Hybrid Quantum Systems: Complementarity of Quantum Privacy and Error-Correction, and Higher Rank Matricial Ranges

by

Mike Ignatius Nelson

A Thesis
presented to
The University of Guelph

In partial fulfilment of requirements
for the degree of
Doctor of Philosophy
in
Physics

Guelph, Ontario, Canada

ABSTRACT

HYBRID QUANTUM SYSTEMS: COMPLEMENTARITY OF QUANTUM PRIVACY AND ERROR-CORRECTION, AND HIGHER RANK MATRICIAL RANGES

Mike Ignatius Nelson
University of Guelph, 2021

Advisors:
Dr. David W. Kribs
Dr. Bei Zeng

The idea to transmit classical bits simultaneously with quantum information over a quantum channel has been explored since near the beginning of research in quantum information theory and computation fields. The process described, which we refer to as hybrid quantum computing, has been examined first with purely information theoretic considerations [1], and then later demonstrated to have benefits over using independent channels [2, 3, 4, 5, 6, 7]. The subject has since lay mostly dormant, until more recent work demonstrating the existence of good hybrid quantum error codes, as well as generalized mathematical results in the structure of error correcting codes.

In this thesis, I outline contributions to understanding criterion for the existence of hybrid codes, natural extensions of quantum computing ideas to the hybrid case as well as demonstrate some interesting practical examples. The thesis is organized in three [or four] main parts. The first considers the subject of the complementary relationship between quantum privacy and error correction in hybrid computing scenarios. Next, I extend these ideas to the approximate cases. Finally we see the introduction of higher rank matricial ranges as a tool to ascertain the existence of hybrid codes and benchmark the hybrid capacity of quantum channels.

DEDICATION

To God Almighty, the ultimate source of my life, and everything that I have, and am able to do. To my family, who have always believed in me, and supported everything I have set out to do. To Mr. and Mrs. Michael Nelson. To Mr. Lawrence Dzar.

ACKNOWLEDGEMENTS

Firstly and chiefly, I would like to thank my advisors David Kribs and Bei Zeng. I am grateful and honoured for the opportunity to work under researchers of their calibre and experience. They have provided me with guidance and oversight, opportunities to connect and collaborate with other excellent researchers and ensured that my needs as a graduate student were always very well met.

Possibly the greatest joy of working as a researcher is the community of curious, intelligent and hardworking individuals I have had the pleasure of working with, authoring works with, and having insightful conversations with. My appreciation goes to Rajesh Pereira, Jeremy Levick, Mizanur Rahaman, Yiu-Tung Poon and Chi-Kwong Li. My gratitude goes out to a great many pleasant graduate school colleagues as well, particularly fellow students at the Institute for Quantum Computing, and the Physics and Mathematics Departments at the University of Guelph. I am also especially thankful for Ninping Cao, a collaborator, and Comfort Mintah, a long term friend through this journey.

I would like to acknowledge all the staff of my academic home, the Department of Physics at the University of Guelph. I am very thankful for all teaching and non-teaching staff of the department, especially Reggi Vallillee, Janice Ilic, Kiley Rider, Jason Thomas, Cindy Wells and Mike Massa. Additionally I am grateful to Eric Poisson and Huan Yang for serving on my advisory committee.

My next thanks goes to Mitacs Canada and the African Institute for Mathematical Sciences in Ghana and Rwanda. My research was partly sponsored through internships

provided by these institutions, which also gave me travel and work opportunities abroad. Special thanks to Prince Osei, an academic mentor of mine, and all staff of the AIMS centres in Ghana and Rwanda, as well as staff of the Quantum Leap Africa centre in Kigali, Rwanda.

I have very deep appreciation for an important family in Canada. I have a tremendous amount of love and gratitude for the pastors and leaders of the River of Life International Fellowship in Guelph: Fule and Adwoa Badoe and Bob Radford. They and many, many other members of that family have been invaluable friends, brothers and sisters: a rich, deep, unending source of support and encouragement. To my ROLIF brothers and sisters, Sophia, Tosin, Annabella, Dennis and Precious, I say thank you.

Now I would like to express my immense gratitude for a fellow academic, former classmate and more importantly a very dear and faithful friend, Samar Elsheikh. Thank you for encouraging words and unending belief for many years.

It is certainly not possible to name everyone who has contributed in some way to this milestone in my academic career. I am eternally grateful to all who have mentored me professionally, and provided the support systems that have made the completion of doctoral studies possible.

TABLE OF CONTENTS

Chapter 1

Introduction

1.1 Introduction

Quantum mechanics was a well-developed physical theory by the end of the first few decades in the 20th century. The subject lays a fundamental understanding of the nature of the material world in which we live. However, while this understanding is at the heart of the technologies powering the modern information and computing age, there are unique and powerful aspects of the theory that have long since not fully realized their possible practical applications to information and computing. Beginning with ideas conceived in the early 1980s [8, 9] and continuing up until the present day, quantum computing is now a major scientific, engineering and entrepreneurial endeavour around the world. On one hand, advances in traditional computing systems (usually, and hereafter, referred to as *classical* computing) have typically depended on increasing the density of transistor circuits built into processing units using photolithography. There is a physical limit to the gains made this way, at which point quantum mechanical effects disrupt the principles of electronics circuits that

classical computing systems operate with. On the other hand, outside of that context, quantum mechanical phenomena are by no means undesirable. The density of information that a quantum system can represent and manipulate (compared to a classical one), owing to unique physical phenomena including superposition of states and quantum entanglement, in theory enables quantum computing processes to outperform their classical counterparts. The advancement in capability is anticipated to better simulate inherently quantum systems and solve hard problems like factoring integers (which has implications for security and encryption in global communications).

That last application would inspire curiosity as to why there has not yet been a breakdown of security systems based on classical computing approaches. While a few quantum-computing based algorithms have been developed and shown to be superior, developing an actual quantum computer to achieve these theoretical targets is a highly non-trivial undertaking. One of the major challenges that needs to be overcome is to protect the physical systems that store and manipulate quantum information from disruption due to quantum decoherence and other noise effects. Physical systems that by themselves exhibit quantum phenomena of interest are difficult, nay impossible, to completely isolate from the interfering environment. In fact, carrying out a computation on said system requires precise manipulation of, as well as measurements to investigate, the system's state. These very acts of control and measurement couple the quantum system to the environment. Ultimately, quantum computing units are highly susceptible to defects. It would not be possible for quantum computing as a venture to have developed any further until a successful demonstration of robust models of quantum computing (see Shor's result).

Quantum error-correction thus developed as a sub-field to address the above problem. This study is about almost as old as quantum computing itself; and to this day there is

active research into various topics in developing so-called fault tolerant quantum computers. Quantum error-correction developed following classical analogues of preserving information fidelity and robust computation. The underlying idea, as we will shortly see, is to add redundant bits to the information. This redundancy provides a safeguard and increases the likelihood that the intended quantum information is carried through a computation process. From the perspective of a physically implemented system with a fixed size, this means giving up some of the system's ideal capacity in order to increase robustness against the effects of noise. For this scheme to be successful, one needs to adequately identify and model the noise that disrupts quantum information. Then, given a good description of what faults occur on the system, quantum information is stored in the physical system in a suitable way. This enables detection of what faults may have occurred in the computation process, and subsequently a determination of what corrective actions must be taken. The way in which quantum information is represented (or encoded) on a system in order to allow recovery from defects is referred to as a quantum error-correcting code.

An important question arises out of the above considerations: how do we optimize the useful capacity of a quantum computing system? Intuitively, one would expect that the more 'noisy' a quantum system is, the less useful information it can robustly encode and compute. One would be correct. This assertion can be made more precise quantitatively, as we will later see. This consideration of the useful capacity of a quantum system is at the heart of the main motivations and outcomes of this research thesis. More to this, are investigations into channel capacity increases by transmitting through it classical and quantum information simultaneously. Heuristically, this approach considers the ability to make a quantum channel more useful by transmitting classical information through it, possibly where no more quantum information could have been robustly represented because of noise

effects. The simultaneous transmission and manipulation of classical and quantum information over a channel is referred to as Hybrid Quantum Computing. Error-correcting codes that protect jointly classical and quantum information in a system we will refer to as hybrid quantum error-correcting codes, or hybrid quantum codes.

Readers familiar with quantum computing will be aware that classical information is often used in conjunction with quantum computing schemes. Protocols such as quantum teleportation and LOCC schemes (local operations and classical communication) make use of separate classical communication channels. In the context of quantum computing protocols, the ability to transmit classical messages over a separate channel is largely considered trivial. The practical advantages of overlaying classical information on a quantum channel have been previously discussed in literature [2, 3]. These considerations, together with recent results in finding good hybrid quantum codes have motivated further studies into the subject.

In this thesis, we outline three main research outcomes with direct applications to hybrid quantum codes and private quantum channels.

1.2 Literature Overview and Thesis Structure

In Chapter 2, we lay down fundamental concepts and discuss some mathematical preliminaries. The chapter summarizes some introductory material in quantum information science ([10] is a primary reference), and discusses private quantum channels and the complementary map.

Chapter 3 discusses the complementary relationship between quantum error correction and private quantum systems. In this chapter, we discuss operator algebra structures that characterize correctable and private algebras, and thereby extend complementarity to a framework appropriate for hybrid quantum codes. The material in this chapter was published

in a research article here [11].

In chapter 4, we turn our attention to quasiorthogonality of operator algebras and their connection to quantum privacy. We introduce a notion of relative privacy and give a result which ties that to approximate quasiorthogonality. A discussion on some practical examples follows. This chapter is based on a published research (see [12]).

In chapter 5, we introduce a definition of the joint rank-$(k : p)$ matricial range motivated by its application to hybrid quantum error-correcting codes. The main result shows a lower bound for the size of a physical system that admits hybrid error-correcting codes of given parameters. A number of considerations following the result are given, followed by some examples. The chapter concludes with a discussion on advantages of hybrid quantum codes. This material was published in an article (see [13]).

Chapter 6 concludes the thesis and discusses directions for further works.

Chapter 2

Preliminaries

2.1 Quantum Information: States, Evolution and Measurement

We begin with a review of some important fundamental concepts in quantum information. Most of the material presented here is fairly standard; there are a number of texts that one can refer to (see for instance [10]). The goal is to then extend these ideas to certain generalizations, including the introduction of hybrid quantum information, which will lay the requisite foundation for the research this thesis details.

The postulates of quantum mechanics are often presented in introductory material for the subject. These are a mathematical axiomatization of the framework to which quantum mechanical systems conform. I will discuss the state space, evolution and measurement of a quantum system. These will first give us the qubit, which is the fundamental unit of information. Then evolution operators, which describe both the noise that disrupt qubits

and the recovery operations that restore them. Finally measurement, which destructively probes the state of a quantum system, and is essential to error-correcting procedures.

In a classical computer, the basic unit of information is a bit, which takes on one of two values, '0' or '1'. Information is represented by an n-bit string, which takes on 2^n distinct states, for some positive integer n. Generally, processing tasks are carried out by series of mappings between bit strings of different lengths.

The quantum computing analogue for a two-level unit of information is the *qubit*. While quantum mechanics allows for more general multi-level systems, or qudits, as well as infinite-dimensional systems, it will be sufficient to restrict our considerations to two-level systems. I will occasionally point out where the mathematical frameworks encompass more general multi-level quantum systems. The physical systems that quantum computers are implemented on exist in collections of configurations, or *states*, that are prepared, manipulated and then read-off. The first postulate tells us that the system's state can be represented by a unit vector in a complex Hilbert space, $\mathcal{H}$. For the qubit, this is the two-dimensional complex Hilbert space $\mathbb{C}^2$. The standard basis for $\mathbb{C}^2$ is typically represented in the following way:

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

using Dirac's bra-ket notation. These are the counterparts of classical bits. Any complex vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ represents a valid state, provided the normalization condition $|\alpha|^2 + |\beta|^2 = 1$ is satisfied. This condition ensures that the total probability of the two possible outcomes of a measurement in the computational basis is unity (see the discussion on measurement below).

Two things are important to point out here. One is that the vector sum is referred to as

a linear superposition of states. The other is that measurement outcomes are not altered by relative phases; meaning the state $|\phi\rangle = \alpha|0\rangle + \gamma\beta|1\rangle$ where γ is a complex number of unit modulus has the same measurement statistics as the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. However, $|\psi\rangle$ and $|\phi\rangle$ are distinct as states. The differing ways in which linear operations on quantum states add or cancel out in their relative phases, as well as operations on superpositions of states, are two of the key aspects of quantum theory that makes it more powerful computationally than its classical counterpart.

Just as there are strings of classical bits, one has composite systems, where multiple qubits are represented by tensor products $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ which are vectors belonging to a 2^n-dimensional composite Hilbert space $\mathcal{H} \otimes \cdots \otimes \mathcal{H}$.

So far, this description holds valid for quantum systems with perfect information about the states. Physicists refer to this as a pure state. One could alternatively describe a statistical ensemble of states, which would better represent the most general case in physical implementations. This includes situations in which there is uncertainty in which pure state a qubit is. The aforementioned general description is given by a density operator, which is a linear operator of the form

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|,$$

where the coefficients p_j are take from some classical probability distribution, and $|\psi_j\rangle\langle\psi_j|$ is an outer product $|\psi\rangle(|\psi\rangle)^\dagger$ of the pure state vector $|\psi\rangle$. Mathematically, a density operator ρ is a positive semi-definite Hermitian matrix with $\text{trace}(\rho) = 1$. The density operator of a pure state satisfies the condition $\rho = \rho^2$. For a qubit, the density operator is a 2×2 complex matrix ($\rho \in M_2$). For the rest of this thesis, M_n is the set of all $n \times n$ matrices with complex entries. The density matrix of a qubit is itself a vector of a 4-dimensional Hilbert space, but we will refer to it as an element of a matrix algebra. Just as with the vectors of pure states,

the density operator of n qubits comprises tensor products of single-qubit density operators with the form $\rho_1 \otimes \cdots \otimes \rho_n$.

Following from the normalization condition, an operator U that transforms pure state vectors is unitary, satisfying the $UU^\dagger = I$. $U^\dagger$ is the Hilbert space adjoint of the operator U. In matrix representation, $U^\dagger$ is the transpose matrix of U with its entries conjugated.

In the density operator description of quantum systems, we consider the evolution of open quantum systems. Closed quantum systems are completely isolated from their environment, and undergo unitary evolution. That is to say, the state $|\psi\rangle$ evolves to a new state $U|\psi\rangle$ described by the action of the unitary operator U. However, more generally, we should consider *open* quantum systems, which have some interaction with an environment. Suppose the quantum system of interest is labeled S, the entire system will be a composite system $\mathcal{H}_S \otimes \mathcal{H}_E$ of S together with an environment E. The composite system is closed and evolves via unitary operators. Suppose a density matrix $\rho = \rho_s \otimes \rho_E$ of the composite system undergoes evolution described by the unitary operator U. Then ρ is transformed to $U\rho U^\dagger$. Since the system S is of primary interest, we can define a map

$$\mathcal{E}(\rho_S) = tr_E\big(U\rho U^\dagger\big)$$

that describes the evolution of just ρ_S by the partial trace over the environment E. The map $\mathcal{E}$ defined in this way has a number of properties. It is linear, which makes it valid for mixed state density matrices. It is also a completely positive map, and preserves the trace of the operator it acts on. Such completely positive, trace-preserving (CTPT) maps $\mathcal{E}$, which we will generally call quantum channels, acting on a density operator ρ have a so-called operator

sum representation

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger.$$

The $\{E_i\}$ are called Kraus operators. They act on the underlying Hilbert space of states and satisfy the condition $\sum_i E_i^\dagger E_i = I$. Of primary interest will be channels that represent errors affecting a state. These will be referred to as error channels, or sometimes just channels where there is no confusion in the context. Another class of evolution operators which will be discussed are recovery operators, which restore a disturbed quantum state to a previous intended one, once the nature of the error operation which occurred has been determined.

A special set of unitary operators on $\mathbb{C}^2$ that will very frequently be employed are the Pauli operators, which in the standard bases, together with the identity operator, are :

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

Tensor products of these operators acting on parts of composite systems will often be encountered, and a compact notation for such is given here. Consider a system of n qubits, which is represented on the Hilbert space $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$, which is n-fold tensor products of $\mathbb{C}^2$. Each of the n qubits is represented on one of the $\mathbb{C}^2$ in the product and an operator of the form X_i is the X operator acting on the i-qubit, and identities elsewhere: $I \otimes I \otimes \cdots \otimes X_i \otimes \cdots \otimes I$. In similar fashion, we can have $Z_1 Z_2$, $X_1 Y_3$ and so on; the notation suppresses identity operators and tensor product symbols, with subscripts to indicate where the operators act.

Lastly, we briefly look at measurement. In quantum mechanics, specifically in the context of finite-dimensional multi-level systems, a measurement operation is represented by a Hermitian operator (A is Hermitian if $A^\dagger = A$.) These operators have a few special properties. They have a set of orthogonal eigenvectors which span the vector space on which

they act, and they have non-negative eigenvalues. Any measurement operation that probes the physical state of a system can be represented by such an operator, whose eigenvalues label the outcomes of the measurement, and whose eigenvectors represent the corresponding physical state obtained by the outcome. Because the eigenvectors of a measurement operator span the state space, any state vector can be written as a linear superposition (with appropriate coefficients) of eigenstates of the measurement operator. According to the Born interpretation, the square modulus of each coefficient, or 'amplitude', is proportional to the probability that the corresponding eigenstate will be observed. Once a system is measured, its sate is said to have 'collapsed' to the outcome of the measurement, and in the absence of an evolution, subsequent measurements will yield the same outcome.

Note that the Pauli operators X, Y and Z are also Hermitian, and are indeed also measurement operators for two-level systems in three different sets of basis states. The eigenstates of the Z operator coincide with the standard basis $\{|0\rangle, |1\rangle\}$. These are particularly important, and are referred to as the *computational basis*. The Pauli group of measurements is used extensively in quantum computation. I make a remark about measurement in quantum mechanical systems. A quantum state, represented by its state vector, can be said to describe the probability distributions of measurement outcomes for different Hermitian operators. Once such a measurement takes place, and the state has collapsed to the observed result, the information in the original state is lost: further manipulations to and measurements of the state no longer happen according to the original state of the system. In a significant way, information is lost when a measurement occurs to probe for some information. Because of this, in quantum information and computation, measurements have to be chosen carefully, and carried out only when necessary. As we see in the discussion of error correction that follows, carefully constructed measurements can obtain only some

information which is useful in recovery procedures, while preserving the information that is essential to a computation process.

2.2 A Brief Summary of Quantum Error Correction

In the creation, manipulation and retention of information, there is a requirement to ensure robustness and fault-tolerance. This is just as true for classical computing as it is essential for quantum computing. The techniques of detecting and correcting errors in the quantum scenario were in fact inspired by their classical counterparts. Let us briefly consider a simple error correcting scheme for classical information.

Suppose that given a stored bit there is some probability p that the bit is reversed, or 'flipped'. This might lead to undesired computing outcomes. A simple scheme of protection will be to append the bit with two extra copies of itself, in the manner

$$0 \to 000$$

$$1 \to 111.$$

This is known as a repetition code. The virtue of this scheme lies in the decreasing likelihood of larger proportions of the bit string being affected by the described error. In a 'majority voting' means of detecting and correcting a possible error, a string is ascribed the value corresponding to the most occurring bit value it contains. For instance, if one encountered 010 after transmission, then one expects the most likely correct string would be 000, and one proceeds after the necessary correction. This scheme is not necessarily perfect for the error. However, a straightforward calculation shows that the scheme fails with a probability

$3p^2 - 2p^3$, which is strictly less than p corresponding to the use of a single bit with no error correction , whenever $p < 0.5$.

The above classical example shows a suitable code for a given noise model (a bit flip error with probability $p < 0.5$) where adding redundancy (or trading off capacity) increases the robustness of an information channel. The bit strings 000 and 111 are referred to as logical '0' and logical '1' respectively, and show how 3 bits are effectively used to compute 1 bit due to the likelihood of errors in transmission.

Error-correcting codes for quantum computing are developed based on the same principle, except there are some subtleties that need to be addressed. First, the no-cloning theorem asserts an arbitrary quantum state cannot be copied. Another is that measurement of a state collapses it into an eigenstate of the measurement operator. Prohibition of state cloning has ramifications on the general means in which states can be transferred and coded onto physical systems. The measurement consideration is important because we would like to detect and correct errors on quantum states, and not destroy them. Thus the means by which a state is examined for errors needs to be carefully designed to make detection and correction possible, while preserving the full linear superposition.

The three qubit bit flip code described briefly here describes how a code is constructed in the quantum case for a similar type of noise model. The error operation is the bit flip operator, the Pauli unitary X, and the channel is one in which with probability p a qubit $|\psi\rangle$ is transformed to the state $X|\psi\rangle$. Restricting to the cases where majority voting would be successful in the classical case, we assume the error affects at most one qubit at a time, or not at all. There are then four cases that need to be distinguished. A similar type of encoding is used, utilizing CNOT gates to achieve the encoding

$$|0\rangle \rightarrow |000\rangle$$

$$|1\rangle \rightarrow |111\rangle.$$

By linearity of quantum operations, we can assume that the state $\alpha|0\rangle + \beta|1\rangle$ is encoded to a logical state represented on the physical system as $\alpha|000\rangle + \beta|111\rangle$. Thus in spite of no-cloning constraints we can attain a representation of a single qubit logical state on a physical system. It is undesirable to examine the entire state at the end of the channel for instances of qubit flips: this would cause the logical qubit to collapse to one of its basis states. We wish to preserve the transmitted qubit, possibly for later utilization, thus a collapsing measurement is non-ideal. We can however carry out a syndrome measurement, represented by a pair of Hermitian operators Z_1Z_2 and Z_2Z_3. I omit the full details here, but this will tell as whether the first and second qubit differ (or second and third, respectively). These outcomes will give us information about whether one of the qubits has been flipped, but will not perturb the probability amplitudes α and β of the original qubit that was encoded. A successful syndrome measurement then leads to an appropriate recovery operation; flipping any affected qubit. The error-correcting scheme is then complete. The quantum three qubit flip code also provides an improvement given the condition $p < 1/2$. Reviewing this fairly simple code allows us to demonstrate how error correction is possible in spite of a couple of subtle considerations in the quantum case.

There is one other issue that needs addressing: the most general class of errors that can occur on a pure state qubit is an infinite continuous set of unitary operators. This is not at all prohibitive in constructing error-correcting codes that can correct arbitrary errors on an

encoded qubit. The solution is an error-correcting scheme that corrects a discrete subset of errors that span the set of applicable unitary error operators. An example of this is the Shor nine-qubit code [14], which protects against an arbitrary error on at most one qubit. The Shor code can detect and correct the set of operators $\{I, X, Z, XZ\}$. A unitary operator can be written as a sum of operators belonging to this set. Due to this, the action of an arbitrary error $E|\psi\rangle$ can be written as a sum of the four terms $|\psi\rangle$, $X|\psi\rangle$, $Z|\psi\rangle$ and $XZ|\psi\rangle$, with appropriate coefficients. Measuring the error syndrome will cause the state to collapse to one of those terms, with a corresponding syndrome value, and the appropriate correction operation will return the state to $|\psi\rangle$. In this work we do not necessarily always concern ourselves with error-correcting codes for arbitrary errors on affected qubits. However, we will always describe error channels by some discrete set of error operators, for which some error-correcting scheme exists.

Considering the two practical examples above illustrates the working ideas behind quantum error correction. We can describe a general theory of the subject, and this will allow further generalizations to the theory hybrid quantum error correction, and connections to private quantum channels, as we will later see. Fundamentally, we say that for quantum error correction to be successful, then for an error channel $\mathcal{E}$ acting on an arbitrary density operator ρ of a state supported on the code subspace C, we have

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho. \tag{2.1}$$

As shown, a logical system is encoded onto a larger physical one, using some suitable encoding circuit. The encoded system of k qubits will be represented on some 2^k subspace C of the physical Hilbert space. As a vector subspace, there is projector P_C onto the code. We would like for the relevant set of error operators $\{E_i\}$ that there is a syndrome measurement

identifying which error has occurred, and subsequently a recovery operation to recover the encoded qubits. Altogether, each image of C under the action of any E_i must be faithful representation of C. Additionally, every E_iC has to be completely distinguishable from every other. These requirements are captured by the well-known Knill-Laflamme quantum error-correcting conditions, a set of equations concisely written as

$$P_C E_i^\dagger E_j P_C = \alpha_{ij} P_C, \tag{2.2}$$

for some complex numbers $\{\alpha_{ij}\}$. If $\{|c_i\rangle\}$ is a set of basis vectors for the subspace C, then the equations are alternatively written as

$$\langle c_i | E_k^\dagger E_l | c_j \rangle = \alpha_{kl} \delta_{ij}. \tag{2.3}$$

We note a connection between these equations and the notion of *higher rank numerical ranges* [15]. Given a matrix $A \in M_n$ and positive integer $k \geq 1$, the *rank-k numerical range of A* is the set of complex numbers given by

$$\Lambda_k(A) = \{\lambda \in \mathbb{C} : PAP = \lambda P, \text{ for some rank-}k \text{ projection } P\}.$$

The $k = 1$ case captures the classical numerical range of the matrix A,

$$W(A) = \{\langle \psi | A | \psi \rangle, \||\psi\rangle\| = 1\}.$$

When $k \geq 2$, the generalizations have interesting mathematical structures and are useful in quantum error correction [16, 17, 18]. In particular, note that, by the Knill-Laflamme equations (2.2), an error model with noise operators E_i has a k-dimensional correctable code

if and only if the rank-k numerical range of every pair $E_i^\dagger E_j$ is jointly non-empty; that is, there is a common rank-k projection (which defines the correctable code subspace) that satisfies the condition for $\Lambda_k(E_i^\dagger E_j)$ to be non-empty simultaneously for all pairs i, j. This motivates the definition of the *joint rank-k numerical range* $\Lambda_k(\mathbf{A})$ seen in [18]. Given an m-tuple of matrices $\mathbf{A} = (A_1, \cdots, A_m)$, $\Lambda_k(\mathbf{A})$ is the following set:

$$\{(\lambda_1, \cdots, \lambda_m) \in \mathbb{C}^m : PA_jP = \lambda_j \text{ for some rank-}k \text{ projector } P \text{ and all } j = 1, \cdots, m\}.$$

In Chapter 5 this generalization of numerical ranges is extended further to the case of hybrid quantum codes.

2.3 Hybrid Quantum Classical Error-Correcting Codes

I will now turn to discussing error correcting codes for the simultaneous transmission of classical and quantum information over a channel. This topic has had various considerations in literature (see [1, 19] for example), however recent constructions of good codes [20] have motivated renewed interest and further studies in hybrid codes. The research outcomes outlined in this thesis are largely motivated by, and center on theoretical and practical considerations for the hybrid transmission of information.

In briefly laying down some fundamental aspects of quantum information theory in this introductory chapter so far, the practical goal is to transmit some k-qubit quantum state $|\psi\rangle$. Owing to the need for error-correction, this state is encoded in some subspace, or more generally, subsystem of the n-qubit physical system that represents the working quantum

computer. Now, in addition to the quantum state, our objective is to recover some m-bit classical word, which would be one element of an $M = 2^m$ sized classical alphabet. To do this, we will need to find a collection $\{C^\nu : \nu = 1, \cdots, M\}$, of M correctable quantum codes to be used over the channel. Based on ν appropriately selected via some classical distribution, we will encode our qubit using an appropriate encoding circuit for C^ν. Transmission and the necessary error-correcting procedure then follow.

As pointed out in [20], there are rather trivial ways of doing this. The least interesting would be to simply use separate channels. Further, by partitioning, a KM dimensional quantum code can transmit M words each using a K-dimensional subcode. Alternatively, we could trade off quantum capacity for classical: say by fixing the basis states of a qubit subsystem to designate classical words. This particular research article succeeds in demonstrating better performing hybrid codes than these trivial constructions. Through various approaches, they find hybrid codes based on the theory stabilizer quantum codes, which correct errors on up to a certain number of qubit subsystems. In the relating works I outline in this thesis, we will see a more general framework for hybrid codes: subcodes need not be of the same dimension, or even the same qudit-type, and so on. Ultimately, we transmit some number of qudits, together with a classical word.

For the particular case of equally sized subspace codes, one can extend the Knill-Laflamme conditions to the hybrid case [20]. Suppose $\{|c^\nu\rangle\}$ is a set of basis vectors for one of the M K-dimensional subspace codes C^ν. Three requirements need to be met. The first, differing code basis states are distinguishable for different classical labels $\nu \neq \mu$. Secondly, the error operators map codes to faithful representations in the physical Hilbert space. Lastly that there is a syndrome measurement that determines which error has occurred if any, and also distinguishes which of the codes was transmitted before an error occurred. These

requirements are summarized by the equations

$$\langle c_i^\nu | E_k^\dagger E_l | c_j^\mu \rangle = \alpha_{kl}^\nu \delta_{ij} \delta_{\mu\nu}, \tag{2.4}$$

where the numbers α_{kl}^ν now depend on the classical labels ν.

2.4 Private Quantum Channels and Complementarity Quantum Channels

2.4.1 Private Quantum Channels

Now we look at a discussion of quantum privacy which motivates a definition for private quantum channels.

Private channels in quantum cryptography were introduced as an analogue of the classical one-time pad, or Vernam cypher. The objective is to transmit information over a channel between two participants, 'Alice' and 'Bob' while mitigating the risk of an eavesdropper 'Eve' obtaining information about the shared message.

In the classical information scenario, Eve could copy and access the n-bit message M. Alice avoids this by encrypting M with an n-bit preshared key K using the 'exclusive or' operation $M \oplus K$ (bit-wise addition modulo 2). The encoded message $M' = M \oplus K$ is transmitted over the channel. This process is reversible, and Bob recovers the message with $M = M' \oplus K$. Eve's copy of the message would be M'. Given M' intercepted over the channel, for any alternate message M_0 from Alice there is a key K_0 such that

$$M_0 \oplus K_0 = M \oplus K.$$

Without knowledge of the specific key K, Eve obtains no information about M. The operation is aptly named the 'one-time pad' because Alice and Bob can only use K as a key once to ensure the privacy of their transmission.

We now turn to the quantum privacy scheme. Alice seeks to send some n-qubit message represented by a density matrix ρ, so that Eve recovers no information about the state. As is the running theme, the quantum scenario has special features not present in classical privacy schemes. The non-cloning theorem forbids Eve from making a copy of an arbitrary quantum state over the channel. Further, any attempt by Eve to probe the state for information will disturb the state, immediately informing Alice and Bob of her intrusion.

To encode, the key Alice uses specifies an element set $\{U_i\}$ of N reversible (unitary) operations to operate on ρ, via some probability distribution p_i, with $\sum p_i = 1$. To account for the most general class of reversible operations Alice can carry out, the state is appended with an ancilla to obtain $\rho \otimes \rho_a$, and the unitary applies to this composite system. The transmitted state is

$$\rho' = U_i\big(\rho \otimes \rho_a\big)U_i^\dagger,$$

and Bob applies the inverse operation U_i^{-1} which he has prior knowledge of. Eve's description of the channel after encoding is

$$\Phi(\rho) = \sum_i p_i\, U_i(\rho \otimes \rho_a)U_i^\dagger.$$

In order to deny Eve any information of transmitted state, her description of the encoded message needs to be independent of ρ. Suppose there is some fixed density matrix ρ_0 such that for some subset S of possible messages contained in the Hilbert space $\mathcal{H}$ of states, we

have

$$\Phi(\rho) = \sum_i p_i \, U_i(\rho \otimes \rho_a)U_i^\dagger = \sigma_0$$

for any $\rho \in S$. We say that Φ is a private quantum channel for the subset S. Recall that from an operational perspective, Φ is an eavesdropper's description of the channel over which messages are transmitted. Bob can always recover the message with the appropriate key operation, but Eve has no knowledge of what was broadcast. In this way, the channel privatizes transmitted messages. This motivates the formal definitions of private quantum channels, subspaces and algebras I discuss later in this thesis. A simple example of transmitting a single qubit privately is given as follows. Given an arbitrary single qubit density operator, one can check that

$$\Phi(\rho) = \frac{1}{4}(\rho + X\rho X^\dagger + Y\rho Y^\dagger + Z\rho Z^\dagger) = \frac{1}{2}I.$$

So in this example, we have the set of single unit unitaries $\{I, X, Y, Z\}$ each applied with probability $\frac{1}{4}$. Eve's description of the channel will always be $\frac{1}{2}I$ irrespective of which density operator was transmitted, but Bob can recover the qubit knowing which unitary was applied.

2.4.2 Complementary Quantum Channels

Suppose that a quntum system of interest is labeled A and is represented on the Hilbert space $\mathcal{H}_A$. The density matrices of the system belong to the set of linear operators on $\mathcal{H}_A$, and a quantum channel is a completely positive and trace-preserving map $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_A)$ acting on $\mathcal{H}_A$. Recall that the properties of a quantum channel were determined through the description of open quantum systems. The Stinespring dilation theorem establishes this [21]. Given a quantum channel Φ, there is a Hilbert space $\mathcal{H}_C$ (with $\dim \mathcal{H}_C \leq (\dim \mathcal{H}_A)^2$),

a state $|\psi_C\rangle \in \mathcal{H}_C$ and a unitary U on $\mathcal{H}_A \otimes \mathcal{H}_C$ such that for all $\rho \in \mathcal{L}(\mathcal{H}_A)$,

$$\Phi(\rho) = \mathrm{Tr}_C \circ \mathcal{U}\left(\rho \otimes |\psi_C\rangle\langle\psi_C|\right) = \mathrm{Tr}_C \circ \mathcal{V}\left(\rho\right), \tag{2.5}$$

where here Tr_C denotes the partial trace map from $\mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_C)$ to $\mathcal{L}(\mathcal{H}_A)$, the map $\mathcal{U}(\cdot) = U(\cdot)U^*$, and $\mathcal{V}(\cdot) = V(\cdot)V^*$ is the map implemented by the isometry $V : \mathcal{H}_A \to \mathcal{H}_A \otimes \mathcal{H}_C$ defined by $V|\psi\rangle = U(|\psi\rangle \otimes |\psi_C\rangle)$. In effect, the channel Φ describes the evolution of an open quantum system A of interest, seen connected to its environment C, and together comprise a system that evolves via a unitary.

The *complementary map* Φ^C of Φ essentially describes how the connected environment $\mathcal{H}_C$ evolves: Φ^C is defined from $\mathcal{L}(\mathcal{H}_A)$ to $\mathcal{L}(\mathcal{H}_C)$ via

$$\Phi^C(\rho) = \mathrm{Tr}_A \circ \mathcal{V}\left(\rho\right). \tag{2.6}$$

Figure 2.1 below summarizes schematically how complementary maps are defined from considering open quantum systems together with their environment. We will consider a unique

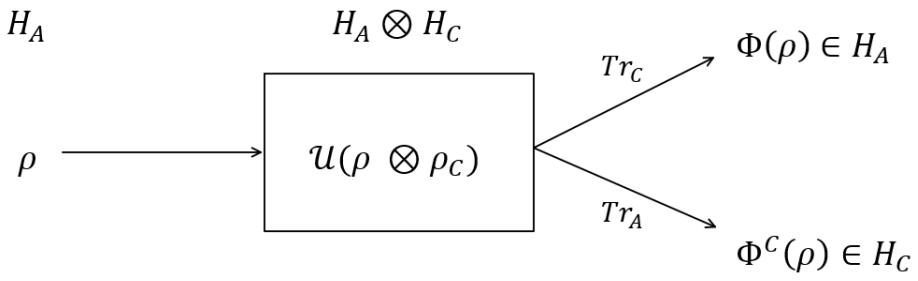

Figure 2.1: Complementary Maps

way of defining the complementary channel Φ^C in this thesis. If there where some alternatively defined copmlementary channel $\Phi' : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_{C'})$ such that $\Phi(\rho) = \mathrm{Tr}_{C'} V_1 \rho V_1^*$ and $\Phi'(\rho) = \mathrm{Tr}_A V_1 \rho V_1^*$ with $V_1 : \mathcal{H}_A \to \mathcal{H}_A \otimes \mathcal{H}_{C'}$, there is a partial isometry $W : \mathcal{H}_C \to \mathcal{H}_{C'}$ such that $\Phi'(\cdot) = W \Phi^C(\cdot) W^*$. When both $\mathcal{H}_C$ and $\mathcal{H}_{C'}$ have dimension equal to the Choi rank of Φ [], they are said to be minimal and W turns out to be a unitary operator. The complementary channel Φ^C is unique in this sense, up to some unitary transformation.

See [22, 23, 24] for further details on complementary channels. Here we only note additionally how the Kraus operators for the two maps Φ, Φ^C are related: If Φ has operator-sum representation $\Phi(\rho) = \sum_i V_i \rho V_i^*$ with Kraus operators $V_i \in \mathcal{L}(\mathcal{H}_A)$ (which are guaranteed to exist by the Stinespring theorem), then the complementary map has representation,

$$\Phi^C(\rho) = \sum_{i,j} \mathrm{Tr}(\rho V_j^* V_i) \, |i\rangle\langle j|,$$

where $\{|i\rangle\}$ is a canonical basis for $\mathbb{C}^d$ identified with $\mathcal{H}_C$, and $d = \dim \mathcal{H}_C$.

In this chapter, we have reviewed some fundamental aspects of quantum information, discussed complementary channels and introduced hybrid quantum error correction for the simultaneous transmission of classical and quantum information. We may now proceed to present research outcomes that make up this thesis. Further definitions and introductions will be made where needed.

Chapter 3

Quantum Complementarity and Operator Structuers

3.1 Introduction

In the previous chapter, we briefly presented quantum error correction, quantum privacy and complementary quantum channels. Quantum complementarity is the inherent relationship between privacy and correction via complementary channels. A quantum code is correctable for a quantum channel if and only if it is private for the channel's complementary map [25]. In this text, we will make this assertion more formal for the context of the operator algebra structures that encompass hybrid codes. Before proceeding, we can give a heuristic discussion of the concept, building on the practical motivations for the formal definitions of quantum correction and quantum privacy discussed in Chapter 2.

The goal of a quantum error-correcting code is ideally to recover an arbitrary quantum state (density matrix) supported on the code by some appropriate procedure, after the effects

of a noisy channel. In effect (refer to Figure 2.1), if we suppose Alice prepared a state ρ and transmitted it through a channel described by Φ, there is always some operation Bob could carry out on $\Phi(\rho)$ to recover ρ in the ideal case. If this were possible for an arbitrary ρ, then in some sense the information represented by ρ is intact in $\Phi(\rho)$, even if $\Phi(\rho)$ is not exactly ρ. This information could not have 'leaked' into the environment, whose perspective we saw as being described by the channel's complementary map $\Phi^C(\rho)$. Another way of saying this is that quantum information of an arbitrary state cannot both be represented on $\Phi(\rho)$ and $\Phi^C(\rho)$: that would manifestly be a violation of the no-cloning theorem. This is precisely the idea behind quantum privacy: the quantum information of ρ is private for the complementary map $\Phi^C(\rho)$. This thus leads us to the statement of complementarity presented in the opening paragraph of this section.

This linkage of two fundamental topics in quantum information has more recently [26] been extended to the complementarity of appropriate notions of correctable operator algebras [27, 28] and private subsystems and algebras [29, 30, 31, 32, 33, 34, 35, 36, 37, 26], and to a setting that embraces descriptions of hybrid classical and quantum information [38, 1, 2, 3, 4, 5, 20, 7]. Historically, quantum error correction is more developed than the theory of private quantum codes and algebras, with origins going back over two decades to the beginnings of modern quantum information science [39, 40, 41, 42, 43, 44]. The complementarity relationship suggests that developments in one field could at the least influence progress in the other. Of particular interest here, we note how completely positive map multiplicative domain structures and techniques [45] have been used to describe traditional quantum error correcting (subspace and subsystem) codes in terms of operator structures associated with quantum channels [46, 47, 48].

There are three main goals of the discussion in this chapter. First, the description of

error correcting codes for a quantum channel in the framework of multiplicative domains is extended to the context of finite-dimensional algebras. Hereafter, by 'algebra' we mean a C^*-algebra, which is a Banach Algebra with a *-operation that satisfies the properties of the Hermitian Adjoint of operators on a Hilbert space (see [49] or further discussion). The next step is to describe codes and algebras private to a given quantum channel through the null spaces of particular operators. By relating these to corresponding multiplicative domains, quantum complementarity is cast in terms of operator algebras. In the last part, we consider the special case of algebras privatized to a quantum state, and give dimension inequalities that compare correctable algebras with their complementary private algebras.

A more detailed organization of the chapter is given here. We start with needed background material on complementary channels, and extend the discussion of correctability of errors and privacy in the introductory chapter to correctable and private algebras. A new simple proof of perfect complementarity is given. In section 3, quantum error correction in terms of multiplicative domains is extended to algebras. Following that, we identify appropriate null spaces that describe private algebra, and explicitly show the complementary relationship between the two structures. The special case of unital channels (channels that preserve the identity) is considered, showing its particular features. The penultimate section is a quantitative comparison of pairs of correctable and private algebras in terms of inequalities relating their dimensions.

The contents of this chapter are adapted from research findings co-authored and published with various collaborators [11]. All authors made contributions to the preparation and review of the original manuscript.

3.2 Complementary Channels and Correctable vs Private Algebras

The notation used is fairly standard, as we have introduced in the second chapter. In this section we introduce further requisite preliminary notions: correctable and private operator algebras based on the formulation from [26]. We shall work with finite-dimensional Hilbert spaces $\mathcal{H}$, where the sets of linear, trace class, and bounded operators coincide: $\mathcal{L}(\mathcal{H}) = \mathcal{T}(\mathcal{H}) = \mathcal{B}(\mathcal{H})$, and so for ease of presentation we use $\mathcal{L}(\mathcal{H})$ to denote these sets.

3.2.1 Correctable Algebras

The general framework for error correction, which generalizes standard quantum error correction and is called "operator algebra quantum error correction" (OAQEC) [27, 28, 50], when applied to the finite-dimensional case makes use of the structure theory for finite-dimensional von Neumann algebras (or equivalently, C*-algebras). Specifically, codes are identified with algebras that up to unitarily equivalence can be decomposed as $\mathcal{A} = \oplus_k (I_{m_k} \otimes M_{n_k})$, where M_n is the set of $n \times n$ complex matrices. An OAQEC code is described as follows in each of the Schrödinger and Heisenberg pictures for quantum dynamics. We shall use the notation $\Phi^\dagger$ for the dual map of Φ defined via the trace inner product: $\mathrm{Tr}(\Phi(\rho)X) = \mathrm{Tr}(\rho\, \Phi^\dagger(X))$.

Definition 3.2.1. *Let $\mathcal{H}$ be a (finite-dimensional) Hilbert space and let Q be a projection on $\mathcal{H}$. Given a channel $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$, a von Neumann subalgebra $\mathcal{A} \subseteq \mathcal{L}(Q\mathcal{H})$ is* **correctable for Φ with respect to** *Q if there exists a channel $\mathcal{R} : \mathcal{L}(\mathcal{H}_C) \to \mathcal{A}$ such that*

$$\mathcal{P}_Q \circ \Phi^\dagger \circ \mathcal{R}^\dagger = id_{\mathcal{A}}, \tag{3.1}$$

where $\mathcal{P}_Q$ is the compression map $\mathcal{P}_Q(\cdot) = Q(\cdot)Q$. When $Q = I$ we simply say $\mathcal{A}$ is **correctable for** Φ.

The case of standard (Knill-Laflamme) error correction is captured with algebras $\mathcal{A} = P_{\mathcal{C}}\mathcal{L}(\mathcal{H})P_{\mathcal{C}}$, where $\mathcal{C}$ is a subspace of $\mathcal{H}$ and $Q = P_{\mathcal{C}}$. When $\mathcal{C} = \mathcal{H}_A \otimes \mathcal{H}_B$ has some tensor decomposition, correctable algebras $\mathcal{A} = P_{\mathcal{C}}(I_A \otimes \mathcal{L}(\mathcal{H}_B))P_{\mathcal{C}}$ are "operator subsystem codes" [51, 52] when $\dim \mathcal{H}_B > 1$ and classical codes when $\dim \mathcal{H}_B = 1$. Algebras $\mathcal{A}$ comprised of direct sums give mixtures of these various possibilities and allow for hybrid classical and quantum information encodings [27, 28, 38]. Such an algebra, with direct sum decomposition as above, is correctable for Φ with respect to its unit projection if and only if for all density operators $\sigma_k^{(i)}$ and probability distributions p_k, there is a channel $\mathcal{R}$ on $\mathcal{H}$ and density operators $\sigma_k^{(1)'}$ such that

$$(\mathcal{R} \circ \Phi) \left(\sum_k p_k (\sigma_k^{(1)} \otimes \sigma_k^{(2)}) \right) = \sum_k p_k (\sigma_k^{(1)'} \otimes \sigma_k^{(2)}). \tag{3.2}$$

3.2.2 Private Algebras

In Chapter 2 we introduced quantum privacy and motivated the its formal definition. What follows here is a more general notion of "private algebras" (see [26] and references therein), a notion most cleanly presented in the Heisenberg picture of quantum mechanics.

Definition 3.2.2. *Let $\mathcal{H}$ be a (finite-dimensional) Hilbert space and let Q be a projection on $\mathcal{H}$. Given a channel $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$, a von Neumann subalgebra $\mathcal{A} \subseteq \mathcal{L}(Q\mathcal{H})$ is* **private for Φ with respect to** *Q if*

$$\mathcal{P}_Q \circ \Phi^\dagger(\mathcal{L}(\mathcal{H})) \subseteq \mathcal{A}' = \{X \in \mathcal{L}(Q\mathcal{H}) \mid [X, A] = 0 \ \forall A \in \mathcal{A}\}. \tag{3.3}$$

When $Q = I$ we simply say $\mathcal{A}$ is **private for** Φ.

This definition is motivated by the notion of an "operator private subsystem" [32, 37]: Suppose we have $\mathcal{H} = (\mathcal{H}_A \otimes \mathcal{H}_B) \oplus (\mathcal{H}_A \otimes \mathcal{H}_B)^\perp$ and a channel Φ on $\mathcal{H}$. Then the subsystem B is called an operator private subsystem for Φ if $\Phi \circ \mathcal{P}_\mathcal{C} = (\Psi \otimes \mathrm{Tr}) \circ \mathcal{P}_\mathcal{C}$ for some channel $\Psi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H})$, where $\mathcal{P}_\mathcal{C}(\cdot) = P_\mathcal{C}(\cdot)P_\mathcal{C}$ with $P_\mathcal{C}$ the projection of $\mathcal{H}$ onto $C = \mathcal{H}_A \otimes \mathcal{H}_B$. One can check through direct calculation and application of the dual map relation that this is equivalent to: $\mathcal{P}_C \circ \Phi^\dagger(\mathcal{L}(\mathcal{H})) \subseteq \mathcal{L}(\mathcal{H}_A) \otimes I_B = (I_A \otimes \mathcal{L}(\mathcal{H}_B))'$; in other words, that the algebra $\mathcal{A} = I_A \otimes \mathcal{L}(\mathcal{H}_B)$ is private for Φ with respect to $P_\mathcal{C}$.

As articulated in [26], use of the "private" terminology is motivated by the fact that any information stored in the operator private subsystem B completely decoheres under the action of Φ. From the Heisenberg perspective, observables on the output system evolve under Φ to observables having the same measurement statistics with respect to the subsystem B. For more general private subalgebras though, not all information about observables in the algebra $\mathcal{A}$ is lost under the action of Φ, just the quantum information: more precisely, the only obtainable information about $\mathcal{A}$ after an application of the channel is the classical information contained in its centre $\mathcal{Z}(\mathcal{A}) = \mathcal{A} \cap \mathcal{A}'$. We recover the original notion of privacy when $\mathcal{A}$ is a von Neumann algebra factor ($\mathcal{Z}(\mathcal{A}) = \mathbb{C}I$), and factors of type I specifically correspond to operator private subsystems. The above definition allows for more general private scenarios as depicted by more general algebras.

3.2.3 Complementarity for Perfect Correction and Privacy

We conclude this section by presenting a simple new proof of complementarity between quantum error correction and privacy in the ideal ($\varepsilon = 0$) case of perfect correction and privacy. We first recall the testable conditions for correctable algebras derived in [27, 28],

which in turn built upon the central Knill-Laflamme conditions for standard [43] and operator [52, 51] quantum error correction.

Theorem 3.2.3. *Let $\mathcal{H}$ be a Hilbert space and let Q be a projection on $\mathcal{H}$. Given a channel $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$, an algebra $\mathcal{A} \subseteq \mathcal{L}(Q\mathcal{H})$ is correctable for Φ with respect to Q if and only if*

$$[QV_j^*V_iQ, X] = 0 \quad \forall X \in \mathcal{A},\ \forall i, j. \tag{3.4}$$

The approximate version of the following proposition was established via dilation theory techniques separately in the finite ([25]) and infinite ([26]) dimensional cases. A new proof of the result is presented below for the ideal case. This proof is different in that it makes use of Kraus operator representations and the relevant operator structures.

Proposition 3.2.4. *Let $\mathcal{A}$ be a subalgebra of $\mathcal{L}(Q\mathcal{H})$, for some Hilbert space $\mathcal{H}$ and projection Q. Let Φ be a channel on $\mathcal{H}$ with complementary channel Φ^C. Then $\mathcal{A}$ is correctable for Φ with respect to Q if and only if $\mathcal{A}$ is private for Φ^C with respect to Q.*

Proof. Suppose first that $\mathcal{A}$ is correctable for Φ with respect to Q. Then Eqs. (3.4) hold. So we let $\rho \in \mathcal{L}(\mathcal{H})$, $Y \in \mathcal{L}(\mathcal{H}_C)$, and $X \in \mathcal{A}$, and compute two identities as follows:

$$\begin{aligned}
\mathrm{Tr}(Q(\Phi^C)^\dagger(Y)QX\rho) &= \mathrm{Tr}(Y\Phi^C(QX\rho Q)) \\
&= \mathrm{Tr}\left(Y\big(\sum_{i,j}\mathrm{Tr}(QX\rho QV_j^*V_i)\big)|i\rangle\langle j|\right) \\
&= \sum_{i,j}\mathrm{Tr}(\rho QV_j^*V_iQX)\,\mathrm{Tr}(Y|i\rangle\langle j|),
\end{aligned}$$

and,

$$\begin{aligned}
\mathrm{Tr}(XQ(\Phi^C)^\dagger(Y)Q\rho) &= \mathrm{Tr}(XQ(\Phi^C)^\dagger(Y)Q\rho) \\
&= \mathrm{Tr}((\Phi^C)^\dagger(Y)Q\rho XQ) \\
&= \mathrm{Tr}(Y\Phi^C(Q\rho XQ)) \\
&= \mathrm{Tr}\left(Y\big(\sum_{i,j}\mathrm{Tr}(Q\rho XQV_j^*V_i)\big)|i\rangle\langle j|\right) \\
&= \sum_{i,j}\mathrm{Tr}(\rho XQV_j^*V_iQ)\,\mathrm{Tr}(Y|i\rangle\langle j|),
\end{aligned}$$

from which we can conclude from Eqs. (3.4) that these two quantities are equal. As X, Y, ρ were arbitrary, it follows that $[\mathcal{P}_Q \circ (\Phi^C)^\dagger(Y), X] = 0$ for all $X \in \mathcal{A}$ and hence $\mathcal{A}$ is private for Φ^C with respect to Q.

For the converse direction, suppose that $\mathcal{A}$ is private for Φ^C with respect to Q. Then $\mathcal{P}_Q \circ (\Phi^C)^\dagger(\mathcal{L}(\mathcal{H}_C)) \subseteq \mathcal{A}'$, and so for all $X \in \mathcal{A}$, $\rho \in \mathcal{L}(\mathcal{H})$, $Y \in \mathcal{L}(\mathcal{H}_C)$ we have

$$\mathrm{Tr}(Q(\Phi^C)^\dagger(Y)QX\rho) = \mathrm{Tr}(XQ(\Phi^C)^\dagger(Y)Q\rho),$$

and hence from the above calculations that

$$\sum_{i,j}\mathrm{Tr}(\rho QV_j^*V_iQX)\langle j|Y|i\rangle = \sum_{i,j}\mathrm{Tr}(\rho XQV_j^*V_iQ)\langle j|Y|i\rangle.$$

To conclude the proof, we now fix a pair i_0, j_0 and apply this identity with $Y = |j_0\rangle\langle i_0|$ to obtain

$$\mathrm{Tr}(\rho QV_{j_0}^*V_{i_0}QX) = \mathrm{Tr}(\rho XQV_{j_0}^*V_{i_0}Q),$$

which holds for all ρ and X. Thus it follows that $[QV_{j_0}^*V_{i_0}Q, X] = 0$ for all $X \in \mathcal{A}$, and

hence by Lemma 3.2.3 we have that $\mathcal{A}$ is correctable for Φ with respect to Q, and the result follows. □

3.3 Complementary Operator Structures

Operator structures have previously been identified that describe quantum error correction; for instance, multiplicative domains for channels and certain generalizations of them were shown to characterize operator and standard quantum error correction as part of the early expanded work on subsystem codes [46, 47]. Below we shall briefly review these structures and then extend the correspondence to OAQEC.

First though, we will identify operator structures that characterize private (subspaces, subsystems, and) algebras. We begin with a simple observation of an elementary connection between the null space of a quantum channel and the sets of states that it privatizes. Let Φ be a channel from M_n to M_m and let S be the null space of Φ. If ρ_1 and ρ_2 are $n \times n$ density matrices, then $\Phi(\rho_1) = \Phi(\rho_2)$ if and only if $\rho_1 - \rho_2 \in S$. This observation suggests that nullspaces of channels can be used to describe privacy, and indeed this is the case.

Lemma 3.3.1. *Let $\mathcal{H}$ be a Hilbert space and let Q be a projection on $\mathcal{H}$. Given a channel $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ with $\Phi(\rho) = \sum_i V_i \rho V_i^*$, the following commutants inside $\mathcal{L}(\mathcal{H})$ coincide:*

$$\{QV_j^* V_i Q\}'_{i,j} = \Big(\big(\ker(\Phi^C \circ \mathcal{P}_Q)\big)^{\perp}\Big)', \tag{3.5}$$

where orthogonality is with respect to the trace inner product.

Proof. By direct calculation using the form of the complementary map, we have

$$(\Phi^C \circ \mathcal{P}_Q)(X) = \Phi^C(QXQ) = \sum_{i,j} \mathrm{Tr}(XQV_j^* V_i Q)\, |i\rangle\langle j|.$$

Hence, $\ker(\Phi^C \circ \mathcal{P}_Q) = (\mathrm{span}\{QV_j^* V_i Q\}_{i,j})^\perp$. □

Theorem 3.3.2. *Let $\mathcal{A}$ be a subalgebra of $\mathcal{L}(Q\mathcal{H})$, for some Hilbert space $\mathcal{H}$ and projection $Q \in \mathcal{L}(\mathcal{H})$. Let Φ be a channel on $\mathcal{H}$ with complementary channel Φ^C. Then $\mathcal{A}$ is private for Φ with respect to Q if and only if $\mathcal{A}$ is contained inside $((\ker(\Phi \circ \mathcal{P}_Q))^\perp)'$.*

Proof. This can be proved by combining Theorem 3.2.3, Proposition 3.2.4 and Lemma 3.3.1, as well as the fact (see chapter 6 of [23]) that $(\Phi^C)^C$ is isometrically equivalent to Φ. □

We can explicitly connect these private structures with the corresponding structures from error correction, the subject of which we now turn. For brevity we shall consider the correctable/private ($Q = I$) case.

Definition 3.3.3. *The* **multiplicative domain**, *$\mathcal{M}(\Phi)$, of a channel $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is the set (in fact an algebra) given by:*

$$\mathcal{M}(\Phi) = \{A \in \mathcal{L}(\mathcal{H}) : \Phi(AX) = \Phi(A)\Phi(X); \Phi(XA) = \Phi(X)\Phi(A)\ \forall X\},$$

where X is taken from $\mathcal{L}(\mathcal{H})$. The multiplicative domain is the largest set on which the restriction of Φ is a $*$-homomorphism (i.e., a representation).

Given a subalgebra $\mathcal{A} \subseteq \mathcal{L}(\mathcal{H})$ and a representation $\pi : \mathcal{A} \to \mathcal{L}(\mathcal{H})$ (that is, π is linear, $\pi(AB) = \pi(A)\pi(B)$ and $\pi(A)^* = \pi(A^*)$ for all $A, B \in \mathcal{A}$), we may also define **generalized**

multiplicative domains *as follows:*

$$\mathcal{M}_\pi(\Phi) = \{A \in \mathcal{A} : \Phi(AX) = \pi(A)\Phi(X); \Phi(XA) = \Phi(X)\pi(A)\ \forall X \in \mathcal{L}(\mathcal{H})\}.$$

The following quantum error correction result was established for subsystem codes in [47], and here we show that it extends to OAQEC. Our proof is built on techniques from [47] and error correction constructions from [27, 28].

Theorem 3.3.4. *Let $\mathcal{A}$ be a subalgebra of $\mathcal{L}(\mathcal{H})$ and let Φ be a channel on $\mathcal{L}(\mathcal{H})$. Then $\mathcal{A}$ is correctable for Φ if and only if $\mathcal{A} = \mathcal{M}_\pi(\Phi)$ for some representation $\pi : \mathcal{A} \to \mathcal{L}(\mathcal{H})$.*

Proof. First suppose $\mathcal{A} = \mathcal{M}_\pi(\Phi)$. So $\Phi(AX) = \pi(A)\Phi(X)$ for all $A \in \mathcal{A}$ and $X \in \mathcal{L}(\mathcal{H})$, $\pi(AB) = \pi(A)\pi(B)$ and $\pi(A)^* = \pi(A^*)$ for all $A, B \in \mathcal{A}$. Then, since Φ is trace-preserving, we have

$$\mathrm{Tr}(AX) = \mathrm{Tr}(\Phi(AX)) = \mathrm{Tr}(\pi(A)\Phi(X)) = \mathrm{Tr}(\Phi^\dagger(\pi(A))X)$$

for all $X \in \mathcal{L}(\mathcal{H})$ and hence $\Phi^\dagger(\pi(A)) = A$ for all $A \in \mathcal{A}$.

Now, let $A \in \mathcal{A}$ and observe since π is a homomorphism and $\Phi^\dagger(\pi(A)) = A$, we have

$$\begin{aligned} \Phi^\dagger(\pi(A)\pi(A^*)) - A\Phi^\dagger(\pi(A^*)) &- \Phi^\dagger(\pi(A))A^* + AA^* \\ &= AA^* - AA^* - AA^* + AA^* \\ &= 0. \end{aligned}$$

However, observe this quantity is also equal to (recalling $\Phi^\dagger(Y) = \sum_i V_i^* Y V_i$ and $\Phi^\dagger$ is unital since Φ is trace-preserving) the following sum when fully expanded:

$$\sum_i (V_i^*\pi(A) - AV_i^*)(V_i^*\pi(A) - AV_i^*)^* = \sum_i (V_i^*\pi(A) - AV_i^*)(\pi(A^*)V_i - V_iA^*).$$

Hence, it follows that each term in this sum is 0, and so we must have (also using the fact that $\mathcal{A}$ is a self-adjoint set)

$$V_i^*\pi(A) = AV_i^* \quad \text{and} \quad \pi(A)V_j = V_jA.$$

Multiply the first equation on the right by V_j and the second equation on the left by V_i^* to obtain

$$AV_i^*V_j = V_i^*\pi(A)V_j = V_i^*V_jA,$$

and thus we have shown that $\mathcal{A} \subseteq \{V_i^*V_j\}'$ and $\mathcal{A}$ is correctable for Φ.

For the converse implication, assume that $\mathcal{A} \subseteq \{V_i^*V_j\}'$. Let $R = \Phi(I) = \sum_i V_iV_i^*$; notice that

$$\Phi(A)R = \sum_{i,j} V_iAV_i^*V_jV_j^* = \sum_{i,j} V_iV_i^*V_jAV_j^* = R\Phi(A), \tag{3.6}$$

and so $\Phi(A)$ commutes with any power of R for all $A \in \mathcal{A}$. Next, observe that

$$\Phi(A)\Phi(X) = \sum_{i,j} V_iAV_i^*V_jXV_j^* = \sum_i V_iV_i^* \sum_j V_jAXV_j^* = R\Phi(AX) \tag{3.7}$$

and similarly,

$$\Phi(X)\Phi(A) = \Phi(XA)R. \tag{3.8}$$

If R is invertible, we then obtain

$$\Phi(AX) = R^{-1}\Phi(A)\Phi(X) = R^{-1/2}\Phi(A)R^{-1/2}\Phi(X);$$

and,

$$\Phi(XA) = \Phi(X)\Phi(A)R^{-1} = \Phi(X)R^{-1/2}\Phi(A)R^{-1/2}.$$

Defining $\pi(A) = R^{-1/2}\Phi(A)R^{-1/2}$ we see that the above can be written as

$$\Phi(AX) = \pi(A)\Phi(X) \quad \text{and} \quad \Phi(XA) = \Phi(X)\pi(A),$$

and we note that for any $A, B \in \mathcal{A}$,

$$\begin{aligned}\pi(A)\pi(B) &= R^{-1/2}\Phi(A)R^{-1}\Phi(B)R^{-1/2} \\ &= R^{-1/2}\Phi(A)\Phi(B)R^{-3/2} \\ &= R^{-1/2}\Phi(AB)R^{-1/2} \\ &= \pi(AB)\end{aligned}$$

where we have used the fact that $\Phi(B)$ commutes with all powers of R and that $\Phi(A)\Phi(B) = \Phi(AB)R$. It follows that $\mathcal{A} = \mathcal{M}_\pi(\Phi)$ as required.

If R is not invertible, we note that $\ker(R) = \cap_i \ker(V_i^*)$ and so if $R|\psi\rangle = 0$, then $\Phi(X)|\psi\rangle = \sum_i V_i X V_i^*|\psi\rangle = 0$ and $\langle\psi|\Phi(X) = \sum_i \langle\psi|V_i X V_i^* = 0$ as well. Hence, if we write $\mathcal{V} = \ker(R)$ and split $\mathcal{H} = \mathcal{V}^\perp \oplus \mathcal{V}$, according to this decomposition $R = Q \oplus 0$ with Q invertible, and $\Phi(X) = \Psi(X) \oplus 0$. Hence, returning to Eq. (3.7) we see that it can be written as

$$(\Psi(A)\Psi(X)) \oplus 0 = (Q\Psi(AX)) \oplus 0,$$

and if we multiply by $Q^{-1} \oplus 0$ we get

$$(Q^{-1}\Psi(A)\Psi(X)) \oplus 0 = \Psi(AX) \oplus 0$$

and hence

$$R^{+}\Phi(A)\Phi(X) = \Phi(AX)$$

where R^{+} is the pseudo-inverse of R. Similarly, we can do the same for Eq. (3.8) and let $\pi(A) = (R^{+})^{-1/2}\Phi(A)(R^{+})^{-1/2}$ to get the desired result that $\mathcal{A} = \mathcal{M}_{\pi}(\Phi)$, and this completes the proof. □

Remark 3.3.5. Observe from the start of the above proof that any correctable algebra for Φ is contained in the range of $\Phi^{\dagger}$. (This was also observed from a different perspective in [28].) We will use this fact in the next section.

Example 3.3.6. As an illustration of this correspondence, consider a 4-qubit channel Φ that models noise given by the possibility of independent bit flips on the first three qubits, and so Φ has four Kraus operators (normalized with probabilities) I, $X_1 = X \otimes I \otimes I \otimes I$, and X_2, X_3 similarly defined with X the Pauli bit flip operator ($X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$). Consider the orthogonal single-qubit subspaces $\mathcal{C}_0 = \text{span}\{|0000\rangle, |1111\rangle\}$, $\mathcal{C}_1 = \text{span}\{|0001\rangle, |1110\rangle\}$. Each of these subspaces is easily seen to be individually correctable for Φ, but more than this, one can check that the hybrid algebra code defined by the subspaces, namely $\mathcal{A} = \mathcal{L}(\mathcal{C}_0) \oplus \mathcal{L}(\mathcal{C}_1)$, is correctable for Φ. The theorem tells us therefore that the code algebra coincides with a generalized multiplicative domain for Φ, $\mathcal{A} = \mathcal{M}_{\pi}(\Phi)$, and indeed, the proof also gives a recipe for constructing the representation: in this case, the representation $\pi : \mathcal{A} \to \mathcal{L}(\mathcal{H})$ is implemented by the four Kraus operators $\{P_{\mathcal{C}}, P_{\mathcal{C}_i}X_i, i = 1, 2, 3\}$, where $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$ and $P_{\mathcal{C}_i} = X_i P_{\mathcal{C}} X_i^{*}$.

Combining the previous result with Theorem 3.3.2, the complementary operator structure relationship is revealed as follows.

Corollary 3.3.7. *Let Φ be a channel on $\mathcal{L}(\mathcal{H})$, and let π be a representation associated with a correctable algebra for Φ (or equivalently a private algebra for Φ^C). Then we have*

$$\mathcal{M}_\pi(\Phi) = \Big(\big(\ker(\Phi^C)\big)^\perp\Big)'.$$

Proof. The forward inclusion follows from Theorem 3.3.2, and the opposite inclusion follows from the second half of the proof of Theorem 3.3.4. □

Remark 3.3.8. The simplest illustration of this relationship comes from the extreme case of a correctable/private pair, the case with $\Phi = \mathrm{id}$ the identity channel on $\mathcal{L}(\mathcal{H})$. Here $\Phi^C(\rho) = \mathrm{Tr}(\rho)$ is the completely depolarizing channel, $\pi = \mathrm{id}$, $Q = I$, and $\mathcal{M}_\pi(\Phi) = \mathcal{L}(\mathcal{H})$. Moreover, $\ker \Phi^C$ is the operator subspace of trace-zero matrices, which is the trace-orthogonal complement of the identity operator I, and hence $(\ker \Phi^C)^\perp$ is the set of scalar multiples of the identity, with commutant equal to $\mathcal{L}(\mathcal{H})$ as given by the result. For the example above, the specific form of the complement is not as straightforward, nevertheless the result yields information on it; namely, in that case $\ker \Phi^C$ can be explicitly computed via the relation $\mathcal{L}(\mathcal{C}_0) \oplus \mathcal{L}(\mathcal{C}_1) = ((\ker \Phi^C)^\perp)'$.

We further note it would be interesting to extend this result to the general projection Q case. This should be possible but there are some technical issues to overcome on how to define the multiplicative domains in that case.

3.3.1 The Special Case of Unital Channels

We finish this section by continuing the analysis in the distinguished special case of unital channels ($\Phi(I) = I$). Many physically relevant channels satisfy this extra condition, such as the previous example. The relevant structures, in particular the multiplicative domains,

have an especially nice characterization.

If $\Phi : \mathcal{A} \to \mathcal{B}$ is a completely positive and unital map between two algebras, then Choi [45] proved that $\mathcal{M}(\Phi)$ has the following internal description:

$$\mathcal{M}(\Phi) = \{A \in \mathcal{A} \,:\, \Phi(A)^*\Phi(A) = \Phi(A^*A),\ \Phi(A)\Phi(A)^* = \Phi(AA^*)\}.$$

When trace preservation is added, so $\Phi(\rho) = \sum_i V_i \rho V_i^*$ is a unital channel, the fixed point theory for such maps [53] can be built upon to prove [54, 46, 48] that $\mathcal{M}(\Phi)$ is equal to the commutant of the operators $V_i^* V_j$, it encodes all unitarily correctable algebras for Φ, written as $\mathrm{UCC}(\Phi)$, and the unital channel $\Phi^\dagger$ acts as a recovery operation; in terms of operator structures this is stated as:

$$\mathcal{M}(\Phi) = \mathrm{UCC}\,(\Phi) = \{V_i^* V_j\}' = \mathrm{Fix}\,(\Phi^\dagger \circ \Phi).$$

We can thus state the following result based on the above.

Corollary 3.3.9. *If $\Phi(\rho) = \sum_i V_i \rho V_i^*$ is a unital channel, then*

$$\mathcal{M}(\Phi) = \{V_i^* V_j\}' = (\ker(\Phi^C)^\perp)'.$$

It is clear that the null space of a channel and its multiplicative domain cannot both be large. This relationship can thus be quantified by the following result in the unital case.

Corollary 3.3.10. *Let Φ be a unital quantum channel on $\mathcal{L}(\mathcal{H})$. Then*

$$\dim(\mathcal{M}(\Phi)) + \dim(\ker(\Phi)) \leq (\dim \mathcal{H})^2$$

with equality if and only if $\Phi^\dagger \circ \Phi$ *is a projection.*

Proof. From the discussion above we know $X \in \mathcal{M}(\Phi)$ if and only if X is an eigenvector of $\Phi^\dagger \circ \Phi$ corresponding to the eigenvalue one. Similarly $X \in \ker(\Phi)$ if and only if X is an eigenvector of $\Phi^\dagger \circ \Phi$ corresponding to the eigenvalue zero. The inequality follows from this. The inequality becomes an equality if and only if all of the eigenvalues of the positive semidefinite operator $\Phi^\dagger \circ \Phi$ are zero and one, which occurs if and only if Φ is a projection. □

We note that since $\mathcal{M}(\Phi)$ is a unital von Neumann subalgebra of some M_n, the projection onto $\mathcal{M}(\Phi)$ would be the trace-preserving conditional expectation onto $\mathcal{M}(\Phi)$, which is the unique channel $\Phi_{\mathcal{A}}$ satisfying:

1. $\Phi_{\mathcal{A}}(A) = A \quad \forall A \in \mathcal{A}$
2. $\Phi_{\mathcal{A}}(A_1 X A_2) = A_1 \Phi_{\mathcal{A}}(X) A_2 \quad \forall A_1, A_2 \in \mathcal{A}, \quad \forall X \in M_n$

Among all unital quantum channels with a particular multiplicative domain $\mathcal{A}$, the trace-preserving conditional expectation onto $\mathcal{A}$ has the largest possible nullspace.

We conclude this section by deriving some relations on the behaviour of the complementary channel and a channel's multiplicative domain in the unital case.

Proposition 3.3.11. *Let* Φ *be a unital channel on* $\mathcal{L}(\mathcal{H})$*. Then for all* $X \in \mathcal{L}(\mathcal{H})$ *and* $A \in \mathcal{M}(\Phi)$*, we have*

$$\Phi^C(AX) = \Phi^C(XA).$$

Proof. We have $A \in \mathcal{M}(\Phi)$ if and only if $AV_i^* V_j = V_i^* V_j A$ for all i, j. So $\mathrm{Tr}(AXV_i^* V_j) = \mathrm{Tr}(XV_i^* V_j A) = \mathrm{Tr}(XAV_i^* V_j)$, and hence

$$\Phi^C(AX) = \sum_{ij} \mathrm{Tr}(AXV_i^* V_j)|i\rangle\langle j| = \sum_{ij} \mathrm{Tr}(XAV_i^* V_j)|i\rangle\langle j| = \Phi^C(XA).$$

□

This result has some interesting consequences.

Corollary 3.3.12. *Let Φ be a unital channel on $\mathcal{L}(\mathcal{H})$. If $\mathcal{M}(\Phi)$ is a von Neumann algebra factor then $\Phi^C(\mathcal{M}(\Phi)) = \mathbb{C}I$.*

Proof. Suppose $A \in \mathcal{M}(\Phi)$ with $tr(A) = 0$. Since $\mathcal{M}(\Phi)$ is a von Neumann algebra factor and hence isomorphic to a matrix algebra, there exists $X, Y \in \mathcal{M}(\Phi)$ such that $A = XY - YX$ and thus $\Phi^C(A) = \Phi^C(XY) - \Phi^C(YX) = 0$. Since every element of $\mathcal{M}(\Phi)$ is the sum of a trace zero element of $\mathcal{M}(\Phi)$ and a multiple of the identity, the result follows. □

Corollary 3.3.13. *Let Φ be a unital channel. Then the set $\Phi^C(\mathcal{M}(\Phi))$ commutes with the set $\Phi^C(\mathcal{M}(\Phi^C))$.*

Proof. Let $A \in \mathcal{M}(\Phi)$ and $X \in \mathcal{M}(\Phi^C)$. Then from the previous result and the multiplicative domain definition, we have $\Phi^C(A)\Phi^C(X) = \Phi^C(AX) = \Phi^C(XA) = \Phi^C(X)\Phi^C(A)$. □

Remark 3.3.14. Regarding the generalized multiplicative domains, in the case that Φ is a unital channel, we have $\mathcal{M}(\Phi) = \{V_i^* V_j\}'$. Hence in this case, all generalized multiplicative domains associated with unital subalgebras lie inside the actual multiplicative domain. Also note that if $\Phi(\rho) = \sum_i V_i \rho V_i^*$ is a channel such that the $V_i = (\dim \mathcal{H})^{-1/2} U_i$, with $\{U_i\}$ a set of unitaries that are mutually orthogonal in the trace inner product, then of course Φ is unital. But also observe that Φ^C is unital as well:

$$\Phi^C(I) = \sum_{ij} \mathrm{Tr}(V_i^* V_j)|i\rangle\langle j| = \sum_i \mathrm{Tr}(V_i^* V_i)|i\rangle\langle i| = \sum_i |i\rangle\langle i| = I.$$

In particular, in the above results the roles of Φ and Φ^C can be interchanged.

An interesting example of this arises when Φ is the conditional expectation onto the diagonal matrices. In this case, $\Phi^C = \Phi$ which means that $\Phi(\mathcal{M}(\Phi)) = \Phi^C(\mathcal{M}(\Phi)) = \Phi^C(\mathcal{M}(\Phi^C))$ must be contained in an abelian subalgebra by Corollary 3.3.13. An easy calculation show that this is indeed the case with $\Phi(\mathcal{M}(\Phi))$ being the algebra of diagonal matrices.

3.4 Operator Algebra Inequalities and the Correction vs Privacy Trade-Off

In this section we build on the analysis above to further quantify complementarity, through inequalities determined by the sizes of the relevant operator algebras corrected or privatized by channels. To simplify the presentation we shall use matrix notation for the algebras and we will focus on the original basic notion of privacy, where an algebra is mapped to a single state: Given a channel $\Phi : M_n \to M_m$ and subalgebra $\mathcal{A}$, we suppose there is a density operator ρ such that

$$\Phi(A) = \mathrm{Tr}(A)\rho \qquad \forall A \in \mathcal{A}.$$

In such a situation, we shall say $\mathcal{A}$ is *privatized to a state* by Φ.

Up to unitary equivalence our algebras, say contained in M_n, have the form

$$\mathcal{A} = \left(\oplus_{k=1}^{N} I_{m_k} \otimes M_{n_k}\right) \oplus 0_K,$$

with $\sum_k m_k n_k + K = n$. The commutant of $\mathcal{A}$ is, up to the same unitary similarity,

$$\mathcal{A}' = \left(\oplus_{k=1}^{N} M_{m_k} \otimes I_{n_k}\right) \oplus M_K.$$

Note that

$$\mathcal{A} \cap \mathcal{A}' = \left(\oplus_{k=1}^{N} \mathbb{C} I_{m_k} \otimes I_{n_k}\right) \oplus 0_K$$

and that the dimension of this algebra (as an operator space) is

$$\dim(\mathcal{A} \cap \mathcal{A}') = N.$$

Finally, we note that $\mathcal{A}$ has a largest central projection $P_{\mathcal{A}}$; up to the same unitary similarity as before,

$$P_{\mathcal{A}} = \left(\oplus_{k=1}^{N} I_{m_k} \otimes I_{n_k}\right) \oplus 0_K.$$

This projection satisfies: $P_{\mathcal{A}} A = A P_{\mathcal{A}} = A$ for all $A \in \mathcal{A}$. Note that $\mathcal{A}$ is a unital algebra if and only if $P_{\mathcal{A}} = I_n$ if and only if $K = 0$. We shall also focus on the unital algebra case in this section.

The next two results refer to the notion of quasiorthogonal algebras. We point the reader to [37] for more on the notion and its connections with privacy.

Definition 3.4.1. *Two unital subalgebras $\mathcal{A}, \mathcal{B} \subseteq M_n$ are said to be* **quasiorthogonal** *if $\operatorname{Tr}(AB) = n^{-1} \operatorname{Tr}(A) \operatorname{Tr}(B)$ for all $A \in \mathcal{A}$ and all $B \in \mathcal{B}$.*

Lemma 3.4.2. *An algebra $\mathcal{B}$ is privatized to a state by Φ if and only if*

$$\operatorname{Tr}(B \Phi^{\dagger}(X)) = \operatorname{Tr}(B) \operatorname{Tr}(\rho X)$$

for all $X \in M_n$ and for all $B \in \mathcal{B}$. If $\mathcal{B}$ is unital, this is equivalent to the quasiorthogonality of $\mathcal{B}$ and $\operatorname{range}(\Phi^{\dagger})$.

Proof. The first statement is trivial. For the second, if $I \in \mathcal{B}$, then $\Phi(I) = n\rho$ and so $\rho = n^{-1}\Phi(I)$. Hence we have $\operatorname{Tr}(B\Phi^{\dagger}(X)) = n^{-1} \operatorname{Tr}(B) \operatorname{Tr}(\Phi(I)X) = n^{-1} \operatorname{Tr}(B) \operatorname{Tr}(\Phi^{\dagger}(X))$. □

Recall in the previous section we saw that a correctable algebra for Φ must lie in the range of $\Phi^\dagger$. The example of $\Phi_{\mathcal{A}}$, the trace-preserving conditional expectation onto a unital algebra $\mathcal{A}$ is instructive. Since $\Phi_{\mathcal{A}} = \Phi_{\mathcal{A}}^\dagger$, the range of $\Phi_{\mathcal{A}}^\dagger$ is $\mathcal{A}$ which clearly is a correctable algebra for $\Phi_{\mathcal{A}}$ as a subalgebra of its fixed point set. It was noted by Petz that two subalgebras $\mathcal{A}$ and $\mathcal{B}$ are quasiorthogonal if and only if $\Phi_{\mathcal{A}}(B)$ is a multiple of the identity for all $B \in \mathcal{B}$ [55, Theorem 3]. Hence a unital algebra $\mathcal{B}$ will be privatized by $\Phi_{\mathcal{A}}$ if and only if it is quasiorthogonal to $\mathcal{A}$. This observation coupled with Lemma 3.4.2 gives us the following characterization of correctable/privatized algebra pairs.

Theorem 3.4.3. *Let $\mathcal{A}$ and $\mathcal{B}$ be unital subalgebras of M_n. Then there exists a quantum channel that corrects $\mathcal{A}$ and privatizes $\mathcal{B}$ to a state if and only if $\mathcal{A}$ and $\mathcal{B}$ are quasiorthogonal.*

We can thus prove the following.

Corollary 3.4.4. *Suppose $\mathcal{A}$ is a correctable algebra for a channel $\Phi : M_n \to M_m$, and $\mathcal{B}$ is a unital algebra privatized to a state by Φ. Then*

$$\dim(\mathcal{A})\dim(\mathcal{B}) \leq n^2.$$

Proof. Since $\mathcal{A}$ and $\mathcal{B}$ are quasiorthogonal by Theorem 3.4.3, for all $A \in \mathcal{A}$ and $B \in \mathcal{B}$, we have $\operatorname{Tr}(AB) = n^{-1} \operatorname{Tr}(A) \operatorname{Tr}(B)$. Let $\{A_i\}_{i=1}^{d_1}$ and $\{B_i\}_{i=1}^{d_2}$ be orthonormal bases (in the trace inner product) for $\mathcal{A}, \mathcal{B}$ respectively. Next form the set $\{A_i B_j\}_{i,j=1}^{d_1,d_2}$ which has $d_1 d_2 = \dim(\mathcal{A}) \dim(\mathcal{B})$ elements and observe that

$$\begin{aligned}
\operatorname{Tr}(A_i B_j (A_k B_l)^*) &= \operatorname{Tr}(A_k^* A_i B_j B_l^*) \\
&= n^{-1} \operatorname{Tr}(A_k^* A_i) \operatorname{Tr}(B_j B_l^*) \\
&= n^{-1} \delta_{ik} \delta_{jl}
\end{aligned}$$

and so $\{A_i B_j\}_{i,j=1}^{d_1,d_2}$ is a set of mutually orthogonal matrices in M_n, and so must have dimension at most n^2. $\square$

Example 3.4.5. As a simple example of a channel and algebras that saturate this inequality, consider an N-qubit system (so $n = 2^N$) and noise given by a channel Φ that completely depolarizes the first k qubits and leaves the final $N - k$ qubits untouched. In this case, we have a correctable (noiseless in fact) algebra $\mathcal{A}$ that is unitarily equivalent to $M_{2^{N-k}}$ and a private algebra $\mathcal{B}$ that is privatized to the maximally mixed state of the first k qubits and is unitarily equivalent to M_{2^k}. Here we thus have: $\dim(\mathcal{A})\dim(\mathcal{B}) = 2^{2(N-k)}2^{2k} = 2^{2N} = n^2$.

Remark 3.4.6. Theorem 3.4.3 suggests a way to quantify the complementarity relations of two subalgebras. Indeed, in [56], a quantity ($c(\mathcal{A}, \mathcal{B})$) was defined for two unital subalgebras of a matrix algebra in terms of the trace of the composition of conditional expectations onto each of the subalgebras. It follows that $1 \leq c(\mathcal{A}, \mathcal{B}) \leq \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\}$. Moreover, $\mathcal{A}$ and $\mathcal{B}$ are quasiorthogonal if and only if $c(\mathcal{A}, \mathcal{B}) = 1$. Now using this quantity one can measure how far away two subalgebras are from being quasiorthogonal. Via Theorem 3.4.3, this allows us to see quantitatively how far away a pair of subalgebras are from being complementary to each other, and we suggest this warrants further investigation.

The following example illustrates the need for the unitality condition in Corollary 3.4.4.

Example 3.4.7. Let $\Phi : M_3 \to M_3$ be the channel whose Kraus operators are

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

which acts by

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \mapsto \begin{pmatrix} a & b & 0 \\ d & e+i & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Observe that the algebra $\mathcal{A} = M_2 \oplus 0$ is correctable for Φ, since on this algebra, Φ acts as the identity. Moreover, $\mathcal{B} = 0 \oplus M_2$ is private for this algebra, since

$$\Phi : \begin{pmatrix} 0 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \mapsto (a+d) \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Both $\mathcal{A}$ and $\mathcal{B}$ are of dimension 4, and so we have $\dim(\mathcal{A})\dim(\mathcal{B}) = 16 \nleq 9$.

We next relate the commutants of correctable/private algebra pairs.

Corollary 3.4.8. *If $\mathcal{A}$ and $\mathcal{B}$ are unital algebras correctable and privatized to a state by $\Phi : M_n \to M_m$ respectively, then*

$$\dim(\mathcal{B}) \leq \dim(\mathcal{A}') \quad \textit{and} \quad \dim(\mathcal{A}) \leq \dim(\mathcal{B}').$$

Proof. The result follows from the theorem above and the fact that unital algebras satisfy $n^2 \leq \dim(\mathcal{A}) \dim(\mathcal{A}')$. □

Note that Example 3.4.7 again serves as a reminder that unitality is necessary: in that example, $\dim(\mathcal{A}') = \dim(\mathcal{B}') = 3$ while $\dim(\mathcal{A}) = \dim(\mathcal{B}) = 4$.

We can also make a statement on the internal structures of correctable and private algebra pairs.

Corollary 3.4.9. *Suppose $\mathcal{A}$ and $\mathcal{B}$ are unital algebras correctable and privatized to a state by Φ respectively. The following are true:*

1. *If $\mathcal{A}$ contains a maximal abelian subalgebra, then $\mathcal{B}$ cannot, unless $\mathcal{A}$ is itself a maximal abelian subalgebra, in which case so is $\mathcal{B}$.*

2. *If $\mathcal{B}$ contains a maximal abelian subalgebra, then $\mathcal{A}$ cannot, unless $\mathcal{B}$ is itself a maximal abelian subalgebra, in which case so is $\mathcal{A}$.*

Proof. This follows from the observation that the commutant of an algebra containing a maximal abelian subalgebra is abelian, and has dimension less than n, while the dimension of $\mathcal{A}$ itself is greater than n. The inequality in Corollary 3.4.8, and a consideration of the equality condition, give the result. □

Further recall from above that all unital correctable algebras $\mathcal{A}$ satisfy $\mathcal{A} \subseteq \{V_i^* V_j\}'$, and hence $\{V_i^* V_j\}'' \subseteq \mathcal{A}'$. Hence, the smallest possible commutant we can put on the right side of the inequality from Corollary 3.4.8 is $\dim(\{V_i^* V_j\}'')$, giving us the following result. (And recall by the von Neumann double commutant theorem, $\{V_i^* V_j\}''$ is equal to the algebra generated by the operators $V_i^* V_j$.)

Corollary 3.4.10. *If $\mathcal{B}$ is a unital algebra privatized to a state by Φ, then*

$$\dim(\mathcal{B}) \leq \dim(\{V_i^* V_j\}'').$$

Remark 3.4.11. We see then that, at least for unital algebras and privatizing to states, these inequalities exhibit an explicit and concrete trade-off between privacy and correction: if a large algebra is correctable for Φ, the size of the largest privatized algebra is constrained to be small, and vice-versa.

Recalling the Kraus operator description of Φ^C, we finish by analyzing what happens for the complement when $\mathcal{A}$ is correctable for Φ.

Proposition 3.4.12. *If $\mathcal{A}$ is correctable for Φ, then*

$$\operatorname{rank}(\Phi^C\big|_{\mathcal{A}}) \leq \dim(\mathcal{A} \cap \mathcal{A}').$$

Proof. We have that $\Phi^C(A)_{ij} = \operatorname{Tr}(V_j^* V_i A)$; using the fact that $A = QAQ$ where Q is the largest central projection in $\mathcal{A}$, the above becomes

$$\operatorname{Tr}(V_j^* V_i Q A Q) = \operatorname{Tr}(Q V_j^* V_i Q A);$$

recalling the previous section, $QV_j^*V_iQ \in \mathcal{A}'$. If $\mathcal{A}$ is unitarily equivalent to $\left(\oplus_{k=1}^N I_{m_k} \otimes M_{n_k}\right) \oplus 0_K$ then $\mathcal{A}'$ is unitarily equivalent to $\left(\oplus_{k=1}^N M_{m_k} \otimes I_{n_k}\right) \oplus M_K$, and so for any A we have that A is unitarily equivalent to $\left(\oplus_{k=1}^N I_{m_k} \otimes A_k\right) \oplus 0_K$ and $QV_j^*V_iQ$ is unitarily equivalent to $\left(\oplus_{k=1}^N V_{ji}^{(k)} \otimes I_{n_k}\right) \oplus 0_K$; and so

$$\operatorname{Tr}(QV_j^*V_iQA) = \operatorname{Tr}\left(\left(\oplus_{k=1}^N V_{ji}^{(k)} \otimes A_k\right) \oplus 0_K\right) = \sum_{k=1}^N \operatorname{Tr}(A_k)\operatorname{Tr}(V_{ij}^{(k)}).$$

Hence

$$\Phi^C(A) = \sum_{i,j} E_{ji}\left(\sum_{k=1}^N \operatorname{Tr}(A_k)\operatorname{Tr}(V_{ij}^{(k)})\right) = \sum_{k=1}^N \operatorname{Tr}(A_k)\Lambda_k,$$

where $\Lambda_k = \sum_{i,j} \operatorname{Tr}(V_{ij}^{(k)})E_{ji}$. Clearly, $N = \dim(\mathcal{A} \cap \mathcal{A}')$ and is obviously an upper bound on the dimension of the range of $\Phi^C(\mathcal{A})$. □

Remark 3.4.13. Considering the general notion of privacy from [26], note that the only information preserved from a private algebra is the information stored in $\mathcal{A} \cap \mathcal{A}'$; as this is

an abelian and hence unitarily diagonalizable algebra, all the information can be considered as simply classical probabilities by reading off the diagonal, and so no genuine quantum information survives. By the analysis in Proposition 3.4.12, we see that if $\mathcal{A}$ is correctable for Φ, all of $\mathcal{A} \setminus (\mathcal{A} \cap \mathcal{A}')$ is sent to 0, and the image of $\mathcal{A}$ under Φ^C depends only on a compression of $\mathcal{A}$ to $\mathcal{A} \cap \mathcal{A}'$. Hence, by the reasoning in the paper [26], this counts as privatization: only classical information from the diagonal can survive.

3.5 Chapter Outlook

In this chapter, we have presented quantum complementarity in a new light: by appropriate operator structures, the complementary relationship between correctable algebras and private algebras was demonstrated. This in turn offers an extension of subject of complementarity to the context of hybrid quantum information. It is precisely these algebras and codes that describe the structure of hybrid quantum codes. As we will see in Chapter 5, implementations of hybrid codes that have been demonstrated in previous literature are particular cases of these algebra structures.

What followed considered dimensions of private and correctable algebras, and gave dimension inequalities that examine the trade-off between correction and privacy in the particular case of algebras privatized to quantum states. This analysis could be taken further; these inequalities could be considered for privatization to more general algebras. The finite-dimensional case is more pertinent to quantum information, however correctable and private algebras have beep identified for general infinite-dimensional (von Neumann) algebras, and extending the presented results to that setting could be an interesting direction for future work.

Chapter 4

Approximately Private Hybrid Quantum Channels and Approximate Quasiorthogonality of Algebras

4.1 Introduction

In the previous chapter, we presented a framework that captured the complementarity of quantum error correction and quantum privacy for the setting of hybrid codes. Because both subjects are connected by the bridge that is complementarity, advancements in the theory of quantum privacy can provide advancements for error-correction, and vice versa. This chapter ventures over to the quantum privacy side of that bridge.

Relevant to this study and its motivation, are mutually unbiased bases. Expressed in quantum information terms, two bases sets of a Hilbert space are mutually unbiased if a state prepared in any one element of one of the bases gives equal probabilities of all outcomes if

a measurement is made in the other bases. This property has applications in a number of quantum information protocols, including quantum key distribution and the detection quantum entanglement. We see then that constructions of mutually unbiased bases are very useful, but there is an unresolved problem surrounding the existence of such: it is not known in general the maximum number of such bases if the dimension of the Hilbert space is not an integer power of a prime number. The basic case is in two dimensions, where there are no more than three mutually unbiased bases. Note for instance, that the eigenvectors of the Pauli X, Y, and Z operators are three sets of mutually unbiased bases. There are however constructions that can saturate quantum systems of arbitrary sizes if conditions are relaxed so we only require that bases sets are approximately unbiased, in some appropriate sense. We study approximate orthogonality between operator algebras that were originally motivated by mutually unbiased bases, and lay a theoretical framework for its connection to approximate quantum privacy (which we introduce). This chapter lays some groundwork for understanding deep connections between quantum error-correction, quantum privacy, quasiorthogonal algebras and approximately mutually unbiased bases, and their various applications in quantum information.

The notion of quasiorthogonality for operator algebras arose from the study of modified forms of orthogonality for algebras and their relative behaviours in a variety of settings in finite-dimensional quantum information. Primarily motivated by mutually unbiased bases (MUB) constructions [57, 58, 59, 60, 61] and their associated commutative algebras initially, over the past decade the work expanded to the non-commutative setting [62, 55, 63, 64, 65, 66]. The study of approximate quasiorthogonality was initiated by introducing a measure of orthogonality between two algebras based on joint properties of their conditional expectation channels, and investigating results on the approximate version for some special cases [56].

From a different direction, still with quantum information motivation, it has recently been recognized that there are connections between the study of quasiorthogonal operator algebras and work in quantum privacy; specifically, on the topic of what are variously known as private quantum channels or codes, decoherence-full or private subspaces and subsystems, and private algebras [29, 30, 32, 31, 25, 33, 34, 35, 26]. In particular, for a number of special cases of channels or algebras, quasiorthogonality has been linked with certain quantum privacy properties in those cases [37, 36, 11], all suggesting a deeper more general link between the topics.

In this chapter, we establish the first general result that ties together approximate quasiorthogonality of operator algebras with approximate privacy for quantum codes presented as algebras. This involves identification of an appropriate notion of relative quantum privacy, with natural assumptions on the algebras and private quantum codes considered. Of potential peripheral interest, this gives a new approach for computing the measure of orthogonality in terms of Choi matrices and Kraus operators for the conditional expectation channels of the associated algebras. We also present examples drawn from the framework for hybrid classical and quantum information theory, from studies of private quantum subsystems, and from work on approximate MUB constructions.

This chapter is organized as follows. The next section includes preliminary material and the derivation of our approach to compute the orthogonality measure. In the third section we define relative approximate privacy of two algebras and present our main result and its proof. The fourth section contains examples and we conclude with a brief outlook discussion.

The contents of this chapter are adapted from research findings co-authored and published with various collaborators [12]. All authors made contributions to the preparation and review of the original manuscript.

4.2 A Measure of Quasiorthogonality of Algebras

Let $M_n(\mathbb{C})$ be the set of $n \times n$ complex matrices. In all of what follows, $\mathcal{A}, \mathcal{B} \subseteq M_n(\mathbb{C})$ are unital $*$-algebras (or finite-dimensional C*-algebras [49]); that is, $I_n \in \mathcal{A}$, if $A \in \mathcal{A}$ so is A^*, and $\mathcal{A}$ is closed under linear combinations and matrix multiplication, and the same is true for $\mathcal{B}$. We refer to the algebra of scalar multiples of the identity $\mathbb{C}I_n$ as the trivial algebra.

Given such $\mathcal{A}$, $\mathcal{B}$ we denote by $\mathcal{E}_\mathcal{A}$, $\mathcal{E}_\mathcal{B}$ the (unique) trace-preserving, unital conditional expectations onto $\mathcal{A}$ and $\mathcal{B}$ respectively. That is, $\mathcal{E}_\mathcal{A} : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ (and similarly for $\mathcal{E}_\mathcal{B}$) is the linear map uniquely characterized by the following conditions:

1. $\mathcal{E}_\mathcal{A}(A) = A$ for all $A \in \mathcal{A}$
2. $\mathcal{E}_\mathcal{A}(X) \succeq 0$ whenever $X \succeq 0$
3. $\mathcal{E}_\mathcal{A}(A_1 X A_2) = A_1 \mathcal{E}_\mathcal{A}(X) A_2$ for all $A_1, A_2 \in \mathcal{A}$ and $X \in M_n(\mathbb{C})$
4. $\mathrm{Tr}(\mathcal{E}_\mathcal{A}(X)) = \mathrm{Tr}(X)$ for all $X \in M_n(\mathbb{C})$.

We refer to $\mathcal{E}_\mathcal{A}$ as the *conditional expectation channel* for $\mathcal{A}$, reflecting standardized use of the term quantum channel to describe completely positive trace-preserving maps.

We now define the key notion of quasiorthogonal algebras, noting the early literature on the subject sometimes referred to the notion as 'orthogonal' or 'complementary'. (We use the 'quasi' prefix as in [56] as it avoids possible confusion with other quantum information notions that use these terms.)

Definition 4.2.1. Two unital $*$-algebras $\mathcal{A}$, $\mathcal{B}$ are *quasiorthogonal* if they satisfy any one of the following equivalent conditions:

1. $\mathrm{Tr}\big((A - \frac{\mathrm{Tr}(A)}{n} I_n)(B - \frac{\mathrm{Tr}(B)}{n} I_n)\big) = 0$ for all $A \in \mathcal{A}$, $B \in \mathcal{B}$

2. $\mathrm{Tr}(AB) = \frac{\mathrm{Tr}(A)\mathrm{Tr}(B)}{n}$ for all $A \in \mathcal{A}$, $B \in \mathcal{B}$

3. $\mathcal{E}_{\mathcal{A}}(B) = \frac{\mathrm{Tr}(B)}{n} I_n$ for all $B \in \mathcal{B}$ and $\mathcal{E}_{\mathcal{B}}(A) = \frac{\mathrm{Tr}(A)}{n} I_n$ for all $A \in \mathcal{A}$

The ideal notion of quantum privacy (the case $\epsilon = 0$ in the definition of the next section) we consider is given as follows.

Definition 4.2.2. Given a unital quantum channel $\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$, we say a unital $*$-algebra $\mathcal{A}$ is *private for* Φ whenever

$$\Phi(A) = \frac{\mathrm{Tr}(A)}{n} I_n,$$

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

Remark 4.2.3. Notice that the third condition from Definition 4.2.1 asserts that if $\mathcal{A}$ and $\mathcal{B}$ are quasiorthogonal then the conditional expectation onto the one algebra privatizes the other. The simplest example of this phenomena can be seen in the extreme case with $\mathcal{A} = M_n$ and $\Phi = \mathcal{D}_n$ is the 'complete depolarizing' channel, $\mathcal{D}_n(X) = n^{-1}\mathrm{Tr}(X) I_n$, which is the conditional expectation channel onto the trivial algebra $\mathcal{B} = \mathbb{C} I_n$. Observe also in this case that $\mathcal{A}$ and $\mathcal{B}$ are quasiorthogonal, which is a simple special case of our main result below.

More general notions of private algebras have been considered in the literature, often with different nomenclature as well, such as private quantum channels, decoherence-full or private subspaces and subsystems, and private algebras [29, 30, 32, 31, 25, 33, 35, 34, 26, 37, 36]. The distinguished special case we consider here captures many of the most naturally occurring examples from these settings, in addition to, as we shall see, allowing us to establish a tight connection with quasiorthogonality in the approximate case.

In [56], Weiner introduced the following quantitative measure of orthogonality for algebras. We will focus on this notion for the rest of the section.

Definition 4.2.4. For $\mathcal{A}, \mathcal{B} \subseteq M_n(\mathbb{C})$ unital $*$-algebras, the *measure of orthogonality* between them is given by

$$Q(\mathcal{A}, \mathcal{B}) := \mathrm{Tr}(T_{\mathcal{A}} T_{\mathcal{B}}) \tag{4.1}$$

where $T_{\mathcal{A}}$ is the (any) matrix representation of $\mathcal{E}_{\mathcal{A}}$ acting on the vector space $M_n(\mathbb{C})$.

We shall make use of the explicit forms of our matrix representations so let us introduce notation $\{|i\rangle : 1 \leq i \leq n\}$ for a fixed orthonormal basis for $\mathbb{C}^n$, and then $E_{ij} = |i\rangle\langle j|$ for the corresponding set of matrix units of M_n, which themselves form an orthonormal basis in the trace inner product; $\langle A, B\rangle = \mathrm{Tr}(B^* A)$, $A, B \in M_n$. We will then work with the 'natural representation' T_Φ [67] for a given linear map $\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$, which is the matrix representation for Φ on $M_{n^2}(\mathbb{C}) \cong M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ defined by the basis $\{E_{ij} \otimes E_{kl}\}$; that is,

$$T_\Phi = \sum_{i,j,k,l} \langle \Phi(E_{kl}), E_{ij}\rangle E_{ik} \otimes E_{jl}.$$

On the other hand, we can consider the Choi matrix [68] for Φ, given by

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

Using the expansion $\Phi(E_{ij}) = \sum_{k,l} \langle \Phi(E_{ij}), E_{kl}\rangle E_{kl}$, we see that C_Φ and T_Φ have the same matrix coefficients up to the (unitarily implemented) permutation that sends $E_{ij} \otimes E_{kl} \mapsto E_{ik} \otimes E_{jl}$.

Hence, if we denote by $C_{\mathcal{A}}$ the Choi matrix of $\mathcal{E}_{\mathcal{A}}$, and similarly for $C_{\mathcal{B}}$, then this discussion leads to the following observation.

Proposition 4.2.5. *Given $*$-algebras $\mathcal{A}$ and $\mathcal{B}$, we have*

$$Q(\mathcal{A}, \mathcal{B}) = \mathrm{Tr}(C_{\mathcal{A}} C_{\mathcal{B}}). \tag{4.2}$$

We shall make use of the following internal description of the Choi matrix for a conditional expectation. Recall that if A is a matrix, $\overline{A}$ is its complex conjugate matrix.

Lemma 4.2.6. *Let $\mathcal{A} \subseteq M_n(\mathbb{C})$ be a $*$-algebra and let $\{A_i\}_{i=1}^{d_1}$ be any orthonormal basis for $\mathcal{A}$ in the trace inner product. Then we have*

$$C_{\mathcal{A}} = \sum_{i=1}^{d_1} \overline{A_i} \otimes A_i. \tag{4.3}$$

Proof. We first extend $\{A_i\}_{i=1}^{d_1}$ to an orthonormal basis on the full matrix space by appending the elements of $\{A_j^{\perp}\}_{j=1}^{n^2-d_1}$. We claim that

$$\sum_{i=1}^{d_1} \overline{A_i} \otimes A_i + \sum_{j=1}^{n^2-d_1} \overline{A_j^{\perp}} \otimes A_j^{\perp} = \sum_{i,j=1}^{n} E_{ij} \otimes E_{ij}. \tag{4.4}$$

To see why this is so, observe that for all $X \in M_n(\mathbb{C})$,

$$(\mathrm{Tr} \otimes \mathrm{id})\Bigg((X^T \otimes I_n)(\sum_{i=1}^{d_1} \overline{A_i} \otimes A_i + \sum_{j=1}^{n^2-d_1} \overline{A_j^{\perp}} \otimes A_j^{\perp}) \Bigg)$$

$$
\begin{aligned}
&= \sum_{i=1}^{d_1} \mathrm{Tr}(X^T \overline{A_i}) A_i + \sum_{j=1}^{n^2-d_1} \mathrm{Tr}(X^T \overline{A_j^\perp}) A_j^\perp \\
&= \sum_{i=1}^{d_1} \mathrm{Tr}(X A_i^*) A_i + \sum_{j=1}^{n^2-d_1} \mathrm{Tr}(X A_j^{\perp *}) A_j^\perp \\
&= \sum_{i=1}^{d_1} < X, A_i > A_i + \sum_{j=1}^{n^2-d_1} < X, A_j^{\perp *} > A_j^\perp \\
&= X,
\end{aligned}
$$

since $\{A_i\} \cup \{A_j^\perp\}$ forms an orthonormal basis for $M_n(\mathbb{C})$. If we denote $B = \sum_{i=1}^{d_1} \overline{A_i} \otimes A_i + \sum_{j=1}^{n^2-d_1} \overline{A_j^\perp} \otimes A_j^\perp$, then we observe that the property encoded above is $(\mathrm{Tr} \otimes \mathrm{id})\big((X^T \otimes I_n)B\big) = X$, which uniquely characterizes B as the Choi matrix of the identity map [67], and so $B = \sum_{i,j=1}^n E_{ij} \otimes \mathrm{id}(E_{ij}) = \sum_{i,j=1}^n E_{ij} \otimes E_{ij}$, as claimed.

Now, we recall that $C_{\mathcal{A}} := (\mathrm{id} \otimes \mathcal{E}_{\mathcal{A}})\big(\sum_{i,j=1}^n E_{ij} \otimes E_{ij}\big)$ and so by Eq. (4.4) we can equivalently say that

$$
C_{\mathcal{A}} = (\mathrm{id} \otimes \mathcal{E}_{\mathcal{A}})\big(B\big) = \sum_{i=1}^{d_1} \overline{A_i} \otimes \mathcal{E}_{\mathcal{A}}(A_i) + \sum_{j=1}^{n^2-d_1} \overline{A_j^\perp} \otimes \mathcal{E}_{\mathcal{A}}(A_j^\perp).
$$

Since $\mathcal{E}_{\mathcal{A}}(A) = A$ for all $A \in \mathcal{A}$, and $\mathcal{E}_{\mathcal{A}}(A_j^\perp) = 0$ for each $A_j^\perp$, the result follows. □

This leads to the following 2-norm type characterization of $Q(\mathcal{A}, \mathcal{B})$.

Corollary 4.2.7. *Let $\mathcal{A}$, $\mathcal{B} \subseteq M_n(\mathbb{C})$ be unital $*$-algebras. Then the measure of orthogonality may equivalently be expressed as:*

$$
Q(\mathcal{A}, \mathcal{B}) = \sum_{i,j=1}^{d_1,d_2} |\mathrm{Tr}(A_i B_j)|^2, \tag{4.5}
$$

for any orthonormal bases $\{A_i\}_{i=1}^{d_1}$, $\{B_j\}_{j=1}^{d_2}$ for $\mathcal{A}$ and $\mathcal{B}$ respectively.

Proof. We apply the formulas of Eqs. (4.2) and (4.3) to obtain:

$$Q(\mathcal{A},\mathcal{B}) = \sum_{i,j=1}^{d_1,d_2} \mathrm{Tr}\big((\overline{A_i}\otimes A_i)(\overline{B_j}\otimes B_j)\big) = \sum_{i,j=1}^{d_1,d_2} |\mathrm{Tr}(A_iB_j)|^2,$$

as required. □

We have stated that $Q(\mathcal{A},\mathcal{B})$ is a measure of orthogonality. This is most explicitly seen through the following elementary observation of Weiner [56]. We give an alternate simple proof based on the descriptions derived here.

Proposition 4.2.8. *Let $\mathcal{A}$, $\mathcal{B} \subseteq M_n(\mathbb{C})$ be unital $*$-algebras. Then $\mathcal{A}$ and $\mathcal{B}$ are quasiorthogonal to one another if and only if $Q(\mathcal{A},\mathcal{B}) = 1$.*

Proof. Let $\{A_i\}_{i=1}^{d_1}$, $\{B_j\}_{j=1}^{d_2}$ be orthonormal bases for $\mathcal{A}$, $\mathcal{B}$ respectively, and suppose $A_1 = B_1 = \frac{1}{\sqrt{n}} I_n$ (which is possible since both algebras are unital), so that $\mathrm{Tr}(A_i) = \mathrm{Tr}(B_j) = 0$ for all $1 < i \leq d_1$, $1 < j \leq d_2$.

Then if $\mathcal{A}$ and $\mathcal{B}$ are quasiorthogonal, and using the fact that A_i, B_j are traceless for $i, j \neq 1$, we have

$$\begin{aligned} Q(\mathcal{A},\mathcal{B}) &= \sum_{i,j=1}^{d_1,d_2} |\mathrm{Tr}(A_iB_j)|^2 = \sum_{i,j=1}^{d_1,d_2} \frac{1}{n^2} |\mathrm{Tr}(A_i)|^2 |\mathrm{Tr}(B_j)|^2 \\ &= \frac{1}{n^2} \Big|\frac{\mathrm{Tr}(I_n)}{\sqrt{n}}\Big|^2 \Big|\frac{\mathrm{Tr}(I_n)}{\sqrt{n}}\Big|^2 = 1. \end{aligned}$$

Conversely, keeping our orthonormal bases for $\mathcal{A}$ and $\mathcal{B}$, suppose that

$$Q(\mathcal{A},\mathcal{B}) = \sum_{i,j=1}^{d_1,d_2} |\mathrm{Tr}(A_iB_j)|^2 = 1.$$

Then, since $A_1 = B_1 = \frac{1}{\sqrt{n}} I_n$, we have

$$1 + \sum_{(i,j)\neq(1,1)} |\mathrm{Tr}(A_i B_j)|^2 = 1,$$

and so $\mathrm{Tr}(A_i B_j) = 0$ except when $(i,j) = (1,1)$.

Thus, for any $A = \frac{\mathrm{Tr}(A)}{n} I_n + \sum_{i=2}^{d_1} a_i A_i$ in $\mathcal{A}$ and $B = \frac{\mathrm{Tr}(B)}{n} I_n + \sum_{j=1}^{d_2} b_j B_j$ in $\mathcal{B}$, we have

$$\begin{aligned} \mathrm{Tr}(AB) &= \frac{\mathrm{Tr}(A)\mathrm{Tr}(B)}{n^2}\mathrm{Tr}(I_n) + \sum_{(i,j)\neq(1,1)} a_i b_j \mathrm{Tr}(A_i B_j) \\ &= \frac{1}{n}\mathrm{Tr}(A)\mathrm{Tr}(B), \end{aligned}$$

which is one of the equivalent conditions for quasiorthogonality. □

Remark 4.2.9. Note that evidently for $\mathcal{A}$, $\mathcal{B}$ unital $*$-algebras, $Q(\mathcal{A},\mathcal{B}) \geq 1$ since both algebras contain $\frac{1}{\sqrt{n}} I_n$. So quasiorthogonality corresponds to the case where Q is minimized, and this naturally leads to the following definition.

Definition 4.2.10. Let $\mathcal{A}$, $\mathcal{B} \subseteq M_n(\mathbb{C})$ be unital $*$-algebras, and let $\epsilon > 0$. If

$$Q(\mathcal{A},\mathcal{B}) \leq 1 + \epsilon,$$

then we say $\mathcal{A}$ and $\mathcal{B}$ are *ϵ-quasiorthogonal*. If for some $\epsilon > 0$ the algebras $\mathcal{A}$ and $\mathcal{B}$ are ϵ-quasiorthogonal, then we say they are *approximately quasiorthogonal.*

4.3 Approximate Relative Quantum Privacy and Relation to Approximately Quasiorthogonal Algebras

We shall consider the following notion of approximate privacy below. First recall the 2-norm of an operator is $||A||_2 = (\mathrm{Tr}(A^*A))^{\frac{1}{2}}$, and so $\langle A, A\rangle = ||A||_2^2$. Also $||\Phi||_2 = \sup_{||X||_2=1} ||\Phi(X)||_2$ for linear maps Φ.

Definition 4.3.1. Let $\mathcal{A}$, $\mathcal{B} \subseteq M_n(\mathbb{C})$ be unital $*$-algebras, and let $\epsilon > 0$. Then we say $\mathcal{B}$ is *ϵ-private relative to $\mathcal{A}$* if

$$||(\mathcal{E}_{\mathcal{A}} - \mathcal{D}_n) \circ \mathcal{E}_{\mathcal{B}}||_2 \leq \epsilon, \tag{4.6}$$

where $\mathcal{D}_n : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ is the complete depolarizing channel. If for some $\epsilon > 0$ the algebra $\mathcal{B}$ is ϵ-private relative to $\mathcal{A}$, then we say $\mathcal{B}$ is *approximately private relative to $\mathcal{A}$.*

Remark 4.3.2. We are motivated to consider the 2-norm here as it is fairly standard in physically motivated quantum information settings, in addition to the description of Q as a particular 2-norm derived in Corollary 4.2.7. We also note that our ϵ-private language is in the spirit of terminology used in the context of approximate privacy previously (e.g. [25]).

We now state and prove our main result.

Theorem 4.3.3. *Let $\mathcal{A}$, $\mathcal{B} \subseteq M_n(\mathbb{C})$ be unital $*$-algebras with at least one of the algebras non-trivial. Then the following conditions are equivalent:*

(i) $\mathcal{A}$ and $\mathcal{B}$ are approximately quasiorthogonal.

(ii) $\mathcal{A}$ is approximately private relative to $\mathcal{B}$.

(*iii*) $\mathcal{B}$ *is approximately private relative to* $\mathcal{A}$.

Proof. Let $\epsilon > 0$, and given the vector space dimensions of $\mathcal{A}$ and $\mathcal{B}$, define $d_{\mathcal{AB}}^{\max} = \max(\dim \mathcal{A}, \dim \mathcal{B})$. As with the notation used above, we pick orthonormal bases $\{A_i\}_{i=1}^{d_1}$ and $\{B_j\}_{j=1}^{d_2}$ with $A_1 = B_1 = \frac{1}{\sqrt{n}} I_n$. (Note that of course $d_j \leq d_{\mathcal{AB}}^{\max}$, $j = 1, 2$.) We will also choose the basis so that $A_i = A_i^*$ for each i, and similarly for B_j.

We will first prove that $\mathcal{B}$ (respectively $\mathcal{A}$) is ϵ-private relative to $\mathcal{A}$ (respectively relative to $\mathcal{B}$) whenever

$$Q(\mathcal{A}, \mathcal{B}) \leq 1 + \epsilon',$$

where $\epsilon' = \epsilon^2 (d_{\mathcal{AB}}^{\max} - 1)^{-1}$; thus showing (*i*) implies both (*ii*) and (*iii*).

To this end, observe that if

$$Q(\mathcal{A}, \mathcal{B}) = 1 + \sum_{(i,j) \neq (1,1)} |\mathrm{Tr}(A_i B_j)|^2 \leq 1 + \epsilon',$$

then it follows that for each $j \neq 1$, we have

$$\sum_{i=2}^{d_1} |\mathrm{Tr}(A_i B_j)|^2 = \sum_{i=2}^{d_1} |\langle A_i, B_j \rangle|^2 \leq \epsilon'.$$

Next, we extend $\{A_i\}_{i=1}^{d_1}$ to an orthonormal basis for the full matrix space by appending elements $\{A_j^{\perp}\}_{j=1}^{n^2 - d_2}$ and express each B_j in terms of this basis:

$$B_j = \frac{\mathrm{Tr}(B_j)}{n} I_n + \sum_{i=2}^{d_1} b_{ji} A_i + \sum_{k=1}^{n^2 - d_1} c_{jk} A_k^{\perp}.$$

By orthonormality of our basis we have $|b_{ji}|^2 = |\mathrm{Tr}(A_i^* B_j)|^2 = |\mathrm{Tr}(A_i B_j)|^2$ for all i, j, and

hence for all $j \neq 1$,

$$\sum_{i=2}^{d_1} |b_{ji}|^2 \leq \epsilon'.$$

Now we apply $\mathcal{E}_{\mathcal{A}}$ to B_j, using its decomposition above and noting that $\langle B_j, I_n \rangle = \mathrm{Tr}(B_j) = 0$ and $\mathcal{E}_{\mathcal{A}}(A_k^{\perp}) = 0$, to obtain $\mathcal{E}_{\mathcal{A}}(B_j) = \sum_{i=2}^{d_1} b_{ji} A_i$. Hence by orthonormality of the A_i we have:

$$\|\mathcal{E}_{\mathcal{A}}(B_j) - \frac{\mathrm{Tr}(B_j)}{n} I_n\|_2^2 = \|\sum_{i=2}^{d_1} b_{ji} A_i\|_2^2 = \sum_{i=2}^{d_1} |b_{ji}|^2 \leq \epsilon'.$$

Finally, we pick an arbitrary $B \in \mathcal{B}$ and decompose it as $B = \frac{\mathrm{Tr}(B)}{n} I_n + \sum_{j=2}^{d_2} c_j B_j$. Observe that $\|B\|_2^2 \geq \sum_j |c_j|^2$. Then applying $\mathcal{E}_{\mathcal{A}}$ we get

$$\mathcal{E}_{\mathcal{A}}(B) - \frac{\mathrm{Tr}(B)}{n} I_n = \sum_{j=2}^{d_2} c_j \mathcal{E}_{\mathcal{A}}(B_j).$$

Thus we have

$$\begin{aligned}
\big(\|\mathcal{E}_{\mathcal{A}}(B) - \frac{\mathrm{Tr}(B)}{n} I_n\|_2\big)^2 &= \big(\|\sum_{j=2}^{d_2} c_j \mathcal{E}_{\mathcal{A}}(B_j)\|_2\big)^2 \\
&\leq \big(\sum_{j=2}^{d_2} |c_j| \|\mathcal{E}_{\mathcal{A}}(B_j)\|_2\big)^2 \\
&\leq \big(\sum_{j=2}^{d_2} |c_j|^2\big)\big(\sum_{j=2}^{d_2} ||\mathcal{E}_{\mathcal{A}}(B_j)||_2^2\big) \\
&\leq \|B\|_2^2 (d_2 - 1)\epsilon' \\
&\leq \epsilon^2 \|B\|_2^2.
\end{aligned}$$

As $B \in \mathcal{B}$ was arbitrary, it follows that $||(\mathcal{E}_{\mathcal{A}} - \mathcal{D}_n) \circ \mathcal{E}_{\mathcal{B}}||_2 \leq \epsilon$, and so $\mathcal{B}$ is ϵ-private relative to $\mathcal{A}$. An analogous proof works to show $\mathcal{A}$ is ϵ-private relative to $\mathcal{B}$.

We complete the proof by proving both (ii) and (iii) imply (i); specifically we will show

that $\mathcal{B}$ being ϵ-private relative to $\mathcal{A}$ and $\mathcal{A}$ being ϵ-private relative to $\mathcal{B}$ both imply that

$$Q(\mathcal{A}, \mathcal{B}) \leq 1 + \epsilon'',$$

where $\epsilon'' = (d_{\mathcal{AB}}^{\max} - 1)\epsilon^2$.

To this end, suppose that $\mathcal{B}$ is ϵ-private relative to $\mathcal{A}$, and so for all $B \in \mathcal{B}$,

$$\|\mathcal{E}_{\mathcal{A}}(B) - \frac{\mathrm{Tr}(B)}{n} I_n\|_2 \leq \epsilon \|B\|_2.$$

As each B_j is traceless and has 2-norm equal to 1, we have $\|\mathcal{E}_{\mathcal{A}}(B_j)\|_2 \leq \epsilon$. So if we write (again using $\langle B_j, I_n \rangle = 0$),

$$B_j = \sum_{i=2}^{d_1} \langle B_j, A_i \rangle A_i + \sum_k \langle B_j, A_i^{\perp} \rangle A_i^{\perp},$$

then we have $\mathcal{E}_{\mathcal{A}}(B_j) = \sum_{i=2}^{d_1} \langle B_j, A_i \rangle A_i$ and so

$$\|\mathcal{E}_{\mathcal{A}}(B_j)\|_2^2 = \sum_{i=2}^{d_1} |\langle B_j, A_i \rangle|^2 \leq \epsilon^2.$$

Finally, it follows that

$$\begin{aligned} Q(\mathcal{A}, \mathcal{B}) &= 1 + \sum_{i \neq 1, j \neq 1} |\langle B_j, A_i \rangle|^2 \\ &= 1 + \sum_{j=2}^{d_2} \Big(\sum_{i=2}^{d_1} |\langle B_j, A_i \rangle|^2 \Big) \\ &\leq 1 + (d_2 - 1)\epsilon^2. \end{aligned}$$

Similarly, $Q(\mathcal{A}, \mathcal{B}) \leq 1 + (d_1 - 1)\epsilon^2$ whenever $\mathcal{A}$ is ϵ-private relative to $\mathcal{B}$, and the result

follows. □

Commutants of algebras often arise in physical applications; that is, the unital algebra $\mathcal{A}' = \{X : XA = AX \ \forall A \in \mathcal{A}\}$ defined by any algebra $\mathcal{A}$. It is natural to ask whether approximately quasiorthogonality and privacy of algebras corresponds to the same for their commutants. While in general this is not true even in the ideal ($\epsilon = 0$) case, there is a situation in which these properties can be linked: as shown in [69, 56], if algebras $\mathcal{A}, \mathcal{B} \subseteq M_n$ are quasiorthogonal, then their commutants $\mathcal{A}', \mathcal{B}'$ are quasiorthogonal if and only if $\dim(\mathcal{A}) \dim(\mathcal{B}) = n^2$.

Motivated by this, we obtain a similar result below in the approximate setting. First we recall a special class of algebras. Note that a unital $*$-subalgebra $\mathcal{A} \subseteq M_n$, up to unitary equivalence, is always of the form

$$\mathcal{A} = \oplus_k (M_{n_k} \otimes 1_{m_k}) \subseteq M_n$$

where $n = \sum_k n_k m_k$ (note that here $\dim \mathcal{A} = \sum_k n_k^2$) with commutant

$$\mathcal{A}' = \oplus_k (1_{n_k} \otimes M_{m_k}(\mathbb{C})) \subseteq M_n.$$

$\mathcal{A}$ is called *homogeneously balanced* if the ratios n_k/m_k are independent of k. It follows easily that $\mathcal{A}$ is homogeneously balanced if and only if so is $\mathcal{A}'$, and there are many algebras that satisfy this condition (see [56] for more discussion and examples). For subalgebras of this special form Theorem 4.3.3 has an interesting application.

Corollary 4.3.4. *Let $\mathcal{A}, \mathcal{B} \subseteq M_n(\mathbb{C})$ be two homogeneously balanced unital subalgebras such that $\dim(\mathcal{A}) \dim(\mathcal{B}) = n^2$. Then $\mathcal{A}, \mathcal{B}$ are approximately quasiorthogonal if and only if $\mathcal{A}, \mathcal{B}$*

are approximately private relative to each other if and only if $\mathcal{A}', \mathcal{B}'$ are approximately quasiorthogonal if and only if $\mathcal{A}', \mathcal{B}'$ are approximately private relative to each other.

Proof. For homogeneously balanced subalgebras $\mathcal{A}, \mathcal{B}$, we have the following relation from [56]:

$$Q(\mathcal{A}', \mathcal{B}') = \frac{n^2}{\dim(\mathcal{A})\dim(\mathcal{B})} Q(\mathcal{A}, \mathcal{B}).$$

With the assumption $\dim(\mathcal{A})\dim(\mathcal{B}) = n^2$, the assertions of the corollary follow directly Theorem 4.3.3. □

4.4 Examples

In this section we apply Theorem 4.3.3 to examples drawn from different quantum information settings.

Example 4.4.1. We first present an example fashioned for illustrative purposes, one that also arises in the context of hybrid quantum information memories, processing, and error correction [38, 27, 28, 50, 5, 20, 7].

Consider the algebra $\mathcal{A} = M_2 \oplus M_2 \subseteq M_4$ of matrices of the form

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

with $A_1, A_2 \in M_2$. From a hybrid classical-quantum information perspective, $\mathcal{A}$ can encode two separate qubits, each with its own classical address.

Additionally, take $\mathcal{B}$ to be the unital $*$-algebra of matrices inside M_4 of the form

$$B = k_1 I_4 + k_2 \begin{pmatrix} 0 & U \\ U^* & 0 \end{pmatrix} = \begin{pmatrix} k_1 I_2 & k_2 U \\ k_2 U^* & k_1 I_2 \end{pmatrix}$$

for complex numbers k_1, k_2 and some fixed unitary $U \in M_2$. One can verify that $\mathcal{A}$ is quasiorthogonal to $\mathcal{B}$, equivalently, $Q(\mathcal{A}, \mathcal{B}) = 1$.

In the specific case that $U = \sigma_x$, the Pauli bit-flip matrix, we now obtain an algebra $\mathcal{C}$ from $\mathcal{B}$ by assuming $\mathcal{B}$ is exposed to some unitary noise V, implemented by the conjugation $C = VBV^*$, $B \in \mathcal{B}$ and $C \in \mathcal{C}$, so $\mathcal{C} = V\mathcal{B}V^*$. The unitary is chosen to reflect minimal noise exposure, in that the unitary is a small perturbation of the identity, $V = e^T$, where

$$T = \begin{pmatrix} \delta & 0 & 0 & 0 \\ 0 & -\delta & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

for some fixed $0 < \delta << 1$.

Then computing $Q(\mathcal{A}, \mathcal{C})$ using our characterization from Corollary 4.2.7 and Mathematica software, we find that

$$Q(\mathcal{A}, \mathcal{C}) = \frac{1}{2}(\cosh 4\delta + \cosh 2\delta).$$

Thus we may apply the theorem above to quantify the approximate privacy of $\mathcal{A}$ and $\mathcal{C}$ in

the following way: for any $\epsilon > 0$ satisfying,

$$\epsilon^2 > 7\left(\frac{1}{2}(\cosh 4\delta + \cosh 2\delta) - 1\right),$$

we have $Q(\mathcal{A}, \mathcal{C}) \leq 1 + \frac{\epsilon^2}{d_{\mathcal{AB}}^{max}-1}$, yielding ϵ-privacy as in the theorem. Note that we have used $d_{\mathcal{AC}}^{\max} = 8$, since $\mathcal{A}$ and $\mathcal{C}$ have dimensions 8 and 2 respectively.

Example 4.4.2. In [34] the first example of a private quantum subsystem [29, 30, 32, 31] was discovered such that no private subspaces existed for the given channel, and error-correction complementarity [25, 35, 26] failed. This example motivated further work and generalizations, including a framing of it in terms of operator algebra language [37, 36]. With the algebra perspective we can apply the theorem above to that example.

Here we take $\mathcal{A} = \triangle_4$ to be the algebra of diagonal matrices inside M_4 with respect to a given basis. Then let $\mathcal{B} = U^*(I_2 \otimes M_2)U$, where U is the unitary

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & -i & 0 \\ 0 & 1 & 0 & i \\ 0 & 1 & 0 & -i \\ 1 & 0 & i & 0 \end{pmatrix}.$$

Then one can check that we have $Q(\mathcal{A}, \mathcal{B}) = 1$; indeed, this can be seen directly through an application of Corollary 4.2.7 or as a consequence of the results from [35]. Now consider

the subalgebra $\mathcal{C} = V^*(I_2 \otimes M_2)V$ defined with the modified unitary $V = Ue^T$, where

$$T = \begin{pmatrix} \delta & 0 & 0 & 0 \\ 0 & -\delta & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

for some $0 < \delta << 1$. Hence, $\mathcal{C} = (e^T)^*\mathcal{B}(e^T)$.

With a choice of basis for the subalgebras and making use of Corollary 4.2.7 again, we can compute

$$Q(\mathcal{A}, \mathcal{C}) = \frac{1}{4} e^{-4\delta} \left(e^{4\delta} + 1\right)^2.$$

Then, for some suitable choice of $\epsilon(\delta)$ we have

$$Q(\mathcal{A}, \mathcal{C}) \leq 1 + \frac{\epsilon(\delta)^2}{3},$$

and by the theorem we have that $\mathcal{A}$ is ϵ-private relative to $\mathcal{C}$ (and vice-versa). Note that in this case, $d_{\mathcal{AB}}^{\max} = 4$.

Example 4.4.3. Another example of quasiorthogonal subalgebras for which we can study the approximate case comes from the study of mutually unbiased bases (MUB) [57, 58, 59, 60, 61].

MUB are useful in many quantum information protocols because of their defining property. Specifically, two orthonormal basis $\{|\phi_i\rangle\}$ and $\{|\psi_k\rangle\}$ of $\mathbb{C}^n$ are *mutually unbiased* if for all $i, k = 1, \ldots, n$,

$$|\langle\phi_i|\psi_k\rangle| = \frac{1}{\sqrt{n}}.$$

There is a maximal abelian subalgebra (MASA) [49] denoted $\mathcal{A}_\psi$ (and similarly $\mathcal{A}_\phi$) in M_n associated with each basis in the following way: $\mathcal{A}_\psi = \text{span}\{P_{\psi_i} : 1 \leq i \leq n\}$ is the linear span of the orthonomal projectors $P_{\psi_i} = |\psi_i\rangle\langle\psi_i| \in M_n$ onto the one-dimensional vector subspaces $\text{span}\{|\psi_i\rangle\} = \mathbb{C}|\psi_i\rangle$. The subalgebras $\mathcal{A}_\psi$, $\mathcal{A}_\phi$ are quasiorthogonal if and only if the bases are mutually unbiased. This can be checked using the fact that

$$\text{Tr}(P_{\psi_i} P_{\phi_k}) = |\langle\psi_i|\phi_k\rangle|^2$$

and the criterion for quasiorthogonality, $Q(\mathcal{A}_\psi, \mathcal{A}_\phi) = 1$ using Corollary 4.2.7 for instance.

The maximum number of MUB in an arbitrary dimension is not known in general (they are known for cases where the dimension is a power of a prime). Here we exploit the concept of "approximate" mutually unbiased bases as discussed in [70, 71].

Given an $\epsilon > 0$, we call a system of $n^2 + n$ vectors in $\mathbb{C}^n$ which are the elements of $n + 1$ orthonormal bases $\mathcal{B}_k = \{\psi_{k,1}, \cdots, \psi_{k,n}\}$ of $\mathbb{C}^n$ where $k = 0, 1, 2, \cdots, n$ ϵ-approximately mutually unbiased bases if

$$|\langle\psi_{k,i}, \psi_{j,l}\rangle|^2 \leq \frac{1+\epsilon}{n},$$

for every $0 \leq k, l \leq n, k \neq l, 1 \leq i, j \leq n$.

One such construction, from [70], asserts the existence of a system of approximately MUBs with an inequality of the following type:

$$|\langle\phi_i|\psi_k\rangle| \leq \left(2 + O(n^{-\frac{1}{10}})\right) n^{-\frac{1}{2}}.$$

Using the above expression and the measure of orthogonality given in Corollary 4.2.7, one sees that the associated MASAs are approximately private and quasiorthogonal for some ϵ.

In the 4-dimensional (two-qubit) case, for instance, one has

$$|\langle\phi_i|\psi_k\rangle| \leq 1 + \lambda(4),$$

where $\lambda(4)$ is some $O(4^{-\frac{3}{5}})$ expression. Thus each pair of MASAs is ϵ-private whenever $\sqrt{3\lambda(4)} < \epsilon$.

4.5 Outlook

We have explicitly linked approximate quasiorthogonality of operator algebras with an appropriate notion of approximate relative privacy for the algebras, determined by the actions of their conditional expectation channels. We focused on unital algebras and the notion of quantum privacy defined by privatizing to the identity operator as this includes many natural examples and it kept the technical issues manageable. That said, we expect it should be possible to extend this result to more general algebras and more general notions of privacy, for instance as has been accomplished for quantum error correction [50] and private quantum codes [26]. Additionally, it could be interesting mathematically to extend the result to the setting of operator systems (self-adjoint, unital operator spaces [72]), though the physical motivation provided by the connection with quantum privacy might be lost. We also wonder if this work could help to generate new constructions of approximate MUB or be applied to the study of SIC-POVM's [70, 71] through focus on the commutative algebra case of our result. We leave these and other investigations to be pursued elsewhere.

Chapter 5

Higher Rank Matricial Ranges and Hybrid Quantum Error Correction

5.1 Introduction

The present chapter introduces certain generalizations of the numerical range of a matrix, which is a useful mathematical object in quantum information because of its connection to quantum error correction. For appropriately defined numerical ranges of the operators of a quantum channel, error-correcting codes exist if and only if the particular numerical ranges are non-empty. This is an alternative and mathematically equivalent statement of conditions for error-correction presented in equations 2.2 and 2.3. Motivated by the overarching theme of hybrid quantum error correcting codes, joint rank matricial ranges are introduced. The primary result given in this chapter is an inequality that characterizes the existence of candidate hybrid codes for an error channel given just parameters of the code. This perspective is helpful for insights it can give about codes for an error channel, depending on

how well the channel is described. For instance, we could potentially say something about error-correction given just the number of error operators, even if we do not know what they are. Following is an elucidation of their application to hybrid quantum error correction, and a brief section at the end that explores the practical advantages of hybrid codes. The contents of this chapter are adapted from research findings co-authored and published with various collaborators [13].

For more than a decade, numerical range tools and techniques have been applied to problems in quantum error correction, starting with the study of higher-rank numerical ranges [17, 16] and broadening and deepening to joint higher-rank numerical ranges and beyond [73, 74, 75, 76, 77, 78, 18, 79]. These efforts have made contributions to coding theory in quantum error correction and have also grown into mathematical investigations of interest in their own right. In this chapter, we expand on this approach to introduce and study a higher rank matricial range motivated both by recent hybrid coding theory advances [20, 7] and the operator algebra framework for hybrid classical and quantum error correction [27, 28]. Our primary initial focus here is on a basic problem for the matricial ranges, namely, how big does a Hilbert space need to be to guarantee the existence of a non-empty matricial range of a given type, without any information on the operators and matrices outside of how many of them there are. As such, we generalize a fundamental result from quantum error correction [44, 18] to the hybrid error correction setting.

The theory of quantum error correction (QEC) originated at the interface between quantum theory and coding theory in classical information transmission and is at the heart of designing those fault-tolerant architectures [39, 40, 41, 42, 43]. It was recognized early on during these investigations that the simultaneous transmission of both quantum and classical information over a quantum channel could also be considered, most cleanly articulated in op-

erator algebra language in [38]. More recently, but still over a decade ago, the framework of "operator algebra quantum error correction" (OAQEC) [27, 28] was introduced. Motivated by a number of considerations, including a generalization of the operator quantum error correction approach [52, 51] to infinite-dimensional Hilbert space [50], it was also recognized that the OAQEC approach could provide a framework for error correction of hybrid classical and quantum information, though this specific line of investigation remained dormant for lack of motivating applications at the time. Moving to the present time and over the past few years, advantages in addressing the tasks of transmitting both quantum and classical information together compared to independent solutions have been discovered, from both information theoretic and coding theoretic points of view [1, 2, 3, 4, 5, 6, 20, 7]. Additionally it is felt that these hybrid codes may find applications in physical descriptions of joint classical-quantum systems, in view of near-future available quantum computing devices [80] and the so-called Noisy Intermediate-Scale Quantum (NISQ) era of computing [81].

This chapter is organized as follows. In the next section we introduce the joint higher rank matricial ranges and we prove the Hilbert space dimension bound result. The subsequent section considers a special case that connects the investigation with hybrid quantum error correction; specifically, for a noisy quantum channel, our formulation of the joint higher rank matricial ranges for the channel's error or "Kraus" operators leads to the conclusion that a hybrid quantum error correcting code exists for the channel if and only if one of these joint matricial ranges associated with the operators is non-empty. As a consequence of the general Hilbert space dimension bound result we establish generalizations of a fundamental early result in the theory of QEC [44, 18] to the hybrid setting. In the penultimate section we explore how hybrid error correction could provide advantages over usual quantum error correction based on this analysis. We consider a number of examples throughout the

presentation and we conclude with a brief future outlook discussion.

5.2 Higher Rank Matricial Ranges

We introduce a definition of joint rank-$(k:p)$ matricial ranges motivated by their application to hybrid quantum error-correcting codes. What follows generalizes the definition of joint rank-k matricial ranges introduced in Chapter 2, which have implications for error-correcting in quantum computing. This section focuses on more mathematical considerations and a presentation of the main theorem and its proof; their relevance to quantum computing is detailed in the section that follows. First is a definition of a mathematical instrument that the chapter centres on.

Definition 5.2.1. Given positive integers $m, n, p, k, K \geq 1$, (K usually being related to k and p), let $\mathcal{P}_K$ be the set of $n \times K$ rank-K partial isometry matrices, so $V^*V = I_K$ for $V \in \mathcal{P}_K$, and let $\mathcal{D}_p$ be the set of diagonal matrices inside the set of $p \times p$ complex matrices M_p. Define the *joint rank* $(k:p)$*-matricial range* of an m-tuple of matrices $\mathbf{A} = (A_1, \ldots, A_m) \in M_n^m$ by

$$\Lambda_{(k:p)}(\mathbf{A}) = \{(D_1, \ldots, D_m) \in \mathcal{D}_p^m : \exists V \in \mathcal{P}_{kp} \text{ such that } V^* A_j V = D_j \otimes I_k \text{ for } j = 1, \ldots, m\}.$$

Observe that when $p = 1$, $\Lambda_{(k:p)}(\mathbf{A})$ becomes the rank-k (joint when $m \geq 2$) numerical range considered in [17, 16, 73, 74, 75, 76, 77, 18, 79] and discussed in Chapter 2. Thus $\Lambda_{(k:1)}(\mathbf{A}) = \Lambda_k(\mathbf{A})$. As we will later see, $\mathbf{A}$ is related to the description of a noise operation to which quantum channels are subject. The contents of a matricial range defined in the manner above characterizes the existence of error-correcting codes for a particular description of noise.

Remark 5.2.2. We first discuss two reductions that we can make without loss of generality.

i. Every matrix $A \in M_n$ has a Hermitian decomposition $A = A_1 + iA_2$, with $A_1, A_2 \in H_n$, the set of $n \times n$ Hermitian matrices. A simple calculation shows that $V^*(A_1 + iA_2)V = D_j \otimes I_k$ if and only if $V^*(A_1)V = Re(D_j \otimes I_k)$, if and only if $V^*(A_2)V = Im(D_j \otimes I_k)$. What is of interest, is that the matricial range of $\mathbf{A}$ is non-empty. Since the above shows non-emptiness of matricial ranges of Hermitian parts implies same for the operators themselves we only need to consider $\Lambda_{(k:p)}(\mathbf{A})$ for $\mathbf{A} \in H_n^m$, where H_n^m is the set of m-tuples of $n \times n$ Hermitian matrices.

ii. Furthermore, suppose $T = (t_{ij}) \in M_m$ is a real invertible matrix, and $(c_1, \ldots, c_m) \in \mathbf{R}^{1\times m}$. Let $\tilde{\mathbf{A}} = (\tilde{A}_1, \ldots, \tilde{A}_m)$, where for $j = 1, \ldots, m$,

$$\tilde{A}_j = \sum_{\ell=1}^{m} t_{\ell,j} A_\ell + c_j I_n.$$

Then one readily shows that $(D_1, \ldots, D_m) \in \Lambda_{(k:p)}(\mathbf{A})$ if and only if $(\tilde{D}_1, \ldots, \tilde{D}_m) \in \Lambda_{(k:p)}(\tilde{\mathbf{A}})$, where $\tilde{D}_j = \sum_{\ell=1}^{m} t_{\ell,j} D_\ell + c_j I_k$ for $j = 1, \ldots, m$. So, the geometry of $\Lambda_{(k:p)}(\mathbf{A})$ is completely determined by $\Lambda_{(k:p)}(\tilde{\mathbf{A}})$.

Now, we can choose a suitable $T = (t_{ij})$ and $(c_1, \ldots, c_m)$ so that $\{\tilde{A}_1, \ldots, \tilde{A}_r, I_n\}$ is linearly independent, and $\tilde{A}_{r+1} = \cdots = \tilde{A}_m = 0_n$. Then the character of $\Lambda_{(k:p)}(\tilde{\mathbf{A}})$ is completely determined by $\Lambda_{(k:p)}(\tilde{A}_1, \ldots, \tilde{A}_r)$.

Hence, in what follows, we always assume that $\{A_1, \ldots, A_m, I_n\}$ is a linearly independent set of Hermitian matrices. Often, simpler error models, such as the completely depolarizing channel for a single qubit will comprise a set of operators with this character. In some more interesting cases, it is helpful to make this reduction.

The result we prove below is a generalization of the main result from [44], which applies to the $p = 1$ case in our notation. One should note that $p = 1$ signifies a reduction from

hybrid quantum error correction, to standard quantum error correction. This result was also proved in [18] via a matrix theoretic approach and we make use of this in our proof. The following lemma states the original result as it was presented in [18] using the present notation.

Lemma 5.2.3. *Let* $\mathbf{A} = (A_1, \ldots, A_m) \in H_n^m$ *and let* $m \geq 1$ *and* $k > 1$. *If*

$$n \geq (k-1)(m+1)^2,$$

then $\Lambda_{(k:1)}(\mathbf{A}) \neq \emptyset$.

It is not hard to see that if $(a_1, \ldots, a_m) \in \Lambda_{kp}(\mathbf{A})$, then $(a_1 I_p, \ldots, a_m I_p) \in \Lambda_{(k:p)}(\mathbf{A})$. Thus a straightforward generalization of Lemma 5.2.3 provides that if $n \geq (kp-1)(m+1)^2$, then $\Lambda_{kp}(\mathbf{A}) \neq \emptyset$; hence $\Lambda_{(k:p)}(\mathbf{A}) \neq \emptyset$. This connection between $\Lambda_{kp}(\mathbf{A})$ and $\Lambda_{(k:p)}(\mathbf{A})$ will be utilized in the proof of the theorem that follows. As discussed in [44], these inequalities quantify the capacities of quantum systems for error-correcting codes of given parameters. The need to optimize lower bounds on system sizes further motivates the result that is provided below. The following theorem thus gives an improvement on the naive bound above.

Theorem 5.2.1. *Let* $\mathbf{A} = (A_1, \ldots, A_m) \in H_n^m$ *and let* $m, p \geq 1$ *and* $k > 1$. *If*

$$n \geq (m+1)((m+1)(k-1) + k(p-1)),$$

then $\Lambda_{(k:p)}(\mathbf{A}) \neq \emptyset$.

Proof. The proof proceeds by induction on the parameter p. When $p = 1$, we have $(m+1)((m+1)(k-1) + k(p-1)) = (k-1)(m+1)^2$, and the result follows from Lemma 5.2.3.

Now suppose $p > 1$. We first assume for $r = p-1$ the inequality in the theorem holds for r in place of p, and and that it implies we can find an $n \times rk$ matrix U_r and $r \times r$ diagonal matrices $D_{j,r}$, $1 \leq j \leq m$ such that $U_r^* U_r = I_{rk}$ and

$$U_r^* A_j U_r = D_{j,r} \otimes I_k,$$

for all $1 \leq j \leq m$. That is to say:

$$n \geq (m+1)((m+1)(k-1) + k(r-1)) \implies \Lambda_{(k:r)}(\mathbf{A}) \neq \emptyset.$$

Note that $(m+1)((m+1)(k-1) + k(p-1)) > (k-1)(m+1)^2$, since $p > 1$. Thus by an application of Lemma 5.2.3 as a result on joint rank-k matricial ranges, there exists an $n \times k$ matrix U_1 and scalars d_j, $1 \leq j \leq m$ such that $U_1^* U_1 = I_k$ and $U_1^* A_j U_1 = d_j I_k$ for all $1 \leq j \leq m$ (as discussed in [18]).

Let U be a unitary matrix whose first ℓ columns span a vector subspace containing the column spaces of $U_1, A_1 U_1, \ldots, A_m U_1$. Then by simple counting $\ell \leq (m+1)k$. Further, one has $U^* A_j U = B_j \oplus C_j$ for some matrices $B_j \in M_\ell$ for $j = 1, \ldots, m$, and $C_j \in M_{n-\ell}$, where

$$n - \ell \geq (m+1)((m+1)(k-1) + k(p-2)).$$

By the induction assumption, $\Lambda_{(k:p-1)}(C_1, \ldots, C_m)$ is non-empty, say, containing an m-tuple of diagonal matrices $(D_{j1}, \ldots, D_{jm}) \in M_{p-1}^m$. So, we can find an $n \times (k-1)(m+1)^2$ matrix U_2 such that $U_2^* A_j U_2 = D_{j\ell} \otimes I_k$ for $j = 1, \ldots, m$. Thus, there is $V = [U_1 | U_2] \in M_{n,pk}$ such that $V^* V = I_{pk}$ and $V^* A_j V = d_j I_k \oplus D_{j\ell} \otimes I_k$ for $j = 1, \ldots, m$. Hence, $\Lambda_{(k:p)}(\mathbf{A}) \neq \emptyset$. $\square$

Remarks 5.2.4. Some observations that can be made from the theorem and proof discussion

are pointed out in the following remarks:

i. Let $n(k,m)$ (respectively, $n(k:p,m)$) be the minimum number such that for all $n \geq n(k,m)$ (respectively, $n(k:p,m)$), we have $\Lambda_k(\mathbf{A}) \neq \emptyset$ (respectively, we have $\Lambda_{(k:p)}(\mathbf{A}) \neq \emptyset$) for all $\mathbf{A} \in H_n^m$. Clearly, we have $n(kp,m) \geq n(k:p,m) \geq kp$. These inequalities relate constructions of hybrid codes from standard quantum error correcting codes discussed in [20]. In Example 5.3.1 and 5.3.3, we will see that sometimes the lower bound can be attained.

ii. The lower bound $(m+1)((m+1)(k-1)+k(p-1)) \geq n(k:p,m)$ in Theorem 5.2.1 is not optimal. The same proof shows that $n(k:p,m) \leq n(k,m)+(m+1)k(p-1)$. So, if we can lower the bound for $n(k,m)$, then we can lower the bound for $n(k:p,m)$. For example, since $n(k,1) = 2k-1$ [16] and $n(k,2) = 3k-2$ [18], we have $n(k:p,1) \leq 2pk-1$ and $n(k:p,2) \leq 3pk-2$. We also note that using Fan and Pall's interlacing theorem [82], one can show that $n(k:p,1) = (p+1)k-1$.

iii. In the proof of Theorem 5.2.1, suppose $U_1^* A_j U_1$ has leading $k \times k$ submatrix equal to $a_{j1} I_k$. Then we can find a unitary X such that $X^* A_j X = (B_{pq}^{(j)})_{1 \leq p,q \leq 2}$ with $B_{11}^{(j)} = a_j I_k$, $B_{12}^{(j)} = 0_{k \times r}$ and $B_{13}^{(j)}$ is $k \times s$ with $s \leq mk$. That is why we can induct on the leading $(n-s) \times (n-s)$ matrices. Of course, we can have some savings if $s < mk$ at any step.

iv. Also, when $m = 1$, it does not matter whether we want $D_j \otimes I_k$ or $C_j \otimes I_k$ for diagonal D_j or general Hermitian C_j. We can diagonalize C_j. Note that if $n = (p+1)k-1$, then the set $\Lambda_{(k:p)}(A)$ is unique if the eigenvalues of A are distinct. It should be possible to say more if there are repeated eigenvalues, and in that case one can lower the requirement of $n \geq (p+1)k-1$.

v. When $\{A_1, \ldots, A_m\}$ is a commuting family, then $A_p + iA_q$ is normal for any $p < q$. The results in [83] might be useful to study this further.

vi. One could also study a more general class of matricial ranges in which Definition 5.2.1 would be viewed as a special case; namely, the definition could be broadened to allow for arbitrary $p \times p$ matrices in the m-tuples of $\Lambda_{(k:p)}(\mathbf{A})$, removing the diagonal matrix restriction. One can generalize Theorem 5.2.1 and obtain other interesting results; see Section 5.

5.3 Application to Hybrid Quantum Error Correction

In quantum information, a *quantum channel* corresponds to a completely positive and trace preserving (CPTP) linear map $\Phi : M_n \to M_n$. By the structure theory of such maps [68], there is a finite set $E_1, \cdots \in M_n$ with $\sum_j E_j^* E_j = I_n$ such that for all $\rho \in M_n$,

$$\Phi(\rho) = \sum_j E_j \rho E_j^*. \tag{5.1}$$

These operators are typically referred to as the *Kraus operators* for Φ [10], and the minimal number of operators E_j required for this operator-sum form of Φ is called the *Choi rank* of Φ, as it is equal to the rank of the Choi matrix for Φ [68]. In the context of quantum error correction, E_j are viewed as the *error operators* for the physical noise model described by Φ.

The OAQEC framework [27, 28] relies on the structure theory for finite-dimensional von Neumann algebras (equivalently C*-algebras) when applied to the finite-dimensional setting [49]. Specifically, codes are characterized by such algebras, which up to unitary equivalence can be uniquely written as $\mathcal{A} = \oplus_i (I_{m_i} \otimes M_{n_i})$. Any M_{n_i} with $n_i > 1$ can encode quantum information; which when $m_i = 1$ corresponds to a standard (subspace) error-correcting

code [39, 40, 41, 42, 43] and when $m_i > 1$ corresponds to an operator quantum error-correcting subsystem code [52, 51]. If there is more than one summand in the matrix algebra decomposition for $\mathcal{A}$, then the algebra is a hybrid of classical and quantum codes. It has been known for some time that algebras can be used to encode hybrid information in this way [38], and OAQEC provides a framework to study hybrid error correction in depth. Of particular interest here, we draw attention to the recent advance in coding theory for hybrid error-correcting codes [20], in which explicit constructions have been derived for a distinguished special case of OAQEC discussed in more detail below.

In the Schrödinger picture for quantum dynamics, an OAQEC code is explicitly described as follows: $\mathcal{A}$ is *correctable* for Φ if there is a CPTP map $\mathcal{R}$ such that for all density operators $\rho_i \in M_{n_i}$, $\sigma_i \in M_{m_i}$ and probability distributions p_i, there are density operators σ_i' such that

$$(\mathcal{R} \circ \Phi) \left(\sum_i p_i (\sigma_i \otimes \rho_i) \right) = \sum_i p_i (\sigma_i' \otimes \rho_i).$$

This condition is perhaps more cleanly phrased in the corresponding Heisenberg picture as follows: $\mathcal{A}$ is correctable for Φ if there is a channel $\mathcal{R}$ such that for all $X \in \mathcal{A}$,

$$\left(\mathcal{P}_{\mathcal{A}} \circ \Phi^\dagger \circ \mathcal{R}^\dagger\right)(X) \;=\; X,$$

where $\Phi^\dagger$ is the Hilbert-Schmidt dual map (i.e., $\mathrm{Tr}(X\Phi(\rho)) = \mathrm{Tr}(\Phi^\dagger(X)\rho)$) and $\mathcal{P}_{\mathcal{A}}(\cdot) = P_{\mathcal{A}}(\cdot)P_{\mathcal{A}}$ with $P_{\mathcal{A}}$ the unit projection of $\mathcal{A}$.

From [27, 28], we have the following useful operational characterization of correctable algebras in terms of the Kraus operators for the channel:

Lemma 5.3.1. *An algebra $\mathcal{A}$ is correctable for a channel $\Phi(\rho) = \sum_i E_i \rho E_i^*$ if and only if*

$$[PE_i^* E_j P, X] = 0 \qquad \forall X \in \mathcal{A}, \tag{5.2}$$

where P is the unit projection of $\mathcal{A}$.

In other words, $\mathcal{A}$ is correctable for Φ if and only if the operators $PE_i^* E_j P$ belong to the commutant $P\mathcal{A}'P = P\mathcal{A}' = \mathcal{A}'P$. Applied to the familiar case of standard quantum error correction, with $\mathcal{A} = M_k$ for some k, we recover the famous Knill-Laflamme conditions [43]: $\{PE_i^* E_j P\}_{i,j} \subseteq \mathbb{C}P$. The result applied to the case $\mathcal{A} = I_m \otimes M_k$ yields the testable conditions from operator quantum error correction [52, 51]: $\{PE_i^* E_j P\}_{i,j} \subseteq M_m \otimes I_k$. Anything else involves direct sums and has a hybrid classical-quantum interpretation as noted above.

We next turn to the distinguished special hybrid case noted above. First some additional notation: we shall assume all our channels act on a Hilbert space $\mathcal{H}$ of dimension $n \geq 1$, and so we may identify $\mathcal{H} = \mathbb{C}^n$ and let $\{|e_i\rangle\}$ be the canonical orthonormal basis. Our algebras $\mathcal{A}$ then are subalgebras of the set of all linear operators $\mathcal{L}(\mathcal{H})$ on $\mathcal{H}$, which in turn is identified with M_n through matrix representations in the basis $|e_i\rangle$. We shall go back and forth between these operator and matrix perspectives as convenient.

As in [20], consider the case that $\mathcal{A} = \oplus_r \mathcal{A}_r$ with each $\mathcal{A}_r = M_k$ for some fixed $k \geq 1$. Let us apply the conditions of Eq. (5.2) to such algebras. Let P_r be the (rank k) projection of $\mathcal{H}$ onto the support of $\mathcal{A}_r$, so that the P_r project onto mutually orthogonal subspaces and $P = \sum_r P_r$ is the unit projection of $\mathcal{A} = \oplus_r P_r \mathcal{L}(\mathcal{H}) P_r$. Observe here the commutant of $\mathcal{A}$ satisfies: $P\mathcal{A}'P = \oplus_r \mathbb{C}P_r$. Thus by Lemma 5.3.1, it follows that $\mathcal{A}$ is correctable for Φ if

and only if for all i, j there are scalars $\lambda_{ij}^{(r)}$ such that

$$PE_i^* E_j P = \sum_r \lambda_{ij}^{(r)} P_r, \tag{5.3}$$

which is equivalent to the equations:

$$P_r E_i^* E_j P_s = \delta_{rs} \lambda_{ij}^{(r)} P_r \qquad \forall r, s. \tag{5.4}$$

Indeed, these are precisely the conditions derived in [20] (see Theorem 4 of [20]).

For what follows, let $\mathcal{V}_r$, $1 \leq r \leq p$ be mutually orthogonal k-dimensional subspaces of $\mathbb{C}^n$ and P_r the orthogonal projection of $\mathbb{C}^n$ onto $\mathcal{V}_r$, for $1 \leq r \leq p$. Following [20], we say that $\{\mathcal{V}_r : 1 \leq i \leq p\}$ is a *hybrid* $(k : p)$ *quantum error correcting code* for the quantum channel Φ if for all i, j and all r there exist scalars $\lambda_{ij}^{(r)}$ such that Eqs. (5.3) are satisfied.

Consideration of the matricial ranges defined above is motivated by the following fact, which can be readily verified from Eqs. (5.4).

Lemma 5.3.2. *A quantum channel Φ as defined in Eq. (5.1) has a hybrid error correcting code of dimensions $(k : p)$ if and only if*

$$\Lambda_{(k:p)}(E_1^* E_1, E_1^* E_2, \ldots, E_r^* E_r) \neq \emptyset.$$

We note that given a rank-kp projection, with say $P = \sum_{i=1}^{kp} |e_i\rangle\langle e_i|$, and diagonal matrices D_j that make $\Lambda_{(k:p)}$ nonempty, we may define the desired projections for $1 \leq r \leq p$, by $P_r = \sum_{i=1}^{k} |e_{(r-1)k+i}\rangle\langle e_{(r-1)k+i}|$.

Theorem 5.3.3. *Let Φ be a quantum channel as defined in Eq. (5.1) with Choi rank equal*

to c. Then Φ *has a hybrid error correcting code of dimensions* $(k:p)$ *if*

$$\dim \mathcal{H} \geq c^2(c^2(k-1)+k(p-1)).$$

Proof. Suppose $\{E_1, \ldots, E_c\}$ is a minimal set of Kraus operators that implement Φ as in (5.1). For $1 \leq j < \ell \leq c$, let $F_{j\ell} = \frac{1}{2}(E_j^* E_\ell + E_\ell^* E_j)$ and $F_{\ell j} = \frac{1}{2i}(E_j^* E_\ell - E_\ell^* E_j)$. Also, let $F_{jj} = E_j^* E_j$ for $1 \leq j \leq c$. Since $\sum_{j=1}^{c} E_j^* E_j = I$, the operator subspace span$\{F_{j\ell} : 1 \leq j,\ \ell \leq c\}$ has a basis $\{A_0 = I, \ldots, A_m\}$ with $m \leq c^2 - 1$. The result now follows from an application of Theorem 5.2.1. □

Theorem 5.3.3 is useful if we have no information about the E_i's, except the number c. If the E_i's are given, we may get a hybrid code even when n is lower than the bound given in Theorem 5.2.1 or 5.3.3. The saving can come from two sources: 1) The subspace spanned by $\{E_i^* E_j : 1 \leq i, j \leq c\}$ can have dimension (over $\mathbb{R}$) smaller than c^2 in particular when restricted to the code, or 2) the operators $\{E_i^* E_j\}$ have some specific structures. We give some examples to demonstrate this.

Example 5.3.1. Consider the error model on a three-qubit system

$$\Phi(\rho) = p(X_2 \rho X_2) + (1-p)\rho,$$

where $X_2 = I \otimes X \otimes I$ and X is the Pauli bit flip operator and $0 < p < 1$ is some fixed probability. It is not hard to see that the codes $C_1 = \text{span}\{|000\rangle, |001\rangle\}$ and $C_2 = \text{span}\{|100\rangle, |101\rangle\}$ together form a correctable hybrid code for Φ. One would seek to examine the matricial range

$$\Lambda_{(k:p)}(E_1^* E_1, E_1^* E_2, E_2^* E_1, E_2^* E_2) = \Lambda_{(k:p)}(I, X_2, X_2, I).$$

By the above reduction to linearly independent sets of Kraus operators, we would be interested in the geometry of $\Lambda_{(k:p)}(X_2)$. Since X_2 is unitarily similar to $I_4 \oplus -I_4$, $\Lambda_{(4:2)}(X_2) = \{\text{diag}(1,-1)\}$. Thus, for this example, we have $m = 1, k = 4, p = 2, n = 8$ and $c = 2$.

Example 5.3.2. Consider the quantum channel on a three-qubit system given by

$$\Phi(\rho) = p_0\rho + p_1 X^{\otimes 3}\rho X^{\otimes 3^*} + p_2 Y^{\otimes 3}\rho Y^{\otimes 3^*} + p_3 Z^{\otimes 3}\rho Z^{\otimes 3^*},$$

where $p_0, \ldots, p_3$ are probabilities summing to 1 and $X^{\otimes 3} = X \otimes X \otimes X$ etc, with the Pauli matrices X, Y, Z.

In this case the relevant operators $E_i^* E_j$ form the 3-tuple $(X^{\otimes 3}, Y^{\otimes 3}, Z^{\otimes 3})$, and we set $m = 3$, $k = 4, p = 1$. Defining a partial isometry $V : \mathbb{C}^4 \to \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ by

$$V = |000\rangle\langle 00| + |011\rangle\langle 01| + |101\rangle\langle 10| + |110\rangle\langle 11|,$$

one can verify that $V^*V = I_4$ and

$$\begin{aligned} V^*(X^{\otimes 3}, Y^{\otimes 3}, Z^{\otimes 3})V &= (0_2 \otimes I_2, 0_2 \otimes I_2, I_2 \otimes I_2) \\ &= (0_4, 0_4, I_4). \end{aligned}$$

Therefore, $\Lambda_4(X^{\otimes 3}, Y^{\otimes 3}, Z^{\otimes 3}) \neq \emptyset$. However, $\Lambda_{(4:2)}(X^{\otimes 3}, Y^{\otimes 3}, Z^{\otimes 3}) = \emptyset$ because $X^{\otimes 3}$ and $Y^{\otimes 3}$ do not commute.

Example 5.3.3. Extend the previous example to a four-qubit system given by

$$\Psi(\rho) = p_0\rho + p_1 X^{\otimes 4}\rho X^{\otimes 4^*} + p_2 Y^{\otimes 4}\rho Y^{\otimes 4^*} + p_3 Z^{\otimes 4}\rho Z^{\otimes 4^*},$$

where $p_0, \ldots, p_3$ are probabilities summing to 1.

In this case the relevant operators $E_i^* E_j$ form the 3-tuple $(X^{\otimes 4}, Y^{\otimes 4}, Z^{\otimes 4})$, and we set $m = 3$. We are going to show that there is a unitary matrix $U \in M_{16}$ such that

$$U^* X^{\otimes 4} U = D_X \otimes I_4, \quad U^* Y^{\otimes 4} U = D_Y \otimes I_4, \quad U^* Z^{\otimes 4} U = D_Z \otimes I_4, \tag{5.5}$$

for some diagonal matrices $D_X, D_Y, D_Z \in M_4$. Hence, we will have $\Lambda_{(4:4)}(X^{\otimes 4}, Y^{\otimes 4}, Z^{\otimes 4}) \neq \emptyset$. In this case, $k = 4, p = 4$ and $n = 16 = kp$. Thus, the smallest possible n is also achieved.

For $J = (j_1 j_2 j_3 j_4) \in \{0,1\}^4$, let $|J\rangle = |j_1 j_2 j_3 j_4\rangle$ and $|J| = \sum_{i=1}^4 j_i$. Since $Y_4|J\rangle = (-1)^{|J|} X_4|J\rangle$, we have

$$\begin{aligned}
X_4(|J\rangle + X_4|J\rangle) &= |J\rangle + X_4|J\rangle \\
X_4(|J\rangle - X_4|J\rangle) &= -(|J\rangle - X_4|J\rangle) \\
Y_4(|J\rangle + X_4|J\rangle) &= \begin{cases} |J\rangle + X_4|J\rangle & \text{if } |J| \text{ is even} \\ -(|J\rangle + X_4|J\rangle) & \text{if } |J| \text{ is odd} \end{cases} \\
Y_4(|J\rangle - X_4|J\rangle) &= \begin{cases} -(|J\rangle - X_4|J\rangle) & \text{if } |J| \text{ is even} \\ (|J\rangle - X_4|J\rangle) & \text{if } |J| \text{ is odd} \end{cases}
\end{aligned} \tag{5.6}$$

Define a unitary matrix $U = \frac{1}{2}[u_1 \cdots u_{16}]$ with columns given by

$$
\begin{aligned}
u_1 &= (|0000\rangle + |1111\rangle) + (|0011\rangle + |1100\rangle), & u_9 &= (|0000\rangle - |1111\rangle) + (|0011\rangle - |1100\rangle),\\
u_2 &= (|0000\rangle + |1111\rangle) - (|0011\rangle + |1100\rangle), & u_{10} &= (|0000\rangle - |1111\rangle) - (|0011\rangle - |1100\rangle),\\
u_3 &= (|0101\rangle + |1010\rangle) + (|0110\rangle + |1001\rangle), & u_{11} &= (|0101\rangle - |1010\rangle) + (|0110\rangle - |1001\rangle),\\
u_4 &= (|0101\rangle + |1010\rangle) - (|0110\rangle + |1001\rangle), & u_{12} &= (|0101\rangle - |1010\rangle) - (|0110\rangle - |1001\rangle),\\
u_5 &= (|0001\rangle + |1110\rangle) + (|0010\rangle + |1101\rangle), & u_{13} &= (|0001\rangle - |1110\rangle) + (|0010\rangle - |1101\rangle),\\
u_6 &= (|0001\rangle + |1110\rangle) - (|0010\rangle + |1101\rangle), & u_{14} &= (|0001\rangle - |1110\rangle) - (|0010\rangle - |1101\rangle),\\
u_7 &= (|0100\rangle + |1011\rangle) + (|0111\rangle + |1000\rangle), & u_{15} &= (|0100\rangle - |1011\rangle) + (|0111\rangle - |1000\rangle),\\
u_8 &= (|0100\rangle + |1011\rangle) - (|0111\rangle + |1000\rangle), & u_{16} &= (|0100\rangle - |1011\rangle) - (|0111\rangle - |1000\rangle).
\end{aligned}
$$

Since, $Z_4 = X_4 Y_4$, by (5.6), we have (5.5) with

$$D_X = \mathrm{diag}(1, 1, -1, -1),\ D_Y = \mathrm{diag}(1, -1, -1, 1) \ \text{ and } \ D_Z = \mathrm{diag}(1, -1, 1, -1)\,. \quad (5.7)$$

Remark 5.3.4. More generally, one can consider the class of correlation channels studied in [84], which has error operators $X^{\otimes n}$, $Y^{\otimes n}$, $Z^{\otimes n}$ normalized with probability coefficients. It is proved there that when n is odd, $\Lambda_{2^{n-1}}\left(X^{\otimes n}, Y^{\otimes n}, Z^{\otimes n}\right) \neq \emptyset$. Thus n qubit codewords encode $(n-1)$ data qubits when n is odd. When n is even, it follows that $\Lambda_{2^{n-2}}\left(X^{\otimes n}, Y^{\otimes n}, Z^{\otimes n}\right) \neq \emptyset$. Using a proof similar to the above example, we can show that $\Lambda_{(2^{n-2}:4)}\left(X^{\otimes n}, Y^{\otimes n}, Z^{\otimes n}\right) = \{(D_X, D_Y, D_Z)\}$, with D_X, D_Y, D_Z given by (5.7). It has been proven in [84] that for n even, $\Lambda_{2^{n-1}}\left(X^{\otimes n}, Y^{\otimes n}, Z^{\otimes n}\right) = \emptyset$. Actually, we can show that $\Lambda_k\left(X^{\otimes n}, Y^{\otimes n}, Z^{\otimes n}\right) = \emptyset$ for all $k > 2^{n-2}$. Therefore, we can encode at most $n-2$ qubits. Using the hybrid code, we can get 2 additional classical bits. Very recently, this scheme has been implemented using IBM's quantum computing framework qiskit [85].

5.4 Exploring Advantages of Hybrid Quantum Error Correction

A straightforward way to form hybrid codes is to use quantum codes to directly transmit classical information. However, it is impractical since quantum resources are more expensive than classical resources. Thus, realistically, hybrid codes are more interesting when the simultaneous transmission of classical information and quantum information do possess advantages. One of such situations is, with a fixed set of operators $\mathbf{A}$, hybrid quantum error correcting codes exist but the corresponding quantum codes do not exist for the same system dimension n, i.e. $\Lambda_{(k:p)}(A) \neq \emptyset$ and $\Lambda_{kp}(A) = \emptyset$.

Proposition 5.4.1. Suppose A is an $n \times n$ Hermitian matrix with eigenvalues $a_1 \geq a_2 \geq \cdots \geq a_n$. Then

$$\Lambda_{kp}(A) = \{t : a_{n+1-kp} \leq t \leq a_{kp}\}$$

$$\Lambda_{(k:p)}(A) = \left\{(t_1, \ldots, t_p) : a_{ik} \leq t_{[i]} \leq a_{n+1-(p-i+1)k} \text{ for } 1 \leq i \leq p\right\},$$

where here, $t_{[1]} \geq t_{[2]} \geq \cdots \geq t_{[n]}$ is a rearrangement of $t_1\, t_2, \cdots, t_n$ in decreasing order.

Proof. The first statement follows from [16]. For the second, by a result of Fan and Pall [82], $b_1 \geq b_2 \cdots \geq b_m$ are the eigenvalues of U^*AU for some $n \times m$ matrix U satisfying $U^*U = I_m$ if and only if

$$a_i \geq b_i \geq a_{n-m+i} \quad \forall\, 1 \leq i \leq m,$$

from which the result follows. □

Remark 5.4.1. (i) If we require the components $(t_1, \ldots, t_p)$ in $\Lambda_{(k:p)}(A)$ to be in decreasing

order, then the "ordered" $\Lambda_{(k:p)}(A)$ is convex.

(ii) $\Lambda_{kp}(A) = [a_{n+1-kp}, a_{kp}]$ is obtained by taking the convex hull of the eigenvalues of A after deleting the $(n - kp + 1)$ largest and smallest eigenvalues. The following proposition is a generalization of this result.

Proposition 5.4.2. Suppose $A_i = \text{diag}(a_1^i, a_2^i, \ldots, a_n^i)$ for $i = 1, \ldots, m$ with $a_j^i \in \mathbb{R}$. Let $\mathbf{a}_j = (a_j^1, a_j^2, \ldots, a_j^m)$ for $j = 1, \ldots, n$. For $S \subseteq \{1, \ldots, n\}$, let $X_S = \text{conv}\{\mathbf{a}_j : j \in S\}$. Then for every $1 \leq k \leq n$,

$$\Lambda_k(\mathbf{A}) \subseteq \cap\{X_S : S \subset \{1, 2, \ldots, n\},\ |S| = n - k + 1\}. \tag{5.8}$$

Proof. It suffices to prove that $\Lambda_k(\mathbf{A}) \subset X_S$ for $S = \{1, 2, \ldots, n - k + 1\}$. Suppose we have $\mathbf{x} = (x_1, x_2 \ldots, x_m) \in \Lambda_k(\mathbf{A})$. Then there exists a rank k projection P such that $PA_iP = x_iP$ for $i = 1, \ldots, m$. Consider the subspace $W = \text{span}\{e_1, \ldots, e_{n-k+1}\}$. Then there exists a unit vector $\mathbf{w} = (w_1, \ldots, w_n)^t \in \mathbb{R}^n$ such that $P\mathbf{w} = \mathbf{w}$. Therefore, for $1 \leq i \leq m$,

$$x_i = x_i\mathbf{w}^*\mathbf{w} = x_i\mathbf{w}^*P\mathbf{w} = \mathbf{w}^*PA_iP\mathbf{w} = w^*A_i\mathbf{w} = \sum_{j=1}^{n-k+1} |w_j|^2 a_j^{i\,\prime}.$$

Hence, $\mathbf{x} = \sum_{j=1}^{n-k+1} |w_j|^2 \mathbf{a}_j \in X_S$. □

By the result in [76], equality holds in (5.8) for $m = 1, 2$. For $m > 2$, $\Lambda_k(\mathbf{A})$ may not be convex and equality may not hold.

Proposition 5.4.3. Let A_i, $1 \leq i \leq m$ be as given in Proposition 5.4.2. Then we have:

(1) If $n \geq (m+1)k - m$, then $\Lambda_k(\mathbf{A}) \neq \emptyset$. The bound $(m+1)k - m$ is best possible; i.e., if $n < (m+1)k - m$, there exist real diagonal matrices $A_1, \ldots, A_m$ such that $\Lambda_k(\mathbf{A}) = \emptyset$.

(2) If $n \geq p((m+1)k-m)$, then $\Lambda_{(k:p)}(\mathbf{A}) \neq \emptyset$.

Proof. The statement (1) follows from Tverberg's Theorem [86] and Proposition 5.4.2. (Also, see Example 5.4.3.)

For (2), note that if $n \geq p((m+1)k-m)$, we can decompose each $A_i = \oplus_{j=1}^{p} A_i^j$ with $A_i^j \in M_{n_j}$, and $n_j \geq (m+1)k-m$. Then, by the result in 1), $\Lambda_k(A_1^j, \ldots, A_m^j) \neq \emptyset$ and the result follows. □

Remark 5.4.2. By the above proposition, for $p((m+1)k-m) \leq n < (m+1)kp-m$, we can construct $A_1, \ldots, A_m$ such that $\Lambda_{kp}(\mathbf{A}) = \emptyset$ and $\Lambda_{(k:p)}(\mathbf{A}) \neq \emptyset$.

Example 5.4.3. Suppose $p((m+1)k-m) \leq n < (m+1)kp-m$. We are going to show that there exist $A_1, \ldots, A_m$ such that $\Lambda_{kp}(\mathbf{A}) = \emptyset$ and $\Lambda_{(k:p)}(\mathbf{A}) \neq \emptyset$.

Let $r = \left[\dfrac{n}{kp-1}\right]$, the greatest integer $\leq \dfrac{n}{kp-1}$. Then $1 \leq r \leq (m+1)$ and $r = m+1$ if and only if $n = (m+1)(kp-1)$. Define for $1 \leq i \leq \min\{r, m\}$, $A_i = \mathrm{diag}(a_1^i, a_2^i, \ldots, a_n^i)$, where $a_i^j = 1$ for $(i-1)(kp-1)+1 \leq j \leq i(kp-1)$ and $a_i^j = 0$ otherwise. Then, by Proposition 5.4.2, $\Lambda_{kp}(\mathbf{A}) = \emptyset$. Since $n \geq p((m+1)k-m)$, by Proposition 5.4.3, $\Lambda_{(k:p)}(\mathbf{A}) \neq \emptyset$. □

5.5 Outlook

As mentioned in Remark 2.5 (vi), one can further extend the definition of $\Lambda_{(k:p)}(\mathbf{A})$ and consider $(B_1, \ldots, B_m) \in M_p^m$ such that $V^* A_j V = B_j \otimes I_k$ for some $n \times pk$ matrix V satisfying $V^*V = I_{pk}$ without requiring $B_1, \ldots, B_m$ to be diagonal matrices as in Definition 2.1. We can then use the recent results and techniques in [79] to show that this set is non-empty if n is sufficiently large. This generalization also has a potential implication to the study of quantum error correcting codes. In particular, one may use random qubits to do the encoding and protect the data bits in the quantum error correction process.

It has been proved that transmitting classical and quantum information simultaneously provides advantages from an information-theoretic perspective [1]. Practical hybrid classical-quantum error correcting codes built on the mathematical techniques introduced here that achieve these advantages could benefit various quantum communication tasks. Communication protocols based on such hybrid codes are expected to enhance the communication security or increase channel capacities. We leave these lines of investigation for future studies.

Chapter 6

Conclusion

This thesis has presented an exploration of three published research projects with strong connections between them. All the parts are motivated by the study of hybrid quantum error correcting codes, which has formed the umbrella of the present work. Chapter 1 gave a broad introduction and motivation for the entirety of the text, and Chapter 2 presented the broadest fundamental concepts: the tenets of quantum information, quantum error correction, hybrid quantum codes, quantum privacy and complementary quantum channels.

The first of the research exposition chapters centered on the complementarity of quantum privacy and quantum error correction. Key to this chapter, is the insight that either theory gives a potentially deeper understanding of the other. Section 3 of this chapter expanded on complementarity between correctable and private algebras. This needed to be done in terms of relevant operator structures. In practical terms, hybrid codes are encoded on such structures, later explained in more detail in Chapter 5. Emerging features of a special subclass of channels, unital channels, were also explored. The last part before concluding quantitatively compared the trade-off between privacy and correction in terms of inequalities

relating their dimensions. The chapter concluded with a brief outlook.

The second expository chapter, the fourth of this thesis, primarily explicitly linked approximate quasiorthogonality of operator algebras with an appropriate notion of approximate privacy of algebras, this notion being newly defined in a natural, well-motived way. The class of unital algebras were of particular focus, as well as quantum privacy defined by privatizing to the identity operator. This particular example is practically relevant, and as well makes the analysis technically tractable. Nevertheless, it is hoped that the results can appropriately be extended to more general algebras and quantum privacy settings. These generalizations have been realized in the related contexts of private quantum codes [26] and quantum error correction [50]. A few examples were presented. Of particular note, was an example relating back to constructions of approximately mutually unbiased bases. Speculatively, this work may be applied to further the constructions of such approximate MUBS, and potentially also to the study of SIC-POVM's [70, 71].

Chapter 5 introduced a definition of the joint higher rank matricial range, a high-order generalization of the numerical ranges of matrices, motivated by their application to the study of hybrid quantum error correcting codes. A chief outcome of that research was to give a dimensional inequality that qualifies the existence of a hybrid error correcting code of given parameters for a given quantum channel. A mentioned in the chapter, such examinations of the capacities of quantum channels have previously been considered. The present work provides an initial result applicable to hybrid quantum codes. Admittedly, as mentioned in the remarks following the proof of the main theorem, and demonstrated with examples, the bound given is not an optimal one. There is a possibility of improving this bound in various contexts, either through understanding the structure of particular channels of interest, or potentially further developing a general result. Note here that the type of

hybrid codes considered in Chapter 5, and the manner in which the matricial ranges are defined, are related. Advances in explicit constructions of hybrid codes with advantageous parameters [20] served as a primary motivation for this work. These codes are a special case of the operator algebra structures discussed in chapters 3 and 5. The definition of Λ can be further extended to accommodate more complex hybrid code structures not captured here.

The benefits of simultaneously transmitting quantum and classical information have been previously been demonstrated in literature [1], primarily from an information-theoretic perspective. The final part of the chapter examined this briefly. This author, together with collaborators, hope that these mathematical explorations assist in laying down a foundation that provides techniques for investigating the existence of hybrid codes, and constructing such codes. Further success will have applications in various aspects of quantum information and computation.

In the final part of this manuscript, some thoughts on potentially signifiant research works are shared. Recently, the theory of quantum error correction, and especially the framework of OAQEC, has been found to be closely related to the realization of the holographic principle in the AdS/CFT correspondence in various ways [87, 88, 89, 90, 91, 92]. Of particular note, Almheiri, Dong and Harlow interpret the complex dictionary in AdS/CFT as the encoding operations of certain operator algebra quantum error correcting codes, and bulk local operators are logical operators for these error correcting codes [87]. Concurrently, holographic methods have inspired new approaches for code design from a geometric perspective [92]. Potentially, some of the theoretical explorations of the works detailed in the research works this thesis includes could potentially have some meaning in these realms of high energy physics. What, perhaps, does complementarity, and the view of quantum error correction in terms of privacy of its complementary channel, mean for explorations in quantum gravity?

Also, looking on works in chapter 5, the approaches that have been applied to the study of hybrid quantum error correcting codes could have some meaning for the connection between quantum error correction and the ongoing search for a theory of quantum gravity.

Bibliography

[1] Igor Devetak and Peter W Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Communications in Mathematical Physics*, 256:287–303, 2005.

[2] Min-Hsiu Hsieh and Mark M Wilde. Entanglement-assisted communication of classical and quantum information. *IEEE Transactions on Information Theory*, 56:4682–4704, 2010.

[3] Jon Yard. *Simultaneous classical-quantum capacities of quantum multiple access channels*. PhD dissertation, Stanford University, 2005.

[4] Isaac Kremsky, Min-Hsiu Hsieh, and Todd A Brun. Classical enhancement of quantum-error-correcting codes. *Physical Review A*, 78:012341, 2008.

[5] Samuel L Braunstein, David W Kribs, and Manas K Patra. Zero-error subspaces of quantum channels. In *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, pages 104–108. IEEE, 2011.

[6] Manas K Patra and Samuel L Braunstein. An algebraic framework for information theory: classical information. *IMA Journal of Mathematical Control and Information*, 30(2):205–238, 2013.

[7] Andrew Nemec and Andreas Klappenecker. Hybrid codes. In *Information Theory Proceedings (ISIT), 2018 IEEE International Symposium on*, pages 796–800. IEEE, 2018.

[8] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of Statistical Physics*, 22(5):563–591, 1980.

[9] Richard P Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7), 1982.

[10] Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[11] David W Kribs, Jeremy Levick, Mike I Nelson, Rajesh Pereira, and Mizanur Rahaman. Quantum complementarity and operator structures. *Quantum Information & Computation*, 19:67–83, 2019.

[12] David W. Kribs, Jeremy Levick, Mike Nelson, Rajesh Pereira, and Mizanur Rahaman. Approximate quasiorthogonality of operator algebras and relative quantum privacy. *Reports on Mathematical Physics*, 87(2):167–181, 2021.

[13] Ningping Cao, David W Kribs, Chi-Kwong Li, Mike I Nelson, Yiu-Tung Poon, and Bei Zeng. Higher rank matricial ranges and hybrid quantum error correction. *Linear and Multilinear Algebra*, pages 1–13, 2020.

[14] A Robert Calderbank, Eric M Rains, PM Shor, and Neil JA Sloane. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 44(4):1369–1387, 1998.

[15] Man-Duen Choi, John Holbrook, David Kribs, and Karol Zyczkowski. Higher-rank numerical ranges of unitary and normal matrices. *Operators and Matrices*, 1:409–426, 2007.

[16] Man-Duen Choi, David W Kribs, and Karol Życzkowski. Higher-rank numerical ranges and compression problems. *Linear Algebra and its Applications*, 418(2-3):828–839, 2006.

[17] Man-Duen Choi, David W Kribs, and Karol Zyczkowski. Quantum error correcting codes from the compression formalism. *Reports on Mathematical Physics*, 58(1):77–91, 2006.

[18] Chi-Kwong Li and Yiu-Tung Poon. Generalized numerical ranges and quantum error correction. *Journal of Operator Theory*, pages 335–351, 2011.

[19] Min-Hsiu Hsieh and Mark M Wilde. Trading classical communication, quantum communication, and entanglement in quantum Shannon theory. *IEEE Transactions on Information Theory*, 56(9):4705–4730, 2010.

[20] Markus Grassl, Sirui Lu, and Bei Zeng. Codes for simultaneous transmission of quantum and classical information. In *Information Theory (ISIT), 2017 IEEE International Symposium on*, pages 1718–1722. IEEE, 2017.

[21] W Forrest Stinespring. Positive functions on C^* -algebras. *Proceedings of the American Mathematical Society*, 6:211–216, 1955.

[22] Alexander S Holevo. Complementary channels and the additivity problem. *Theory of Probability & Its Applications*, 51:92–100, 2007.

[23] Alexander S Holevo. *Quantum Systems, Channels, Information: A mathematical introduction*. Walter De Gruyter, 2013.

[24] Michael Horodecki, Peter W. Shor, and Mary Beth Ruskai. Entanglement breaking channels. *Reviews in Mathematical Physics*, 15:629–641, 2003.

[25] Dennis Kretschmann, David W Kribs, and Robert W Spekkens. Complementarity of private and correctable subsystems in quantum cryptography and error correction. *Physical Review A*, 78:032330, Sep 2008.

[26] Jason Crann, David W Kribs, Rupert H Levene, and Ivan G Todorov. Private algebras in quantum information and infinite-dimensional complementarity. *Journal of Mathematical Physics*, 57:015208, 2016.

[27] Cédric Bény, Achim Kempf, and David W Kribs. Generalization of quantum error correction via the Heisenberg picture. *Physical Review Letters*, 98:100502, 2007.

[28] Cédric Bény, Achim Kempf, and David W Kribs. Quantum error correction of observables. *Physical Review A*, 76(4):042303, 2007.

[29] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. *IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 547–553, 2000.

[30] P. Oscar Boykin and Vwani Roychowdhury. Optimal encryption of quantum bits. *Physical Review A*, 67:042317, 2003.

[31] Stephen D Bartlett, Patrick Hayden, and Robert W Spekkens. Random subspaces for encryption based on a private shared Cartesian frame. *Physical Review A*, 72:052329, 2005.

[32] Stephen D Bartlett, Terry Rudolph, and Robert W Spekkens. Decoherence-full subsystems and the cryptographic power of a private shared reference frame. *Physical Review A*, 70:032307, 2004.

[33] Amber Church, David W. Kribs, Rajesh Pereira, and Sarah Plosker. Private quantum channels, conditional expectations, and trace vectors. *Quantum Information & Computation*, 11:774–783, 2011.

[34] Tomas Jochym-O'Connor, David W Kribs, Raymond Laflamme, and Sarah Plosker. Private quantum subsystems. *Physical Review Letters*, 111:030502, 2013.

[35] Tomas Jochym-O'Connor, David W Kribs, Raymond Laflamme, and Sarah Plosker. Quantum subsystems: exploring the complementarity of quantum privacy and error correction. *Physical Review A*, 90:032305, 2014.

[36] J. Levick, D. W. Kribs, and R. Pereira. Quantum privacy and Schur product channels. *Reports on Mathematical Physics*, 80:333–347, December 2017.

[37] Jeremy Levick, Tomas Jochym-O'Connor, David W Kribs, Raymond Laflamme, and Rajesh Pereira. Private subsystems and quasiorthogonal operator algebras. *Journal of Physics A: Mathematical and Theoretical*, 49:125302, 2016.

[38] Greg Kuperberg. The capacity of hybrid quantum memory. *IEEE Transactions on Information Theory*, 49(6):1465–1473, 2003.

[39] Peter W Shor. Scheme for reducing decoherence in quantum computer memory. *Physical review A*, 52(4):R2493, 1995.

[40] Andrew M Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77:793, 1996.

[41] Daniel Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Physical Review A*, 54(3):1862, 1996.

[42] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed state entanglement and quantum entanglement. *Physical Review A*, 54:3824, 1996.

[43] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Physical Review A*, 55:900–911, Feb 1997.

[44] Emanuel Knill, Raymond Laflamme, and Lorenza Viola. Theory of quantum error correction for general noise. *Physical Review Letters*, 84(11):2525, 2000.

[45] Man Duen Choi. A Schwarz inequality for positive linear maps on C^*-algebras. *Illinois Journal of Mathematics*, 18:565–574, 1974.

[46] Man-Duen Choi, Nathaniel Johnston, and David W Kribs. The multiplicative domain in quantum error correction. *Journal of Physics A: Mathematical and Theoretical*, 42:245303, 2009.

[47] Nathaniel Johnston and David W Kribs. Generalized multiplicative domains and quantum error correction. *Proceedings of the American Mathematical Society*, 139:627–639, 2011.

[48] Mizanur Rahaman. Multiplicative properties of quantum channels. *Journal of Physics A: Mathematical and Theoretical*, 50:345302, 2017.

[49] Kenneth R. Davidson. *C*-algebras by example*. Fields Institute Monograph Series, American Mathematical Society, 1996.

[50] Cédric Bény, Achim Kempf, and David W Kribs. Quantum error correction on infinite-dimensional Hilbert space. *Journal of Mathematical Physics*, 50:062108, 2009.

[51] David W Kribs, Raymond Laflamme, David Poulin, and Maia Lesosky. Operator quantum error correction. *Quantum Information & Computation*, 6(4):382–399, 2006.

[52] David Kribs, Raymond Laflamme, and David Poulin. Unified and generalized approach to quantum error correction. *Physical Review Letters*, 94(18):180501, 2005.

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

[54] David W. Kribs and Robert W. Spekkens. Quantum error-correcting subsystems are unitarily recoverable subsystems. *Physical Review A*, 74:042329, Oct 2006.

[55] Dénes Petz. Complementarity in quantum systems. *Reports on Mathematical Physics*, 59:209–224, 2007.

[56] Mihály Weiner. On orthogonal systems of matrix algebras. *Linear Algebra and its Applications*, 433:520–533, 2010.

[57] Somshubhro Bandyopadhyay, P. Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002.

[58] Andreas Klappenecker and Martin Roetteler. Constructions of mutually unbiased bases. *Proceedings 7th International Conference on Finite Fields, Springer LNCS*, pages 137–144, 2004.

[59] Gen Kimura, Hajime Tanaka, and Masanao Ozawa. Solution to the mean king's problem with mutually unbiased bases for arbitrary levels. *Physical Review A*, 73(5):050301, 2006.

[60] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 8(04):535–640, 2010.

[61] Christoph Spengler, Marcus Huber, Stephen Brierley, Theodor Adaktylos, and Beatrix C Hiesmayr. Entanglement detection via mutually unbiased bases. *Physical Review A*, 86(2):022311, 2012.

[62] Hiromichi Ohno, Dénes Petz, and András Szántó. Quasi-orthogonal subalgebras of 4×4 matrices. *Linear Algebra and its Applications*, 425(1):109–118, 2007.

[63] Dénes Petz and Jonas Kahn. Complementary reductions for two qubits. *Journal of Mathematical Physics*, 48(1):012107, 2007.

[64] Hiromichi Ohno. Quasi-orthogonal subalgebras of matrix algebras. *Linear Algebra and its Applications*, 429(8-9):2146–2158, 2008.

[65] Dénes Petz, András Szántó, and Mihály Weiner. Complementarity and the algebraic structure of four-level quantum systems. *Infinite Dimensional Analysis, Quantum Probability and Related Topics*, 12(01):99–116, 2009.

[66] Dénes Petz. Algebraic complementarity in quantum theory. *Journal of Mathematical Physics*, 51:015215, 2010.

[67] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

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

[69] H. Ohno and D. Petz. Generalizations of Pauli channels. *Acta Mathematica Hungarica*, 124(1-2):165–177, 2009.

[70] Andreas Klappenecker, Martin Rötteler, Igor E Shparlinski, and Arne Winterhof. On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states. *Journal of Mathematical Physics*, 46(8):082104, 2005.

[71] Igor E Shparlinski and Arne Winterhof. Constructions of approximately mutually unbiased bases. In *Latin American Symposium on Theoretical Informatics*, pages 793–799. Springer, 2006.

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

[73] Hugo J Woerdeman. The higher rank numerical range is convex. *Linear and Multilinear Algebra*, 56(1-2):65–67, 2008.

[74] Chi-Kwong Li, Yiu-Tung Poon, and Nung-Sing Sze. Higher rank numerical ranges and low rank perturbations of quantum channels. *Journal of Mathematical Analysis and Applications*, 348(2):843–855, 2008.

[75] Man-Duen Choi, Michael Giesinger, John A Holbrook, and David W Kribs. Geometry of higher-rank numerical ranges. *Linear and Multilinear Algebra*, 56(1-2):53–64, 2008.

[76] Chi-Kwong Li and Nung-Sing Sze. Canonical forms, higher rank numerical ranges, totally isotropic subspaces, and matrix equations. *Proceedings of the American Mathematical Society*, 136(9):3013–3023, 2008.

[77] Chi-Kwong Li, Yiu-Tung Poon, and Nung-Sing Sze. Condition for the higher rank numerical range to be non-empty. *Linear and Multilinear Algebra*, 57(4):365–368, 2009.

[78] David W Kribs, Aron Pasieka, Martin Laforest, Colin Ryan, and Marcus Silva. Research problems on numerical ranges in quantum computing. *Linear and Multilinear Algebra*, 57(5):491–502, 2009.

[79] Pan-Shun Lau, Chi-Kwong Li, Yiu-Tung Poon, and Nung-Sing Sze. Convexity and star-shapedness of matricial range. *Journal of Functional Analysis*, 275(9):2497–2515, 2018.

[80] Ze-Liang Xiang, Sahel Ashhab, JQ You, and Franco Nori. Hybrid quantum circuits: Superconducting circuits interacting with other quantum systems. *Reviews of Modern Physics*, 85(2):623, 2013.

[81] John Preskill. Quantum computing in the NISQ era and beyond. *Quantum*, 2:79, 2018.

[82] Ky Fan and Gordan Pall. Imbedding conditions for Hermitian and normal matrices. *Canadian Journal of Mathematics*, 9:298–304, 1957.

[83] Hwa-Long Gau, Chi-Kwong Li, Yiu-Tung Poon, and Nung-Sing Sze. Higher rank numerical ranges of normal matrices. *SIAM Journal of Matrix Analysis and its Applications*, 32:23–43, 2011.

[84] Chi-Kwong Li, Mikio Nakahara, Yiu-Tung Poon, Nung-Sing Sze, and Hiroyuki Tomita. Efficient quantum error correction for fully correlated noise. *Physics Letters A*, 375(37):3255–3258, 2011.

[85] Chi-Kwong Li, Seth Lyles, and Yiu-Tung Poon. Error correction schemes for fully correlated quantum channels protecting both quantum and classical information. *Quantum Information Processing*, 19(5):1–17, 2020.

[86] Helge Tverberg. A generalization of Radon's theorem. *Journal of the London Mathematical Society*, 1(1):123–128, 1966.

[87] Ahmed Almheiri, Xi Dong, and Daniel Harlow. Bulk locality and quantum error correction in AdS/CFT. *Journal of High Energy Physics*, 2015(4):163, 2015.

[88] Fernando Pastawski, Beni Yoshida, Daniel Harlow, and John Preskill. Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence. *Journal of High Energy Physics*, 2015(6):149, 2015.

[89] Daniel Harlow. The Ryu–Takayanagi formula from quantum error correction. *Communications in Mathematical Physics*, 354(3):865–912, 2017.

[90] Fabio Sanches and Sean J Weinberg. Holographic entanglement entropy conjecture for general spacetimes. *Physical Review D*, 94(8):084034, 2016.

[91] Leander Fiedler, Pieter Naaijkens, and Tobias J Osborne. Jones index, secret sharing and total quantum dimension. *New Journal of Physics*, 19(2):023039, 2017.

[92] Fernando Pastawski and John Preskill. Code properties from holographic geometries. *Physical Review X*, 7(2):021022, 2017.