D_k(B_1, ..., B_m) \neq \varnothing$.

4.1 Conditions for the Non-Emptiness of $\Lambda_k(A_1, ..., A_m)$

We now come to an important question in the field of quantum error correction: For what triples $(n,k,m) \in \mathbb{N}^3$ is a k-dimensional code guaranteed to exist for any quantum

channel $\Phi : M_n \to M_d$ with $\dim(S_\Phi) = m+1$? We have seen above that this is equivalent to asking when $\Lambda_k(A_1, ..., A_m) \neq \varnothing$ for any $A_1, ..., A_m \in \mathcal{H}_n$, where $\mathcal{H}_n$ is the set of all Hermitian matrices in M_n. A common approach to answering this question is to find a relation between n, k and m that guarantees that $D_k(B_1, ..., B_m) \neq \varnothing$ for some basis $\{B_1, ..., B_m\} \subset S_\Phi$, then extending that to a relation that guarantees a k-dimensional code for Φ using a specific application of Tverberg's Theorem [14], which is written below.

Theorem 4.2. *Let $m, k \in \mathbb{N}$, let $n \geq (m+1)(k-1)+1$ and let $D_1, ..., D_m \in M_n(\mathbb{R})$ be diagonal. Then $\Lambda_k(D_1, ..., D_m) \neq \varnothing$.*

Tverberg also proves that this bound is minimal. That is, for $n < (m+1)(k-1)+1$, there are $D_1, ..., D_m \in \mathcal{D}_n$ such that $\Lambda_k(D_1, ..., D_m) = \varnothing$. For ease of reference, let $r(k, m)$ be the minimum value of n s.t. $\Lambda_k(A_1, ..., A_m) \neq \varnothing$ for any $A_1, ..., A_m \in \mathcal{H}_n$. In [5], Knill, Laflamme and Viola found the following bound:

Theorem 4.3. *Let $n \geq (m+1)(k-1)+1$, and let $A_1, ..., A_m \in \mathbb{H}_n$. Then $D_k(A_1, ..., A_m) \neq \varnothing$.*

Proof. The proof is short, and so we will include it. Let $v_1 \in \mathbb{C}^n$, and for some ℓ, $1 \leq \ell < k$, assume that we can choose $v_1, ..., v_\ell \in \mathbb{C}^n$ so that for some $I = C^{(0)}, C^{(1)}, ..., C^{(m)} \in M_\ell$, letting $A_0 = I$,

$$v_i^* A_h v_j = c_{i,j}^{(h)} \delta_{i,j} \text{ for } 0 \leq h \leq m, 1 \leq i, j \leq \ell$$

Then, since $\ell(m+1) \leq (k-1)(m+1) < n$, there is a $v_{\ell+1}$ that is orthogonal to $A_h v_i$ for $0 \leq h \leq m$, $1 \leq i \leq \ell$. Then, by induction, there is a $v_1, ..., v_k \in \mathbb{C}^n$ s.t. for some $I = C^{(0)}, ..., C^{(m)} \in M_k$, $v_i^* A_h v_j = c_{i,j}^{(h)} \delta_{i,j}$ for $0 \leq h \leq m$, $1 \leq i, j \leq k$. Let $V = [\ v_1 \ \cdots \ v_k\ ]$. Then $V \in \mathbb{C}^{n \times k}$, $V^*V = I_k$ and $V^* A_i V$ is diagonal for $1 \leq i \leq m$, so $D_k(A_1, ..., A_m) \neq \varnothing$. □

We can then use Theorem 4.2 to get

$$r(k,m) \leq (m+1)\big((m+1)(k-1)+1-1\big)+1 = (m+1)^2(k-1)+1$$

Due to the fact that Knill, Laflamme and Viola apply Theorem 4.2 in a slightly different way, the bound they give in their paper is $k-1$ higher than this, but this is the essence of their approach. In [8], Li and Poon improve this bound to $r(k,m) \leq (m+1)^2(k-1)$ by letting the first vector they choose be an eigenvector of A_1. Finally, in [15], Weaver proves that $\Lambda_k(A_1,...,A_m) \neq \varnothing$ for all $A_1,...,A_m \in \mathcal{H}_n$ if $(k-1)(m+1)+1 \leq \lceil \frac{n}{m} \rceil$. His proof of this condition uses a similar technique to that used in our proof of Theorem 4.9. We can see that this condition is equivalent to $r(k,m) \leq m(m+1)(k-1)+1$ if we consider the case $n = m(m+1)(k-1)+1$. Then we have

$$\left\lceil \frac{m(m+1)(k-1)+1}{m} \right\rceil = (m+1)(k-1) + \left\lceil \frac{1}{m} \right\rceil = (m+1)(k-1)+1,$$

so for $n \geq m(m+1)(k-1)+1$, Weaver's condition is satisfied.

We improve on this upper bound for $r(k,m)$ in the next few theorems. First, there is a $U \in \mathbb{C}^{n\times k}$ such that $U^*U = I_k$ and U^*A_iU diagonal for $1 \leq i \leq m$ if and only if there is an orthonormal set $\{u_1,...,u_k\} \subset \mathbb{C}^n$ such that $0 = u_i^*u_j = u_i^*A_1u_j = \cdots = u_i^*A_mu_j$ for $1 \leq i,j \leq k$ with $i \neq j$. Since we are concerned with finding when D_k is non-empty for some basis of the operator system of a quantum channel Φ, we can assume that $A_1,...,A_m \in \mathcal{H}_n$. So, we only need to consider $1 \leq i < j \leq k$.

Let $n \in \mathbb{N}$, let $A_1, ..., A_{2n-3} \in \mathcal{H}_n$ and define $x = [\ x_1 \quad \cdots \quad x_n\ ]^*$ and $y = [\ y_1 \quad \cdots \quad y_n\ ]^T$, where $x_1, ..., x_n, y_1, ..., y_n$ are indeterminates. Then

$$\begin{aligned} x^*y &= \sum_{i=1}^{n} x_i y_i, \\ x^*A_1y &= \sum_{i,j=1}^{n} (A_1)_{i,j}\ x_i y_j, \\ &\vdots \\ x^*A_{2n-3}y &= \sum_{i,j=1}^{n} (A_{2n-3})_{i,j}\ x_i y_j \end{aligned}$$

are $2(n-1)$ forms on the $2(n-1)$-dimensional projective variety $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$. Then, by Proposition 2.9, these forms have a common zero, which is represented by some $(u, v) \in (\mathbb{C}^n \setminus \{0\})^2$ s.t.

$$u^*v = u^*A_1v = \cdots = u^*A_{2n-3}v = 0.$$

This proves the following theorem:

Theorem 4.4. *Let $n \geq 2$. Then for any $A_1, ..., A_{2n-3} \in \mathcal{H}_n$, $D_2(A_1, ..., A_{2n-3}) \neq \varnothing$.*

This result is actually quite surprising if we view it in a slightly different context. Consider the vector space $\text{span}(v, A_1v, ..., A_{2n-3}v)$. By the result above, the dimension of this space of $2n-2$ vectors is less than or equal to $n-1$. So, for an appropriate choice of $v \in \mathbb{C}^n$, given any n matrices in $\text{span}(A_1, ..., A_{2n-3})$, there is a $c \in \mathbb{C}^n$ s.t. v is a zero eigenvector of $\sum_{i=1}^{n} c_i A_i$.

To give a more specific example, given $A_1, A_2, A_3 \in \mathcal{H}_3$, we can find a unitary matrix $U \in \mathcal{U}_3$ such that the leading principal 2×2 submatrix of U^*A_1U, U^*A_2U and U^*A_3U is diagonal. Even for n this small, this result was previously unknown.

Furthermore, the next two theorems will show that this is the least upper bound on m s.t. $D_2(A_1, ..., A_m) \neq \varnothing$ for any $A_1, ..., A_m \in \mathcal{H}_n$. For $A \in M_n$, $\alpha, \beta \in [n] = \{1, ..., n\}$, let $A[\alpha : \beta] = (a_{i,j})_{i\in\alpha, j\in\beta}$.

Theorem 4.5. *For any $n \in \mathbb{N}$, there is a $V \in \mathcal{U}(n)$ s.t. $\det\big(V[\alpha : \beta]\big) \neq 0$ for all $\alpha, \beta \subset [n]$ s.t. $|\alpha| = |\beta|$.*

Proof. Let $\alpha, \beta \subset [n]$ such that $|\alpha| = |\beta| = k$. Define $f : \mathcal{U}(n) \to \mathbb{C}$ as $f(V) = \det\big(V[\alpha : \beta]\big)$ for all $V \in \mathcal{U}(n)$. Then f is a polynomial, and is therefore a continuous function. So,

$$\{V \in \mathcal{U}(n) : \det\big(V[\alpha : \beta]\big) \neq 0\} = f^{-1}\big((-\infty, 0) \cup (0, \infty)\big) \text{ is open.}$$

Let $V \in \mathcal{U}(n)$ s.t. $\det\big(V[\alpha : \beta]\big) = 0$, let $r = \text{rank}(V[\alpha : \beta])$ and let $S \subset \alpha$ be s.t. $\{V[i : \beta] : i \in S\}$ spans the rows of $V[\alpha : \beta]$. Since V is unitary, its columns are linearly independent, so

$$\dim\big(\text{span}(v_i : i \in \alpha)\big) = k$$

Then, there is a $p \in [n] \setminus \alpha$ s.t. $V[p : \beta]$ is not in the span of the rows of $V[\alpha : \beta]$. Let $q \in \alpha \setminus S$, and define $U_{p,q}(t) : [0, 1] \to \mathcal{U}(n)$ as follows: Let $\big(U_{p,q}(t)\big)_{p,q} = \big(U_{p,q}(t)\big)_{q,p} = it$, let $\big(U_{p,q}(t)\big)_{p,p} = \big(U_{p,q}(t)\big)_{q,q} = \sqrt{1 - t^2}$ and let $\big(U_{p,q}(t)\big)_{i,j} = \delta_{i,j}$ for all other entries.

For any $\varepsilon > 0$, let $t < \sqrt{\frac{\varepsilon}{8}(2 - \frac{\varepsilon}{8})}$, and define $V^{(1)} = U_{p,q}(t)V$. Then $\text{rank}\big(V^{(1)}[\alpha : \beta]\big) = r + 1$ and, using the matrix norm $||A|| = \text{tr}(A^*A)$ for every $A \in M_n$,

$$||V - V^{(1)}|| = ||(I - U_{p,q}(t))V|| = ||I - U_{p,q}(t)||$$

$$= 4(1 - \sqrt{1 - t^2}) < 4\left(1 - \sqrt{1 - \frac{\varepsilon}{4} + \frac{\varepsilon^2}{64}}\right) = \frac{\varepsilon}{2}$$

Using a similar method, we can construct $V^{(2)}, ..., V^{(k-r)}$ s.t. $V^{(k-r)} \in \mathcal{U}(n)$, $\text{rank}\left(V^{(k-r)}[\alpha : \beta]\right) = k$, and

$$||V - V^{(k-r)}|| \leq ||V - V^{(1)}|| + \sum_{i=2}^{k-r} ||V^{(i-1)} - V^{(i)}|| < \sum_{i=1}^{k-r} \frac{\varepsilon}{2^i} < \varepsilon$$

So, the set $\left\{V \in \mathcal{U}(n) : \det\left(V[\alpha : \beta]\right) \neq 0\right\}$ is open and dense in $\mathcal{U}(n)$. Since there are a finite number of $\alpha, \beta \subset [n]$ s.t. $|\alpha| = |\beta|$, by the Baire category theorem,

$$\left\{V \in \mathcal{U}(n) : \det\left(V[\alpha : \beta]\right) \neq 0 \; \forall \; \alpha, \beta \subset [n] \text{ s.t. } |\alpha| = |\beta|\right\}$$

$$= \bigcap_{\substack{\alpha,\beta \subset [n] \\ |\alpha| = |\beta|}} \left\{V \in \mathcal{U}(n) : \det\left(V[\alpha : \beta]\right) \neq 0\right\}$$

is dense in $\mathcal{U}(n)$, and is therefore non-empty. □

Having established the existence of such a matrix, we can now use it to construct $A_1, ..., A_{2n-2} \in \mathcal{H}_n$ s.t. $D_2(A_1, ..., A_{2n-2}) = \varnothing$.

Theorem 4.6. *Let $n \geq 2$, and let $V \in \mathcal{U}(n)$ s.t. $\det\left(V[\alpha : \beta]\right) \neq 0$ for any $\alpha, \beta \subset [n]$ s.t. $|\alpha| = |\beta|$. Then, if e_i is the i-th standard basis vector for $\mathbb{C}^n$,*

$$D_2(e_1 e_1^*, ..., e_{n-1} e_{n-1}^*, v_1 v_1^*, ..., v_{n-1} v_{n-1}^*) = \varnothing$$

Proof. Since $\det(v_{i,j}) \neq 0 \; \forall \; \{i\}, \{j\} \subset [n]$, $e_i^* v_j \neq 0$ for $1 \leq i, j \leq n$. Let $S, T \subset [n]$ s.t. $|S| + |T| = k \leq n$. Then $V\big[[n] \setminus S : T\big]$ is a $(n - |S|) \times (k - |S|)$ matrix, and so contains a nonsingular $(k - |S|) \times (k - |S|)$ submatrix by the conditions on V. Then $\dim\left(\text{span}(e_i, v_j : i \in S, j \in T)\right) = k$.

Let $x, y \in \mathbb{C}^n$ be nonzero, and suppose $x^*y = x^*e_ie_i^*y = x^*v_iv_i^*y = 0$ for $1 \leq i \leq n-1$. Let $P = \{e_1, ..., e_{n-1}, v_1, ..., v_{n-1}\}$. For any vector $v \in \mathbb{C}^n$, $x^*vv^*y = 0$ iff. either $x \perp v$ or $y \perp v$ so the union of $x^\perp \cap P$ and $y^\perp \cap P$ covers P.
Since $\dim\big(\text{span}(e_i, v_j : i \in S, j \in T)\big) = k$ for any $S, T \subset [n]$ such that $|S| + |T| = k \leq n$ and $\dim(x^\perp) = n-1$, $|x^\perp \cap P| \leq n-1$. Similarly, $|y^\perp \cap P| \leq n-1$, so $x^\perp \cap y^\perp \cap P = \varnothing$ and $|x^\perp \cap P| = |y^\perp \cap P| = n-1$.

Then there are $S, T \subset [n-1]$, not necessarily non-empty, such that $x \perp \text{span}(e_i, v_j : i \in S, j \in T)$ and $|S| + |T| = n-1$. Since $|S \cup \{n\}| + |T| = n$,

$$\dim\big(\text{span}(\{e_i, v_j : i \in S \cup \{n\}, j \in T)\big) = n,$$

so $\{e_i, v_j : i \in S \cup \{n\}, j \in T\}$ is a basis for $\mathbb{C}^n$.
Then, since $x \perp \text{span}(e_i, v_j : i \in S, j \in T)$, $x^*e_n \neq 0$. Similarly, $y^*e_n \neq 0$. Since $x^*e_i = 0$ for all $i \in S$ and $y^*e_i = 0$ for all $i \in [n-1] \setminus S$,

$$x^*y = \overline{x_n}y_n = (x^*e_n)(e_n^*y) \neq 0$$

This contradicts $x^*y = 0$, so $D_2(e_1e_1^*, ..., e_{n-1}e_{n-1}^*, v_1v_1^*, ..., v_{n-1}v_{n-1}^*) = \varnothing$. □

Unfortunately, for $k > 2$, we cannot construct indeterminate vectors $u_1, ..., u_k$ over $\mathbb{C}$ s.t. $u_i^*u_j$ is holomorphic for every $i, j \in [k]$ with $i < j$, so we cannot apply Proposition 2.9 in the same manner to the problem for $k > 2$. However, we can directly construct the first $k-2$ vectors, which results in the following bound:

Theorem 4.7. *Let $m \geq 1$, $k \geq 2$ and $n \geq \frac{m+3}{2} + m(k-2)$. Then $D_k(A_1, ..., A_m) \neq \varnothing$ for any $A_1, ..., A_m \in \mathcal{H}_n$.*

Proof. : We proceed by induction on k. For $k = 2$, the result follows from Theorem 4.4.

Suppose the result holds for some $k \geq 2$. Let $m \geq 1$, let $n \geq \frac{m+3}{2} + m((k+1)-2)$, let $A_0 = I, A_1, ..., A_m \in \mathcal{H}_n$ and let $\mathcal{S} = \text{span}(I, A_1, ..., A_m)$. Without loss of generalization, we can assume that $A_1 = \text{diag}(a_1, \cdots, a_n)$ is diagonal. Let $u_1 = e_1$. Then $A_1 u_1 = a_1 u_1$, so $\dim(\mathcal{S}u_1) = d \leq m$. Then there is a $W \in \mathcal{U}(n)$ such that $W(\mathcal{S}u_1) = \text{span}(e_i : 1 \leq i \leq d)$. Let $B_1, ..., B_m$ be the bottom right $(n-d) \times (n-d)$ submatrix of $WA_1W^*, ..., WA_mW^*$, respectively. Then, since

$$n - d \geq n - m \geq \frac{m+3}{2} + m(k-2),$$

by the inductive assumption, there are $v_2, \ldots, v_{k+1} \in \mathbb{C}^{n-d}$ such that

$$0 = v_j^* v_i = v_j^* B_1 v_i = \cdots = v_j^* B_m v_i \text{ for all } 2 \leq i < j \leq k+1$$

Let $u_j = W^* \begin{bmatrix} 0 \\ \\ v_j \end{bmatrix}$ for $2 \leq j \leq k+1$. Then for $j = 2, \ldots, k+1$ and $\ell = 0, 1, \ldots, m$, $u_j^* A_\ell u_1 = (Wu_j)^*(WA_\ell u_1) = 0$. Therefore,

$$0 = u_j^* u_i = u_j^* A_1 u_i = \cdots = u_j^* A_m u_i \text{ for all } 1 \leq i < j \leq k+1.$$

So, if we let $U = [\ u_1 \quad \cdots \quad u_{k+1}\ ]$, $U^*U = I_{k+1}$ and U^*A_iU is diagonal for $1 \leq i \leq m$. Then $D_{k+1}(A_1, ..., A_m) \neq \varnothing$. □

While we do not know in general whether this bound is optimal, we have seen that it is optimal for $k = 2$, it is clearly optimal for $m = 1$, and we will now show it is also optimal for $m = 2$.

Theorem 4.8. *Let $k \geq 2$ and let*

$$A_1 = \begin{pmatrix} I_{k-1} & 0 \\ 0 & -I_{k-1} \end{pmatrix}, \; A_2 = \begin{pmatrix} 0 & I_{k-1} \\ I_{k-1} & 0 \end{pmatrix}$$

Then $D_k(A_1, A_2) = \varnothing$.

Proof. : Let $k \geq 2$, $n = 2k - 2$, and A_1, A_2 be defined as in the statement of the theorem. Suppose to the contrary that $D_k(A_1, A_2) \neq \varnothing$. Then there exists an orthonormal set $\{u_1, \ldots, u_k\}$ of vectors in $\mathbb{C}^n$ such that

$$u_i^* u_j = u_i^* A_1 u_j = u_i^* A_2 u_j = 0 \text{ for } 1 \leq i < j \leq k.$$

Writing $u_i = \begin{pmatrix} u_i^{(1)} \\ u_i^{(2)} \end{pmatrix}$, where $u_i^{(1)}, u_i^{(2)} \in \mathbb{C}^{k-1}$, we have

$$\begin{aligned} u_i^* u_j &= \left(u_i^{(1)}\right)^* u_j^{(1)} + \left(u_i^{(2)}\right)^* u_j^{(2)}, \\ u_i^* A_1 u_j &= \left(u_i^{(1)}\right)^* u_j^{(1)} - \left(u_i^{(2)}\right)^* u_j^{(2)}, \\ u_i^* A_2 u_j &= \left(u_i^{(1)}\right)^* u_j^{(2)} + \left(u_i^{(2)}\right)^* u_j^{(1)}. \end{aligned}$$

So we have

$$\left(u_i^{(1)}\right)^* u_j^{(1)} = \left(u_i^{(2)}\right)^* u_j^{(2)} = \left(u_i^{(1)}\right)^* u_j^{(2)} + \left(u_i^{(2)}\right)^* u_j^{(1)} = 0 \text{ for } 1 \leq i < j \leq k. \qquad (2)$$

By rearranging the indices, we may assume that for some $0 \leq m_1 \leq m_2 \leq k$, $u_i^{(1)} = u_j^{(2)} = 0$ for $1 \leq i \leq m_1 < j \leq m_2$ and $u_i^{(1)}, u_i^{(2)} \neq 0$ for all $m_2 < i \leq k$. Then $u_i^{(2)}, u_j^{(1)} \neq 0$ for all $1 \leq i \leq m_1 < j \leq m_2$. By (2), $\{u_i^{(2)}, u_j^{(1)} : 1 \leq i \leq m_1 < j \leq m_2\} \cup \{u_i^{(1)} : m_2 < i \leq k\}$ is an orthogonal family of k nonzero vectors in $\mathbb{C}^{k-1}$, a contradiction. $\square$

Finally, we would like to extend these results to find a lower bound $r(k,m) \in \mathbb{N}$ such that, given $k, m \in \mathbb{N}$, $\Lambda_k(A_1, ..., A_m) \neq \varnothing$ for all $A_1, ..., A_m \in \mathcal{H}_n$ if $n \geq r(k,m)$. However, in this case, in addition to the condition that there exists a $U \in \mathbb{C}^{n\times k}$ s.t. $U^*U = I_k$ and $u_i^* u_j = u_i^* A_\ell u_j = 0$ for $1 \leq i < j \leq k$, $1 \leq \ell \leq m$, we have the condition $u_i^* A_\ell u_i = u_j^* A_\ell u_j$ for $1 \leq i < j \leq k$, $1 \leq \ell \leq m$. This condition cannot be expressed as a polynomial over $\mathbb{C}$, and so we cannot apply Proposition 2.9. However, we can apply Theorem 4.2.

Let $m \in \mathbb{N}$, $k \geq 2$ and let $q = (m+1)(k-1)+1$. Then by Theorem 4.7, if $n \geq \frac{m+3}{2} + m(q-2)$, $D_q(A_1, ..., A_m) \neq \varnothing$ for any $A_1, ..., A_m \in \mathcal{H}_n$. Since $U^*AU \in \mathcal{H}_n$ whenever $A \in \mathcal{H}_n$ and diagonal Hermitian matrices are real-valued, we then have $\Lambda_k(A_1, ..., A_m) \neq \varnothing$ by Theorem 4.2. This proves the following result:

Theorem 4.9. *Let $m \in \mathbb{N}, k \geq 2$, and let $n \geq \frac{m+3}{2} + m((m+1)(k-1)-1)$. Then for any $A_1, ..., A_m \in \mathcal{H}_n$, $\Lambda_k(A_1, ..., A_m) \neq \varnothing$.*

So $r(k,m) \leq \lceil \frac{m+3}{2} \rceil + m\big((m+1)(k-1)-1\big)$. This result improves on the bound $r(k,m) \leq m(m+1)(k-1)+1$ proved in [15] by $\lfloor \frac{m-1}{2} \rfloor$, where $\lfloor x \rfloor = \max\{a \in \mathbb{Z} : a \leq x\}$, and is therefore the best known bound for general m, k. However, there are some techniques that can improve on this bound for smaller values of m. First, due to [3] and [9], we have $r(k,1) = 2k-1$ and $r(k,2) = 3k-2$. Using these bounds and some additional techniques, we can also get better bounds for $3 \leq m \leq 7$.

Theorem 4.10. *Let $k \geq 1$ and $n \geq 6k-5$. Then for any $A_1, A_2, A_3 \in \mathcal{H}_n$, $\Lambda_k(A_1, A_2, A_3) \neq \varnothing$.*

Proof. For $m = 3, n \geq 2(3k-2)-1 = 6k-5$, let $A_1, A_2, A_3 \in \mathcal{H}_n$. Since $r(k,1) = 2k-1$, we can find a $P_1 \in \mathcal{P}_{3k-2}(n)$ s.t. $P_1 A_1 P_1 = \lambda P_1$ for some $\lambda \in \mathbb{C}$. Since $P_1 \in \mathcal{P}_k(n)$, it can be written $P_1 = UU^*$ for some $U \in \mathbb{C}^{n\times k}$ such that $U^*U = I_k$, we have $U^*A_1U = \lambda I_k$. Letting $B_2 = U^*A_2U, B_3 = U^*A_3U \in \mathcal{H}_{3k-2}$, we have $\Lambda_k(B_2, B_3) \neq \varnothing$, so there is a

$P_2 = VV^* \in \mathcal{P}_k(3k-2)$ s.t. $(P_2B_2P_2, P_2B_3P_2) = (c_1P_2, c_2P_2)$ for some $c_1, c_2 \in \mathbb{C}$. Then, letting $P = UVV^*U^*$, we have $P \in \mathcal{P}_k$ and $(PA_1P, PA_2P, PA_3P) = (\lambda P, c_1P, c_2P)$, so $\Lambda_k(A_1, A_2, A_3) \neq \varnothing$. □

A similar technique can be applied for $m = 4$, this time separating $A_1, A_2, A_3, A_4 \in \mathcal{H}_n$ into two sets of two. This will give us $n(4, k) \leq 9k - 8$. We utilize similar techniques for $m = 5, 6, 7, 8$, resulting in the table below, the columns of which give m, then the upper bound on $r(k, m)$ we can get using these techniques, which we will call $r'(k, m)$, the bound $r(k, m) \leq m(m + 1)(k - 1) + 1$ found in [15], and finally the new bound from Theorem 4.9. Note that for $m = 8$, our bound and the bound from [15] is actually better than $r'(k, m)$, and the value $\lceil \frac{m+3}{2} \rceil + m((m + 1)(k - 1) - 1) - r'(k, m)$ gets progressively larger as m increases past 8.

Table 4.1 *First column*: Number of matrices, *Second column*: Best upper bound on $r(k, m)$ achievable for m matrices using techniques similar to the proof of Theorem 4.10, *Third column*: Weaver's bound for m matrices, *Fourth column*: The bound from Theorem 4.9 for m matrices

m	$r'(k, m)$	$m(m + 1)(k - 1) + 1$	$\lceil \frac{m+3}{2} \rceil + m\big((m + 1)(k - 1) - 1\big)$
1	$2k - 1$	$2k - 1$	$2k - 1$
2	$3k - 2$	$6k - 5$	$6k - 5$
3	$6k - 5$	$12k - 11$	$12(k - 1)$
4	$9k - 8$	$20k - 19$	$20(k - 1)$
5	$18k - 17$	$30k - 29$	$30k - 31$
6	$27k - 26$	$42k - 41$	$42k - 43$
7	$54k - 53$	$56k - 55$	$56k - 58$
8	**81k-80**	**72k-71**	**72k-74**
9	**144k-146**	**90k-89**	**90k-93**

4.2 Geometry of $\Lambda_k(A_1, ..., A_m)$

Having considered the question of when $\Lambda_k(A_1, ..., A_m) \neq \varnothing$ for any $A_1, ..., A_m \in \mathcal{H}_n$, we now turn to a consideration of the geometric properties $\Lambda_k(A_1, ..., A_m)$ possesses when it is, in fact, non-empty. Since every point in $\Lambda_k(A_1, ..., A_m)$ represents a k-dimensional quantum error correcting code for any $\Phi : M_n \to M_n$ s.t. $S_\Phi \subset \text{span}(I, A_1, ..., A_m)$, having some understanding of the geometry of $\Lambda_k(A_1, ..., A_m)$ could be very useful. There are two geometric properties that have been the primary focus of research with respect to this question, namely *convexity* and *star-shape*.

We call a set $S \subset \mathbb{C}^n$ *convex* if, for any $x, y \in S$ and any $t \in [0, 1]$, $tx + (1 - t)y \in S$. Then the *convex hull* of S is $\text{conv}(S) := \cap\{T \subseteq \mathbb{C}^n : S \subset T, T \text{ is convex}\}$. From [7], we have $\Lambda_1(A_1, ..., A_m)$ is convex for every $A_1, ..., A_m \in \mathcal{H}_n$ for $m = 3, n \geq 3$. We also have the following result from [10]:

Theorem 4.11. *Suppose $A \in M_n$ and $1 \leq r < k$. Then*

$$\Lambda_k(A) = \cap\{\Lambda_{k-r}(X^*AX) : X \in \mathbb{C}^{n\times(n-r)}, X^*X = I_{n-r}\}$$

Letting $r = k - 1$, we get $\Lambda_k(A) = \cap\{W(X^*AX) : X \in \mathbb{C}^{n\times(n-1)}, X^*X = I_{n-1}\}$. Since the numerical range of every square matrix is convex by the Toeplitz-Hausdorff Theorem [16], $\Lambda_k(A)$ is convex for every matrix $A \in M_n$. Furthermore, any matrix $A \in M_n$ can be written as $A = A_1 + iA_2$ for some $A_1, A_2 \in \mathcal{H}_n$, so for any $U \in \mathbb{C}^{n\times k}$ s.t. $U^*U = I_k$ and $U^*AU = U^*A_1U + iU^*A_2U = \lambda I_k$, we have $(U^*A_1U, U^*A_2U) = (\lambda_1 I_k, \lambda_2 I_k)$. By the Spectral Decomposition Theorem, for some $D_1 = \text{diag}(d_{1,1}, ..., d_{n,n}) \in \mathbb{R}^{n\times n}$, $U_1 \in \mathcal{U}_n$ and any $x \in \mathbb{C}^n$

$$x^*A_1x = x^*U_1^*D_1U_1x = \sum_{i=1}^{n} |x_i|^2 d_{i,i} \in \mathbb{R}$$

So, $\lambda_1, \lambda_2 \in \mathbb{R}$. Let $a, b \in \Lambda_k(A)$. Then, since $\Lambda_k(A)$ is convex, for every $t \in [0,1]$ there is a $U_t \in \mathbb{C}^{n\times k}$ s.t.

$$\begin{aligned} U_t^* A_1 U_t + iU_t^* A_2 U_t = U_t^* A U_t &= (ta + (1-t)b)I_k \\ &= (t(a_1 + ia_2) + (1-t)(b_1 + ib_2))I_k \\ &= (ta_1 + (1-t)b_1)I_k + i(ta_2 + (1-t)b_2)I_k \end{aligned}$$

Then $U_t^* A_1 U_t = (ta_1 + (1-t)b_1)I_k$ and $U_t^* A_2 U_t = (ta_2 + (1-t)b_2)I_k$, and therefore $\Lambda_k(A_1, A_2)$ is convex.

On the other hand, we can have $\Lambda_k(A_1, ..., A_m)$ be nonconvex for $m \geq 3$. We find the following example in [8]:

Example. Let $B_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, B_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, B_3 = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$. We can see by straightforward calculation that $\Lambda_1(B_1, B_2, B_3) = W(B_1, B_2, B_3) = \{v \in \mathbb{C}^3 : ||v|| = 1\}$, which is not convex. Then, for $m \geq 3$, $k > 1$, let $A_j = B_j \otimes I_k$, and let $A_i = 0_{2k}$ for $3 < i \leq m$. Then $\Lambda_k(A_1, ..., A_m) \cong W(B_1, B_2, B_3)$, and is therefore not convex.

Finally, in [7], Li and Poon found that for $n > 1, m \geq 4$, there are $A_1, ..., A_m \in \mathcal{H}_n$ s.t. $\Lambda_1(A_1, ..., A_m)$ is not convex.

Theorem 4.12. *Suppose A_1, A_2, A_3 are Hermitian matrices such that $\{I, A_1, A_2, A_3\}$ is linearly independent. Then there exists a Hermitian matrix A_4 such that $W(A_1, A_2, A_3, A_4)$ is not convex.*

So, the conditions under which $\Lambda_k(A_1, ..., A_m)$ is convex for all $A_1, ..., A_m \in \mathcal{H}_n$ are quite limited. However, for large enough n, $\Lambda_k(A_1, ..., A_m)$ does have a property called *star-shaped*.

Definition 4.13. Let $S \subset \mathbb{C}^n$. Then S is *star-shaped* if there is an $x \in S$ s.t. for all $y \in S, t \in [0,1]$, $tx + (1-t)y \in S$. We call x a *star center* of S.

In [8], Li and Poon proved the following condition under which $\Lambda_k(A_1, ..., A_m)$ is star-shaped for all $A_1, ..., A_m \in \mathcal{H}_n$:

Theorem 4.14. *Let $A_1, ..., A_m \in \mathcal{H}_n$, and let $k \in \mathbb{N}$. If $\Lambda_{\hat{k}}(A_1, ..., A_m) \neq \varnothing$ for some $\hat{k} \geq (m+2)k$, then $\Lambda_k(A_1, ..., A_m)$ is star-shaped, and every element of conv $\Lambda_{\hat{k}}(A_1, ..., A_m)$ is a star-center for $\Lambda_k(A_1, ..., A_m)$.*

We can combine this with the result proved in Theorem 4.9, and we get

Theorem 4.15. *Let $m \geq 1, k \geq 2$, let $n \geq \frac{m+3}{2} + m\big((m+1)((m+2)k-1)-1\big)$ and let $A_1, ..., A_m \in \mathcal{H}_n$. Then $\Lambda_k(A_1, ..., A_m)$ is star-shaped.*

Previously the best known bound was $n \geq (m+1)^2((m+2)k-1)$ from [8]. The difference between this bound and ours is

$$(m+1)(m+2)k - \left\lceil \frac{m+5}{2} \right\rceil,$$

which is quite significant even at low values of m, k.

CHAPTER 5. FUTURE WORK

There are several questions that are still open for investigation in this area. First, the techniques used in the proof of Theorem 4.10 show that finding a lower bound on n s.t. $D_k(A_1, ..., A_m) \neq \varnothing$ for all $A_1, ..., A_m \in \mathcal{H}_n$ then applying Theorem 4.2 to replace k with $(m+1)(k-1)+1$ is inefficient. That is, it results in bounds that are significantly higher for some values of m, k than bounds that can be achieved using different techniques. However, the only alternate techniques found thus far either cannot extend beyond low values of m or k, or are only superior for low values of m. Finding a new technique that improves the bounds we have for general m, k would be a significant step forward.

Second, it it still an open question whether we have the best bound for n above which $D_k(A_1, ..., A_m) \neq \varnothing$ for all $A_1, ..., A_m \in \mathcal{H}_n$. We know the best bound for $k = 2$ and $m = 2$, and the best bound for $m = 1$ and $k = 1$ is trivial. However, we do not know if the methods used to extend our bounds to higher values of m and k are optimal. The particular application of the Bezout theorem that we use does give us an indication of where we could start, though.

Let $k, m > 2$, $n \in \mathbb{N}$, let $A_0 = I, A_1, ..., A_m \in \mathcal{H}_n$ and let $v \in \mathbb{C}^n$. Then, if $\dim(\text{span}(v, A_1 v, ..., A_m v)) = d \leq m$, for any $\alpha \subset \{0, ..., m\}$ with $|\alpha| = d + 1$, there is some $c^{(\alpha)} \in \mathbb{C}^{d+1}$ s.t. $\sum_{i \in \alpha} c_i^{(\alpha)} A_i v = 0$. Each such equation is composed of n forms on $\mathbb{P}^{n-1} \times \mathbb{P}^d$, and there are $p = \begin{pmatrix} m+1 \\ d+1 \end{pmatrix}$ such equations, for a total of $p \cdot n$ forms on $\mathbb{P}^{n-1} \times \left(\mathbb{P}^d\right)^p$. Then, by Bezout's Theorem, if $p \cdot n \leq n - 1 + p \cdot d$, there is always a nonzero solution. Some exploration into these numbers shows that the inequality is always satisfied for $d = m$ (as would be expected, since we can always choose v to be an eigenvector of A_1) and for $d = m - 1$, the inequality becomes $n \leq m - \frac{2}{m}$, which is equivalent to $n \leq m - 1$ for

$m \geq 2$. This bound obviously has some holes in it, since we know that $D_k(A_1, ..., A_m) \neq \varnothing$ for $A_1, ..., A_m \in \mathcal{H}_m$. However, it does give us a set of forms to study, and hopefully we can find some properties of the projective variety given by this set of forms.

Finally, the quantum channels we deal with are often artificially general. In real world applications, there are particular errors that are likely to occur if any error occurs at all, and most other errors are so unlikely that they can be ignored. For instance, the bit flip error $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and the phase flip error $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ have been widely studied because they occur more often, and there is a specific type of operator system that assumes that no more than r errors of this type occur during the transmission. Another example that has been studied is an error caused by a stable fault in the communication line, which would cause the same error to be applied to every bit in the quantum state. We would represent this using the quantum channel $\Phi(\rho) = (X^{\otimes r})\rho(X^{\otimes r})^*$, where $X \in \mathcal{U}_{2^s}$ and rs is the number of qubits in the system. The operator systems produced by such quantum channels can sometimes be corrected much more efficiently than just a general quantum channel $\Phi : M_n \to M_n$ with $\dim(S_\Phi) = m + 1$. There are a lot of important questions about the general case that could provide a baseline if they were solved, but when it comes to applying the theory practically, some communication between pure mathematicians and the physicists dealing directly with the physical problem can certainly help frame the problem better.

REFERENCES

[1] M.D. Choi, *Completely Positive Linear Maps on Complex Matrices,* Linear Algebra and its Applications, 10:3 (1975), 285-290

[2] F.M. DeAssis, E.B. Guedes, R.A.C. Medeiros, *Quantum Zero-Error Information Theory,* Springer, 2016

[3] K. Fan and G. Pall, *Embedding Conditions for Hermitian and Normal Matrices,* Canad. J. Math. 9 (1957), 298-304

[4] E. Knill, R. Laflamme, *A Theory of Quantum Error-Correcting Codes,* Physical Review A., 55:2 (1997), 900-911

[5] E. Knill, R. Laflamme, L. Viola, *Theory of Quantum Error Correction for General Noise,* Phys Rev Lett., 84:11 (2000), 2525-2528

[6] C.K. Li, M. Nakahara, Y.T. Poon, N.S. Sze, H. Tomita, *Recovery in quantum error correction for general noise without measurement* Quantum Information and Computation, 12 (2012), 149-158

[7] C.K. Li, Y.T. Poon, *Convexity of the joint numerical range,* J. Matrix Analysis Appl., 21 (1999), 668-678

[8] C.K. Li, Y.T. Poon, *Generalized Numerical Ranges and Quantum Error Correction,* J. Operator Theory, 66:2 (2011), 335-351

[9] C.K. Li, Y.T. Poon, N.S. Sze, *Condition for the higher rank numerical range to be non-empty,* Linear and Multilinear Algebra, 57 (2009), 365-368

[10] C.K. Li, Y.T. Poon, N.S. Sze, *Higher rank numerical ranges and low rank perturbations of quantum channels,* Journal of Mathematical Analysis and Applications, 348:2 (2008), 843-855

[11] C.K. Li, N.K. Sze, *Canonical forms, higher rank numerical ranges, totally isotropic subspaces, and matrix equations,* Proc. Amer. Math. Soc., 136:9 (2008), 3013–3023.

[12] Paulsen. (Winter 2016). *Entanglement and Non-Locality* [Lecture Notes], Retrieved from

`http://www.math.uwaterloo.ca/~vpaulsen/EntanglementAndNonlocality_LectureNotes_7.pdf`

[13] I.R. Shafarevich, *Basic Algebraic Geometry 1: Varieties in Projective Space,* 3rd ed., Springer, 2013

[14] H. Tverberg, *A generalization of Radon's theorem,* J. Lond. Math. Soc., 41 (1966), 123-128.

[15] N. Weaver, *The "Quantum" Turan Problem for Operator Systems,* Pacific Journal of Mathematics, 301 (2019), 335-349

[16] F. Zhang, *Matrix Theory: Basic Results and Techniques,* 2nd ed., Springer, 2011