STABILIZED DISTANCE MEASURES AND QUANTUM ERROR CORRECTION

A Thesis

Presented to

The Faculty of Graduate Studies

of

The University of Guelph

by

NATHANIEL D. JOHNSTON

In partial fulfilment of requirements

for the degree of

Master of Science

June, 2008

ABSTRACT

STABILIZED DISTANCE MEASURES AND QUANTUM ERROR CORRECTION

Nathaniel Johnston

University of Guelph

2008

Advisors:

Professor J. Holbrook

Professor D. Kribs

Quantum information theory is a quickly-growing area of research that presents no shortage of mathematical challenges. In this thesis, two basic analytic and algebraic problems of interest in quantum information are considered. The first problem considered is that of computing a crucial distance measure for linear maps on finite-dimensional Hilbert space, given by the the diamond and completely bounded norms of differences of quantum operations. Based on the theory of completely bounded maps, an algorithm to compute the diamond and completely bounded norms of arbitrary linear maps is formulated and presented. The algorithm is applied to derive a new proof and formula for the distance between arbitrary unitary maps. Finally,

an implementation of the algorithm *via* MATLAB is presented, and its efficiency is discussed. Attention is next turned to quantum error correction, where a new algebraic characterization of error-correcting codes is derived. These results are used to explicitly compute a correction operation, and a new characterization of correctable subsystems in terms of representation theory is obtained.

To My Parents

for instilling in me the desire to learn

Acknowledgements

The CB norm algorithm of Chapter 3 was originally developed by Vern Paulsen and presented at the February 2007 Banff Workshop on Operator Structures in Quantum Information Theory. Vern Paulsen is also thanked for helpful e-mails that led to Theorem 3.3.4, and Man-Duen Choi is thanked for helpful conversations leading to many of the results of Chapter 4. Many thanks of course go to my advisors and committees, and special thanks in particular are extended to David Kribs for providing an interest in quantum error correction, the means to study it, and immeasurable help over the last two years.

Thanks to my entire family for teaching me from a very young age that there's nothing greater in this world than learning. Thanks to Kim, Nick, Shaughnessy, and all of the math students that I have had the pleasure of studying with over the past several years for sharing thoughts, problems, solutions, and everything in between. Finally, thanks to Kathryn for always being there. Whether I need someone to listen to me complain about the math problem of the week that is driving me nuts, or someone to help me shift an image down to the next page in LaTeX, you never fail.

Table of Contents

Chapter 1

Introduction

1.1 Quantum Distance Measures

The need for physically significant and computable distance measures for quantum operations and channels is of fundamental importance in quantum information science [31]. Most importantly, it is often necessary to determine how far apart two quantum operations, represented by completely positive maps, are from each other in some meaningful sense. The *diamond norm* was introduced in [21] for this purpose. It arises from physical considerations and satisfies the important stability property desired for such measures [1, 13]. Interestingly, the diamond norm is intimately related to the *completely bounded norm*, a notion that has been studied in operator theory for different reasons over the past four decades [33].

On finite dimensional Hilbert spaces, every linear map has a finite completely

bounded (CB) norm. Thus, completely bounded maps are precisely the linear maps in the finite dimensional case. In operator theory, CB maps are the natural maps between operator spaces. Computing the norms of CB maps between certain operator spaces introduced in [35] has provided the impetus for recent progress on multiplicativity conjectures for quantum channels [10, 11, 15, 43]. CB maps and norms have also arisen in a wide variety of other recent investigations in quantum information science, including [17, 19, 22, 29, 36, 38, 42], though the CB terminology has not always been used.

In this thesis, based on the classical and contemporary theory of completely bounded maps, an algorithm to compute completely bounded and diamond norms for arbitrary linear maps on finite dimensional Hilbert spaces is derived. Along the way, a brief introduction to completely bounded map theory, including the generalized Stinespring theorem and Choi-Kraus representation for such maps, is provided. An implementation of the algorithm *via* MATLAB is then presented. Finally, the algorithm's efficiency is discussed and it is noted how it is potentially optimal in some sense. This work has been accepted to appear in Quantum Information and Computation [18].

In Chapter 2 a detailed introduction to operator spaces, completely positive maps, completely bounded maps, the completely bounded norm, and their relationship to quantum information theory is presented. The discussion of completely bounded maps provided in Section 2.2.2 is of particular importance and is motivated by the

presentation given in [33]. Chapter 3 develops the theory of completely bounded maps further and introduces an algorithm for computing it. The algorithm is then applied to derive a formula for the CB norm of one particular family of physically important maps. An implementation of the algorithm *via* MATLAB is provided in Section 3.3.4.

1.2 Quantum Error Correction

The problem of correcting errors in quantum information to maintain coherence is of paramount importance if quantum computers are to ever become a concrete reality. It has long been known that quantum channels often permit *correctable codes* [2, 14, 23, 37, 40] – subspaces of the overlying Hilbert space in which the states may be corrected via another quantum channel. This idea was extended in [26, 27] to *correctable subsystems*, which generalize both correctable codes and the well-studied areas of *noiseless subsystems* and *decoherence-free subspaces* [12, 20, 24, 30, 32, 44, 45].

Chapter 4 recalls some of the basic ideas of correctable codes and subsystems, while developing a new way of characterizing them. A well-known result about what quantum channels "look like" when restricted to a correctable code is provided and commented on in Section 4.1.1. This result is used to characterize correctable codes in terms of representations in Section 4.1.2. Finally, Sections 4.2.1 and 4.2.2 generalize these results to the subsystem setting.

Chapter 2

Preliminaries

2.1 C*-Algebras and Operator Spaces

Much of the mathematical formulation of quantum mechanics is based on the theory of Hilbert spaces and C*-algebras, and a familiarity with both will be assumed throughout this work. The definition of an (abstract) C*-algebra is provided for completeness, but for basic properties of C*-algebras, the reader is pointed to [9].

Denote the space of $n \times m$ matrices over some ring $\mathcal{V}$ by $\mathcal{M}_{n,m}(\mathcal{V})$. When $\mathcal{V} = \mathbb{C}$, set $M_{n,m} = M_{n,m}(\mathbb{C})$ as a notational convenience. Similarly, when $m = n$ set $M_n(\mathcal{V}) = M_{n,n}(\mathcal{V})$ and $M_n = M_{n,n}$. C*-algebras can be thought of intuitively as generalizations of M_n.

Definition 2.1.1. *A* **C*-algebra** $\mathcal{A}$ *is a Banach *-algebra such that* $\|a^\dagger a\| = \|a\|^2$ *for all* $a \in \mathcal{A}$.

It may be worth noting at this point that while the mathematical convention is to use $*$ to represent the adjoint operation, this thesis will favour the † notation instead, as that is the usual convention in quantum information theory.

Given a (separable) Hilbert space $\mathcal{H}$, denote the set of bounded linear operators on $\mathcal{H}$ by $\mathcal{B}(\mathcal{H})$. Given operators $T_{i,j} \in \mathcal{B}(\mathcal{H}), 1 \leq i \leq m, 1 \leq j \leq n$, identify the $m \times n$ matrix of operators, $(T_{i,j})$, with an operator from $\mathcal{H}^{(n)} = \mathcal{H} \oplus \ldots \oplus \mathcal{H}$ (n copies) to $\mathcal{H}^{(m)} = \mathcal{H} \oplus \ldots \oplus \mathcal{H}$ (m copies) by regarding vectors in these spaces as columns and performing matrix multiplication. That is, identify $M_{m,n}(\mathcal{B}(\mathcal{H})) \equiv \mathcal{B}(\mathcal{H}^{(n)}, \mathcal{H}^{(m)})$. This endows $M_{m,n}(\mathcal{B}(\mathcal{H}))$ with a norm and this collection of norms on $\mathcal{B}(\mathcal{H})$ is often referred to as the set of *matrix norms* on $\mathcal{B}(\mathcal{H})$.

Definition 2.1.2. *Let $\mathcal{A}$ be a C*-algebra and let $\mathcal{M} \subseteq \mathcal{A}$ be a subspace. Then the inclusion $M_{m,n}(\mathcal{M}) \subseteq M_{m,n}(\mathcal{A})$ endows this vector space with a collection of matrix norms and $\mathcal{M}$, together with this collection of matrix norms on $M_{m,n}(\mathcal{M})$, is called a (concrete)* **operator space**.

Thus, an operator space carries not just an inherited norm structure, but these additional matrix norms. C*-algebras are defined abstractly, but every abstract algebra is isomorphic to a concrete C*-algebra given by a subalgebra of some $B(\mathcal{H})$ that is closed under both the operator norm ($||\cdot||$) and adjoint (†) operation. If $\mathcal{A}$ is any C*-algebra and $\pi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{H})$ is a one-to-one †-homomorphism (and hence an isometry), then the collection of norms on $M_{m,n}(\pi(\mathcal{A}))$ is independent of the particular representation π, and hence, the operator space structure of a C*-algebra is indepen-

dent of the particular representation. Hence, each subspace $\mathcal{M} \subseteq \mathcal{A}$ is also endowed with a particular collection of matrix norms and so a subspace of a C*-algebra is also referred to as an operator space, when its matrix norm structure is to be emphasized.

A self-adjoint variation of operator spaces may also be defined and will be of much use throughout this work.

Definition 2.1.3. *If $\mathcal{A}$ is a unital C*-algebra, then a $\dagger$-closed subspace $\mathcal{S} \subseteq \mathcal{A}$ such that $1 \in \mathcal{S}$ is called an* **operator system**.

Thus, operator systems are operator spaces and have matrix norms. But the additional hypotheses guarantee that if $\mathcal{A}^+$ denotes the positive elements of the C*-algebra $\mathcal{A}$, then $\mathcal{S}$ is the span of $\mathcal{S}^+ \equiv \mathcal{S} \cap \mathcal{A}^+$, which is a cone in $\mathcal{S}$. It is also the case that $M_n(\mathcal{S})$ is the span of $M_n(\mathcal{S})^+ = M_n(\mathcal{S}) \cap M_n(\mathcal{A})^+$. The vector spaces $M_n(\mathcal{S})$ together with the cones $M_n(\mathcal{S})^+$ are often referred to as the *matrix ordering* on $\mathcal{S}$.

In order to illustrate these definitions, an operator system that will be of use later is defined here.

Definition 2.1.4. *Let $\mathcal{A}$ be a unital C*-algebra and let $\mathcal{M} \subseteq \mathcal{A}$ be an operator space. Then define an operator system $\mathcal{S}_{\mathcal{M}} \subseteq M_2(\mathcal{A})$, by*

$$\mathcal{S}_{\mathcal{M}} \equiv \left\{ \begin{bmatrix} \lambda 1 & a \\ b^\dagger & \mu 1 \end{bmatrix} : \lambda, \mu \in \mathbb{C}, a, b \in \mathcal{M} \right\}.$$

Indeed, $\mathcal{S}_{\mathcal{M}}$ is an operator system because $\lambda = \mu = 1$ and $a = b = 0$ gives the unit element of $M_2(\mathcal{A})$, $\mathcal{S}_{\mathcal{M}}$ is clearly a subspace (because $\mathcal{M}$ is a subspace), and $\mathcal{S}_{\mathcal{M}}$ is closed under $\dagger$.

2.2 Linear Maps on Operator Spaces

Throughout much of the later work of this thesis, attention will restricted to working with linear maps from M_n to M_k. Since quantum mechanics is linear, it is not surprising that evolution of quantum states (or observables) is modelled by these types of maps. This section will provide a more broad introduction to some special classes of linear maps in the setting of C*-algebras and operator spaces, as much of the discussion of completely bounded maps in particular is much more interesting in this more general setting.

2.2.1 Positive and Completely Positive Maps

Let $\mathcal{A}$ and $\mathcal{B}$ be C*-algebras, $\mathcal{S} \subseteq \mathcal{A}$ be an operator system, and $\phi : \mathcal{S} \mapsto \mathcal{B}$ be a linear map. ϕ is said to be *positive* if it maps positive elements of $\mathcal{S}$ to positive elements of $\mathcal{B}$. From ϕ one can construct a family of maps $\phi_m : M_m(\mathcal{S}) \mapsto M_m(\mathcal{B})$ $(m \geq 1)$ by letting $(a_{ij}) \in M_m(\mathcal{S})$ be an $m \times m$ matrix of operators and setting

$$\phi_m\big((a_{ij})\big) \equiv \big(\phi(a_{ij})\big) = \begin{bmatrix} \phi(a_{11}) & \phi(a_{12}) & \cdots & \phi(a_{1m}) \\ \phi(a_{21}) & \phi(a_{22}) & \cdots & \phi(a_{2m}) \\ \vdots & \vdots & \ddots & \vdots \\ \phi(a_{m1}) & \phi(a_{m2}) & \cdots & \phi(a_{mm}) \end{bmatrix}.$$

Note that ϕ_m is sometimes written as $id_m \otimes \phi$ and $M_m(\mathcal{S})$ is sometimes written as $M_m \otimes \mathcal{S}$. Building from these ideas, some new classes of maps can be defined:

Definition 2.2.1. *The map ϕ is said to be m-**positive** if ϕ_m is positive.*

Definition 2.2.2. *The map ϕ is said to be* **completely positive** *(CP) if it is m-positive $\forall m \geq 1$.*

An example is now provided to clarify Definitions 2.2.1 and 2.2.2 and introduce one important class of completely positive maps.

Example 2.2.3. *Let $\mathcal{A}$ and $\mathcal{B}$ be C^*-algebras and $\pi : \mathcal{A} \mapsto \mathcal{B}$ be a $\dagger$-homomorphism. If $(a_{ij}) \in M_n(\mathcal{A})$ is positive, then $\exists (b_{ij}) \in M_n(\mathcal{A})$ such that $(a_{ij}) = (b_{ij})^\dagger (b_{ij}) = (\sum_k b_{ki}^\dagger b_{kj})$ and so*

$$\pi_n\big((a_{ij})\big) = \big(\pi(a_{ij})\big) = \Big(\pi\big(\sum_k b_{ki}^\dagger b_{kj}\big)\Big) = \big(\sum_k \pi(b_{ki})^\dagger \pi(b_{kj})\big) = \big(\pi(b_{ij})\big)^\dagger \big(\pi(b_{ij})\big),$$

which is positive. It follows that π is n-positive and is thus completely positive, because n was arbitrary.

Clearly any map that is completely positive must be positive, but it is not immediately clear from the above definitions that there exist maps that are positive but not completely positive. To clarify this point, another example is provided.

Example 2.2.4. *Let $\phi : M_2 \mapsto M_2$ be the 2×2 transpose map. It is easy to see that the eigenvalues of a are exactly the eigenvalues of $\phi(a) = a^T$ for any $a \in M_2$, and thus ϕ is a positive map. To see that ϕ is not completely positive simply note that*

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

is positive (its eigenvalues are $2, 0, 0$*, and* 0*) but*

$$\phi_2\Big(\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}\Big) = \begin{bmatrix} \phi(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}) & \phi(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}) \\ \phi(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}) & \phi(\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is not positive (its eigenvalues are $1, 1, 1$*, and* -1*). It follows that* ϕ *is not* 2*-positive and thus not completely positive.*

Example 2.2.4 shows that there are some very simple positive maps that are not completely positive. One might wonder if there is a simple way to test whether or not a map is completely positive. Theorem 2.2.5 shows that there is indeed such a method when ϕ maps from M_n to M_k, and in particular that the method used in Example 2.2.4 works not only when a map is not completely positive but also when it *is* completely positive.

Theorem 2.2.5 (Choi [7])**.** *Let* $\phi : M_n \mapsto M_k$ *be a linear map and let* $\{E_{ij}\}$ *be the standard matrix units (ie. the* (i, j)*-entry of* E_{ij} *is* 1 *and all other entries are* 0*). Then the following are equivalent:*

1. ϕ *is completely positive.*

2. ϕ *is* n*-positive.*

3. *The matrix* $\phi_n\big((E_{ij})\big) = \big(\phi(E_{ij})\big)$ *is positive.*

The $kn \times kn$ matrix $\phi_n\big((E_{ij})\big)$ of condition 3 above is known as the *Choi matrix* of ϕ, and checking its positivity is usually one of the easiest ways of checking whether or not $\phi : M_n \mapsto M_k$ is completely positive.

A fundamental result for completely positive maps is *Stinespring's Representation Theorem*, which helps answer the question of what completely positive maps "look like". In order to help motivate this theorem, an example is provided.

Example 2.2.6. *Let $\mathcal{A}$ be a unital C*-algebra, $\mathcal{H}$ and $\mathcal{K}$ be Hilbert spaces, $V : \mathcal{H} \mapsto \mathcal{K}$ be a bounded operator, and $\pi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{K})$ be a unital $\dagger$-homomorphism. Then define a linear map $\phi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{H})$ by $\phi(a) = V^\dagger \pi(a) V$. If $(a_{ij}) \in M_n(\mathcal{A})$ is positive, then*

$$\phi_n\left((a_{ij})\right) = \left(\phi\left(a_{ij}\right)\right) = \left(V^\dagger \pi\left(a_{ij}\right) V\right) = \left(I_n \otimes V\right)^\dagger \pi_n\left((a_{ij})\right)\left(I_n \otimes V\right),$$

where I_n is the $n \times n$ identity matrix. It was seen in Example 2.2.3 that $\dagger$-homomorphisms are completely positive, and thus it follows from the above work that ϕ is completely positive as well.

Stinespring's Representation Theorem says that not only are maps of the form given in Example 2.2.6 completely positive, but more importantly that all completely positive maps can be written in that form.

Theorem 2.2.7 (Stinespring's Representation Theorem)**.** *Let $\mathcal{A}$ be a unital C*-algebra and let $\phi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{H})$ be a completely positive map. Then there exists a Hilbert space $\mathcal{K}$, a bounded operator $V : \mathcal{H} \mapsto \mathcal{K}$, and a unital $\dagger$-homomorphism, $\pi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{K})$ such that $\phi(a) = V^\dagger \pi(a) V$, for every $a \in \mathcal{A}$.*

Note that in Stinespring's theorem, one also has that $\|\phi(1)\| = \|V^\dagger V\| = \|V\|^2$. Theorem 3.2.2 will show that this quantity is also equal to $\|\phi\|_{cb}$, where $\|\cdot\|_{cb}$ is the *completely bounded norm*, which will be defined in the next section.

Stinespring's representation theorem has a particularly nice form when $\mathcal{A} = M_n$, $\mathcal{B}(\mathcal{H}) = M_k$, and ϕ is *unital* (ie. $\phi(I_n) = I_k$). To see why this is the case, note that all representations of M_n are unitarily equivalent to an ampliation of the identity representation [9]. Since ϕ is unital, it is the case that $I_k = \phi(I_n) = V^\dagger V$, and hence V is an isometry. The subspace $V\mathbb{C}^k \subseteq \mathcal{K}$ can then be identified with $\mathbb{C}^k$ and so ϕ can be written as $\phi(a) = V^\dagger(I_d \otimes a)V$, where I_d is an identity matrix of appropriate size. $V^\dagger$ then can be written as a row block matrix $V^\dagger = [A_1 \ A_2 \ \cdots \ A_d]$, and it follows that $\phi(a) = \sum_i^d A_i a A_i^\dagger$. The *Choi-Kraus representation theorem* for completely positive maps from M_n to M_k shows that this result holds even if ϕ is not unital.

Theorem 2.2.8 (Choi-Kraus Representation Theorem [7, 25])**.** *Let $\phi : M_n \mapsto M_k$ be a completely positive map. Then there exist matrices $A_i \in M_{k,n}, 1 \leq i \leq nk$, such that $\phi(a) = \sum_i A_i a A_i^\dagger$ for all $a \in M_n$.*

When speaking about a completely positive map $\phi : M_n \mapsto M_k$, a family of matrices $\{A_i\}$ as described by Theorem 2.2.8 is called a *Choi-Kraus representation* of ϕ, and the operators themselves are known as its *Kraus operators*.

Remark 2.2.9. *The Choi-Kraus representation for a given map is not unique, as it can be seen that if (u_{ij}) is a unitary matrix, then setting $B_i = \sum_j u_{ij} A_j$ gives $\{B_i\}$ as another Choi-Kraus representation of ϕ. In fact, it is not difficult to see that if the A_i's are linearly independent, then* all *linearly independent Choi-Kraus representations of ϕ can be obtained in this way – a fact that will be mirrored by the algorithm to be presented in Section 3.3.1.*

In spite of the above remark, when speaking of a completely positive map with a given representation in mind, it may be said that $\phi = \{A_i\}$ for convenience.

In order to illustrate these results, another example is provided. It will be seen later that the map examined in Example 2.2.10 represents an important, physically significant quantum operation.

Example 2.2.10. *Let $\phi : M_2 \mapsto M_2$ be defined by $\phi(a) = \frac{1}{2}\mathrm{Tr}(a)I_2$, where I_2 is the 2×2 identity matrix. By proceeding similarly to Example 2.2.4 it is easy to see that*

$$\phi_2(\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}) = \begin{bmatrix} \phi(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}) & \phi(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}) \\ \phi(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}) & \phi(\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}) \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

which is clearly positive. It thus follows from Theorem 2.2.5 that ϕ is completely positive. Theorem 2.2.8 then says that there exist matrices $A_i \in M_2, 1 \leq i \leq 4$, such that $\phi(a) = \frac{1}{2}\mathrm{Tr}(a)I_2 = \sum_i A_i a A_i^\dagger$ for all $a \in M_2$. Indeed, if one recalls the 2×2 Pauli matrices

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

then it is not difficult to verify that one Choi-Kraus representation of ϕ is given by the 4 matrices $\{\frac{1}{2}I_2, \frac{1}{2}X, \frac{1}{2}Y, \frac{1}{2}Z\}$. That is,

$$\phi(a) = \frac{1}{2}\mathrm{Tr}(a)I_2 = \frac{1}{4}(a + XaX^\dagger + YaY^\dagger + ZaZ^\dagger) \text{ for all } a \in M_2.$$

Finally, one last famous result about completely positive maps is provided to round out the discussion of this section. It is worth noting that the proof of the following theorem relies on the Hahn-Banach extension theorem of functional analysis.

Theorem 2.2.11 (Arveson's Extension Theorem)**.** *Let $\mathcal{S} \subseteq \mathcal{A}$ be an operator system and let $\phi : \mathcal{S} \mapsto \mathcal{B}(\mathcal{H})$ be completely positive. Then there exists a completely positive map $\psi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{H})$ that extends ϕ, that is, such that $\psi(a) = \phi(a)$ for all $a \in \mathcal{S}$.*

2.2.2 Completely Bounded Maps

Much of the discussion and many results of this section will mirror those of Section 2.2.1, as completely bounded (CB) maps are a generalization of completely positive maps – something that is made explicit by Theorems 2.3.5 and 3.2.2. Also, many of the results of this section are presented merely for completeness and to highlight the role that completely boundedness plays in the realm of operator theory. The focus of much of the later work of this paper will be restricted to CB maps on M_n, which are exactly the linear maps $\phi : M_n \to M_k$; a fact that will explored in more depth in Section 3.1.

Definition 2.2.12. *Given a C^*-algebra $\mathcal{A}$, an operator space $\mathcal{M} \subseteq \mathcal{A}$, and a linear map $\phi : \mathcal{M} \mapsto \mathcal{B}(\mathcal{H})$, it is said that ϕ is* **completely bounded** *if*

$$\|\phi\|_{cb} \equiv \sup_n \|\phi_n\|$$

is finite. Here $||\phi_n|| = \sup\left\{||\phi_n((a_{ij}))|| \ : \ (a_{ij}) \in M_n(\mathcal{M}),\ ||(a_{ij})|| \leq 1\right\}$.

It turns out that $\|\cdot\|_{cb}$ is a norm and is thus known as the *completely bounded (CB) norm.* More generally, any time that $\mathcal{M}$ and $\mathcal{N}$ are two spaces, both endowed

with a family of matrix norms, one can define the completely bounded norm of a map $\phi : \mathcal{M} \mapsto \mathcal{N}$ in analogy with Definition 2.2.12.

Similar to Theorems 2.2.7 and 2.2.8, there are representation theorems for completely bounded maps. The generalized Stinespring theorem is presented first, and it will be specialized to the finite-dimensional case subsequently.

Theorem 2.2.13 (The Generalized Stinespring Theorem)**.** *Let $\mathcal{A}$ be a unital C*-algebra and let $\phi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{H})$ be a completely bounded map. Then there exists a Hilbert space $\mathcal{K}$, bounded operators $V, W : \mathcal{H} \mapsto \mathcal{K}$ and a unital $\dagger$-homomorphism $\pi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{K})$, such that $\|\phi\|_{cb} = \|V\|\|W\|$ and $\phi(a) = V^\dagger \pi(a) W$ for all $a \in \mathcal{A}$.*

In the finite dimensional case of a completely bounded map $\phi : M_n \mapsto M_k$, the corresponding canonical form arises in a way similar to that described in the completely positive case. Indeed, Theorem 2.2.13 induces a matrix sum representation of CB maps from M_n to M_k as follows.

Theorem 2.2.14 (CB Representation Theorem)**.** *Let $\phi : M_n \mapsto M_k$ be a linear map. Then there exist matrices $A_i \in M_{k,n}, 1 \leq i \leq nk$, and matrices $B_i \in M_{n,k}, 1 \leq i \leq nk$, such that*

$$\phi(a) = \sum_{i=1}^{nk} A_i a B_i,$$

with $\|\phi\|_{cb}^2 = \|\sum_i A_i A_i^\dagger\| \|\sum_i B_i^\dagger B_i\|$.

When speaking about a linear map ϕ, a representation $\phi(a) = \sum_i A_i a B_i$ as described by Theorem 2.2.14 is called a *generalized Choi-Kraus representation* of ϕ.

Since the Choi-Kraus representation of a given completely positive map is not unique, it is not surprising that the generalized Choi-Kraus representation of a given completely bounded map is also not unique.

In addition to providing a useful representation of arbitrary linear maps between complex matrix spaces, Theorem 2.2.14 provides a starting point for computing the completely bounded norm of such maps. Although the norm equality described by the theorem does not hold for all generalized Choi-Kraus representations of the map, it will be seen shortly that it is always the case that $\|\phi\|_{cb}^2 \leq \|\sum_i A_i A_i^\dagger\| \|\sum_i B_i^\dagger B_i\|$. This avenue will be explored in some detail in Chapter 3.

As a simple example of a completely bounded map, consider again the 2×2 transpose map.

Example 2.2.15. *Let $\phi : M_2 \mapsto M_2$ be the 2×2 transpose map. It was seen in Example 2.2.4 that ϕ is not completely positive, but it is indeed completely bounded. Theorem 2.2.14 says that there must exist matrices $A_i, B_i \in M_2, 1 \leq i \leq 4$, such that*

$$\phi(a) = a^T = \sum_i A_i a B_i \quad \forall a \in M_2.$$

Indeed, if one recalls the 2×2 standard matrix units,

$$E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

then it is not difficult to verify that $\phi(a) = \sum_{i,j=1}^2 E_{ij} a E_{ij}$ defines one generalized Choi-Kraus representation of ϕ. That is,

$$\phi(a) = a^T = E_{11} a E_{11} + E_{12} a E_{12} + E_{21} a E_{21} + E_{22} a E_{22} \quad \forall a \in M_2.$$

In general, the $n \times n$ transpose map is also completely bounded (but not completely positive) for any $n \geq 2$, and it has a generalized Choi-Kraus representation given by $a^T = \sum_{i,j=1}^{n} E_{ij} a E_{ij}$, where $\{E_{ij}\}$ is any family of matrix units on M_n. It will be seen in Example 3.2.5 that this generalized Choi-Kraus representation actually satisfies the norm equality of Theorem 2.2.14.

Finally, this section is completed by sketching some of the ideas used in the proof of an extension theorem for completely bounded maps. In order to work up to this theorem, a lemma involving the operator system $\mathcal{S}_{\mathcal{M}}$ of Definition 2.1.4 is first presented.

Lemma 2.2.16. *Let $\mathcal{A}$ be a unital C*-algebra, $\mathcal{M} \subseteq \mathcal{A}$ be an operator space and let $\phi : \mathcal{M} \mapsto \mathcal{B}(\mathcal{H})$ be a linear map. Then $\|\phi\|_{cb} \leq 1$ if and only if $\Phi : \mathcal{S}_{\mathcal{M}} \mapsto M_2(\mathcal{B}(\mathcal{H}))$ is completely positive, where*

$$\Phi\Big(\begin{bmatrix} \lambda 1 & a \\ b^\dagger & \mu 1 \end{bmatrix}\Big) = \begin{bmatrix} \lambda I_{\mathcal{H}} & \phi(a) \\ \phi(b)^\dagger & \mu I_{\mathcal{H}} \end{bmatrix}.$$

In particular, using this identification of completely contractive ($||\phi||_{cb} \leq 1$) maps with "corners" of unital completely positive maps can be used to derive a version of Arveson's Extension Theorem for completely bounded maps. First scale ϕ so that $\|\phi\|_{cb} = 1$, then apply Arveson's Extension Theorem to extend $\Phi : \mathcal{S}_{\mathcal{M}} \mapsto M_2(\mathcal{B}(\mathcal{H}))$ to $\Psi : M_2(\mathcal{A}) \mapsto M_2(\mathcal{B}(\mathcal{H}))$, and finally let ψ be the corresponding $(1,2)$ matrix corner of Ψ. It is clear that ψ extends ϕ, but Wittstock's Extension Theorem goes one step further and says that $\|\psi\|_{cb} = \|\phi\|_{cb}$.

Theorem 2.2.17 (Wittstock's Extension Theorem)**.** *Let $\mathcal{M} \subseteq \mathcal{A}$ be an operator space and let $\phi : \mathcal{M} \mapsto \mathcal{B}(\mathcal{H})$ be completely bounded. Then there exists a completely bounded map $\psi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{H})$ that extends ϕ and satisfies $\|\psi\|_{cb} = \|\phi\|_{cb}$.*

2.3 Representing Quantum Information

In quantum information theory, it is sometimes convenient to represent pure quantum states mathematically as unit vectors $|\psi\rangle \in \mathbb{C}^n$. Representing states in this way can become cumbersome, however, as mixed states require *ensembles* of vectors $\{(p_i, |\psi_i\rangle)\}$ to be represented completely, where $\{p_i\}$ is a discrete probability distribution. Furthermore, representing quantum states in this way contains redundant information, as $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ represent the same quantum state for any $\theta \in [0, 2\pi)$. Thus, quantum states are also often represented by *density matrices*:

Definition 2.3.1. *A matrix $\rho \in M_n$ is said to be a* **density matrix** *if it is Hermitian, positive-semidefinite and has* $\mathrm{Tr}(\rho) = 1$.

The density matrix ρ for a given pure quantum state can be obtained from its vector representation $|\psi\rangle$ by the simple formula $\rho = |\psi\rangle\langle\psi|$, where $\langle\psi| \equiv |\psi\rangle^\dagger$. Similarly, the density matrix for a mixed quantum state can be obtained from its ensemble $\{p_i, |\psi_i\rangle\}$ by the formula $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Density matrices encompass all of the information contained in their corresponding quantum states, while providing a clean and compact way of writing the information down mathematically.

In addition to states, quantum systems have *observables*, which are modeled by self-adjoint operators in M_n. There are two (equivalent) ways of looking at the evolution of quantum information over time – the *Schrödinger picture* and the *Heisenberg picture*. In the Schrödinger picture, states evolve over time, while observables remain fixed. In the Heisenberg picture, just the opposite is true – observables evolve over time and states remain fixed.

2.3.1 Quantum Channels as Completely Positive Maps

In the Schrödinger picture, evolution of a quantum state represented by the density matrix ρ is represented by a linear map $\mathcal{E}$ that maps density matrices to density matrices. It is clear then that $\mathcal{E}$ must be positive and trace-preserving. However, it is also required that $id_n \otimes \mathcal{E}$ be positive for all $n \geq 1$ so that positivity of ρ will be preserved even if there is an ancillary quantum system that is independent of the system that ρ lives in – $\mathcal{E}$ must therefore be completely positive. This is the motivation for the following definition.

Definition 2.3.2. *A completely positive, trace-preserving linear map* $\mathcal{E} : M_n \mapsto M_n$ *is called a* **quantum channel** *or a* **quantum operation**.

If $\{E_i\}$ is a Choi-Kraus representation of $\mathcal{E}$ as in Theorem 2.2.8, then it is not difficult to see that the trace-preservation requirement of $\mathcal{E}$ is equivalent to the requirement that $\sum_i E_i^\dagger E_i = I_n$.

To see how the evolution of observables is modelled in the Heisenberg picture, one first must define an inner product on M_n.

Definition 2.3.3. *Let $a, b \in M_n$. Then the* **Hilbert-Schmidt inner product** *of a and b is given by $\langle a, b\rangle_{HS} \equiv \mathrm{Tr}(b^\dagger a)$.*

It is not difficult to verify that this is in fact a valid inner product, and that it actually induces the familiar Frobenius norm on the space M_n.

With the Hilbert-Schmidt inner product in mind, one can now construct the dual map $\mathcal{E}^\dagger$ of $\mathcal{E}$ in the usual way as the unique map such that $\langle \mathcal{E}(a), b\rangle_{HS} = \langle a, \mathcal{E}^\dagger(b)\rangle_{HS}$ $\forall a, b \in M_n$. It is not difficult to see that if $\mathcal{E} = \{E_i\}$ then $\mathcal{E}^\dagger = \{E_i^\dagger\}$, so $\mathcal{E}^\dagger$ is also completely positive. In fact, if $\phi : M_n \mapsto M_k$ is completely bounded with generalized Choi-Kraus representation $\phi(a) = \sum_i A_i a B_i$, then $\phi^\dagger : M_k \mapsto M_n$ is completely bounded and has the representation $\phi^\dagger(b) = \sum_i A_i^\dagger b B_i^\dagger$.

Now recall that if ρ is a density matrix and X is an observable, then the expected value is given by $\mathrm{Tr}(\rho X)$. Thus, if evolution is given in the Schrödinger picture by the map $\mathcal{E}$, the new expected value will be given by $\mathrm{Tr}(\mathcal{E}(\rho)X)$. This can be interpreted as the observables evolving rather than the states evolving because $\mathrm{Tr}(\mathcal{E}(\rho)X) = \mathrm{Tr}(\rho\mathcal{E}^\dagger(X))$, and so $\mathcal{E}^\dagger$ models evolution in the Heisenberg picture.

It was seen that $\mathcal{E}$ is trace-preserving, so there must be some restriction on $\mathcal{E}^\dagger$ besides complete positivity. Well, note that

$$\mathrm{Tr}(a) = \mathrm{Tr}(\mathcal{E}(a)) = \mathrm{Tr}(I_n\mathcal{E}(a)) = \mathrm{Tr}(\mathcal{E}^\dagger(I_n)a) \quad \forall\, a \in M_n.$$

It follows that $\mathcal{E}^\dagger(I_n) = I_n$ (ie. $\mathcal{E}^\dagger$ is *unital*). It similarly follows that if $\mathcal{E}$ is itself unital, then $\mathcal{E}^\dagger$ is trace-preserving and therefore a quantum channel itself.

In order to illustrate these concepts, recall the completely positive map given in Example 2.2.10.

Example 2.3.4. *Let $\phi : M_2 \mapsto M_2$ be defined by $\phi(a) = \frac{1}{2}\mathrm{Tr}(a)I_2$. It is clear that $\mathrm{Tr}(\phi(a)) = \mathrm{Tr}(\frac{1}{2}\mathrm{Tr}(a)I_2) = \frac{1}{2}(\mathrm{Tr}(a) + \mathrm{Tr}(a)) = \mathrm{Tr}(a)$ and so ϕ is a valid quantum channel. Indeed, ϕ is known as the completely depolarizing channel because it turns any density matrix into $\frac{1}{2}I_2$.*

It was seen earlier that one particular Choi-Kraus representation for ϕ is given by $\left\{\frac{1}{2}I_2, \frac{1}{2}X, \frac{1}{2}Y, \frac{1}{2}Z\right\}$. Much more is true, and what follows will emphasize the non-uniqueness of a given map's Choi-Kraus representation.

Let $\left\{A_i\right\}$ be a family of 4 matrices that form an orthonormal basis for M_2 under the Hilbert-Schmidt inner product. That is,

$$\mathrm{Tr}(A_i^\dagger A_j) = \delta_{i,j} \quad \forall\, 1 \leq i, j \leq 4, \tag{2.1}$$

where $\delta_{i,j}$ is the Kronecker delta. It then follows that $\left\{\frac{1}{\sqrt{2}}A_i\right\}$ is a Choi-Kraus representation of ϕ. To see why this is the case, note that $\left\{\frac{1}{\sqrt{2}}I_2, \frac{1}{\sqrt{2}}X, \frac{1}{\sqrt{2}}Y, \frac{1}{\sqrt{2}}Z\right\}$ is one such basis of M_2, so it follows that any other matrix in M_2 can be written as a linear combination of those four matrices. In particular, there exist constants $\{u_{ij}\}_{i,j=1}^4$ such that

$$A_i = \frac{1}{\sqrt{2}}u_{i1}I_2 + \frac{1}{\sqrt{2}}u_{i2}X + \frac{1}{\sqrt{2}}u_{i3}Y + \frac{1}{\sqrt{2}}u_{i4}Z \quad \forall\, 1 \leq i \leq 4.$$

It is not difficult to verify then that Equation (2.1) implies that (u_{ij}) is a unitary matrix, and thus the result follows from Remark 2.2.9.

It is not surprising that this result extends quite simply to the completely depolarizing channel on M_n. That is, if $\psi : M_n \mapsto M_n$ is defined by $\psi(a) = \frac{1}{n}\mathrm{Tr}(a)I_n$, then ψ is a quantum channel such that if $\{B_i\}$ is a family of n^2 matrices that form an orthonormal basis for M_n under the Hilbert-Schmidt inner product, then $\psi = \{\frac{1}{\sqrt{n}}B_i\}$ defines a Choi-Kraus representation of ψ.

Finally, it is easy to see that $\psi = \psi^\dagger$, because

$$\mathrm{Tr}(\psi(a)b) = \mathrm{Tr}\big(\tfrac{1}{n}\mathrm{Tr}(a)b\big) = \tfrac{1}{n}\mathrm{Tr}(a)\mathrm{Tr}(b) = \mathrm{Tr}\big(a(\tfrac{1}{n}\mathrm{Tr}(b))\big) = \mathrm{Tr}(a\psi(b)) \quad \forall\, a, b \in M_n.$$

2.3.2 Differences of Quantum Channels as CB Maps

In quantum information one is often interested in properties of differences $\mathcal{E} - \mathcal{F}$ between pairs of quantum channels. Such a difference is still completely bounded, though not necessarily completely positive. Indeed, the linear span of the completely positive maps is exactly the set of completely bounded maps – a fact that is implied by the following theorem.

Theorem 2.3.5 (Wittstock's Decomposition Theorem)**.** *Let $\mathcal{A}$ be a C*-algebra with unit and let $\phi : \mathcal{A} \mapsto \mathcal{B}(\mathcal{H})$ be completely bounded. Then ϕ can be written as a linear combination of four or fewer completely positive maps.*

Note that Wittstock's decomposition theorem parallels the corresponding statement about general operators and positive operators on $\mathcal{H}$, though the proof is more

delicate and follows as a result of the generalized Stinespring theorem.

In the finite-dimensional case of maps $\phi : M_n \mapsto M_k$ and $\psi : M_n \mapsto M_k$ that are given by Choi-Kraus representations $\phi = \{A_i\}$ and $\psi = \{B_i\}$, it is easy to construct a generalized Choi-Kraus representation for $\phi - \psi$ by noting that

$$(\phi - \psi)(a) = \sum_i A_i a A_i^\dagger + \sum_i B_i a (-B_i^\dagger).$$

If the above representation of $\phi - \psi$ contains more than nk summands, the map can be run through Steps 1 through 3 of the algorithm described in Section 3.3.1 to remove linear dependencies in the representation.

Chapter 3

Computation and Estimation of the CB/$\diamond$ Norm

3.1 CB and $\diamond$ Norms in Quantum Information

The CB norm has been introduced and some of its basic properties have been examined, but it remains to be seen why it is *useful* in the context of quantum information theory. Certainly it can be used as a measure of distance between quantum channels by defining $d(\mathcal{E}, \mathcal{F}) \equiv \|\mathcal{E} - \mathcal{F}\|_{cb}$, but any other norm can define a distance measure between quantum channels in an analogous way. Indeed, there are several other commonly-used norms for linear maps. For example, the 1-norm of a linear map ϕ is given by $||\phi||_1 = \sup_{||a||_1 \leq 1} ||\phi(a)||_1$, where $||a||_1 = \mathrm{Tr}(\sqrt{a^\dagger a})$. The operator norm of ϕ is $||\phi|| = \sup_{||a|| \leq 1} ||\phi(a)||$, where $||a|| = \sup_{||\xi|| \leq 1} ||a\xi||$.

The problem with using the 1-norm or the operator norm as a distance measure for quantum channels is that neither of the distance measures defined by these norms satisfies the *stabilization property* for distance measures of quantum channels [1, 13, 21]:

$$d(id_m \otimes \mathcal{E}, id_m \otimes \mathcal{F}) = d(\mathcal{E}, \mathcal{F}) \quad \forall m \geq 1.$$

This property is desirable because it implies that the distance between quantum operations is unaffected by any ancillary quantum system that is independent of the original system. The *diamond norm* is defined in [1, 21] in such a way that it satisfies the stabilization property. Although it was originally defined through partial traces, the following definition was shown to be equivalent.

Definition 3.1.1. *For a linear map* $\phi : M_n \mapsto M_k$*, the* **diamond norm** *is given by*

$$||\phi||_\diamond \equiv ||\phi_n||_1.$$

It is not immediately clear from its definition why the diamond norm satisfies the stabilization property. It is the case, however, that the stabilization property is satisfied by the CB norm. To see why the diamond norm satisfies the stabilization property, some auxiliary results are provided that will help establish a link between the diamond norm and the CB norm.

First note that it is easily verified that $\|\phi_m\| \leq \|\phi_{m+1}\|$ and $\|\phi_m\| \leq m\|\phi\|$ for all $m \geq 1$ ([33], Chapter 1). Note also that $||\mathcal{U}\,\phi||_{cb} = ||\phi||_{cb} = ||\phi\mathcal{U}||_{cb}$ for every unitarily implemented map $\mathcal{U}(\cdot) = U(\cdot)U^\dagger$. Furthermore, one has that $||\phi \otimes \psi||_{cb} = ||\phi||_{cb}||\psi||_{cb}$,

and $||id||_{cb} = 1$. The identification of Theorem 3.1.2 shows that the corresponding properties hold for the diamond norm.

In order to establish the link between the completely bounded norm and the diamond norm, note that a theorem of Smith [33, 39] says that the CB norm stabilizes in the sense that if $\phi : M_n \mapsto M_k$ then $||\phi||_{cb} = ||\phi_k||$. One may then make use of the duality relationship [6] given by $||\phi|| = ||\phi^\dagger||_1$, to see that

$$||\phi||_{cb} = ||\phi_k|| = ||\phi_k^\dagger||_1 = ||\phi^\dagger||_\diamond,$$

since $\phi^\dagger : M_k \mapsto M_n$.

Putting these results together yields the following theorem [39].

Theorem 3.1.2. *Let $\phi : M_n \mapsto M_k$ be a linear map. Then*

$$\|\phi\|_{cb} = \|\phi^\dagger\|_\diamond = \|\phi_k\| \leq k\|\phi\|.$$

Using the fact that these maps appear as dual pairs, it is not hard to see that for $\psi : M_m \mapsto M_j$, one has that $\|\psi\|_\diamond = \|\psi^\dagger\|_{cb} \leq m\|\psi^\dagger\|$ and the stability of the diamond norm [1, 21] is the dual version of Smith's stability for the CB norm [39].

For maps whose domain is M_n and range is an arbitrary operator space, a result of Haagerup shows that, in general, $\|\phi\|_{cb} \neq \|\phi_m\|$, no matter how large one takes m ([33], p. 114). However, there *is* an upper bound that can derived. To this end, it is enough to know that given a finite dimensional normed space X, there exists a constant $\alpha(X)$ called the *alpha constant* of the space, with the property that

$$\|\phi\|_{cb} \leq \alpha(X)\|\phi\|$$

for any map with domain that is an operator space that is isometrically isomorphic to X as normed spaces. Given two finite dimensional normed spaces X, Y of the same dimension one has

$$\alpha(X) \leq d(X,Y)\alpha(Y),$$

where $d(X,Y)$ denotes the *Banach-Mazur distance* between the spaces. These concepts and results are explained in more detail in [34].

Theorem 3.1.3. *Let $\mathcal{M}$ be an operator space and let $\phi : M_n \mapsto \mathcal{M}$ be a linear map. Then $\|\phi\|_{cb} \leq \sqrt{n^3}\|\phi\|$.*

Proof. Let $\|a\|_2$ denote the Frobenius norm of a matrix $a \in M_n$. Note that M_n with the Frobenius norm is isometrically isomorphic to $\mathbb{C}^{n^2}$ with the standard 2-norm. It is well-known that $\|a\| \leq \|a\|_2 \leq \sqrt{n}\|a\|$, and thus the Banach-Mazur distance satisfies $d(M_n, \mathbb{C}^{n^2}) \leq \sqrt{n}$.

Hence, $\alpha(M_n) \leq d(M_n, \mathbb{C}^{n^2})\alpha(\mathbb{C}^{n^2}) \leq \sqrt{n}\alpha(\mathbb{C}^{n^2})$. Finally, it was shown in [34] that $\alpha(\mathbb{C}^m) \leq \sqrt{m}$, from which the result follows. ■

Combining this result with Theorem 3.1.2 gives the following corollary.

Corollary 3.1.4. *Let $\phi : M_n \to M_k$ be a linear map. Then $\|\phi\|_{cb} \leq \min\{k, \sqrt{n^3}\}\,||\phi||$ and $\|\phi\|_\diamond \leq \min\{n, \sqrt{k^3}\}\,||\phi^\dagger||$.*

3.2 Special Cases of the CB/$\diamond$ Norm

It will be seen that exactly computing the CB norm of a general CB map seems to be a very difficult task, so attention in this section will be restricted to certain classes of CB maps. Perhaps one of the most obvious classes of completely bounded maps to look at is the class of completely positive maps, and it turns out that there is indeed a simple way of calculating the CB norm of these maps.

It can be seen by combining the Choi-Kraus representation theorem and Theorem 2.2.14 that if $\phi : M_n \mapsto M_k$ is completely positive, then

$$\|\phi\|_{cb} = \|\sum_i A_i A_i^\dagger\|^{\frac{1}{2}} \|\sum_i A_i A_i^\dagger\|^{\frac{1}{2}} = \|\sum_i A_i A_i^\dagger\| = \|\phi(I_n)\|.$$

It turns out that this result holds no matter what the domain and range of ϕ are, and a proof of this fact is provided for completeness. A technical lemma is first presented.

Lemma 3.2.1. *Let $\mathcal{H}$ be a Hilbert space and let $A, P \in \mathcal{B}(\mathcal{H})$ such that $P \geq 0$. Then $\begin{bmatrix} P & A \\ A^* & P \end{bmatrix} \geq 0$ implies that $\|A\| \leq \|P\|$. Furthermore, if $P = I$ then the converse also holds.*

Proof. To show the forward implication, note that if $\begin{bmatrix} P & A \\ A^* & P \end{bmatrix} \geq 0$ then it follows that $\left\langle \begin{bmatrix} P & A \\ A^* & P \end{bmatrix} \begin{bmatrix} x \\ -y \end{bmatrix} \middle| \begin{bmatrix} x \\ -y \end{bmatrix} \right\rangle \geq 0 \ \forall x, y \in \mathcal{H}$ s.t. $\|x\| = \|y\| = 1$. Thus, $\langle Px|x\rangle + \langle Py|y\rangle \geq \langle Ay|x\rangle + \langle x|Ay\rangle = 2Re\left(\langle Ay|x\rangle\right)$. Also, the Cauchy-Schwarz Inequality says that $\langle Px|x\rangle + \langle Py|y\rangle \leq \|Px\|\|x\| + \|Py\|\|y\| \leq 2\|P\|$ since $\|x\| = \|y\| = 1$. Thus, $\|P\| \geq Re\left(\langle Ay|x\rangle\right) \forall x, y \in \mathcal{H}$ s.t. $\|x\| = \|y\| = 1$. A little thought reveals that this

is equivalent to $\|P\| \geq |\langle Ay|x\rangle| \, \forall x, y \in \mathcal{H}$ s.t. $\|x\| = \|y\| = 1$, which immediately implies that $\|A\| \leq \|P\|$.

To show the converse when $P = I$, build a contradiction by assuming that $\|A\| \leq \|I\| = 1$ and that $\exists x, y \in \mathcal{H}$ such that $\left\langle \begin{bmatrix} I & A \\ A^* & I \end{bmatrix} \begin{bmatrix} x \\ -y \end{bmatrix} \middle| \begin{bmatrix} x \\ -y \end{bmatrix} \right\rangle < 0$. It then follows that $\|x\|^2 + \|y\|^2 < \langle Ay|x\rangle + \langle x|Ay\rangle$.

The Cauchy-Schwarz Inequality then says that $\langle Ay|x\rangle + \langle x|Ay\rangle \leq \|Ay\| \, \|x\| + \|x\| \, \|Ay\| \leq 2 \|A\| \, \|x\| \, \|y\| \leq 2 \|x\| \, \|y\|$. Thus, $\|x\|^2 + \|y\|^2 < 2 \|x\| \, \|y\|$ and so $(\|x\| - \|y\|)^2 < 0$, completing the contradiction. ■

As a result of Lemma 3.2.1, the following theorem is readily proved. Note that Theorem 3.2.2 provides confirmation once more that completely bounded maps generalize completely positive maps.

Theorem 3.2.2. *Let $\mathcal{S} \subseteq \mathcal{A}$ be an operator system, let $\mathcal{B}$ be a C*-algebra, and let $\phi : \mathcal{S} \to \mathcal{B}$ be a completely positive map. Then ϕ is completely bounded and $\|\phi\|_{cb} = \|\phi\| = \|\phi(1)\|$.*

Proof. First note that $\|\phi(1)\| \leq \|\phi\| \leq \|\phi\|_{cb}$, so it is only necessary to show that $\|\phi\|_{cb} \leq \|\phi(1)\|$.

Fix n and let $A \in \mathcal{M}_n(\mathcal{S})$ be such that $\|A\| \leq 1$, and let I_n be the unit of $\mathcal{M}_n(\mathcal{A})$. Then Lemma 3.2.1 tells us that $\begin{bmatrix} I_n & A \\ A^* & I_n \end{bmatrix} \geq 0$. Since ϕ is completely positive, it then follows that $\phi_{2n}\left(\begin{bmatrix} I_n & A \\ A & I_n \end{bmatrix} \right) = \begin{bmatrix} \phi_n(I_n) & \phi_n(A) \\ \phi_n(A)^* & \phi_n(I_n) \end{bmatrix} \geq 0$. Making use of Lemma 3.2.1 again shows that $\|\phi_n(A)\| \leq \|\phi_n(I_n)\| = \|\phi(1)\|$. Since this inequality holds for any

such A, the proof is complete. ■

Theorem 3.2.2 can now be used to determine the diamond norm of completely positive maps by using the dual relationship of Theorem 3.1.2 and recalling that if $\phi : M_n \mapsto M_k$ is completely positive then $\phi^\dagger$ is also completely positive. The following corollary follows from the fact that if $\mathcal{E}$ is a quantum channel then $\mathcal{E}^\dagger$ is unital.

Corollary 3.2.3. *Let $\mathcal{E} : M_n \mapsto M_n$ be a quantum channel. Then $||\mathcal{E}||_\diamond = ||\mathcal{E}^\dagger||_{cb} = 1$.*

Before proceeding to try to calculate the CB norm of other types of maps, first suppose that a particular generalized Choi-Kraus representation of some CB map ϕ is given by $\phi(a) = \sum_{i=1}^m A_i a B_i$. It then follows that

$$\phi_n((a_{ij})) = \left[(I_n \otimes A_1) \cdots (I_n \otimes A_m)\right] (I_m \otimes (a_{ij})) \begin{bmatrix} (I_n \otimes B_1) \\ \vdots \\ (I_n \otimes B_m) \end{bmatrix}.$$

Hence,

$$\|\phi\|_{cb} \leq \| \left[A_1 \cdots A_m\right] \| \| \begin{bmatrix} B_1 \\ \vdots \\ B_m \end{bmatrix} \| = \| \sum_{i=1}^m A_i A_i^\dagger \|^{\frac{1}{2}} \| \sum_{i=1}^m B_i^\dagger B_i \|^{\frac{1}{2}}.$$

This also leads to the following extremely useful corollary of Theorem 2.2.14.

Corollary 3.2.4. *Let $\phi : M_n \mapsto M_k$ be a linear map. Then*

$$\|\phi\|_{cb} = \|\phi^\dagger\|_\diamond = \inf \left\{ \| \sum_i A_i A_i^\dagger \|^{\frac{1}{2}} \| \sum_i B_i^\dagger B_i \|^{\frac{1}{2}} \right\},$$

where the infimum is taken over all generalized Choi-Kraus representations of ϕ.

By taking advantage of the above corollary, it may be possible to calculate the exact CB norm of a given map even if it is not completely positive. As a simple example, consider again the 2×2 transpose map.

Example 3.2.5. *Let $\phi : M_2 \mapsto M_2$ be the 2×2 transpose map. It was seen in Example 2.2.15 that one generalized Choi-Kraus representation of ϕ is given by the matrices*

$$A_1 = B_1 = E_{11} \qquad A_2 = B_2 = E_{12} \qquad A_3 = B_3 = E_{21} \qquad A_4 = B_4 = E_{22},$$

where $\{E_{ij}\}$ are the standard 2×2 matrix units. It then follows from Corollary 3.2.4 that

$$\|\phi\|_{cb} \leq \left\| \sum_{i,j=1}^{2} E_{i,j} E_{i,j}^{\dagger} \right\|^{\frac{1}{2}} \left\| \sum_{i,j=1}^{2} E_{i,j}^{\dagger} E_{i,j} \right\|^{\frac{1}{2}} = \left\| \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \right\|^{\frac{1}{2}} \left\| \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \right\|^{\frac{1}{2}} = 2$$

Also, it is not difficult to verify that $\left\| \begin{bmatrix} E_{11} & E_{21} \\ E_{12} & E_{22} \end{bmatrix} \right\| = 1$ and

$$\left\| \phi_2\left(\begin{bmatrix} E_{11} & E_{21} \\ E_{12} & E_{22} \end{bmatrix} \right) \right\| = \left\| \begin{bmatrix} \phi(E_{11}) & \phi(E_{21}) \\ \phi(E_{12}) & \phi(E_{22}) \end{bmatrix} \right\| = \left\| \begin{bmatrix} E_{11} & E_{12} \\ E_{21} & E_{22} \end{bmatrix} \right\| = 2.$$

It thus follows that $\|\phi\|_{cb} = 2$. Also, it is not difficult to see that $\phi^{\dagger} = \phi$ here, so it follows from Theorem 3.1.2 that $\|\phi\|_{\diamond} = 2$ as well. This same method can be used to show that if $\psi : M_n \mapsto M_n$ is the $n \times n$ transpose map, then $\|\psi\|_{cb} = \|\psi\|_{\diamond} = n$.

There is one final family of completely bounded maps whose CB norm is exactly calculable that will be presented in this paper – those of the form $\phi = \mathcal{U} - \mathcal{V}$, where $\mathcal{U}$ and $\mathcal{V}$ are unitarily-implemented maps. Because the techniques used to derive the

CB norm of such maps have not yet been presented, further discussion of such maps is deferred to Section 3.3.3.

3.3 CB Norm Estimation Algorithm

Although it has been seen that the CB norm of certain maps can be easily calculated, exactly calculating the CB norm of a general CB map seems to require computing a complicated infimum over families of matrices. CB norms can be *estimated*, however, and Corollary 3.2.4 provides the starting point for an algorithm that does exactly that.

3.3.1 Description of the Algorithm

Let $\phi : M_n \mapsto M_k$ be a linear map with some given generalized Choi-Kraus representation $\phi(a) = \sum_{i=1}^{m} A_i a B_i$. By Corollary 3.2.4 it follows that one way to compute the CB norm ϕ is to do a minimization of the quantity $\left\| \sum_i A_i A_i^\dagger \right\|^{\frac{1}{2}} \left\| \sum_i B_i^\dagger B_i \right\|^{\frac{1}{2}}$ over all generalized Choi-Kraus representations of ϕ. This turns out to be somewhat more attainable than might be imagined and an algorithm for estimating the CB/$\diamond$-norm of such maps is presented here. The algorithm is described first – its mathematical justification is saved for Section 3.3.2.

Step 1. Find a basis, $\{C_1, ..., C_l\}$ for the span of $\{B_1, ..., B_m\}$ and express

$$B_i = \sum_j d_{i,j} C_j.$$

Step 2. Using the expressions for each B_i as a linear combination of C_j one may re-write $\phi(a) = \sum_{j=1}^{l} D_j a C_j$. In fact,

$$\phi(a) = \sum_i A_i a \Big(\sum_j d_{i,j} C_j \Big) = \sum_j \Big(\sum_i d_{i,j} A_i \Big) a C_j.$$

Thus,

$$D_j = \sum_i d_{i,j} A_i.$$

Step 3. Find a basis $\{E_1, ..., E_p\}$ for the span of $\{D_1, ..., D_l\}$ and express each D_j as a linear combination of E_i's. Repeat Step 2 to obtain

$$\phi(a) = \sum_{i=1}^{p} E_i a F_i,$$

where the F_i's are the corresponding linear combinations of the C_j's.

Remarkably, at this stage Proposition 3.3.3 says that the sets $\{E_1, ..., E_p\}$ and $\{F_1, ..., F_p\}$ are linearly independent, and hence this process terminates.

Step 4. Given an invertible $S = (s_{i,j}) \in M_p$ with inverse $S^{-1} = (t_{i,j}) \in M_p$, let $H_i = \sum_j s_{i,j} F_j$, and $G_j = \sum_i t_{i,j} E_i$. Then

$$\|\phi\|_{cb} = \inf \Big\{ \big\| \sum_i G_i G_i^\dagger \big\|^{\frac{1}{2}} \big\| \sum_i H_i^\dagger H_i \big\|^{\frac{1}{2}} \Big\},$$

where the infimum is taken over all invertible matrices S.

This algorithm reduces the computation of $\|\phi\|_{cb}$ to a series of matrix computations and only the last step might involve a difficult minimization. Theorem 3.3.4 shows how to perform this minimization for one particular family of maps, and the

implementation *via* MATLAB provided in Section 3.3.4 approximates this minimization in general by randomly selecting several invertible matrices S and taking the smallest resulting norm estimate.

Note that in Step 4 of the algorithm, it is not necessary to consider all invertible matrices S because it may sometimes happen that two different matrices lead to the same generalized Choi-Kraus representation. Indeed, the minimization of Step 4 can be re-written as

$$\inf\left\{\left\|\begin{bmatrix}E_1 & \cdots & E_p\end{bmatrix}\left((S^\dagger S)^{-1}\otimes I_n\right)\begin{bmatrix}E_1^\dagger \\ \vdots \\ E_p^\dagger\end{bmatrix}\right\|^{\frac{1}{2}}\left\|\begin{bmatrix}F_1^\dagger & \cdots & F_p^\dagger\end{bmatrix}\left(S^\dagger S\otimes I_n\right)\begin{bmatrix}F_1 \\ \vdots \\ F_p\end{bmatrix}\right\|^{\frac{1}{2}}\right\},$$

where the infimum is taken over all invertible matrices S. Since this quantity only depends on $S^\dagger S$, it may be assumed without loss of generality that S is Hermitian and positive-definite. Alternatively, the Cholesky decomposition says that any Hermitian positive-definite matrix can be decomposed as $U^\dagger U$, where U is an upper triangular matrix with positive real entries along the diagonal. It may thus be assumed that S is upper-triangular and has positive real diagonal entries.

It can be further assumed that the eigenvalues of S are in the interval $(0, 1]$ because it is not difficult to see that multiplying S by a constant does not change the resulting norm estimate.

3.3.2 Mathematical Justification

To begin to justify the algorithm, begin with the last step. It was mentioned earlier that that if $\phi = \{A_i\}$ is a completely positive map, then setting $B_i = \sum_j u_{ij} A_j$

gives $\{B_i\}$ as another Choi-Kraus representation for the same map, provided (u_{ij}) is unitary. Step 4 of the algorithm can be thought of as a generalization of this fact to CB maps. Indeed, it is not difficult to see that $\phi(a) = \sum_i G_i a H_i$, because

$$\sum_i G_i a H_i = \begin{bmatrix} G_1 \cdots G_p \end{bmatrix} (I_p \otimes a) \begin{bmatrix} H_1 \\ \vdots \\ H_p \end{bmatrix}$$

$$= \begin{bmatrix} E_1 \cdots E_p \end{bmatrix} (S^{-1} \otimes I_n)(I_p \otimes a)(S \otimes I_n) \begin{bmatrix} F_1 \\ \vdots \\ F_p \end{bmatrix} = \sum_i E_i a F_i = \phi(a),$$

since the three tensor products above mutually commute. Note that the scalar matrices S and S^{-1} behave like "environmental operators", that is, they are operators that act exclusively on the environment of an open quantum system. Note also that all linearly-independent generalized Choi-Kraus representations of ϕ can be obtained in this way, because this process in effect takes arbitrary linear combinations of the E_i's and then modifies the F_i's accordingly – a process that Proposition 3.3.2 guarantees is sufficient.

Next it must be seen that the linear maps from M_n to M_k, which are denoted by $\mathcal{L}(M_n, M_k)$, can be identified with the tensor product $M_{k,n} \otimes M_{n,k}$ via the map that sends an elementary tensor, $A \otimes B$, to the map $\phi(a) = AaB$. It is easily seen that this extends to a linear map, $\Gamma : M_{k,n} \otimes M_{n,k} \mapsto \mathcal{L}(M_n, M_k)$. A simple dimension-counting argument shows that Γ is one-to-one and onto (both spaces have dimension k^2n^2).

Now endow $M_{k,n} \otimes M_{n,k}$ with a norm so that Γ will be an isometry when $\mathcal{L}(M_n, M_k)$ is endowed with the CB norm. By the CB representation theorem, it is easy to see

that defining a norm $\|\cdot\|_h$ for $U \in M_{k,n} \otimes M_{n,k}$ by

$$\|U\|_h = \inf\left\{ \|\sum_i A_i A_i^\dagger\|^{\frac{1}{2}} \|\sum_i B_i^\dagger B_i\|^{\frac{1}{2}} \right\},$$

where the infimum is taken over all ways to represent $U = \sum_i A_i \otimes B_i$ as a sum of elementary tensors, gives $\|U\|_h = \|\Gamma(U)\|_{cb}$.

The above tensor norm is called the *Haagerup tensor norm* in honor of U. Haagerup who was the first to notice the above identification. Write $M_{k,n} \otimes_h M_{n,k}$ to denote the tensor product endowed with this norm and note that the preceding few paragraphs act as a simple proof of the following theorem.

Theorem 3.3.1 (Haagerup)**.** *The map* $\Gamma : M_{k,n} \otimes_h M_{n,k} \mapsto CB(M_n, M_k)$ *defined by* $\Gamma(A \otimes B)(a) = AaB$ *is an isometric isomorphism.*

Here $CB(M_n, M_k)$ denotes the space of linear maps from M_n to M_k endowed with the completely bounded norm. The above isomorphism was greatly extended in work of Haagerup and Effros-Kishimoto to other identifications between spaces of completely bounded maps and Haagerup tensor products.

Theorem 3.3.1 reduces the justification of the estimation algorithm to showing that if $\phi = \Gamma(U)$, then the algorithm correctly computes $\|U\|_h$. The fact that this algorithm correctly computes $\|U\|_h$ for any operator space is proved in [5]. The key ideas of this proof are outlined below. To this end, some results about the tensor product of vector spaces are provided.

Recall that if $\mathcal{V}$ and $\mathcal{W}$ are vector spaces, then every element of $\mathcal{V} \otimes \mathcal{W}$ is a finite

sum of elementary tensors. The least number of elementary tensors that can be used to represent an element $U \in \mathcal{V} \otimes \mathcal{W}$ is called the *rank* of U and is denoted by rank (U). The following two propositions described in [5] are readily proved by applying maps of the form $f \otimes id_W$ and $id_V \otimes g$ to U, where f and g are linear functionals.

Proposition 3.3.2. *Let $U \in \mathcal{V} \otimes \mathcal{W}$. If $U = \sum_{i=1}^{p} A_i \otimes B_i$ then $p = rank(U)$ if and only if $\{A_1, \ldots, A_p\}$ is a linearly independent set and $\{B_1, \ldots, B_p\}$ is a linearly independent set. Moreover, if $U = \sum_{i=1}^{p} E_i \otimes F_i$ is another way to represent U as a sum of elementary tensors, then*

$$span\{A_1, \ldots, A_p\} = span\{E_1, \ldots, E_p\}$$

and

$$span\{B_1, \ldots, B_p\} = span\{F_1, \ldots, F_p\}.$$

Proposition 3.3.3. *Let $U \in \mathcal{V} \otimes \mathcal{W}$. If Steps 1 and Step 2 of the estimation algorithm are applied to $U = \sum_{i=1}^{m} A_i \otimes B_i$, to obtain $U = \sum_{i=1}^{p} E_i \otimes F_i$, then $\{E_1, \ldots, E_p\}$ and $\{F_1, \ldots, F_p\}$ will be linearly independent sets and hence $rank(U) = p$.*

The remainder of the proof of the justification of the algorithm is to show that at each stage, removing the linear dependencies among the elements in the sum for U reduces the Haagerup norm. Attention here will be restricted to an examination of Step 1 and Step 2 of the algorithm, as Step 3 behaves symmetrically. Upon choosing the basis $\{C_1, \ldots, C_l\}$ and expressing $B_i = \sum_j d_{i,j} C_j$, one may write the polar decomposition of the matrix $(d_{i,j}) = (w_{i,j})(p_{i,j})$, where $W = (w_{i,j})$ is an $m \times l$

partial isometry and $P = (p_{i,j})$ is an invertible $l \times l$ positive matrix. It then follows that $B_i = \sum_i w_{i,j} \tilde{C}_j$, where $\tilde{C}_i = \sum_j p_{i,j} C_j$. In this case, the set $\{\tilde{C}_1, \ldots, \tilde{C}_l\}$ is another basis for the span of $\{C_1, \ldots, C_l\}$ and $\sum_i \tilde{C}_i{}^\dagger \tilde{C}_i = \sum_i C_i^\dagger C_i$. Moreover, using this basis, one can obtain another representation for $\phi(a) = \sum_{j=1}^{l} \tilde{D}_j a \tilde{C}_j$, where $\tilde{D}_j = \sum_i w_{i,j} A_i$. Again, since P is invertible, the span of $\{\tilde{D}_1, \ldots, \tilde{D}_l\}$ is the same as the span of $\{D_1, \ldots, D_l\}$. Moreover, since W is a partial isometry, one finds that $\sum_i \tilde{D}_i \tilde{D}_i{}^\dagger \leq \sum_i A_i A_i^\dagger$. Hence, removing linear dependencies among the elements in the sum for u can never increase the norm quantity inside the definition of the Haagerup tensor norm. It thus follows that it is sufficient to take the infimum over all ways to represent $U = \sum_i^p A_i \otimes B_i$ where $\{A_1, \ldots, A_p\}$ and $\{B_1, \ldots, B_p\}$ are linearly independent sets.

This proves that the quantity defining the Haagerup tensor norm (which is the same as the CB norm) must be attained when the coefficients of the generalized Choi-Kraus representation are linearly independent, and hence represented by some choice of basis for $span\{E_1, ..., E_p\}$ and $span\{F_1, ..., F_p\}$.

3.3.3 Applying the Algorithm

In quantum information, maps given by the difference of two (distinct) unitary maps form the most elementary class of linear, non-completely positive maps of interest. The proof of the theorem to follow shows how the algorithm can be used to derive a simple geometric technique that computes the exact stabilized norm for maps

in this class. Note that this result can be derived from a technical result of Herrero ([16], Theorem 3.31), which is proved using operator theoretic machinery. Moreover, the result is also stated more recently in [1] without proof. This proof is new and elementary and gives a good illustration of the algorithm at work. By the unitary invariance of the CB/$\diamond$ norm, observe that one can compute the norm of any map $\mathcal{U} - \mathcal{V}$ once it is known how to compute it for any map of the form $\mathcal{U} - id$.

Theorem 3.3.4. *Let $U \in M_n$ be a unitary operator and let $\phi : M_n \mapsto M_n$ be given by $\phi(a) = UaU^\dagger - a$. Then $\|\phi\|_{cb} = \|\phi^\dagger\|_{cb} = \|\phi\|_\diamond = \|\phi^\dagger\|_\diamond$ is equal to the diameter of the smallest closed disc in $\mathbb{C}$ that contains all of the eigenvalues of U.*

Proof. If U is a scalar multiple of I then $\phi \equiv 0$ so the result immediately follows. Thus, assume from here on that U is not a scalar multiple of I. It then follows from Step 4 of the algorithm that

$$\|\phi\|_{cb} = \inf\left\{ \left\| \begin{bmatrix} U^\dagger & I \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \right\| \left\| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} U \\ -I \end{bmatrix} \right\| \right\},$$

where the infimum is over all invertible 2×2 scalar matrices. Now let $\mathbf{v} = [a \quad c]^T$ and $\mathbf{w} = [b \quad d]^T$ so that

$$\begin{aligned} \left\| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} U \\ -I \end{bmatrix} \right\|^2 &= \left\| \begin{bmatrix} aU - bI \\ cU - dI \end{bmatrix} \right\|^2 \\ &= \left\| (|a|^2 + |b|^2 + |c|^2 + |d|^2)I - (\bar{a}b + \bar{c}d)U^\dagger - (a\bar{b} + c\bar{d})U \right\| \\ &= \left\| (\|\mathbf{v}\|^2 + \|\mathbf{w}\|^2)I - 2Re(\langle \mathbf{v}, \mathbf{w} \rangle U) \right\|. \end{aligned}$$

Let $D = ad - bc$ be the determinant of the matrix. Then a similar calculation shows

that

$$\left\| D^{-1} \begin{bmatrix} U^\dagger & I \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \right\|^2 = |D|^{-2} \left\| (\|\mathbf{v}\|^2 + \|\mathbf{w}\|^2) I - 2Re(\langle \mathbf{v}, \mathbf{w} \rangle U) \right\|.$$

It thus follows that

$$\|\phi\|_{cb} = \inf \left\{ |D|^{-1} \|(\|\mathbf{v}\|^2 + \|\mathbf{w}\|^2) I - 2Re(\langle \mathbf{v}, \mathbf{w} \rangle U)\| \right\},$$

where the infimum is taken over all 2×1 complex vectors $\mathbf{v}$ and $\mathbf{w}$.

Now it is clear that this minimum will be attained when $\mathbf{v}$ and $\mathbf{w}$ are rotated such that $\min_i \{Re(\langle \mathbf{v}, \mathbf{w} \rangle \lambda_i)\}$ is as large as possible (while keeping $\mathbf{v}$ and $\mathbf{w}$ of fixed length), where λ_i ranges over all eigenvalues of U. Thus, since multiplying $\mathbf{w}$ by $e^{i\alpha}$ will not change $|D|$, it follows that

$$\|\phi\|_{cb} = \inf \left\{ |D|^{-1} \left\| (\|\mathbf{v}\|^2 + \|\mathbf{w}\|^2) I - 2Re(\langle \mathbf{v}, \mathbf{w} \rangle e^{i\alpha} U) \right\| \right\},$$

where α is such that the minimum real part of the eigenvalues of $e^{i\alpha}U$ is as large as possible. Define r to be this largest minimum real eigenvalue part.

Now, similar to before, $\mathbf{w}$ can be multiplied by $e^{i\beta}$ so that $|\langle \mathbf{v}, \mathbf{w} \rangle| = \langle \mathbf{v}, e^{i\beta} \mathbf{w} \rangle$, and so it follows that

$$\|\phi\|_{cb} = \inf \left\{ |D|^{-1} \left\| (\|\mathbf{v}\|^2 + \|\mathbf{w}\|^2) I - 2 \left| \langle \mathbf{v}, \mathbf{w} \rangle \right| r I \right\| \right\},$$

where the infimum is now taken over all 2×1 real vectors $\mathbf{v}$ and $\mathbf{w}$. It is now clear that it can be assumed without loss of generality that $\|\mathbf{v}\|^2 + \|\mathbf{w}\|^2 = 1$. It also follows from some simple algebra that, given any two vectors $\mathbf{v}$ and $\mathbf{w}$ such that

$\|\mathbf{v}\| \neq \|\mathbf{w}\|$, the value within this infimum will be made smaller by scaling $\mathbf{v}$ and $\mathbf{w}$ so that $\|\mathbf{v}\|^2 = \|\mathbf{w}\|^2 = \frac{1}{2}$.

It then immediately follows from expanding out the terms within the infimum that this is equivalent to the following minimization problem:

$$\|\phi\|_{cb} = \min\left\{\frac{1 - 2\,|ab + cd|\,r}{|ad - bc|}\right\}$$
$$\text{subject to } \; a^2 + c^2 = b^2 + d^2 = \frac{1}{2}.$$

Now, if $r \leq 0$ then it is easy to see that this minimum is equal to 2 by setting $a = d = \frac{1}{\sqrt{2}}$ and $b = c = 0$. Thus, it only remains to prove the result in the case when $r > 0$. If $r > 0$ then it is clear that this minimization problem is equivalent to the one obtained by removing the absolute value bars in the numerator. To proceed, form the Lagrangian of this problem:

$$\Lambda = \frac{1 - 2\,(ab + cd)\,r}{|ad - bc|} + \lambda_1\left(a^2 + c^2 - \frac{1}{2}\right) + \lambda_2\left(b^2 + d^2 - \frac{1}{2}\right)$$

Setting $\frac{\partial \Lambda}{\partial b} = \frac{\partial \Lambda}{\partial d}$ produces the equation

$$\langle \mathbf{v}|\mathbf{w}\rangle = ab + cd = 2\left(a^2 + c^2\right)\left(b^2 + d^2\right) r = \frac{r}{2}$$

This, however, implies that $\theta = \arccos(r)$, where θ is the angle between $\mathbf{v}$ and $\mathbf{w}$. Thus, this problem is minimized by vectors $\mathbf{v}$ and $\mathbf{w}$ that are each of length $\frac{1}{\sqrt{2}}$ and separated by an angle $\arccos(r)$. This in turn implies that $|D| = \|\mathbf{v}\|\,\|\mathbf{w}\| \sin\theta = \frac{1}{2}\sqrt{1 - r^2}$. Plugging this and $ab + cd = \frac{r}{2}$ into the formula to be minimized, one obtains the formula

$$\|\phi\|_{cb} = 2\sqrt{1 - r^2}.$$

It now is a simple geometric argument (see Figure 3.1) that finally shows that this value is equal to the diameter of the smallest closed disc enclosing the eigenvalues of U, completing the proof. ■

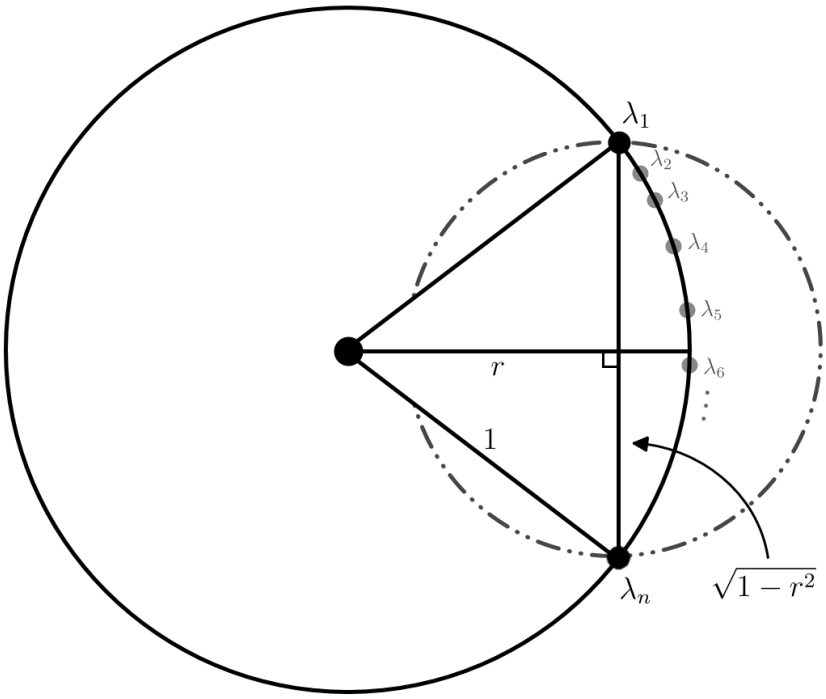

Figure 3.1: The unit ball of $\mathbb{C}$ with the eigenvalues $\lambda_1, \ldots, \lambda_n$ of U rotated such that their minimum real part is as large as possible. It is simply the Pythagorean theorem that shows that $2\sqrt{1-r^2}$ is equal to the diameter of the smallest closed disc that contains all of the eigenvalues of U.

3.3.4 MATLAB Implementation

The implementation of the algorithm *via* MATLAB that is presented here is split up into several functions, which will be described as their code is presented. Variable names within the code have been kept as close as possible to their counterparts presented in Section 3.3.1. After the code has been presented and briefly explained, an example that shows how the code is used is provided and the results of the algorithm are compared to the result of Theorem 3.3.4.

The main function of this implementation is `CBNorm`; it calls upon the other functions to estimate the CB norm of the given map. `CBNorm` begins by determining whether or not the given map is completely positive, and if so returns the map's exact CB norm, using the result of Theorem 3.2.2. If the map is not completely positive, the algorithm described in Section 3.3.1 begins to run.

The inputs to the function are `A`, an array of the map's A operators in one of its generalized Choi-Kraus representations; `B`, an array of the map's B operators in the same representation; and `its`, the number of random matrices to be used to estimate the norm (a higher number will on average produce a more accurate estimate of the CB norm but will take longer to compute).

```
function [res] = CBNorm(A,B,its)

k = size(A,1);
n = size(A,2);
m = size(A,3);

if IsCPMap(A,B,m,n,k)
```

```
  c = n*m;
  res = norm(reshape(A,n,c)*reshape(permute(B,[2,1,3]),n,c)');
else
  res = min(k,n^(3/2));
  [E,F,v] = MakeLinIndep(A,B,m,n,k);
  ST1 = eye(v);
  ST2 = eye(v);
  for j = 1:its
    H = zeros(n,k,v);
    G = zeros(k,n,v);
    for x = 1:v
      for y = 1:v
        H(:,:,x) = H(:,:,x) + ST1(x,y)*F(:,:,y);
        G(:,:,x) = G(:,:,x) + ST2(y,x)*E(:,:,y);
      end
    end
    HHCB = reshape(permute(H,[2,1,3]),k,n*v);
    GGCB = reshape(G,k,n*v);
    res = min([sqrt(norm(GGCB*GGCB')*norm(HHCB*HHCB')),res]);
    [ST1,ST2] = RandomPositive(v);
  end
end
```

The procedures `IsCPMap` and `IsPosMatrix` jointly determine whether or not the completely bounded map that it is given is actually a completely positive map by determining whether or not its Choi matrix is positive. These procedures are optional for the algorithm; they simply serve to allow the algorithm to compute the CB norm of completely positive maps more quickly and more accurately than it otherwise could.

```
function [res]=IsCPMap(A,B,m,n,k)

if ~(n == k)
  res = 0;
else
  C = zeros(n,n,n,n);
```

```
  for i = 1:n
    for j = 1:n
      MU = zeros(n);
      MU(i,j) = 1;
      for l = 1:m
        C(:,:,i,j) = C(:,:,i,j) + (A(:,:,l) * MU * B(:,:,l));
      end
    end
  end
  res = IsPosMatrix(reshape(permute(C,[1,3,2,4]),n^2,n^2));
end


function [res]=IsPosMatrix(A)

res = (min(eig(A+A')) > -(max([max(max(A)),size(A,1)])*eps));
```

The procedures `MakeLinIndep` and `NextIndex` perform Steps 1 through 3 of the algorithm. They are reasonably straightforward and follow the theoretical discussion earlier quite closely.

```
function [E,F,v] = MakeLinIndep(A,B,m,n,k)

BM = reshape(B,n*k,m)';
[d,u,z] = ModGaussElim(BM);
for x = 1:u
  C(:,:,x) = B(:,:,NextIndex(z,x));
  D(:,:,x) = zeros(k,n);
  for y = 1:m
    D(:,:,x) = D(:,:,x) + d(y,NextIndex(z,x))*A(:,:,y);
  end
end
DM = reshape(D,n*k,u)';
[g,v,w] = ModGaussElim(DM);
for x = 1:v
  E(:,:,x) = D(:,:,NextIndex(w,x));
  F(:,:,x) = zeros(n,k);
  for y = 1:u
    F(:,:,x) = F(:,:,x) + g(y,NextIndex(w,x))*C(:,:,y);
```

```
  end
end


function [res] = NextIndex(z,x)

if (min(size(z)) > 0)
    res = 0;
    j = 1;
    while j <= x
        res = res + 1;
        adj = (max (z == res));
        j = j + (1 - adj);
    end
else
    res = x;
end
```

The procedure `ModGaussElim` performs Gaussian elimination and returns detailed information about the linear dependencies of the rows of the input matrix. The purpose of writing an implementation of Gaussian elimination rather than using MATLAB's built-in `rref` function is so that the $d_{i,j}$ values described in Step 2 of the algorithm may be extracted at the same time. This reduces the order of Steps 1 through 3 from $\mathcal{O}(k^4n^4)$ to $\mathcal{O}(k^3n^3)$.

```
function [B,r,z] = ModGaussElim(A)

thresh = max([max(max(A)),size(A,1)]) * eps;
m = size(A,1);
n = size(A,2);
z = find(max(abs(A')) < thresh);
r = m - sum(z > 0);
A = [A eye(m)];
i = 1;
j = 1;
while ((i <= m) && (j <= n))
```

```
  i = 1;
  maxi = 0;
  maxval = 0;
  for k = 1:m
    if (abs(A(k,j)) > maxval) && ...
        ((j == 1) || (min(A(k,1:max([j-1,1])) == 0) == 1))
      maxi = k;
      maxval = abs(A(maxi,j));
    end
  end
  if ~(maxi == 0)
    if ~(abs(A(maxi,j)) < thresh)
      i = maxi;
      TA = A(i,:)./A(i,j);
      for u = 1:m
        if ~(i == u) && ~(abs(A(u,j)) < thresh)
          A(u,:) = A(u,:) - A(u,j)*TA;
          if (min((abs(zeros(1,n) - A(u,1:n))) < thresh) == 1)
            r = r - 1;
            z(m - r) = u;
          end
        end
      end
    else
      i = m + 1;
    end
  end
  j = j + 1;
end
B = eye(m);
for i = 1:(m - r)
  B(z(i),:) = -conj(A(z(i),(n+1):(n+m)));
  B(z(i),z(i)) = 0;
end
```

The minimization in Step 4 of the algorithm is approximated by repeatedly calling on the function `RandomPositive`, which generates a random positive-definite matrix (and its inverse) with eigenvalues in the interval $(0, 1]$. This is achieved by generating

a diagonal matrix with entries contained in that interval and conjugating by a random unitary matrix. The random unitary matrix is constructed by generating a matrix with uniformly random entries from the square with corners at 0 and $1+i$ and then orthonormalizing its columns via MATLAB's `orth` function.

```
function [P1,P2] = RandomPositive(n)

r = 0;
RD = diag(rand(1,n)+eps);
while (r < n)
  RM = rand(n) + i*rand(n);
  r = round(rank(RM));
end
U = orth(RM);
P1 = U*RD*U';
P2 = inv(P1);
```

To use the provided code, first copy all of the above functions into a single file and save it under the name `CBNorm.m` in your MATLAB scripts directory. As an illustration of how this implementation of the algorithm may be used, consider a special case of the class of maps described by Theorem 3.3.4.

Example 3.3.5. *Let U be a 3×3 unitary matrix with eigenvalues $e^{\left(\frac{5i\pi}{4}\right)}, e^{(i\pi)}$, and $e^{\left(\frac{3i\pi}{4}\right)}$. Then the following code runs 1000 iterations of the algorithm to estimate the CB norm of the map $\phi(a) = U^{\dagger}aU - a$.*

```
>> A(:,:,1) = diag([exp(-5*i*pi/4),exp(-i*pi),exp(-3*i*pi/4)]);
>> A(:,:,2) = eye(3);
>> B(:,:,1) = diag([exp(5*i*pi/4),exp(i*pi),exp(3*i*pi/4)]);
>> B(:,:,2) = -eye(3);
>> CBNorm(A,B,1000)
```

Running this code gave an output of 1.4390 *in about half of a second on laptop with a 1.60GHz processor and 2Gb of RAM. Theorem 3.3.4 says however that* $\|\phi\|_{cb} = \sqrt{2}$*, so the computed estimate has a relative error of about* 1.75%*. To get a more accurate estimate, one could of course increase the number of iterations from* 1000*, and it should be clear how to modify this code to find the CB norm of other maps.*

3.3.5 Efficiency

To look at the efficiency of the algorithm, consider Steps 1 - 3 separately from Step 4, as Steps 1 - 3 need only be run once for a given map, while the implementation of the algorithm *via* MATLAB given in Section 3.3.4 requires that Step 4 be run multiple times for the same map.

First note that the most efficient algorithm that could possibly exist for computing the CB norm of a general completely bounded map is $\mathcal{O}(k^2n^2)$, which can be seen by observing that a general completely bounded map will have about kn linearly independent generalized Choi-Kraus operators, each of which will have kn entries that must each be read at least once. One can observe, however, that the efficiency of Steps 1 - 3 of this algorithm is $\mathcal{O}(k^3n^3)$, as Gaussian elimination must be applied to a matrix of dimension about $kn \times kn$.

After the generalized Choi-Kraus operators of the map are made to be linearly independent by Steps 1 - 3 of the algorithm, one can proceed to the given implementation of Step 4, which (for a fixed number of iterations) has efficiency that can be

seen to be $\mathcal{O}(k^3n^2)$ if one performs matrix multiplication using the standard matrix multiplication algorithm. This result follows from the facts that computing $\sum_i G_i G_i^\dagger$ and $\sum_i H_i^\dagger H_i$ "naively" from the families of matrices $\{G_i\}$ and $\{H_i\}$ takes $\mathcal{O}(k^3n^2)$ time, and all of the other operations in Step 4 are at least as efficient as $\mathcal{O}(k^2n^2)$.

As a bit of an aside, note that the method of randomly generating matrices implemented in Section 3.3.4 actually has a running time of $\mathcal{O}(k^3n^3)$ because it requires orthonormalizing a set of about kn vectors of dimension about kn. However, it is not difficult to implement a method of generating random matrices of appropriate size in $\mathcal{O}(k^2n^2)$ time – simply generate a $kn \times kn$ upper triangular matrix with entries uniformly chosen at random from the square with corners at 0 and $1+i$. This matrix can be both generated and inverted in $\mathcal{O}(k^2n^2)$ time. The slower method of generating matrices that is implemented is used because it seems to provide better CB norm estimates in practice.

It may be beneficial (particularly if $n = k$) to make use of faster matrix multiplication algorithms such as the Strassen Algorithm [41] to perform the matrix multiplications required in Step 4. The use of fast matrix multiplication algorithms reduces the running time of Step 4 to $\mathcal{O}(kn \cdot \max\{k,n\}^\omega)$, where ω is the *exponent of matrix multiplication* [8]. As a result of this, it follows that if either of the two conjectures in [8] that imply that $\omega = 2$ hold, then for a given fixed number of iterations, the implementation of Step 4 provided in Section 3.3.4 can be made as close to $\mathcal{O}(kn \cdot \max\{k,n\}^2)$ as desired. In particular, if $n = k$, then this becomes $\mathcal{O}(n^4)$,

which is optimal in the sense of big-O notation.

Chapter 4

Quantum Error Correction

4.1 Correctable Subspaces

Throughout this chapter, instead of assuming that the quantum system of interest is represented on M_n, focus will be shifted slightly to $\mathcal{B}(\mathcal{H})$, where $\mathcal{H}$ is a general finite-dimensional Hilbert space. All of the results from Sections 2.2 and 2.3 regarding maps from $M_n \mapsto M_k$ carry over to this new setting; the switch is made merely to retain consistency with the relevant literature.

4.1.1 Definitions and Preliminaries

Given a quantum system S represented on a Hilbert space $\mathcal{H}^S \equiv \mathcal{H}$, let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ be a quantum channel. If $\mathcal{C} \subseteq \mathcal{H}$ is a subspace, then $\mathcal{C}$ is said to be a *correctable code* or *correctable subspace* if there exists another quantum channel

$\mathcal{R} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ such that

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho \quad \forall \rho \in \mathcal{B}(\mathcal{C}).$$

In this situation, $\mathcal{R}$ is called a *correction operation*. If $\mathcal{R} = id_{\mathcal{H}}$ is a valid correction operation, then $\mathcal{C}$ is called a *decoherence-free subspace* [12, 30, 44].

It is well-known that $\mathcal{C}$ being correctable is equivalent to the existence of a matrix (λ_{ij}) such that [2, 23]:

$$P_{\mathcal{C}} E_i^{\dagger} E_j P_{\mathcal{C}} = \lambda_{ij} P_{\mathcal{C}} \quad \forall\, i, j, \tag{4.1}$$

where $P_{\mathcal{C}}$ is the orthogonal projection onto $\mathcal{C}$ and $\{E_i\}$ is a Choi-Kraus representation of $\mathcal{E}$. These matrix equations are known as the *Knill-Laflamme conditions* and are easily checked once a given subspace $\mathcal{C}$ is proposed as correctable. Also, Remark 2.2.9 implies that the existence of the matrix (λ_{ij}) is independent of the particular Choi-Kraus representation used, although the matrix itself depends on that representation.

Lemma 4.1.1. *Let $\mathcal{H}$ be a Hilbert space, let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$, and let $\mathcal{C} \subseteq \mathcal{H}$ be a subspace. Then $\mathcal{C}$ is correctable for $\mathcal{E}$ if and only if there is a randomized unitary channel $\mathcal{F} = \{\sqrt{p_i} U_i\}$ such that $\mathcal{E}(\rho) = \mathcal{F}(\rho)$ for all $\rho \in \mathcal{B}(\mathcal{C})$ and $P_{\mathcal{C}} U_i^{\dagger} U_j P_{\mathcal{C}} = 0$ for all $i \neq j$.*

Proof. To prove the "only if" direction, first note that if $\mathcal{C}$ is correctable for $\mathcal{E}$ then the Knill-Laflamme conditions (4.1) imply that there exists a matrix (λ_{ij}) such that

$$(I_m \otimes P_{\mathcal{C}}) \begin{bmatrix} E_1 & E_2 & \cdots & E_m \end{bmatrix}^{\dagger} \begin{bmatrix} E_1 & E_2 & \cdots & E_m \end{bmatrix} (I_m \otimes P_{\mathcal{C}}) = (\lambda_{ij}) \otimes P_{\mathcal{C}}.$$

Thus, the matrix (λ_{ij}) is positive-semidefinite and has trace 1 (and is thus a density matrix). It follows that there is a unitary matrix $U = (u_{ij})$ such that $U(\lambda_{ij})U^\dagger$ is diagonal (call this diagonal matrix $D = (d_{ij})$). Then define a quantum channel $\mathcal{F} = \{F_i\}$ where

$$F_i = \sum_j \overline{u_{ij}} E_j.$$

Indeed, Remark 2.2.9 says that $\mathcal{E} = \mathcal{F}$. Moreover, for all i, j,

$$\begin{aligned} P_{\mathcal{C}} F_i^\dagger F_j P_{\mathcal{C}} &= \sum_{k,l} u_{ik}\overline{u_{jl}} P_{\mathcal{C}} E_k^\dagger E_l P_{\mathcal{C}} \\ &= \sum_{k,l} u_{ik}\overline{u_{jl}} \lambda_{kl} P_{\mathcal{C}} \\ &= d_{ij} P_{\mathcal{C}}. \end{aligned}$$

Thus $P_{\mathcal{C}} F_i^\dagger F_j P_{\mathcal{C}} = 0$ for all $i \neq j$. Setting $p_i = d_{ii}$ and extending $\frac{1}{\sqrt{p_i}} F_i$ outside of $\mathcal{C}$ to a unitary U_i completes this direction of the proof.

To see the other implication, simply note that if $\mathcal{R} = \{P_{\mathcal{C}} U_i^\dagger\}$ then $\mathcal{R} \circ \mathcal{E}(\rho) = \rho$ for all $\rho \in \mathcal{B}(\mathcal{H})$. This correction operation will be discussed in more detail at the end of the proof of Theorem 4.1.3. ■

To illustrate Lemma 4.1.1 and the Knill-Laflamme conditions, a simple example is provided.

Example 4.1.2. *Let I_2 be the 2×2 identity matrix, let $U \in M_2$ and $V \in M_2$ be unitary matrices, and let $q \in [0, 1)$. Then consider the channel $\mathcal{E} : M_4 \mapsto M_4$ given*

by the 4 Kraus operators in the standard basis

$$E_1 = \alpha \begin{bmatrix} I_2 & U \\ 0 & 0 \end{bmatrix} \quad E_2 = \alpha \begin{bmatrix} I_2 & -U \\ 0 & 0 \end{bmatrix} \quad E_3 = \beta \begin{bmatrix} I_2 & V \\ I_2 & V \end{bmatrix} \quad E_4 = \beta \begin{bmatrix} I_2 & -V \\ -I_2 & V \end{bmatrix},$$

where $\alpha = \sqrt{\frac{q}{2}}$ *and* $\beta = \frac{\sqrt{1-q}}{2}$. *It is straightforward to see that* $\mathcal{E}$ *preserves traces and is thus a valid quantum channel. One can also verify that one correctable subspace for* $\mathcal{E}$ *is defined by* $\mathcal{C} \equiv span\{ \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}^T, \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}^T \}$ *because*

$$P_{\mathcal{C}} = \begin{bmatrix} I_2 & 0 \\ 0 & 0 \end{bmatrix}$$

and so

$$\begin{aligned} P_{\mathcal{C}} E_3^\dagger E_4 P_{\mathcal{C}} &= 0 \\ P_{\mathcal{C}} E_3^\dagger E_3 P_{\mathcal{C}} = P_{\mathcal{C}} E_4^\dagger E_4 P_{\mathcal{C}} &= \Big(\frac{1-q}{2}\Big) P_{\mathcal{C}} \\ P_{\mathcal{C}} E_1^\dagger E_1 P_{\mathcal{C}} = P_{\mathcal{C}} E_2^\dagger E_2 P_{\mathcal{C}} = P_{\mathcal{C}} E_1^\dagger E_2 P_{\mathcal{C}} &= \frac{q}{2} P_{\mathcal{C}} \\ P_{\mathcal{C}} E_1^\dagger E_3 P_{\mathcal{C}} = P_{\mathcal{C}} E_1^\dagger E_4 P_{\mathcal{C}} = P_{\mathcal{C}} E_2^\dagger E_3 P_{\mathcal{C}} = P_{\mathcal{C}} E_2^\dagger E_4 P_{\mathcal{C}} &= \Big(\frac{\sqrt{q-q^2}}{2\sqrt{2}}\Big) P_{\mathcal{C}}, \end{aligned}$$

which verifies that the Knill-Laflamme conditions are satisfied. Lemma 4.1.1 then says that there exists a randomized unitary channel $\mathcal{F}$ *such that* $\mathcal{E}|_{\mathcal{C}} = \mathcal{F}|_{\mathcal{C}}$.

Indeed, if one recalls the Pauli X matrix $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ *then it is not difficult to verify that* $\mathcal{F} = \big\{ \frac{\sqrt{1+q}}{\sqrt{2}} I_2 \otimes I_2, \frac{\sqrt{1-q}}{\sqrt{2}} X \otimes I_2 \big\}$ *is such a channel because for all* $\rho \in M_2$ *it is the case that*

$$\mathcal{E}\Big(\begin{bmatrix} \rho & 0 \\ 0 & 0 \end{bmatrix} \Big) = \begin{bmatrix} \big(\frac{1+q}{2}\big)\rho & 0 \\ 0 & \big(\frac{1-q}{2}\big)\rho \end{bmatrix} = \mathcal{F}\Big(\begin{bmatrix} \rho & 0 \\ 0 & 0 \end{bmatrix} \Big).$$

4.1.2 Characterization of Correctable Codes

Theorem 4.1.3. *Let $\mathcal{H}$ be a Hilbert space, let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$, and let $\mathcal{C} \subseteq \mathcal{H}$ be a subspace. Then the following are equivalent:*

1. *$\mathcal{C}$ is a correctable code for $\mathcal{E}$.*

2. *$\exists$ a $\dagger$-homomorphism $\pi : \mathcal{B}(\mathcal{C}) \mapsto \mathcal{B}(\mathcal{H})$ such that*

$$\mathcal{E}(\rho) = \pi(\rho)\mathcal{E}(P_{\mathcal{C}}) = \mathcal{E}(P_{\mathcal{C}})\pi(\rho) \quad \forall\, \rho \in \mathcal{B}(\mathcal{C}).$$

Furthermore, the correction operation looks like $\pi^\dagger$ when restricted to $\mathcal{E}\big(\mathcal{B}(\mathcal{C})\big)$.

Proof. Begin by proving the implication *1* $\Rightarrow$ *2*. Since $\mathcal{C}$ is correctable for $\mathcal{E}$, it follows that Lemma 4.1.1 says that there exists a randomized unitary channel $\mathcal{F} = \{\sqrt{p_i}U_i\}$ such that $\mathcal{F}(\rho) = \mathcal{E}(\rho)$ for all $\rho \in \mathcal{B}(\mathcal{C})$ and $P_{\mathcal{C}}U_i^\dagger U_j P_{\mathcal{C}} = 0$ whenever $i \neq j$.

Let $V_i = U_i P_{\mathcal{C}}$ and define a $\dagger$-homomorphism $\pi : \mathcal{B}(\mathcal{C}) \mapsto \mathcal{B}(\mathcal{H})$ by $\pi(\rho) = \sum_j V_j \rho V_j^\dagger$. It then follows that

$$\mathcal{E}(P_{\mathcal{C}})\pi(\rho) = \Big(\sum_i p_i V_i V_i^\dagger\Big)\Big(\sum_j V_j \rho V_j^\dagger\Big) = \sum_i p_i V_i \rho V_i^\dagger = \mathcal{E}(\rho) \quad \forall\, \rho \in \mathcal{B}(\mathcal{C}).$$

A similar argument shows that $\mathcal{E}(\rho) = \pi(\rho)\mathcal{E}(P_C)$ for all $\rho \in \mathcal{B}(\mathcal{C})$.

To see why *2* $\Rightarrow$ *1*, note that if $\mathcal{E}(\rho) = \pi(\rho)\mathcal{E}(P_C)$ for all $\rho \in \mathcal{B}(\mathcal{C})$, then

$$\mathrm{Tr}\,(\rho) = \mathrm{Tr}\,(\mathcal{E}(\rho)) = \mathrm{Tr}\,(\pi(\rho)\mathcal{E}(P_{\mathcal{C}})) = \mathrm{Tr}\,\big(\rho\pi^\dagger(\mathcal{E}(P_{\mathcal{C}}))\big) \quad \forall\, \rho \in \mathcal{B}(\mathcal{C}).$$

From this it immediately follows that

$$P_{\mathcal{C}} = \pi^\dagger(\mathcal{E}(P_{\mathcal{C}})). \tag{4.2}$$

Similarly, $\mathrm{Tr}(\pi^\dagger(\alpha)\beta\gamma) = \mathrm{Tr}(\alpha\pi(\beta\gamma)) = \mathrm{Tr}(\alpha\pi(\beta)\pi(\gamma)) = \mathrm{Tr}(\pi^\dagger(\alpha\pi(\beta))\gamma)$ for all $\alpha \in \mathcal{B}(\mathcal{H}), \beta, \gamma \in \mathcal{B}(\mathcal{C})$. Since this equation holds for all $\gamma \in \mathcal{B}(\mathcal{C})$ in particular, it follows that

$$\pi^\dagger(\alpha)\beta = \pi^\dagger(\alpha\pi(\beta)) \quad \forall\, \alpha \in \mathcal{B}(\mathcal{H}), \beta \in \mathcal{B}(\mathcal{C}). \tag{4.3}$$

Multiplying Equation (4.2) on the right by an arbitrary $\rho \in \mathcal{B}(\mathcal{C})$ now shows that $\rho = \pi^\dagger(\mathcal{E}(P_C))\rho$. If Equation (4.3) is then applied with $\alpha = \mathcal{E}(P_\mathcal{C})$ and $\beta = \rho$, it then follows that $\rho = \pi^\dagger(\mathcal{E}(P_\mathcal{C})\pi(\rho)) = \pi^\dagger(\mathcal{E}(\rho))$ for all $\rho \in \mathcal{B}(\mathcal{C})$.

To complete the proof, note that although $\pi^\dagger$ is not in general trace-preserving (and thus not a valid quantum channel), it can easily be modified to be trace-preserving by extending its family of Kraus operators $\left\{V_i^\dagger\right\}$ to a full set of partial isometries such that $V_i^\dagger V_j = 0$ for all $i \neq j$. This works because it is then the case that $\left\{V_i V_i^\dagger\right\}$ is a maximal family of mutually orthogonal projections, so they sum to the identity. ■

By following along through the proofs presented thus far in this chapter, a method for explicitly computing the correction operation given a correctable subspace for $\mathcal{E}$ immediately becomes clear. Indeed, the matrix (λ_{ij}) described by the Knill-Laflamme conditions is trivial to compute, and constructing the randomized unitary channel of Lemma 4.1.1 was shown to be nothing more than a linear algebra exercise. If $\mathcal{F} = \left\{\sqrt{p_i}U_i\right\}$ is that randomized unitary channel, then the the correction operation described by Theorem 4.1.3 is given by $\mathcal{R} = \left\{V_i^\dagger\right\}$ (where $V_i = U_i P_\mathcal{C}$), possibly

with some extra partial isometries to ensure that it preserves traces. Similarly, the †-homomorphism described by Theorem 4.1.3 is given by $\pi = \{V_i\}$.

To briefly illustrate these ideas, return to the channel introduced in Example 4.1.2.

Example 4.1.4. *Recall that* $\mathcal{C} = span\{ \begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}^T, \begin{bmatrix}0 & 1 & 0 & 0\end{bmatrix}^T \}$ *and that the randomized unitary channel given by Lemma 4.1.1 is* $\mathcal{F} = \{\frac{\sqrt{1+q}}{\sqrt{2}} I_2 \otimes I_2, \frac{\sqrt{1-q}}{\sqrt{2}} X \otimes I_2\}$. *From this it immediately follows that*

$$\mathcal{R}(\sigma) = \begin{bmatrix} I_2 & 0 \\ 0 & 0 \end{bmatrix} \sigma \begin{bmatrix} I_2 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & I_2 \\ 0 & 0 \end{bmatrix} \sigma \begin{bmatrix} 0 & 0 \\ I_2 & 0 \end{bmatrix} = \begin{bmatrix} \mathrm{Tr}_1(\sigma) & 0 \\ 0 & 0 \end{bmatrix} \quad \forall\, \sigma \in M_4$$

and

$$\pi(\rho) = \begin{bmatrix} I_2 \\ 0 \end{bmatrix} \rho \begin{bmatrix} I_2 & 0 \end{bmatrix} + \begin{bmatrix} 0 \\ I_2 \end{bmatrix} \rho \begin{bmatrix} 0 & I_2 \end{bmatrix} = \begin{bmatrix} \rho & 0 \\ 0 & \rho \end{bmatrix} \quad \forall\, \rho \in M_2,$$

where Tr_1 *denotes the partial trace over the first system when* M_4 *is written as the tensor product* $M_2 \otimes M_2$ *and* M_2 *is considered in the standard basis.*

Note that $\mathcal{R}$ *is indeed a valid correction operation for this channel on the subspace* $\mathcal{C}$ *because* $\mathcal{R} \circ \mathcal{E}\left(\begin{bmatrix} \rho & 0 \\ 0 & 0 \end{bmatrix} \right) = \mathcal{R}\left(\begin{bmatrix} (\frac{1+q}{2})\rho & 0 \\ 0 & (\frac{1-q}{2})\rho \end{bmatrix} \right) = \begin{bmatrix} \rho & 0 \\ 0 & 0 \end{bmatrix}$ *for all* $\rho \in M_2$.

4.2 Correctable Subsystems

One inherent shortcoming of the correctable subspace notion of correctability is that it does not allow for nontrivial evolution of an ancillary quantum system. There is no physical reason why one should care about the state of the ancillary quantum system – if the state that needs to be recovered is ρ and the channel takes the input

state $\sigma \otimes \rho$, then an output state of $\tau \otimes \rho$ is just as useful as an output state of $\sigma \otimes \rho$, regardless of the state τ. This is the motivation for defining *correctable subsystems* for quantum channels.

4.2.1 Definitions and Preliminaries

Let S be a quantum system represented on a (finite-dimensional) Hilbert space $\mathcal{H}^S \equiv \mathcal{H}$ and let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ be a quantum channel as before. It is said that a quantum system B is a *subsystem* of S if there is a representation of B on a Hilbert space $\mathcal{H}^B$ such that

$$\mathcal{H}^S = \left(\mathcal{H}^A \otimes \mathcal{H}^B\right) \oplus \left(\mathcal{H}^A \otimes \mathcal{H}^B\right)^{\perp}, \tag{4.4}$$

where A is another subsystem of S represented on the Hilbert space $\mathcal{H}^A$. Define $\mathcal{C} = \mathcal{H}^A \otimes \mathcal{H}^B$ and let $P_{\mathcal{C}}$ be the orthogonal projection onto $\mathcal{C}$. What follows is the definition of the correctable subsystem notion of correctability.

Definition 4.2.1. *Given a Hilbert space $\mathcal{H}^S$ and a decomposition as in Equation (4.4), B is said to be a* **correctable subsystem** *if there exists a quantum channel $\mathcal{R}$ such that*

$$\forall\, \rho^A \;\forall\, \rho^B, \exists\, \tau^A \text{ such that } \mathcal{R} \circ \mathcal{E}(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B.$$

Note that correctable subsystems generalize correctable subspaces, as the correctable subspace case is recovered exactly when $\dim(A) = 1$. As was the case with

subspaces, the channel $\mathcal{R}$ is called a *correction operation*. Also, if $id_{\mathcal{H}}$ is a valid correction operation then B is said to be a *noiseless subsystem*.

One can also define approximately correctable subsystems by making use of the diamond norm introduced in Section 3.1.

Definition 4.2.2. *Given $\varepsilon \geq 0$, B is said to be an ε-**correctable subsystem** for $\mathcal{E}$ if there is a channel $\mathcal{R} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ and a channel $\mathcal{N}_A : \mathcal{B}(\mathcal{H}^A) \mapsto \mathcal{B}(\mathcal{H}^A)$ such that*

$$\left\| \mathcal{R} \circ \mathcal{E} \circ \mathcal{P}_{\mathcal{C}} - \mathcal{N}_A \otimes id_B \right\|_{\diamond} \leq \varepsilon,$$

where $\mathcal{P}_{\mathcal{C}}$ is the map with the single Kraus operator $\{P_{\mathcal{C}}\}$.

The notions of approximately correctable subspaces and approximately noiseless subsystems arise in ways analogous to those given earlier. Also, note that if $\varepsilon = 0$ then the original definition of correctable subsystems is recovered.

It was also shown in [26, 27] that B being correctable for $\mathcal{E} = \{E_i\}_{i=1}^m$ is equivalent to the existence of a family of operators $\{F_{ij}\}$ on $\mathcal{H}^A$ such that

$$P_{\mathcal{C}} E_i^{\dagger} E_j P_{\mathcal{C}} = F_{ij} \otimes I_B \quad \forall\, i, j. \tag{4.5}$$

These equations are known as the *testable conditions* and they generalize the Knill-Laflamme conditions given earlier. Based on this family of matrix equations, a subsystem version of Lemma 4.1.1 can be derived that shows what channels look like on correctable subsystems.

Lemma 4.2.3 ([28], Appendix A)**.** *Let $\mathcal{H}$ be a Hilbert space, let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ be a channel, and let $\mathcal{C} \equiv \mathcal{H}^A \otimes \mathcal{H}^B \subseteq \mathcal{H}$ be a subspace. Then B is correctable for $\mathcal{E}$ if and only if there is a CP map $\mathcal{G} = \{U_i(D_i \otimes I_B)\}$ with U_i unitary for all i such that $\mathcal{E}(I_A \otimes \rho^B) = \mathcal{G}(I_A \otimes \rho^B)$ for all $\rho^B \in \mathcal{B}(\mathcal{H}^B)$, $P_{\mathcal{C}} U_i^\dagger U_j P_{\mathcal{C}} = 0$ for all $i \neq j$, and D_i is a positive diagonal operator for all i.*

Proof. To prove the "only if" direction, begin by noting that the testable conditions (4.5) imply that operator block matrix $F = (F_{ij})$ is positive because

$$(I_m \otimes P_{\mathcal{C}}) \begin{bmatrix} E_1 & E_2 & \cdots & E_m \end{bmatrix}^\dagger \begin{bmatrix} E_1 & E_2 & \cdots & E_m \end{bmatrix} (I_m \otimes P_{\mathcal{C}}) = F \otimes I_B.$$

Next let U be a unitary such that $UFU^\dagger = D$ is diagonal and let $U = (U_{ij})$ and $D = (D_{ij})$ be the associated block decompositions. Then

$$\sum_{k,l} U_{ik} F_{kl} U_{jl}^\dagger = D_{ij} \quad \forall\, i, j, \tag{4.6}$$

and

$$\sum_{k} U_{ki}^\dagger U_{kj} = \delta_{ij} I_A \quad \forall\, i, j. \tag{4.7}$$

Define the CP map $\mathcal{G} = \{G_i\}$ where for all i,

$$G_i = E_i P_{\mathcal{C}}^\perp + \sum_j E_j (U_{ij}^\dagger \otimes I_B) P_{\mathcal{C}}.$$

Then by Equations (4.5) and (4.6), it follows that for all i, j,

$$\begin{aligned}
P_{\mathcal{C}} G_i^\dagger G_j P_{\mathcal{C}} &= P_{\mathcal{C}}\big(P_{\mathcal{C}}^\perp E_i^\dagger + \sum_k P_{\mathcal{C}}(U_{ik} \otimes I_B) E_k^\dagger\big)\big(E_j P_{\mathcal{C}}^\perp + \sum_l E_l (U_{jl}^\dagger \otimes I_B) P_{\mathcal{C}}\big) P_{\mathcal{C}} \\
&= \sum_{k,l} P_{\mathcal{C}}(U_{ik} \otimes I_B) E_k^\dagger E_l (U_{jl}^\dagger \otimes I_B) P_{\mathcal{C}} \\
&= \sum_{k,l} (U_{ik} \otimes I_B) P_{\mathcal{C}} E_k^\dagger E_l P_{\mathcal{C}} (U_{jl}^\dagger \otimes I_B) \\
&= \Big(\sum_{k,l} U_{ik} F_{kl} U_{jl}^\dagger\Big) \otimes I_B \\
&= D_{ij} \otimes I_B.
\end{aligned}$$

Note in particular that this means that $P_{\mathcal{C}} G_i^\dagger G_j P_{\mathcal{C}} = 0$ whenever $i \neq j$. Moreover, Equation (4.7) yields for all $\rho^B \in \mathcal{B}(\mathcal{H}^B)$ that

$$\begin{aligned}
\mathcal{G}(I_A \otimes \rho^B) &= \sum_i G_i (I_A \otimes \rho^B) G_i^\dagger \\
&= \sum_i \Big(E_i P_{\mathcal{C}}^\perp + \sum_j E_j (U_{ij}^\dagger \otimes I_B)\Big)(I_A \otimes \rho^B)\Big(P_{\mathcal{C}}^\perp E_i^\dagger + \sum_j (U_{ij} \otimes I_B) E_j^\dagger\Big) \\
&= \sum_{i,j,k} \big(E_j (U_{ij}^\dagger \otimes I_B) P_{\mathcal{C}}\big)(I_A \otimes \rho^B)\big(P_{\mathcal{C}}(U_{ik} \otimes I_B) E_k^\dagger\big) \\
&= \sum_{j,k} E_j (\Big(\sum_i U_{ij}^\dagger U_{ik}\Big) \otimes \rho^B) E_k^\dagger \\
&= \sum_j E_j (I_A \otimes \rho^B) E_j^\dagger \\
&= \mathcal{E}(I_A \otimes \rho^B).
\end{aligned}$$

By the polar decomposition applied to each $G_i P_{\mathcal{C}}$ and the fact that these operators have mutually orthogonal ranges, there are partial isometries V_i with mutually

orthogonal ranges for distinct i such that

$$G_i P_{\mathcal{C}} = V_i \sqrt{P_{\mathcal{C}} G_i^\dagger G_i P_{\mathcal{C}}} = V_i \big(\sqrt{D_{ii}} \otimes I_B \big).$$

Letting $D_i = \sqrt{D_{ii}}$ and extending each V_i to a unitary U_i on the whole space completes this direction of the proof.

To see the other implication, note that the map given by the Kraus operators $\{P_{\mathcal{C}} U_i^\dagger\}$ can be slightly modified to be a valid correction operation in exactly the same manner as was done in the subspace case. ■

To illustrate Lemma 4.2.3 and the testable conditions, another example is presented.

Example 4.2.4. *Let $U, V \in M_2$ be unitary matrices and let $q \in [0, 1)$. Then consider the channel $\mathcal{E} : M_4 \mapsto M_4$ given by the 2 Kraus operators in the standard basis*

$$E_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} \alpha U & i\beta U \\ -i\beta V & \alpha V \end{bmatrix} \qquad E_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} \alpha U & -i\beta U \\ i\beta V & \alpha V \end{bmatrix},$$

where $\alpha = \sqrt{q}$ and $\beta = \sqrt{1-q}$. Proceeding similarly to the subspace example earlier, it can be verified that if M_4 is decomposed as $M_4 = M_2 \otimes M_2$, then the second M_2 is a correctable subsystem for $\mathcal{E}$ because $P_{\mathcal{C}} = I_4$ and so

$$P_{\mathcal{C}} E_1^\dagger E_1 P_{\mathcal{C}} = \frac{1}{2} \begin{bmatrix} 1 & 2i\alpha\beta \\ -2i\alpha\beta & 1 \end{bmatrix} \otimes I_2$$

$$P_{\mathcal{C}} E_1^\dagger E_2 P_{\mathcal{C}} = \frac{1}{2} \begin{bmatrix} 2q-1 & 0 \\ 0 & 2q-1 \end{bmatrix} \otimes I_2$$

$$P_{\mathcal{C}} E_2^\dagger E_2 P_{\mathcal{C}} = \frac{1}{2}\begin{bmatrix} 1 & -2i\alpha\beta \\ 2i\alpha\beta & 1 \end{bmatrix} \otimes I_2,$$

which shows that the testable conditions are satisfied. There must then exist a channel $\mathcal{G}$ *of the form described by Lemma 4.2.3 such that* $\mathcal{E}(I_2 \otimes \rho) = \mathcal{G}(I_2 \otimes \rho)$ *for all* $\rho \in M_2$.

Indeed, it is not difficult to verify that one such channel is given by the single Kraus operator $\begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix}(I_2 \otimes I_2) = \begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix}$ *because* $\mathcal{E}(I_2 \otimes \rho) = \begin{bmatrix} U\rho U^\dagger & 0 \\ 0 & V\rho V^\dagger \end{bmatrix}$ *for all* $\rho \in M_2$. *The fact that the "D" matrix of the first subsystem described by Lemma 4.2.3 is equal to* I_2 *should not be misinterpreted as implying that there is no non-trivial evolution on that subsystem. Indeed, it can be shown that another Choi-Kraus representation of* $\mathcal{E}$ *is given by the two Kraus operators*

$$E_1 = \begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix}(\alpha I_2 \otimes I_2) \qquad E_2 = \begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix}(\beta Y \otimes I_2),$$

where Y *is the Pauli* Y *matrix. The fact that* $\mathcal{E}$ *can be written in this way, which highlights the correctability of the* B *subsystem and the evolution of the ancillary* A *subsystem, is a general result that will be presented in Theorem 4.2.7.*

4.2.2 Characterization of Correctable Subsystems

Theorem 4.2.5. *Let* $\mathcal{H}$ *be a Hilbert space, let* $\mathcal{E} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ *be a channel, and let* $\mathcal{C} = \mathcal{H}^A \otimes \mathcal{H}^B \subseteq \mathcal{H}$ *be a subspace. Then the following are equivalent:*

1. B *is a correctable subsystem for* $\mathcal{E}$.

2. $\exists$ *a* $\dagger$*-homomorphism* $\pi : \mathcal{B}(\mathcal{C}) \mapsto \mathcal{B}(\mathcal{H})$ *such that*

$$\mathcal{E}(I_A \otimes \rho^B) = \pi(I_A \otimes \rho^B)\mathcal{E}(P_{\mathcal{C}}) = \mathcal{E}(P_{\mathcal{C}})\pi(I_A \otimes \rho^B) \quad \forall\, \rho^B \in \mathcal{B}(\mathcal{H}^B).$$

Furthermore, the correction operation looks like $\pi^\dagger$ *when restricted to* $\mathcal{E}\big(\mathcal{B}(\mathcal{C})\big)$.

Proof. Begin by proving the implication *1* $\Rightarrow$ *2*. Since B is correctable for $\mathcal{E}$, Lemma 4.2.3 says that there exists a channel $\mathcal{G} = \{U_i(D_i \otimes I_B)\}$ such that $\{U_i\}$ is a family of unitaries such that $P_{\mathcal{C}} U_i^\dagger U_j P_{\mathcal{C}} = 0$ whenever $i \neq j$, and $\mathcal{G}(I_A \otimes \rho^B) = \mathcal{E}(I_A \otimes \rho^B)$ for all ρ^B.

Let $V_i = U_i P_{\mathcal{C}}$ and define a $\dagger$-homomorphism $\pi : \mathcal{B}(\mathcal{C}) \mapsto \mathcal{B}(\mathcal{H})$ by $\pi(\rho) = \sum_i V_i \rho V_i^\dagger$. It then follows that for all $\rho^B \in \mathcal{B}(\mathcal{H}^B)$,

$$\begin{aligned}
\mathcal{E}(P_{\mathcal{C}})\pi(I_A \otimes \rho^B) &= \Big(\sum_i V_i(D_i \otimes I_B)P_{\mathcal{C}}(D_i^\dagger \otimes I_B)V_i^\dagger\Big)\Big(\sum_j V_j(I_A \otimes \rho^B)V_j^\dagger\Big) \\
&= \sum_i V_i(D_i \otimes I_B)P_{\mathcal{C}}(D_i^\dagger \otimes I_B)(I_A \otimes \rho^B)V_i^\dagger \\
&= \sum_i V_i(D_i \otimes I_B)(I_A \otimes \rho^B)(D_i^\dagger \otimes I_B)V_i^\dagger \\
&= \mathcal{E}(I_A \otimes \rho^B).
\end{aligned}$$

A similar argument shows that $\mathcal{E}(I_A \otimes \rho^B) = \pi(I_A \otimes \rho^B)\mathcal{E}(P_{\mathcal{C}}) \quad \forall\, \rho^B \in \mathcal{B}(\mathcal{H}^B)$.

To see why *2* $\Rightarrow$ *1*, we show that the subsystem $\mathcal{B}$ is correctable. First note that the representation π defines a subspace and subsystems $\mathcal{C}' = \mathcal{A}' \otimes \mathcal{B}'$ with $\mathcal{B}'$ the same dimension as $\mathcal{B}$ and an isometry $V : \mathcal{B} \to \mathcal{B}'$ such that

$$\pi(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = I_{\mathcal{A}'} \otimes \mathcal{V}(\rho_{\mathcal{B}}) \quad \forall \rho_{\mathcal{B}},$$

where $\mathcal{V}(\rho_{\mathcal{B}}) = V \rho_{\mathcal{B}} V^\dagger$. Further, as $\mathcal{E}(P_{\mathcal{C}})$ commutes with $\pi(I_A \otimes \rho^B)$ for all ρ^B, it follows that $P_{\mathcal{C}'}\mathcal{E}(P_{\mathcal{C}})P_{\mathcal{C}'} = \sigma_{\mathcal{A}'} \otimes I_{\mathcal{B}'}$ for some positive operator $\sigma_{\mathcal{A}'} \in \mathcal{L}(\mathcal{A}')$ with

trace equal to $\dim \mathcal{C}$. Thus we have for all $\rho_{\mathcal{B}}$,

$$\begin{aligned}\mathcal{E}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) &= \pi(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})\mathcal{E}(P_{\mathcal{C}}) \\ &= (I_{\mathcal{A}'} \otimes \mathcal{V}(\rho_{\mathcal{B}}))(\sigma_{\mathcal{A}'} \otimes I_{\mathcal{B}'}) \\ &= \sigma_{\mathcal{A}'} \otimes \mathcal{V}(\rho_{\mathcal{B}}).\end{aligned}$$

Now define a channel $\mathcal{R}$ on $\mathcal{H}$ such that $\mathcal{R} \circ \mathcal{P}_{\mathcal{C}'} = (\mathcal{D}_{\mathcal{A}|\mathcal{A}'} \otimes \mathcal{V}^\dagger) \circ \mathcal{P}_{\mathcal{C}'}$, where $\mathcal{D}_{\mathcal{A}|\mathcal{A}'}$ is the complete depolarizing channel from $\mathcal{A}'$ to $\mathcal{A}$, and it follows that $(\mathcal{R} \circ \mathcal{E})(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}$ for all $\rho_{\mathcal{B}}$. This shows that B is a correctable subsystem, and completes the proof. ■

Just as was the case in the subspace situation, these proofs can be followed to give a method for computing the correction operation given a correctable subsystem for $\mathcal{E}$. In order to illustrate this theorem, consider again the channel and correctable subsystem of Example 4.2.4.

Example 4.2.6. *It trivially follows from the proof of Theorem 4.2.5 that the correction operation and the †-homomorphism described are given by*

$$\mathcal{R}(\sigma) = \begin{bmatrix} U^\dagger & 0 \\ 0 & V^\dagger \end{bmatrix} \sigma \begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix} \quad \forall\, \sigma \in M_4$$

and

$$\pi(\rho) = \begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix} \rho \begin{bmatrix} U^\dagger & 0 \\ 0 & V^\dagger \end{bmatrix} \quad \forall\, \rho \in M_4.$$

It is easy to see that $\mathcal{R}$ is indeed a valid correction operation in light of the various ways of writing $\mathcal{E}$ given in the previous example.

It was seen in Lemma 4.2.3 that when B is a correctable subsystem for $\mathcal{E}$, there is a channel $\mathcal{G}$ whose Kraus operators have mutually orthogonal ranges such that $\mathcal{E}(I_A \otimes \rho^B) = \mathcal{G}(I_A \otimes \rho^B)$. The following theorem extends this result to all of $A \otimes B$ and provides a simple way of looking at correctable subsystems.

Theorem 4.2.7. *Let $\mathcal{H}$ be a Hilbert space, let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ be a channel, and let $\mathcal{C} \equiv \mathcal{H}^A \otimes \mathcal{H}^B \subseteq \mathcal{H}$ be a subspace. Then B is correctable for $\mathcal{E}$ if and only if there is a family of unitary operators $\{U_i\}$ with $P_{\mathcal{C}} U_i^\dagger U_j P_{\mathcal{C}} = 0$ for all $i \neq j$ and a quantum channel $\mathcal{N}_A : \mathcal{B}(\mathcal{H}^A) \mapsto \mathcal{B}(\mathcal{H}^A)$ with Kraus operators $\{N_{i,j}\}$ such that $\mathcal{E}(\rho) = \mathcal{F}(\rho)$ for all $\rho \in \mathcal{B}(\mathcal{C})$, where $\mathcal{F} : \mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ is the quantum channel given by the Kraus operators $\{U_i(N_{i,j} \otimes I_B)\}$.*

Proof. As with two previous proofs in this work, the "if" direction follows by constructing a correction operation $\mathcal{R} = \{P_{\mathcal{C}} U_i^\dagger\}$ and extending its Kraus operators to a full set of partial isometries with mutually orthogonal initial subspaces.

To prove the "only if" direction, first let $|\psi\rangle \in \mathcal{H}^B$ be a unit vector and set $P = |\psi\rangle\langle\psi|$. Suppose that $\{|\alpha_k\rangle\}$ is an orthonormal basis for $\mathcal{H}^A$ and set $A_k = |\alpha_k\rangle\langle\alpha_k|$.

Now define $Q_i = U_i(I_A \otimes P)U_i^\dagger$, where $\{U_i\}$ is the family of unitary operators given by Lemma 4.2.3. Note that each Q_i is an orthogonal projection. Furthermore, it is not difficult to verify that

$$0 \leq \sum_i Q_i \mathcal{E}(A_k \otimes P) Q_i \leq \mathcal{E}(A_k \otimes P) \leq \mathcal{E}(I_A \otimes P) = \sum_i U_i (D_i^2 \otimes P) U_i^\dagger,$$

where $\{D_i\}$ is the family of positive diagonal operators given by Lemma 4.2.3. Since

the above inequalities hold for all k and

$$\mathcal{E}(I_A \otimes P) = \sum_k \mathcal{E}(A_k \otimes P) = \sum_{i,k} Q_i \mathcal{E}(A_k \otimes P) Q_i,$$

it follows that $\sum_i Q_i \mathcal{E}(A_k \otimes P) Q_i = \mathcal{E}(A_k \otimes P)$ for all k. A simple dimension-counting argument then shows that $\mathcal{E}(A_k \otimes P)$ must be of the form

$$\mathcal{E}(A_k \otimes P) = \sum_i U_i(\sigma_{i,k,\psi} \otimes P) U_i^\dagger.$$

It can also be shown that the operators $\{\sigma_{i,k,\psi}\}$ do not depend on $|\psi\rangle$. To this end, assume that $\dim(\mathcal{H}^B) = 2$ for clarity. The general case follows analogously.

Let $|\psi_l\rangle$, $l = 1, 2$ be an orthonormal basis for $\mathcal{H}^B$. Let $P_l = |\psi_l\rangle\langle\psi_l|$ and set $P_\pm = |\pm\rangle\langle\pm|$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|\psi_1\rangle \pm |\psi_2\rangle)$. Then by the above argument, there are positive operators $\{\sigma_{i,k,l}\}$ and $\{\sigma_{i,k,\pm}\}$ on $\mathcal{H}^A$ such that

$$\mathcal{E}(A_k \otimes P_l) = \sum_i U_i(\sigma_{i,k,l} \otimes P_l) U_i^\dagger \quad \text{and} \quad \mathcal{E}(A_k \otimes P_\pm) = \sum_i U_i(\sigma_{i,k,\pm} \otimes P_\pm) U_i^\dagger.$$

It then follows that

$$\begin{aligned}\mathcal{E}(A_k \otimes I_B) &= \sum_i U_i(\sigma_{i,k,1} \otimes P_1) U_i^\dagger + \sum_i U_i(\sigma_{i,k,2} \otimes P_2) U_i^\dagger \\ &= \sum_i U_i(\sigma_{i,k,+} \otimes P_+) U_i^\dagger + \sum_i U_i(\sigma_{i,k,-} \otimes P_-) U_i^\dagger\end{aligned}$$

Multiplying this equation on the left by $(I_A \otimes P_1) U_i^\dagger$ and on the right by $U_i(I_A \otimes P_1)$ shows that

$$\sigma_{i,k,1} \otimes P_1 = \frac{1}{2}(\sigma_{i,k,+} + \sigma_{i,k,-}) \otimes P_1.$$

Similarly, multiplying on the left by $(I_A \otimes P_2)U_i^\dagger$ and on the right by $U_i(I_A \otimes P_2)$ shows that the same equation holds with P_2. Thus, $\sigma_{i,k,1} = \sigma_{i,k,2}$. Furthermore, this equality holds regardless of i and k, and $|\psi_1\rangle$ and $|\psi_2\rangle$ were chosen arbitrarily. It thus follows that the $\{\sigma_{i,k,\psi}\}$ operators do not depend on ψ, and so linearity of $\mathcal{E}$ shows that for all σ^A there exist positive operators $\{\tau_i^A\}$ such that

$$\mathcal{E}(\sigma^A \otimes \rho^B) = \sum_i U_i(\tau_i^A \otimes \rho^B)U_i^\dagger \quad \forall\, \rho^B,$$

which completes the proof. ■

Note that the proof of Theorem 4.2.7 provides no indication of how to find the channel $\mathcal{N}_A$ acting on the ancillary subsystem. However, the unitary operators that it describes are exactly the unitary operators described by Lemma 4.2.3, which are not difficult to compute.

Chapter 5

Conclusions and Future Work

5.1 Improving the CB Norm Algorithm

The algorithm presented in Section 3.3 for computing the CB/$\diamond$ norm of linear maps provides a means for easily estimating the CB norm of an arbitrary CB map between complex matrix spaces. The algorithm was used to derive a formula for the CB norm of difference of unitary maps, and it has been seen that the algorithm is optimal in some (admittedly loose) sense.

Although the algorithm works well for low-dimensional examples and certain "nice" maps such as those of Theorem 3.3.4, exactly computing the minimization of Step 4 is still a very difficult problem in general. One obvious open problem is to build on this algorithm to find a method to compute the exact CB norm of an arbitrary linear map. Failing that, there is still room for improvement in the estimation

algorithm.

Indeed, the implementation of Step 4 in particular has room for improvement, as no in-depth analysis of the matrices used in the minimization has been carried out. Can matrices that lead to similar CB norm estimates be characterized in any way? Are there families of matrices that can be ruled out before being used, as they would lead to high estimates? Are there other methods of choosing matrices (such as evolutionary algorithms) that lead to better estimates, on average? Is there a way to compute the estimate in $\mathcal{O}(k^2n^2)$ time?

5.2 Further Characterization of QEC

Lemma 4.2.3 and Theorem 4.2.7 of Section 4.2 provide a simple way of picturing correctable subsystems; the correctability of the channel comes from what looks like a randomized unitary channel along with some evolution on the ancillary subsystem. Similarly, Theorem 4.2.5 provides a way of thinking about correctable subsystems in terms of representations. It could be enlightening to connect theses results with the Heisenberg picture of correctability developed in [3, 4].

Bibliography

[1] D. Aharonov, A. Kitaev, N. Nisan, *Quantum circuits with mixed states,* Proc. 30th ACM Symposium on Theory of Computation (STOC) (1997), 20-30. 1, 24, 25, 38

[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Physical Review A **54**, 3824 (1996). 3, 52

[3] C. Beny, A. Kempf, D.W. Kribs, *Generalization of quantum error correction via the Heisenberg picture*, Physical Review Letters, **98**, 100502 (2007). E-print:arxiv.org/quant-ph/0608071. 70

[4] C. Beny, A. Kempf, D.W. Kribs, *Quantum error correction of observables*, Physical Review A, **76**, 042303 (2007). E-print:arxiv.org/0705.1574. 70

[5] D.P. Blecher and V.I. Paulsen, *Tensor products of operator spaces,* J. Funct. Anal. **99** (1991), 262-292. 35, 36

[6] O. Bratteli, D.W. Robinson, *Operator Algebras and Quantum Statistical Mechanics 1*, 2nd edition (Springer, Berlin, 1987). 25

[7] M. Choi, *Completely Positive Linear Maps on Complex matrices*, Linear Algebra and Its Applications **10** (1975), 285-290. 9, 11

[8] H. Cohn, C. Umans, R. Kleinberg, B. Szegedy, *Group-theoretic Algorithms for Matrix Multiplication,* Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science 2005, IEEE Computer Society, 2005, 438-449. 49

[9] K. R. Davidson, C*-*algebras by example, Fields Institute Monographs* Amer. Math. Soc., Providence, 1996. 4, 11

[10] F. Dupuis, P. Hayden, D. Leung, A. Winter, *The maximal p-norm multiplicativity conjecture is really, really false,* in preparation, 2007. 2

[11] I. Devetak, M. Junge, C. King, M.B. Ruskai, *Multiplicativity of completely bounded p-norms implies a new additivity result,* arXiv:quant-ph/0506196 (2005). 2

[12] L.-M. Duan, G.-C. Guo, *Preserving coherence in quantum computation by pairing quantum bits*, Physical Review Letters **79** 1953 (1997). 3, 52

[13] A. Gilchrist, N.K. Langford, M. Nielsen, *Distance measures to compare real and ideal quantum processes,* Physical Review A **71**, 062310 (2005). 1, 24

[14] D. Gottesman, Physical Review A **54** 1862 (1996). 3

[15] P. Hayden, *The maximal p-norm multiplicativity conjecture is false,* arXiv:0707.3291 (2007). 2

[16] D.A. Herrero, *Approximation of Hilbert space operators, Volume 1 Second edition,* Longman Scientific & Technical **224**, Essex, 1989. 38

[17] A. Jencova, *A relation between completely bounded norms and conjugate channels,* arXiv:quant-ph/0601071 (2006). 2

[18] N. Johnston, D.W. Kribs, V.I. Paulsen, *Computing stabilized norms for quantum operations via the theory of completely bounded maps*, to appear in QIC. 2

[19] T.F. Jordan, A. Shaji, E.C.G. Sudarshan, *Dynamics of initially entangled open quantum systems,* Phys. Rev. A **70**, 052110 (2004). 2

[20] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Physical Review A **63**, 42307 (2001). 3

[21] A.Yu. Kitaev, *Quantum computations: algorithms and error correction,* Russian Math. Surveys **52** (1997), 1191-1249. 1, 24, 25

[22] D. Kretschmann, D. W. Kribs, R. Spekkens, *Complementarity of correctable and private subsystems,* in preparation, 2007. 2

[23] E. Knill and R. Laflamme, Physical Review A **55**, 900 (1997). 3, 52

[24] E. Knill, R. Laflamme, and L. Viola, Physical Review Letters **84**, 2525 (2000). 3

[25] K. Kraus, *General state changes in quantum theory*, Ann. Physics **64** (1971), 311-335. 11

[26] D.W. Kribs, R. Laflamme, D. Poulin, *A unified and generalized approach to quantum error correction*, Physical Review Letters, **94**, 180501 (2005). 3, 59

[27] D.W. Kribs, R. Laflamme, D. Poulin, M. Lesosky, *Operator quantum error correction*, Quantum Information & Computation, **6** (2006), 382–399. 3, 59

[28] D.W. Kribs, R.W. Spekkens, *Quantum error correcting subsystems are unitarily recoverable subsystems*, Physical Review A, **74**, 042329 (2006). 60

[29] D. Kretschmann, D. Schlingemann, R. F. Werner, *The information-disturbance tradeoff and the continuity of Stinespring's representation,* arXiv:quant-ph/0605009 (2006). 2

[30] D. A. Lidar, I. L. Chuang, K. B.Whaley, *Decoherence free subspaces for quantum computation*, Physical Review Letters **81**, 2594 (1998). 3, 52

[31] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000. 1

[32] G.M. Palma, K.-A. Suominen and A. Ekert, Proc. Royal Soc. A **452**, 567 (1996). 3

[33] V. I. Paulsen, *Completely Bounded Maps and Operator Algebras,* Cambridge Studies in Advanced Mathematics **78**, Cambridge University Press, Cambridge, 2003. 1, 3, 24, 25

[34] V.I. Paulsen, *Representations of Function Algebras, Abstract Operator Spaces, and Banach Space Geometry,* J. Funct. Anal., **109** (1992), 113–129. 26

[35] G. Pisier, *Non-commutative vector valued L_p-spaces and p-summing maps,* Soc. Math. France, Asterisque **247** (1998), 1–131. 2

[36] D. Perez-Garcia, M.M. Wolf, C. Palazuelos, I. Villanueva, M. Junge, *Unbounded violation of tripartite Bell inequalities,* arXiv:quant-ph/0702189 (2007). 2

[37] P. W. Shor, Physical Review A **52**, R2493 (1995). 3

[38] A. Shabani, D.A. Lidar, *Linear quantum error correction,* arXiv:0708.1953 (2007). 2

[39] R.R. Smith, *Completely bounded maps between C^*-algebras,* J. London Math. Soc. **27** (1983), 157–166. 25

[40] A. M. Steane, Physical Review Letters **77**, 793 (1996). 3

[41] Strassen, Volker, *Gaussian Elimination is not Optimal,* Numer. Math. **13** (1969), 354–356. 49

[42] J. Watrous, *Notes on super-operator norms induced by Schatten norms,* Quantum Information & Computation **5** (2005), 58–68. 2

[43] A. Winter, *The maximal output p-norm of quantum channels is not multiplicative for any $p > 2$,* arXiv:0707.0402 (2007). 2

[44] P. Zanardi, M. Rasetti, *Noiseless quantum codes*, Physical Review Letters **79**, 3306 (1997). 3, 52

[45] P. Zanardi, Physical Review A **63**, 12301 (2001). 3