Quantum Error Correction and Entanglement Wedge Reconstruction

Ben Karsberg

August 19, 2022

MSc in Theoretical Physics
The University of Edinburgh
2021

Abstract

This is where you summarise the contents of your dissertation. It should be at least 100 words, but not more than 200 words.

Declaration

I declare that this dissertation was composed entirely by myself.

Chapters 2 and 3 provide an introduction to the subject area and a description of previous work on this topic. They do not contain original research.

Chapter 4 describes work that was done entirely by me. The results of this chapter have been obtained previously by Anne T Matta, but the methods used here are different in some important (or minor) ways.

Chapters 4 through 6 contain my original work. The work described in Chapter 4 was done in collaboration with Professor Carole Ann O'Malley and her PhD student Jake O'Bean. Chapter 5 presents original work done entirely by me.

State whether calculations were done using Mathematica, SymPy, etc, with (or without) gamma matrix code, master integrals, the Super-Duper software package, etc. In other words, you should refer to any software that you used during your project. For example, Monte Carlo simulation packages, hydrodynamics packages, measurement code, fitting code, tensor algebra or calculus packages, Feynman diagram packages, etc.

State whether any software you used was written by you from scratch, by your supervisor (or by whoever), or if it's a standard package.

Personal Statement

You **must** *include a Personal Statement in your dissertation. This should describe what you did during the project, and when you did it. Give an account of problems you faced and how you attempted to overcome them. The examples below are based on personal statements from MSc and MPhys projects in previous years, with (mostly-obvious) changes to make them anonymous.*

Example 1: an analytical project

The project began with an introduction to the spinor-helicity formalism in four dimensions, with my main source material being H. Elvang's "Scattering Amplitudes in Gauge Theory and Gravity" [1]. I read the first chapter, and acquainted myself with the formalism, and how it worked in a practical sense.

Once I felt more comfortable with it, we moved onto the six-dimensional spinor-helicity formalism paper, where I spent some time gaining as strong an understanding of how the formalism worked, and proving identities.

The next stage was to learn about the generalised unitarity procedure, with the end goal being to use it to calculate coefficients for some one loop integral, likely involving massive particles. Learning how this worked took some time, and proved to be some of the most difficult material for me to understand. [5] [13]

It wasn't until later that we began to consider applying what I had learned to a Kaluza-Klein reduction, which ended up being the main focus of the project. It mixed well with the general theme of "extra-dimensional theory" the project began with, and allowed me to apply all that I'd learned and prepared for so far. The vast majority of my remaining time was spent calculating coefficients for the scalar box contribution to the gluon-gluon to two-Kaluza-Klein-particle amplitude, overcoming a number of problems and errors, to finally have human-readable, and presentable results.

During the course of the project, I met with my supervisor every week, in order to discuss my progress and the direction I would head next. Toward the end, the frequency of our meetings increased somewhat, as I began to finish my calculations.

I started writing this dissertation in mid-July, and I spent the first three weeks of August working on it full-time.

Overall, I feel that the project was a success, and I found it to be extremely enjoyable throughout.

Example 2: a computational project

I spent the first 2 weeks of the project reading the material surrounding my project - mainly [1] and [2]. I also began to plan out how I would implement the algorithms in C++, in doing this I gained an understanding of what the main goals of the first half of my project would be and how they could be achieved. I identified which Monte Carlo observables would be useful to measure in these simulations.

For the next 3 weeks I implemented the standard Atlantic City algorithm and debugged my code whilst developing analysis tools in python. I compared the results from my simulations to the results from [3] (for the Random Osculator) and [4] for the EvenMoreRandom Osculator. Having obtained positive results for the Random Osculator I started reading up on Heaviside Articulation. I examined how to integrate a Heaviside Articulator into the simulation in order to produce the most efficient simulation - the solution I decided on was to use a package called HeaviArt[5].

Following this I began to integrate the Heaviside Articulator into my code and test it against the regular algorithm. In addition to this I ran longer simulations to verify my findings without Articulation.

In mid July I finished implementing Heaviside Articulation into my code and began looking into how to quantify any improvement in speed gained by this algorithm. As July progressed I started looking into how to integrate the EvenMoreRandom Osculator into my code - this was the most complicated part of the project, as discussed in the body of this report. Despite much effort on my part, I couldn't get the results produced by the new algorithm to agree with the old ones. Following further study of the literature, and long discussions with Jack O'Bean, it turned out that the original form of Heaviside Articulation didn't applied to the EvenMoreRandom Osculator. With the help of Jack and my supervisor, I then developed the new version described in this report. I also did analytical calculations of the Four-Point Green-and-White- Function to two orders higher than had been published previously in the literature.

For the final parts of the summer I worked mainly on perfecting the algorithm for the Random Osculator and implementing the EvenMoreRandom Osculators algorithm with the improved Heaviside Articulation. The final results were encouraging, but more work is clearly needed. To this end, I have been awarded a studentship by the British University of Lifelong Learning to extend this work during my PhD Studies at the non-existent Scottish Highlands Institute of Technology in Inveroxter.

I started writing this dissertation in mid-July, and I spent the first three weeks of August working on it full-time.

Example 3: a very mathematical project

[In preparation]

Acknowledgements

I would like to thank everyone at the University of Edinburgh who supported me through the MSc. program, and without whom I never would have been able to reach this project, let alone complete it.

I would like to extend enormous thanks to my supervisor Joan Simon for his expertise, guidance, and incredible and detailed feedback on all aspects of the project, as well as timely replies to my emails!

I also wish to thank my parents, Liz and Alan, for their continued support and encouragement throughout this year.

Thank you to Joe also - several valuable conversations about various aspects of this project have proved hugely useful.

I would finally like to thank several of my friends: James, Dan, Laurence, Tom, Millie, Louis, Sophie, Simon, and Jacob. Without your continued advice on my anxieties, humour, and just general incredible support, I doubt I'd have had the resilience to complete this MSc.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Ever since David Deutsch and Richard Josza introduced their famous algorithm [4] demonstrating a problem which a quantum computer could solve exponentially faster than a classical computer, quantum computing has been an active area of research. A few years later when Peter Shor described a quantum algorithm to factorise integers in polynomial time [15], it became clear that quantum computers held vast potential; if Shor's algorithm could be implemented with enough qubits, then almost every cryptographic scheme used throughout the World could be broken!

Luckily for anyone relying on cryptographic procedures such as these, qubits are immensely delicate and sensitive to changes in their environment. They are prone to suffering errors and decoherence, irreparably ruining computations. Even to this day, the largest number factorised using Shor's algorithm is 21 [12] - far smaller than the huge numbers needed to break cryptographic protocols!

A few years later in 1995, Shor proposed a potential solution: *quantum error correction* [14]. The idea was relatively simple - encode one logical qubit in nine physical qubits in such a way that the single qubit was protected from arbitrary errors. Shor's code was quickly improved upon, with a (minimal) five qubit code which could protect against arbitrary single qubit errors being published in 2001 [9].

While quantum computing has in many ways moved on from simple factorisation, error correction remains an active field of research. With the proof of the *quantum threshold theorem* [1][10][8] which states that a quantum computer with a *physical* error rate below a certain threshold can suppress the *logical* error rate to arbitrarily low levels, quantum error correction is considered by many as the most likely way to build a fully fault-tolerant quantum computer.

Recently, an unexpected link between quantum error correction and the structure of space-time was discovered. The AdS/CFT correspondence in the field of holography (itself a branch of string theory) posits a relationship between quantum gravity in an anti-de Sitter space, and a conformal field theory on the boundary [11]. In 2015, Ahmed Almheiri, Xi Dong, and Daniel Harlow discovered that in the language of quantum error correction, a certain aspect of AdS/CFT known as *subregion duality* could be elucidated [2]. Explicitly, certain error correcting procedures have various properties which can be interpreted naturally in holography. Such codes have come to be known as *holographic error correcting codes*, and they have already provided simple toy models to explore the emergence of space-time. From a quantum error correction perspective, it is also hoped that holography can inspire new error correcting codes to be developed.

The goal of this dissertation is to present the basic theory of holographic error correction in a self-contained way, aimed at those with a background in quantum computing rather than holography. Therefore, the focus will be almost entirely on the quantum information perspective, with any comments on holography being present purely for intuition.

This dissertation is structured as follows. Chapter 2 will present all the relevant background theory in error correction, assuming an understanding of quantum mechanics and quantum computing. Those looking for a more detailed exposition of these topics would be well-advised to read Nielsen and Chuang's textbook [13]. This chapter also contains a brief discussion on the relevant aspects of holography in a somewhat 'non-rigourous' way. Chapter 3 will present the main results and proofs of [5] - this paper is the primary reference for holographic error correction in general, presenting the three basic theorems of the field in a self-contained way. We change some of the conventions used by Harlow to be more relevant to quantum computing, describing error correction via an *encoding isometry* rather than a *code subspace* as Harlow does. Chapter 4 presents some generalisations of holographic error correction, including *approximate codes*, *state-specific codes*, and *non-isometric codes*, all adapted from [3]. Finally, chapter 5 will present a summary of the project and suggestions as to the future direction of the field.

Chapter 2

Error Correction: An Introduction

In this chapter, we present the theory of quantum error correction. We begin with a discussion of the analogous topic in the classical regime to build up some intuition, before moving on to the quantum world. We work through the generalities, before discussing quantum *erasure* correction - the main focus of this project. These discussions are adapted from [13] and [5].

2.1 The Classical Bit-Flip

To gain some intuition for error-correction, we don't even need to start with a quantum process. Instead, we present the *classical bit-flip code.* While the ideas are basic and situation-specific, the key features of the process carry through to the quantum case.

Suppose Alice wishes to send a single bit to Bob across a noisy communication channel. In this example, we model the noise as a bit-flip - there is a fixed probability p for the transmitted bit to flip state from a 0 to a 1 or a 1 to a 0. Alice is afraid that Bob will receive the incorrect bit value, so she instead copies her bit three times and sends all three bits to Bob instead. When Bob receives the three bits, he takes the majority bit value to be the correct message; that way, if 1 or fewer of the bits flip, Bob will receive the correct message!

This method is not perfect though. It could be the case that 2 or more bits flip in the channel, and Bob could receive the incorrect message. Assuming the noise acts *independently* on each transmitted bit, the probability of this happening is

$$\mathbb{P}(2 \text{ or more flips}) = 3p^2(1-p) + p^3, \tag{2.1.1}$$

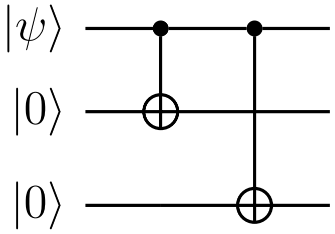
which is strictly less than p for $0 < p < 1/2$. Therefore so long as p is less than $1/2$, Bob has an increased chance of receiving Alice's intended message.

While this is a very simple example, there are some salient features which are common to all error-correcting processes, both quantum and classical. First, Alice *encodes* her bit (called the *logical bit*) by copying it three times (where the encoded bits are called the *physical bits*). She then sends the physical bits to Bob, where they encounter *noise* in the process, potentially flipping. When the Bits reach Bob, he needs to determine whether a bit-flip occurred - called *error detection* - and if so, he *corrects* it by flipping back the corresponding physical bit, before finally *decoding* the message. Schematically:

$$0 \xrightarrow{\text{Encoding}} 000 \xrightarrow{\text{Noise}} 001 \xrightarrow{\text{Correction}} 000 \xrightarrow{\text{Decoding}} 0.$$

2.2 The Quantum Bit-Flip

The quantum situation is exactly analogous, except this time Alice wishes to send a qubit to Bob. The quantum channel acts analogously too, flipping each of the computational basis states (essentially applying a X gate) with a fixed probability p. The *no-cloning theorem* prevents Alice copying her arbitrary qubit though, so she has to be a bit more creative with encoding it. She does this by means of a quantum circuit taking $|0\rangle \to |000\rangle$ and $|1\rangle \to |111\rangle$; explicitly



(2.2.1)

Note in particular that the physical encoded state is **not** equal to three copies of the logical state: $|\psi\rangle = a\,|0\rangle + b\,|1\rangle \to a\,|000\rangle + b\,|111\rangle \neq |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$, so no-cloning is certainly not violated.

Suppose Alice does all this, and sends Bob the encoded physical qubits. Bob needs to check whether a bit-flip occurred on any of the individual qubits, so he performs a projective measurement with projectors

$$\begin{aligned}
P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111| \qquad &&\text{(no error)}\\
P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| \qquad &&\text{(qubit 1 flipped)}\\
P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| \qquad &&\text{(qubit 2 flipped)}\\
P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110| \qquad &&\text{(qubit 3 flipped).}
\end{aligned} \tag{2.2.2}$$

This is called a *syndrome measurement.* To see that this works, suppose only the first physical qubit flips, so Bob receives $|E\rangle \equiv a\,|100\rangle + b\,|011\rangle$. In this case, $\langle E|P_1|E\rangle = 1$, so the measurement returns 1 with certainty, and Bob can establish that the first qubit flipped. Also note that $P_1\,|E\rangle = |E\rangle$, so the measurement does not change the state.

Bob's final task is to recover the original logical qubit. The outcome of the syndrome measurement tells him which physical qubit flipped (if any), and so he can just flip the corresponding qubit back by applying an X gate. He can then just perform a measurement of the corrected state to obtain the original amplitudes.

This process is again imperfect. If two or more qubits flip, then Bob cannot recover the original state with this process. However, an identical calculation to the classical case shows us that it improves the probability that Bob can reconstruct the original state so long as $p < 1/2$.

2.3 Quantum Noise

The above examples provide basic examples of error correction. However, in order to talk about error correction in full generality, we need some general theory. In particular, how to model arbitrary noise for quantum systems, which is done through *quantum operations.*

2.3.1 Quantum Operations

In general, an isolated or *closed* quantum system evolves in time under the action of a unitary operator. That is, if a closed system is initially in state ρ, at a later time it will be in the state $U\rho U^\dagger$ for some unitary operator U. In practice though, quantum systems are *open* and interact with their environment, so we cannot just assume that our system of interest evolves unitarily. If a system is initially in state ρ and evolves to state ρ', to be fully general we simply write

$$\rho' = \mathcal{E}(\rho), \tag{2.3.1}$$

where $\mathcal{E}$ is a map from density operators to density operators on the state space of the system. This, in the loosest possible sense, defines a quantum operation.

To be more explicit, suppose our system of interest is initially in the state ρ, and the environment is in ρ_{env}. The full state system-environment state is then $\rho \otimes \rho_{\text{env}}$, and taken together is a closed system, so it evolves unitarily as

$$\rho \otimes \rho_{\text{env}} \to U\left(\rho \otimes \rho_{\text{env}}\right) U^\dagger. \tag{2.3.2}$$

To find the quantum operation governing the evolution of ρ alone, we can take a partial trace over the environment:

$$\mathcal{E}(\rho) = \mathrm{Tr}_{\mathrm{env}}\left[U(\rho \otimes \rho_{\mathrm{env}})U^\dagger\right]. \tag{2.3.3}$$

This is a more concrete definition of a quantum operation. One immediate issue though is that evolution of the principal system is expressed in terms of operators involving the environment, which we may not have access to in full. There is however a way around this.

2.3.2 Operator-Sum Representation

Suppose $\{|e_k\rangle\}$ is an orthonormal basis for the environment system such that the initial state of the environment is $\rho_{\mathrm{env}} = |e_0\rangle\langle e_0|$. Then, we can rewrite 2.3.3 as

$$\mathcal{E}(\rho) = \sum_k \langle e_k| U\Big[\rho \otimes |e_0\rangle\langle e_0|\Big]U^\dagger |e_k\rangle \equiv \sum_k E_k \rho E_k^\dagger, \tag{2.3.4}$$

where we implicitly define $E_k \equiv \langle e_k|U|e_0\rangle$. These are operators on the principal system of interest only, so fix our issue! This is called the *operator-sum representation* or *Kraus representation* of $\mathcal{E}$, and the set $\{E_k\}$ are called its *operation elements.*

The operation elements have a completeness property; since $\mathcal{E}(\rho)$ must itself be a density matrix, we require $\mathrm{Tr}(\mathcal{E}(\rho)) = 1$. Therefore

$$1 = \mathrm{Tr}\left(\sum_k E_k \rho E_k^\dagger\right) = \mathrm{Tr}\left(\sum_k \rho E_k^\dagger E_k\right) \tag{2.3.5}$$

holds for all states ρ, and so

$$\sum_k E_k^\dagger E_k = I. \tag{2.3.6}$$

If this equation is satisfied, $\mathcal{E}$ is called a *trace-preserving operation.* We assume all operations from here on out to be trace-preserving, unless stated otherwise.

The operator-sum representation of a quantum operation is not unique. The following theorem characterises this, stated without proof.

Theorem 2.3.1 (Unitary freedom in the operator-sum representation)**.** *Suppose $\{E_1, \dots, E_m\}$ and $\{F_1, \dots, F_n\}$ are operation elements of operations $\mathcal{E}$ and $\mathcal{F}$ respectively. Append zero operators to the shorter list of elements to ensure $m = n$. Then, $\mathcal{E} = \mathcal{F}$ if and only if $E_i = \sum_j u_{ij} F_j$, where u_{ij} are the elements of an $m \times m$ unitary matrix.*

2.3.3 Axiomatisation

Quantum operations can alternatively be defined axiomatically, with no reference to an environment at all; this is often neater, especially for our purposes. We therefore define the following.

Definition 2.3.1 (Quantum Operation)**.** A map $\mathcal{E}$ from the set of density operators on $\mathcal{H}_1$ to the set of density operators on $\mathcal{H}_2$ is called a quantum operation if it satisfies:

1. $\mathrm{Tr}(\mathcal{E}(\rho))$ is the probability that the process represented by $\mathcal{E}$ occurs, so $0 \leq \mathrm{Tr}(\mathcal{E}(\rho)) \leq 1$.
2. $\mathcal{E}$ is *convex-linear*; that is, for a set of probabilities $\{p_i\}$ and density matrices $\{\rho_i\}$, we have
$$\mathcal{E}\left(\sum_i p_i\rho_i\right) = \sum_i p_i\mathcal{E}(\rho_i). \tag{2.3.7}$$
3. $\mathcal{E}$ is a completely positive map; so for any positive operator A, $\mathcal{E}(A)$ is also a positive operator. More generally, if we introduce an auxiliary system R, $(I_R \otimes \mathcal{E})(B)$ is positive for any positive operator B on $R \otimes \mathcal{H}_1$.

Note that the first property here reduces to $\mathrm{Tr}(\mathcal{E}(\rho)) = 1$ for trace-preserving operations. We can in fact show that any map $\mathcal{E}$ satisfying these properties has an operator-sum representation, which is formalised by the following theorem, again stated without proof:

Theorem 2.3.2. *A map $\mathcal{E}$ from the set of density operators on $\mathcal{H}_1$ to the set of density operators on $\mathcal{H}_2$ satisfies the above axioms if and only if*

$$\mathcal{E}(\rho) = \sum_i E_i\rho E_i^\dagger \tag{2.3.8}$$

for some set of operators $E_i : \mathcal{H}_1 \to \mathcal{H}_2$, and $\sum_i E_i^\dagger E_i \leq I$.

We now present a basic example of a quantum operation, showing how the action of the bit-flip channel can be modelled.

Example 2.3.1 (The quantum bit-flip)**.** *Consider the quantum operation from the set of density matrices of a single qubit to itself, defined by operation elements*

$$E_0 \equiv \sqrt{1-p}I = \sqrt{1-p}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \quad E_1 \equiv \sqrt{p}X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}. \tag{2.3.9}$$

The action of this operation on a state ρ is therefore

$$\mathcal{E}(\rho) = (1-p)\rho + pX\rho X. \tag{2.3.10}$$

It therefore 'does nothing' to ρ with probability $1-p$, and flips each basis element of ρ with probability p, exactly matching the bit-flip channel!

2.3.4 General Theory of Error Correction

We now have the necessary theory to talk about the general theory behind quantum error-correction. A logical state ρ with support on a *logical space* $\mathcal{H}_L$ is encoded by an isometry $V : \mathcal{H}_L \to \mathcal{H}$, where the image of the isometry is called a *code subspace* $\mathcal{H}_{\text{code}} \subseteq \mathcal{H}$, which has equal dimensionality to $\mathcal{H}_L$. We call $\mathcal{H}$ the *physical space*. In the bit-flip code for example, V is specified by the quantum circuit 2.2.1, and $\mathcal{H}_{\text{code}} = \text{span}\{V\left|0\right\rangle, V\left|1\right\rangle\} = \{\left|000\right\rangle, \left|111\right\rangle\}$. After encoding, the state is subjected to noise (modelled by a quantum operation), a syndrome measurement is performed to diagnose the type of error which occurred (if any), and then a recovery operation is performed to obtain the original state. Note that different errors have to correspond to orthogonal subspaces of the full Hilbert space $\mathcal{H}$ in order to be reliably distinguished by the syndrome measurement.

In general, we make no assumptions about the full recovery procedure - in particular, we do not assume it is necessarily a two-stage detection-recovery process. We only assume that the noise is modelled by a quantum operation $\mathcal{E}$, and the correction is performed by a quantum operation $\mathcal{R}$. For error correction to be deemed successful, we require that for any state ρ with support on $\mathcal{H}_{\text{code}}$

$$(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho, \tag{2.3.11}$$

where we have a proportionality constant rather than equality to account for the possibility that the noise may not be trace-preserving (for example, if it takes a measurement).

Not all errors are correctable. This is characterised by the *quantum error correction conditions*, which can be stated as the following theorem:

Theorem 2.3.3 (Quantum error-correction conditions)**.** *Suppose $V : \mathcal{H}_L \to \mathcal{H}$ is an encoding isometry, and that P_{code} is the projector onto its image $\mathcal{H}_{code}$. Suppose $\mathcal{E}$ is a quantum operation modelling noise, with elements $\{E_i\}$. An error correction operation $\mathcal{R}$ correcting $\mathcal{E}$ on $\mathcal{H}_{code}$ exists if and only if*

$$P_{code}E_i^\dagger E_j P_{code} = \alpha_{ij} P_{code} \tag{2.3.12}$$

where α_{ij} are the elements of a complex hermitian matrix.

From now on, we call the set $\{E_i\}$ *errors* rather than operation elements, and if an $\mathcal{R}$ exists then we say they are a *correctable set* of errors.
In general, we may not know the form of the noise precisely, but the error correction conditions can be adapted to characterise an equivalence class of noise which an isometry and correction operation $\mathcal{R}$ can correct for.

Theorem 2.3.4. *Suppose $V : \mathcal{H}_L \to \mathcal{H}$ is an encoding isometry with image $\mathcal{H}_{code}$, and $\mathcal{R}$ is the full error-correcting operation correcting $\mathcal{E}$ with errors $\{E_i\}$. Then, $\mathcal{R}$ corrects for $\mathcal{F}$ with errors $\{F_i\}$ if*

$$F_i = \sum_i m_{ij} E_j \tag{2.3.13}$$

for all i, and m_{ij} are some the elements of a complex matrix m on $\mathcal{H}_{code}$.

This is a useful statement, as we can talk about a class of errors $\{E_i\}$ which are correctable rather than a class of noises $\mathcal{E}$. For example, if we can find a process satisfying

$$P_{\text{code}} \sigma_i^1 \sigma_j^1 P_{\text{code}} = \alpha_{ij} P_{\text{code}} \tag{2.3.14}$$

for the Pauli matrices, then we can correct for **arbitrary** single qubit errors, since any single qubit operation has operation elements which can be chosen to be proportional to the Pauli matrices. Shor's code [14] can do this, for example.

2.4 Quantum Erasure

For our purposes, a class of errors called *quantum erasures* are particularly important. An erasure is defined as the channel acting to erase a **known** of subsystem of the physical space. Formally, we suppose that the physical space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$ has a tensor product structure. One representation of the erasure channel is then

$$\mathcal{E}(\rho) = \text{Tr}_{\overline{A}}(\rho), \tag{2.4.1}$$

for any state on $\mathcal{H}$. Note that this takes states on $\mathcal{H}$ to states on $\mathcal{H}_A$ only. To extract the operation elements, we let $\{|a\rangle\}$ and $\{|\overline{a}\rangle\}$ be orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_{\overline{A}}$ respectively. We can then rewrite 2.4.1 as

$$\mathcal{E}(\rho) = \sum_{\overline{a}} \langle \overline{a} | \rho | \overline{a} \rangle \,, \tag{2.4.2}$$

from which we can read off operation elements

$$E_{\overline{a}} \equiv I_A \otimes \langle \overline{a}| = \sum_a |a\rangle \langle a| \otimes \langle \overline{a}| \,. \tag{2.4.3}$$

The natural question to ask is what the quantum error correction conditions 2.3.3 reduce to for erasures. To work this out, we can compute

$$E_{\overline{a}}^{\dagger}E_{\overline{b}} = (I_A \otimes |\overline{a}\rangle)(I_A \otimes \langle\overline{b}|) = I_A \otimes |\overline{a}\rangle \langle\overline{b}| \,, \tag{2.4.4}$$

and so 2.3.12 then reduces to

$$P_{\text{code}} |\overline{a}\rangle \langle\overline{b}| P_{\text{code}} = \alpha_{\overline{a}\overline{b}} P_{\text{code}} \tag{2.4.5}$$

where we drop the I_A for notational simplicity since the $|\overline{a}\rangle$s do not have any action on the A subsystem. Even more simply, we can just write

$$P_{\text{code}} |\overline{a}\rangle \langle\overline{b}| P_{\text{code}} \propto P_{\text{code}}. \tag{2.4.6}$$

This will have an important implication when we come to look at theorem 3.1 of [5]. Note that an arbitrary operator $X_{\overline{A}}$ acting on $\mathcal{H}_{\overline{A}}$ can be decomposed in the $\{|\overline{a}\rangle\}$ basis as

$$X_{\overline{A}} \equiv \sum_{\overline{a},\overline{b}} x_{\overline{a},\overline{b}} |\overline{a}\rangle \langle\overline{b}| \tag{2.4.7}$$

for some $x_{\overline{a},\overline{b}} \in \mathbb{C}$. Therefore, if 2.4.5 holds, we have

$$P_{\text{code}} X_{\overline{A}} P_{\text{code}} \propto P_{\text{code}}. \tag{2.4.8}$$

This is precisely condition 3 of theorem 3.1 of [5].

Chapter 3

Holographic Error Correction

In this section, we state and prove the three theorems of [5]. We use the language of encoding isometries as in [6] rather than the code subspace language of [5], as it makes constructing examples via a quantum circuit considerably easier. The three theorems are in increasing generality; the first describes *conventional erasure correction*, the second *subsystem error correction*, and the third *operator algebra error correction*. They all characterise whether an erasure is correctable in the sense of complete state recovery; approximate state recovery is covered in chapter 4.

3.1 Conventional Erasure Correction

We now present theorem 3.1 of [5] from the encoding isometry point of view.

Theorem 3.1.1. *Let $V : \mathcal{H}_L \to \mathcal{H}$ be an encoding isometry, where $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$, and $\mathcal{H}_{code} \subseteq \mathcal{H}$ is the image of V. Define an orthonormal basis $\{|\tilde{i}\rangle\}$ of $\mathcal{H}_L$, and let $|\phi\rangle \equiv \frac{1}{\sqrt{|R|}} |i\rangle_R (V|\tilde{i}\rangle)_{A\overline{A}}$, where R is an auxiliary system with $\mathcal{H}_R = \mathcal{H}_L$, The following statements are then equivalent:*

1. *$|R| \leq |A|$, and if we decompose $\mathcal{H}_A = (\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}) \oplus \mathcal{H}_{A_3}$ with $|A_1| = |R|$ and $|A_3| < |R|$, then there exists a unitary transformation U_A on $\mathcal{H}_A$ and a state $|\chi\rangle_{A_2\overline{A}} \in \mathcal{H}_{A_2\overline{A}}$ such that*

$$(U_A \otimes I_{\overline{A}})(V|\tilde{i}\rangle)_{A\overline{A}} = |i\rangle_{A_1} \otimes |\chi\rangle_{A_2\overline{A}}\,, \tag{3.1.1}$$

where $|i\rangle_{A_1}$ is an orthonormal basis for $\mathcal{H}_{A_1}$.

2. *For any operator $\tilde{O}$ acting within $\mathcal{H}_L$, there exists an operator O_A on $\mathcal{H}_A$ such that for any state $|\tilde{\psi}\rangle \in \mathcal{H}_L$, we have*

$$\begin{aligned} O_A V |\tilde{\psi}\rangle &= V\tilde{O}|\tilde{\psi}\rangle \\ O_A^\dagger V |\tilde{\psi}\rangle &= V\tilde{O}^\dagger|\tilde{\psi}\rangle . \end{aligned} \tag{3.1.2}$$

3. *For any operator $X_{\overline{A}}$ on $\mathcal{H}_{\overline{A}}$, we have*

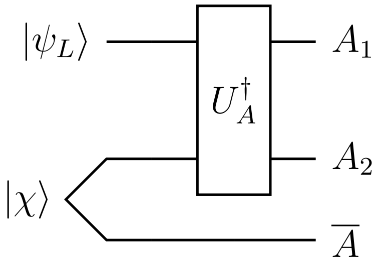
$$P_{code} X_{\overline{A}} P_{code} \propto P_{code} \tag{3.1.3}$$

where P_{code} is the projector onto $\mathcal{H}_{code}$. Alternatively, if $P_L = \sum_i |\tilde{i}\rangle\langle\tilde{i}|$ is the projector onto $\mathcal{H}_L$, then $P_{code} = VP_LV^\dagger$ is its image under V.

4. *In the state $|\phi\rangle$, we have*

$$\rho_{R\overline{A}}[\phi] = \rho_R[\phi] \otimes \rho_{\overline{A}}[\phi]. \tag{3.1.4}$$

Before proving this, let's go over some of the intuition behind each statement, and what all the objects in this theorem refer to. $\overline{A}$ is the erased subsystem, and A is preserved under erasure. 3.1.1 is the statement of full state recovery; we can recover the matrix elements of any state on $\mathcal{H}_{\text{code}}$ in full on subsystem A_1 by applying some unitary U_A, without access to $\overline{A}$ at all. We can visualise this by means of a circuit diagram:



A natural question about 3.1.1 is asking what the significance of $|\chi\rangle$ is. This is elucidated in the proof, but essentially it turns out that $|\chi\rangle$ is an arbitrary purification of $\rho_{\overline{A}}[\phi]$ on A_2. 3.1.2 says that any logical operator on $\mathcal{H}_L$ can be equivalently represented by an operator acting on the A subsystem only. 3.1.3 is just equation 2.4.8; the quantum error correction conditions adapted to erasures. In a more physically intuitive way, this says that performing a measurement of any operator on the erased subsystem $\overline{A}$ cannot disturb the encoded information - a plausible condition for erasure to be correctable. In some sense, this means that all information about the original state is contained in the A system. 3.1.4 states

that operators on the auxiliary system R and operators on the erased subsystem $\overline{A}$ are not correlated.
We now present the proof of this theorem.

Proof. (1) $\implies$ (2): Define $O_A \equiv U_A^\dagger O_{A_1} U_A$, where O_{A_1} is an operator on $\mathcal{H}_{A_1}$ with the same matrix elements as $\tilde{O}$ has on $\mathcal{H}_L$; that is

$$\langle\tilde{i}|\tilde{O}|\tilde{j}\rangle_{A\overline{A}} = \langle i|O_{A_1}|j\rangle_{A_1}$$

which is always possible since $|A_1| = |R| = |\mathcal{H}_L|$. Now, note that 3.1.2 can be alternatively phrased as the statement that for any $\tilde{O}$, there exists a corresponding O_A with

$$\begin{aligned}\langle\tilde{i}|V^\dagger O_A V|\tilde{j}\rangle &= \langle\tilde{i}|\tilde{O}|\tilde{j}\rangle \\ \langle\tilde{i}|V^\dagger O_A^\dagger V|\tilde{j}\rangle &= \langle\tilde{i}|\tilde{O}^\dagger|\tilde{j}\rangle\,.\end{aligned} \tag{3.1.5}$$

We can then just check these are satisfied by our O_A:

$$\begin{aligned}\langle\tilde{i}|V^\dagger O_A V|\tilde{j}\rangle &= \langle\tilde{i}|V^\dagger U_A^\dagger O_{A_1} U_A V|\tilde{j}\rangle \\ &= (\langle i|_{A_1}\langle\chi|_{A_2\overline{A}})O_{A_1}(|j\rangle_{A_1}|\chi\rangle_{A_2\overline{A}}) \\ &= \langle i|O_{A_1}|j\rangle_{A_1}\langle\chi|\chi\rangle_{A_2\overline{A}} \\ &= \langle\tilde{i}|\tilde{O}|\tilde{j}\rangle\end{aligned} \tag{3.1.6}$$

with similar for $O_A^\dagger$, as claimed.
(2) $\implies$ (3): This implication is by contradiction. We can rewrite 3.1.3 as the statement that $P_L V^\dagger X_{\overline{A}} V P_L \propto P_L$. So suppose there was some $X_{\overline{A}}$ such that $P_L V^\dagger X_{\overline{A}} V P_L \not\propto P_L$. Now, Schur's lemma in this context states that the only non-trivial operators commuting with all other operators on $\mathcal{H}_L$ are scalar multiples of the identity. Since $V^\dagger X_{\overline{A}} V$ is not the identity, there must be some $\tilde{O}$ on $\mathcal{H}_L$ which doesn't commute with $V^\dagger X_{\overline{A}} V$, and some $|\tilde{\psi}\rangle \in \mathcal{H}_L$ such that:

$$\langle\tilde{\psi}|[P_L V^\dagger X_{\overline{A}} P_L, \tilde{O}]|\tilde{\psi}\rangle = \langle\tilde{\psi}|[V^\dagger X_{\overline{A}} V, \tilde{O}]|\tilde{\psi}\rangle \neq 0. \tag{3.1.7}$$

But such an $\tilde{O}$ cannot have a representation O_A on $\mathcal{H}_A$ as defined in 3.1.2, since this would by definition commute with $X_{\overline{A}}$; if it had such an O_A, then $\langle\tilde{\psi}|[V^\dagger X_{\overline{A}} V, \tilde{O}]|\tilde{\psi}\rangle = \langle\tilde{\psi}|[V^\dagger X_{\overline{A}} V, V^\dagger O_A V]|\tilde{\psi}\rangle = \langle\tilde{\psi}|V^\dagger[X_{\overline{A}}, O_A]V|\tilde{\psi}\rangle = 0$, which is a contradiction.
(3) $\implies$ (4): Consider arbitrary operators O_R on $\mathcal{H}_R$ and $X_{\overline{A}}$ on $\mathcal{H}_{\overline{A}}$. If we denote the constant of proportionality in 3.1.3 as $\lambda \in \mathbb{C}$, we have

$$P_{\text{code}} X_{\overline{A}} P_{\text{code}} = \lambda P_{\text{code}}, \tag{3.1.8}$$

so taking the inner product with $|\phi\rangle$:

$$\langle\phi|P_{\text{code}} X_{\overline{A}} P_{\text{code}}|\phi\rangle = \langle\phi|X_{\overline{A}}|\phi\rangle = \lambda\langle\phi|P_{\text{code}}|\phi\rangle = \lambda\langle\phi|\phi\rangle = \lambda, \tag{3.1.9}$$

so $\langle\phi|X_{\overline{A}}|\phi\rangle = \lambda$. But this implies

$$\begin{aligned} \langle\phi|X_{\overline{A}}O_R|\phi\rangle &= \langle\phi|P_{\text{code}}O_R X_{\overline{A}}P_{\text{code}}|\phi\rangle \\ &= \langle\phi|O_R P_{\text{code}}X_{\overline{A}}P_{\text{code}}|\phi\rangle \\ &= \langle\phi|O_R\lambda P_{\text{code}}|\phi\rangle \\ &= \langle\phi|O_R|\phi\rangle\,\langle\phi|X_{\overline{A}}|\phi\rangle \end{aligned} \tag{3.1.10}$$

since $P_{\text{code}}\,|\phi\rangle = |\phi\rangle$. Therefore, so long as $\langle\phi|O_R|\phi\rangle$ and $\langle\phi|X_{\overline{A}}|\phi\rangle$ are non-zero for any such O_R and $X_{\overline{A}}$, we have $\rho_{R\overline{A}}[\phi] = \rho_R[\phi]\otimes\rho_{\overline{A}}[\phi]$.
(4) $\implies$ (1): First, note that by definition, $|\phi\rangle$ is a purification of $\rho_{R\overline{A}}[\phi] = \rho_R[\phi]\otimes\rho_{\overline{A}}[\phi]$ on subsystem A. Also note that $|\phi\rangle$ maximally entangles R with A:

$$\rho_R[\phi] = \mathrm{Tr}_{A\overline{A}}\left(\frac{1}{|R|}\sum_{ij}|i\rangle\,\langle j|_R\,(V\,|\tilde{i}\rangle\,\langle\tilde{j}|\,V^\dagger)_{A\overline{A}}\right) = \frac{1}{|R|}\sum_i |i\rangle\,\langle i|_R = \frac{I_R}{|R|} \tag{3.1.11}$$

since $\rho_R[\phi] = I/|R|$ is the maximally mixed state. This means that 3.1.4 becomes

$$\rho_{R\overline{A}}[\phi] = \frac{I_R}{|R|}\otimes\rho_{\overline{A}}[\phi]. \tag{3.1.12}$$

Next, we perform long division on A. Say k is the largest integer such that $|A| = k|R| + r$ and $r < |R|$. Then, there exists a factorisation $\mathcal{H}_A = (\mathcal{H}_{A_1}\otimes\mathcal{H}_{A_2})\oplus\mathcal{H}_{A_3}$ such that $|A_1| = |R|$, $|A_2| = k$, and $|A_3| = r$.
We now define the following state:

$$|\Psi\rangle_{RA_1} \equiv \frac{1}{\sqrt{|R|}}\sum_i |i\rangle_R\,|i\rangle_{A_1}\,, \tag{3.1.13}$$

which is a purification of $\rho_R[\phi]$ on A_1. We also define $|\chi\rangle_{A_2\overline{A}}$ to be an arbitrary purification of $\rho_{\overline{A}}[\phi]$ on A_2. Note that the state

$$|\phi'\rangle \equiv |\Psi\rangle_{RA_1}\otimes|\chi\rangle_{A_2\overline{A}} \tag{3.1.14}$$

then purifies $\rho_{R\overline{A}}[\phi]$ on A_1A_2:

$$\begin{aligned} \mathrm{Tr}_{A_1A_2}\left(|\Psi\rangle\,\langle\Psi|_{RA_1}\otimes|\chi\rangle\,\langle\chi|_{A_2\overline{A}}\right) &= \mathrm{Tr}_{A_1}\left(|\Psi\rangle\,\langle\Psi|_{RA_1}\right)\mathrm{Tr}_{A_2}\left(|\chi\rangle\,\langle\chi|_{A_2\overline{A}}\right) \\ &= \rho_R[\phi]\otimes\rho_{\overline{A}}[\phi]. \end{aligned} \tag{3.1.15}$$

Such a factorisation exists since the R and $\overline{A}$ registers are unentangled in 3.1.12. In a purification, the dimension of the purifying system A_1 needs to be at least as big as the rank of the state being purified, so we therefore have $|A_1| = |R|$ (since $\rho_R[\phi]$ is maximally mixed), and $\mathrm{rank}\,(\rho_{\overline{A}}[\phi]) \leq |A_2|$.

However, purifications are unitarily equivalent on the purifying system - A in our case - so there exists a unitary U_A on $\mathcal{H}_A$ taking $|\phi\rangle = U_A |\phi'\rangle$. Overall, we therefore have:

$$
\begin{aligned}
(U_A \otimes I_{\overline{A}}) \left(\frac{1}{\sqrt{|R|}} \sum_i |i\rangle_R \, (V\, |\tilde{i}\rangle)_{A\overline{A}} \right) &= \frac{1}{\sqrt{|R|}} \sum_i |i\rangle_R \, |i\rangle_{A_1} \otimes |\chi\rangle_{A_2\overline{A}} \\
\implies (U_A \otimes I_{\overline{A}}) V\, |\tilde{i}\rangle_{A\overline{A}} &= |i\rangle_{A_1} \otimes |\chi\rangle_{A_2\overline{A}}
\end{aligned}
\tag{3.1.16}
$$

as claimed. □

One important facet of this theorem is that it does not specify the full set of subsystems $\overline{A}$ which can be erased and still corrected. It may be that some choices of $\overline{A}$ are not correctable; we need to apply the theorem to each choice in turn and check.
We now present two example of conventional erasure correction.

An Example

In this example, we refer to *qutrits*. A qutrit is exactly analogous to a qubit, except the underlying Hilbert space has three basis elements, which we denote $\{|\tilde{0}\rangle, |\tilde{1}\rangle, |\tilde{2}\rangle\}$. An arbitrary qutrit can then be written

$$
|\tilde{\psi}\rangle = \sum_{i=0}^{2} a_i \, |\tilde{i}\rangle \tag{3.1.17}
$$

where $\sum_{i=0}^{2} |a_i|^2 = 1$. Suppose Alice wishes to send this qutrit to Bob through a channel which acts to erase 1 of every three transmitted qutrits with certainty. To protect for this, Alice encodes her qutrit into the logical code subspace $\mathcal{H}_{\text{code}} = \text{span}(|0\rangle, |1\rangle, |2\rangle)$, defined by

$$
\begin{aligned}
|0\rangle &= \frac{1}{\sqrt{3}}(\widetilde{|000\rangle} + \widetilde{|111\rangle} + \widetilde{|222\rangle}) \\
|1\rangle &= \frac{1}{\sqrt{3}}(\widetilde{|012\rangle} + \widetilde{|120\rangle} + \widetilde{|201\rangle}). \\
|2\rangle &= \frac{1}{\sqrt{3}}(\widetilde{|021\rangle} + \widetilde{|102\rangle} + \widetilde{|210\rangle})
\end{aligned}
\tag{3.1.18}
$$

Explicitly, the encoding isometry V can be written

$$
V = |0\rangle \langle\tilde{0}| + |1\rangle \langle\tilde{1}| + |2\rangle \langle\tilde{2}| \,. \tag{3.1.19}
$$

Suppose that the erasure acts on the third qutrit of $\mathcal{H}_{\text{code}}$. Bob then only has access to the first two qutrits, but he can still recover the original state. Define a unitary operator on the first two qutrits by

$$\begin{aligned} U_{12} \equiv\, & |\widetilde{00}\rangle \langle\widetilde{00}| + |\widetilde{01}\rangle \langle\widetilde{11}| + |\widetilde{02}\rangle \langle\widetilde{22}| + |\widetilde{12}\rangle \langle\widetilde{01}| + |\widetilde{10}\rangle \langle\widetilde{12}| + |\widetilde{11}\rangle \langle\widetilde{20}| \\ & + |\widetilde{21}\rangle \langle\widetilde{02}| + |\widetilde{22}\rangle \langle\widetilde{10}| + |\widetilde{20}\rangle \langle\widetilde{21}| \,, \end{aligned} \tag{3.1.20}$$

which does nothing to $|\widetilde{00}\rangle$, and permutes the remaining 8 basis states as

$$|\widetilde{11}\rangle \to |\widetilde{01}\rangle \to |\widetilde{12}\rangle \to |\widetilde{10}\rangle \to |\widetilde{22}\rangle \to |\widetilde{02}\rangle \to |\widetilde{21}\rangle \to |\widetilde{20}\rangle \to |\widetilde{11}\rangle \,. \tag{3.1.21}$$

We can then compute that

$$(U_{12} \otimes I_3)\, |i\rangle = |\tilde{i}\rangle_1 \otimes \frac{1}{\sqrt{3}}(|\widetilde{00}\rangle + |\widetilde{11}\rangle + |\widetilde{22}\rangle)_{23} \equiv |\tilde{i}\rangle_1 \otimes |\chi\rangle_{23} \,, \tag{3.1.22}$$

which explicitly shows state recovery is possible given access to only the first two qutrits, since then

$$(U_{12} \otimes I_3)V\, |\tilde{\psi}\rangle = |\tilde{\psi}\rangle_1 \otimes |\chi\rangle_{23} \,. \tag{3.1.23}$$

This procedure holds irrelevant of which qutrit has been erased; we can just define a unitary operator with equivalent action to 3.1.20 acting on the remaining two qutrits. In terms of operator reconstructability 3.1.2. Suppose $\tilde{O}$ acts on the space of a single qutrit as

$$\tilde{O}\, |\tilde{i}\rangle = \sum_{j=0}^{2} (O)_{ji}\, |\tilde{j}\rangle \,. \tag{3.1.24}$$

We can then find a corresponding operator O_{12} on the first two qutrits of $\mathcal{H}_{\text{code}}$ which has an identical action to $\tilde{O}$ on the whole space

$$O_{12}\, |i\rangle = \sum_{j=0}^{2} (O)_{ji}\, |j\rangle \,. \tag{3.1.25}$$

This is done by just defining

$$O_{12} \equiv U_{12}^{\dagger} \tilde{O} U_{12} \tag{3.1.26}$$

where we take $\tilde{O}$ to act on the first qutrit only.

3.2 Subsystem Error Correction

The generalisation of conventional erasure correction which encompasses situations where we can recover some information on A and some on $\overline{A}$ is called *subsystem error correction*. This is theorem 2 of [5]. This theorem is as follows.

Theorem 3.2.1. *Let $V : \mathcal{H}_L \to \mathcal{H}$ be an encoding isometry, where $\mathcal{H}_L = \mathcal{H}_a \otimes \mathcal{H}_{\overline{a}}$ and $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$. Define orthonormal bases $\{|\tilde{i}\rangle\}$ of $\mathcal{H}_a$ and $\{|\tilde{j}\rangle\}$ of $\mathcal{H}_{\overline{a}}$, and let $|\phi\rangle \equiv \frac{1}{\sqrt{|R||\overline{R}|}} \sum_{i,j} |i\rangle_R |j\rangle_{\overline{R}} (V |\widetilde{ij}\rangle)_{A\overline{A}}$ where R and $\overline{R}$ are auxiliary systems with $\mathcal{H}_R = \mathcal{H}_a$ and $\mathcal{H}_{\overline{R}} = \mathcal{H}_{\overline{a}}$. The following statements are then equivalent:*

1. *$|a| \leq |A|$, and if we decompose $\mathcal{H}_A = (\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}) \oplus \mathcal{H}_{A_3}$, where $|A_1| = |a|$, and $|A_3| \leq |a|$, then there exists a unitary transformation U_A on $\mathcal{H}_A$ and a set of orthonormal states $|\chi_j\rangle_{A_2\overline{A}} \in \mathcal{H}_{A_2\overline{A}}$ such that*

$$(U_A \otimes I_{\overline{A}}) V |\widetilde{ij}\rangle = |i\rangle_{A_1} \otimes |\chi_j\rangle_{A_2\overline{A}}, \tag{3.2.1}$$

   where $\{|i\rangle_{A_1}\}$ is an orthonormal basis of $\mathcal{H}_{A_1}$.

2. *For any operator $\tilde{O}_a$ acting within $\mathcal{H}_a$, there exists an operator O_A on $\mathcal{H}_A$ such that for any state $|\tilde{\psi}\rangle \in \mathcal{H}_L$, we have*

$$\begin{aligned} O_A V |\tilde{\psi}\rangle &= V \tilde{O}_a |\tilde{\psi}\rangle \\ O_A^\dagger V |\tilde{\psi}\rangle &= V \tilde{O}_a^\dagger |\tilde{\psi}\rangle \end{aligned}. \tag{3.2.2}$$

3. *For any operator $X_{\overline{A}}$ on $\mathcal{H}_A$, we have*

$$P_{code} X_{\overline{A}} P_{code} = (I_a \otimes X_{\overline{a}}) P_{code}, \tag{3.2.3}$$

   where P_{code} is the projector onto the image of V; that is, if $P_L = \sum_{i,j} |\widetilde{ij}\rangle \langle \widetilde{ij}|$ is the projector onto $\mathcal{H}_L$, then $P_{code} = V P_L V^\dagger$.

4. *In the state $|\phi\rangle$, we have*

$$\rho_{R\overline{RA}}[\phi] = \rho_R[\phi] \otimes \rho_{\overline{RA}}[\phi]. \tag{3.2.4}$$

The proof of this is virtually identical to that of theorem 3.0.1, only that we must now keep track of the $\mathcal{H}_a$ subsystem. Moreover, it is a straightforward special case of *operator algebra error correction* in the next section, so we do not go through the proof.

An Example

3.3 Operator Algebra Error Correction

In this section, we present the third (and most general) theorem of [5]: operator algebra erasure correction. However, in order to make sense of this, we need the theory of *von Neumann algebras* on finite-dimensional Hilbert spaces. We present the necessary results here; readers looking for a more detailed exposition of von Neumann algebras should consult appendix A of [5], or [7] for a more ‘mathematical’ set of notes applicable to the infinite dimensional case.

3.3.1 von Neumann Algebras

Definition 3.3.1. A **von Neumann algebra** on a finite dimensional Hilbert space $\mathcal{H}$ is any set of linear operators $M \subseteq \mathcal{L}(\mathcal{H})$ such that:

- M contains all scalar multiples of the identity: $\forall \lambda \in \mathbb{C}$, $\lambda I \in M$, where I is the identity operator.
- M is closed under Hermitian conjugation: $\forall x \in M$, $x^\dagger \in M$.
- M is closed under multiplication: $\forall x, y \in M$, $xy \in M$.
- M is closed under addition: $\forall x, y \in M$, $x + y \in M$.

Note the notation of operators written in lower case rather than upper case as is common. This is because we are treating the operators as elements of an algebra, rather than individual operators in their own right. We will occasionally refer to a von Neumann algebra by its *generators*: the minimal set of operators which under the operations of conjugation, multiplication, and addition, can construct all other operators in M. We denote this $M = \langle x, y, \ldots \rangle$ for the algebra generated by $a, b, \ldots$.
Any von Neumann algebra induces two ‘natural’ associated algebras: the *commutant* and the *centre*.

Definition 3.3.2 (Commutant)**.** Given a von Neumann algebra M on $\mathcal{H}$, its **commutant**, denoted M', is the set of all operators on $\mathcal{H}$ which commute with M; that is

$$M' \equiv \{y \in \mathcal{L}(\mathcal{H}) \,|\, xy = yx,\, \forall x \in M\}. \tag{3.3.1}$$

Definition 3.3.3 (Centre)**.** Given a von Neumann algebra M on $\mathcal{H}$, its **centre**, denoted Z_M, is the set of all operators on $\mathcal{H}$ in both M and M'; that is

$$Z_M \equiv M \cap M'. \tag{3.3.2}$$

In classifying von Neumann algebras, there is a special role for algebras which have a centre containing only scalar multiples of the identity. Such an algebra is called a *factor*.

Definition 3.3.4 (Factor algebra)**.** A von Neumann algebra M on $\mathcal{H}$ is called a **factor** if Z_M contains only scalar multiples of the identity; that is

$$Z_M \equiv \langle I \rangle = \{\lambda I \,|\, \lambda \in \mathbb{C}\} \tag{3.3.3}$$

3.3.2 Classification of von Neumann Algebras

In order to apply the theory of von Neumann algebras to error correction, we need two powerful classification theorems. We first classify factor algebras.

Theorem 3.3.1. *Suppose M is a factor on $\mathcal{H}$. Then there exists a tensor factorisation $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$ such that $M = \mathcal{L}(\mathcal{H}_A) \otimes I_{\overline{A}}$ and $M' = I_A \otimes \mathcal{L}(\mathcal{H}_{\overline{A}})$.*

In other words, M induces a tensor factorisation $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$, and it is then the set of all linear operators on the tensor factor $\mathcal{H}_A$. For more general von Neumann algebras, this classification generalises to something called a *Wedderburn decomposition.*

Theorem 3.3.2. *Suppose M is a von Neumann algebra on $\mathcal{H}$. Then there exists a block-decomposition*

$$\mathcal{H} = \left[\, \oplus_\alpha \left(\mathcal{H}_{A_\alpha} \otimes \mathcal{H}_{\overline{A}_\alpha}\right)\right] \oplus \mathcal{H}_0 \tag{3.3.4}$$

in terms of which M and M' are block-diagonal, with corresponding decompositions

$$M = \left[\, \oplus_\alpha \left(\mathcal{L}(\mathcal{H}_{A_\alpha}) \otimes I_{\overline{A}_\alpha}\right)\right] \oplus 0, \quad M' = \left[\, \oplus_\alpha \left(I_{A_\alpha} \otimes \mathcal{L}(\mathcal{H}_{\overline{A}_\alpha})\right)\right] \oplus 0. \tag{3.3.5}$$

Here, $\mathcal{H}_0$ is the null space, and 0 is the zero operator on $\mathcal{H}_0$.

For ease of notation, we usually drop the direct sum with the null space. The decompositions 3.3.5 are called Wedderburn decompositions.

Examples

We now give a series of examples of these classification theorems to build intuition, beginning with the classification of factors.

Example 3.3.1. *The von Neumann algebra $M = \mathcal{L}(\mathbb{C}^2) \otimes I$ on $\mathcal{H} = \mathbb{C}^4$ is a factor. It has Wedderburn decomposition*

$$M = \mathcal{L}(\mathbb{C}^2) \otimes I = \begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{pmatrix}, \tag{3.3.6}$$

where $a, b, c, d \in \mathbb{C}$. The commutant is $M' = I \otimes \mathcal{L}(\mathbb{C}^2)$.

Our next example is a more complex one, exhibiting the block-diagonal structure of 3.3.5.

Example 3.3.2. *Consider the von Neumann algebra* $M = \langle Z \otimes I \otimes I, I \otimes X \otimes I, I \otimes Z \otimes I\rangle$, *where* X *and* Z *are Pauli matrices, over* $\mathcal{H} = \mathbb{C}^8$. *This induces a decomposition of* $\mathcal{H}$ *as*

$$\mathcal{H} = \oplus_{\alpha=1}^{2}(\mathbb{C}^2 \otimes \mathbb{C}^2), \tag{3.3.7}$$

and M *has Wedderburn decomposition*

$$M = \oplus_{\alpha=1}^{2}(\mathcal{L}(\mathbb{C}^2) \otimes I) = \left(\begin{array}{cccc|cccc} a & 0 & b & 0 & & & & \\ 0 & a & 0 & b & & & & \\ c & 0 & d & 0 & & \mathbf{0} & & \\ 0 & c & 0 & d & & & & \\ \hline & & & & e & 0 & f & 0 \\ & & & & 0 & e & 0 & f \\ & \mathbf{0} & & & g & 0 & h & 0 \\ & & & & 0 & g & 0 & h \end{array}\right), \tag{3.3.8}$$

where $a, \dots, h \in \mathbb{C}$. *The commutant is* $M' = \oplus_{\alpha=0}^{1}(I \otimes \mathcal{L}(\mathbb{C}^2))$.

So far this is all a bit abstract. With a view to linking this to error correction, suppose we have a von Neumann algebra M on $\mathcal{H}_L$. Then we have a decomposition

$$\mathcal{H}_L = \oplus_\alpha(\mathcal{H}_{L_\alpha} \otimes \mathcal{H}_{\overline{L}_\alpha}) \tag{3.3.9}$$

such that M is the set of all operators which are block diagonal in α, and acts as $\tilde{O}_{L_\alpha} \otimes I_{\overline{L}_\alpha}$ within each block, where $\tilde{O}_{L_\alpha}$ is an arbitrary linear operator on $\mathcal{H}_{L_\alpha}$. In matrix form, for some $\tilde{O} \in M$, we can write:

$$\tilde{O} = \begin{pmatrix} \tilde{O}_{L_1} \otimes I_{\overline{L}_1} & 0 & \cdots \\ 0 & \tilde{O}_{L_2} \otimes I_{\overline{L}_2} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}. \tag{3.3.10}$$

The commutant similarly consists of operators $\tilde{O}' \in M'$ which have matrix form:

$$\tilde{O}' = \begin{pmatrix} I_{L_1} \otimes \tilde{O}'_{\overline{L}_1} & 0 & \cdots \\ 0 & I_{L_2} \otimes \tilde{O}'_{\overline{L}_2} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}. \tag{3.3.11}$$

Also in matrix notation, the centre Z_M consists of operators $\tilde{\Lambda}$ of the form:

$$\tilde{\Lambda} = \begin{pmatrix} \lambda_1(I_{L_1} \otimes I_{\overline{L}_1}) & 0 & \cdots \\ 0 & \lambda_2(I_{L_2} \otimes I_{\overline{L}_2}) & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}, \tag{3.3.12}$$

where $\lambda_\alpha \in \mathbb{C}$.
We can actually introduce a basis for a Hilbert space $\mathcal{H}$ with a von Neumann algebra M, which is 'compatible' with the induced decomposition. Choose orthonormal bases $\{|\widetilde{\alpha, i}\rangle\}$ and $\{|\widetilde{\alpha, j}\rangle\}$ of $\mathcal{H}_{L_\alpha}$ and $\mathcal{H}_{\overline{L}_\alpha}$ respectively; we use these to build a basis for the entire Hilbert space

$$|\widetilde{\alpha, ij}\rangle \equiv |\widetilde{\alpha, i}\rangle \otimes |\widetilde{\alpha, j}\rangle \,. \tag{3.3.13}$$

3.3.3 Algebraic States and Entropy

Given a state ρ on $\mathcal{H}$ and a Hermitian operator O, the expectation value of O on ρ is typically defined as

$$\mathbb{E}_\rho(O) = \mathrm{Tr}(O\rho). \tag{3.3.14}$$

In what follows, we will often wish to compute the expectation values of operators in a von Neumann algebra M. An arbitrary state ρ is typically *not* an element of M, and contains more information than is necessary to compute expectations on M. This is the motivation for defining a so-called *algebraic state* - a version of the state which is in some sense 'visible' from M. We denote this by ρ_M. The following theorem precisely defines what we mean by this.

Theorem 3.3.3. *Suppose M is a von Neumann algebra on $\mathcal{H}$, and let $\rho \in End(\mathcal{H})$ be a state. Then, there exists a unique state $\rho_M \in M$ such that*

$$Tr(x\rho_M) = Tr(x\rho) \iff \mathbb{E}_{\rho_M}(x) = \mathbb{E}_\rho(x) \tag{3.3.15}$$

for all $x \in M$.

This theorem states that in computing expectation values of elements of M, we can replace ρ by ρ_M.
We can actually write down an explicit form for ρ_M. We do this for factors first. From 3.3.1, we know that if M is a factor on $\mathcal{H}$, then there exists a factorisation $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$ such that $M = \mathcal{L}(\mathcal{H}_A) \otimes I_{\overline{A}}$. Defining the reduced state

$$\rho_A \equiv \mathrm{Tr}_{\overline{A}}\rho, \tag{3.3.16}$$

we see that the unique algebraic state obeying 3.3.3 is just

$$\rho_M \equiv \rho_A \otimes \frac{I_{\overline{A}}}{|\overline{A}|}. \tag{3.3.17}$$

For a general von Neumann algebra, we can do similar. From 3.3.2, we know that if M is a von Neumann algebra on $\mathcal{H}$, then there exists a decomposition

$$\mathcal{H} = \oplus_\alpha(\mathcal{H}_{A_\alpha} \otimes \mathcal{H}_{\overline{A}_\alpha}), \tag{3.3.18}$$

in terms of which

$$M = \oplus_\alpha (\mathcal{L}(\mathcal{H}_{A_\alpha}) \otimes I_{\overline{A}_\alpha}). \tag{3.3.19}$$

Any state ρ can be written in block form with respect to the decomposition 3.3.18, and since M is block-diagonal, only the diagonal blocks of ρ will contribute to expectation values. We denote the $\alpha\alpha'$th block of ρ by $\rho_{\alpha\alpha'}$; we can then define

$$p_\alpha \rho_{A_\alpha} \equiv \mathrm{Tr}_{\overline{A}_\alpha} \rho_{\alpha\alpha}, \tag{3.3.20}$$

where $p_\alpha \in \mathbb{R}^+$, chosen so that $\mathrm{Tr}_{A_\alpha} \rho_{A_\alpha} = 1$. Since $\mathrm{Tr}\rho = 1$, we see that $\sum_\alpha p_\alpha = 1$, so the p_α can be interpreted as probabilities. Finally, we can define the unique algebraic state obeying 3.3.3 as

$$\rho_M \equiv \oplus_\alpha \left(p_\alpha \rho_{A_\alpha} \otimes \frac{I_{\overline{A}_\alpha}}{|\overline{A}_\alpha|} \right), \tag{3.3.21}$$

which is clearly Hermitian, non-negative, has trace one, and is of the form 3.3.18 and so is in M, and gives the same expectation values for any element of M.
From 3.3.17, we see that when M is a factor, the von Neumann entropy of ρ_M is equivalent to the von Neumann entropy of the reduced state ρ_A. This suggests that we should introduce a generalisation of the von Neumann entropy for a state ρ on an algebra M, which we define as follows:

Definition 3.3.5 (Algebraic entropy)**.** Let ρ be an arbitrary state, and M a von Neumann algebra. The algebraic entropy of ρ with respect to M is

$$S(\rho, M) \equiv -\sum_\alpha \mathrm{Tr}_{A_\alpha}(p_\alpha \rho_{A_\alpha} \log(p_\alpha \rho_{A_\alpha})) = -\sum_\alpha p_\alpha \log p_\alpha + \sum_\alpha p_\alpha S(\rho_{A_\alpha}) \tag{3.3.22}$$

where $S(\rho_{A_\alpha}) \equiv -\mathrm{Tr}_A(\rho_{A_\alpha} \log \rho_{A_\alpha})$ is the von Neumann entropy of the reduced state ρ_{A_α} as defined in 3.3.20.

We can interpret this as having two parts: a classical term consisting of the Shannon entropy $-\sum_\alpha p_\alpha \log p_\alpha$ of the probability distribution p_α, and a quantum term associated to the von Neumann entropies of each diagonal block of ρ, weighted by the probabilities. We clearly see that when M is a factor, this reduces to the standard von Neumann entropy since the classical Shannon entropy of the probabilities p_α vanishes.
We can also define the notion of *algebraic relative entropy.*

Definition 3.3.6. Given two states ρ, σ on M, the algebraic relative entropy between them is

$$S(\rho|\sigma, M) = \sum_\alpha p_\alpha^{\{\rho\}} \log \frac{p_\alpha^{\{\rho\}}}{p_\alpha^{\{\sigma\}}} + \sum_\alpha p_\alpha^{\{\rho\}} S(\rho_{A_\alpha}|\sigma_{A_\alpha}), \tag{3.3.23}$$

where $p_\alpha^{\{\rho\}}$ and $p_\alpha^{\{\sigma\}}$ are the probability distributions corresponding to ρ and σ respectively, and $S(\rho_{A_\alpha}|\sigma_{A_\alpha})$ is the relative entropy between ρ_{A_α} and σ_{A_α}.

There's a lot of notation here, so we present an example.

Example 3.3.3. *Consider the von Neumann algebra and Hilbert space of 3.3.2, which has two diagonal blocks given by $\alpha = 1, 2$. Consider the GHZ state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \in \mathcal{H}$. The density matrix of this state has diagonal blocks*

$$\rho_{11} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \rho_{22} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{3.3.24}$$

Tracing out the corresponding blocks, we find

$$\rho_{A_1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \rho_{A_1} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \tag{3.3.25}$$

and $p_1 = p_2 = 1/2$. We can then compute

$$S(\rho, M) = -2\left(\frac{1}{2}\log\frac{1}{2}\right) + \frac{1}{2}S(\rho_{A_1}) + \frac{1}{2}S(\rho_{A_2}) = 1. \tag{3.3.26}$$

3.4 Operator-Algebra Error Correction

We are now able to present theorem 5.1 of [5].

Theorem 3.4.1. *Let $V : \mathcal{H}_L \to \mathcal{H}$ be an encoding isometry with image $\mathcal{H}_{code} \subseteq \mathcal{H}$, where $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$. Say we have a von Neumann algebra M on $\mathcal{H}_L$. Define orthonormal basis $\{|\widetilde{\alpha, ij}\rangle\}$ of $\mathcal{H}_L$ as in 3.3.13, which is compatible with the decomposition $\mathcal{H}_L = \oplus_\alpha(\mathcal{H}_{L_\alpha} \otimes \mathcal{H}_{\overline{L}_\alpha})$ induced by M. Let $|\phi\rangle \equiv \frac{1}{\sqrt{|R|}}\sum_{\alpha,i,j}|\alpha, ij\rangle_R\,(V|\widetilde{\alpha, ij}\rangle)_{A\overline{A}}$, where R is an auxiliary system with $\mathcal{H}_R = \mathcal{H}_L$. The following statements are then equivalent:*

1. *$\sum_\alpha |L_\alpha| \leq |A|$, and we can decompose $\mathcal{H}_A = \oplus_\alpha(\mathcal{H}_{A_1^\alpha} \otimes \mathcal{H}_{A_2^\alpha}) \oplus \mathcal{H}_{A_3}$ with $|A_1^\alpha| = |L_\alpha|$ such that there exists a unitary transformation U_A on $\mathcal{H}_A$ and sets of orthonormal states $|\chi_{\alpha,j}\rangle_{A_2^\alpha\overline{A}} \in \mathcal{H}_{A_2^\alpha\overline{A}}$ such that*

   $$(U_A \otimes I_{\overline{A}})V|\widetilde{\alpha, ij}\rangle = |\alpha, i\rangle_{A_1^\alpha} \otimes |\chi_{\alpha,j}\rangle_{A_2^\alpha\overline{A}}, \tag{3.4.1}$$

   where $\{|\alpha, i\rangle_{A_1^\alpha}\}$ is an orthonormal basis for $\mathcal{H}_{A_1^\alpha}$.

2. *For any operator $\tilde{O} \in M$, there exists an operator O_A on $\mathcal{H}_A$ such that for any state $|\tilde{\psi}\rangle \in \mathcal{H}_L$, we have*

$$\begin{aligned} O_A V |\tilde{\psi}\rangle &= V\tilde{O} |\tilde{\psi}\rangle \\ O_A^\dagger V |\tilde{\psi}\rangle &= V\tilde{O}^\dagger |\tilde{\psi}\rangle . \end{aligned} \tag{3.4.2}$$

3. *For any operator $X_{\overline{A}}$ on $\mathcal{H}_{\overline{A}}$, we have*

$$P_{code} X_{\overline{A}} P_{code} = V X' V^\dagger P_{code}, \tag{3.4.3}$$

where $X' \in M'$ is an element of the commutant, and P_{code} is the image of the projector onto $\mathcal{H}_L$ under V (or the projector onto $\mathcal{H}_{code}$); that is, if $P_L = \sum_{\alpha,i,j} |\widetilde{\alpha, ij}\rangle \langle\widetilde{\alpha, ij}|$, then $P_{code} = V P_L V^\dagger$.

4. *For any operator $\tilde{O} \in M$, we have*

$$[O_R, \rho_{R\overline{A}}[\phi]] = 0, \tag{3.4.4}$$

where O_R is the unique operator on $\mathcal{H}_R$ such that

$$\begin{aligned} O_R |\phi\rangle &= V\tilde{O}V^\dagger |\phi\rangle \\ O_R^\dagger |\phi\rangle &= V\tilde{O}^\dagger V^\dagger |\phi\rangle . \end{aligned} \tag{3.4.5}$$

Similar to the last theorem, this characterises in some sense ‘how well’ a code subspace can correct a subalgebra M for the erasure of $\overline{A}$. In fact, it reduces to subsystem erasure correction when M is a factor, and to conventional erasure correction when $M = \mathcal{L}(\mathcal{H}_L)$ is the full set of linear operators on $\mathcal{H}_L$.

Proof. (1) $\implies$ (2): Define $O_A \equiv U_A^\dagger(\oplus_\alpha(O_{A_1^\alpha} \otimes I_{A_2^\alpha}))U_A$, where $O_{A_1^\alpha}$ is an operator acting on $\mathcal{H}_{A_1^\alpha}$ in the same way as $\tilde{O}_{a_\alpha}$ from 3.3.10 does on $\mathcal{H}_{a_\alpha}$. 3.4.1 is then immediate, following the same steps as in the proof of conventional erasure correction.

(2) $\implies$ (3): This implication is by contradiction. Suppose that $P_{\text{code}} X_{\overline{A}} P_{\text{code}} = V x' V^\dagger P_{\text{code}}$, where $x' \in \mathcal{L}(\mathcal{H}_L)$ but $x' \notin M'$. Therefore there must be some operator $\tilde{O} \in M$ which does not commute with x', and so there must be a state $|\tilde{\psi}\rangle \in \mathcal{H}_L$ such that

$$\langle\tilde{\psi}|[x', \tilde{O}]|\tilde{\psi}\rangle = \langle\tilde{\psi}|[V^\dagger P_{\text{code}} X_{\overline{A}} P_{\text{code}} V, \tilde{O}]|\tilde{\psi}\rangle = \langle\tilde{\psi}|V^\dagger[X_{\overline{A}}, V\tilde{O}V^\dagger]V|\tilde{\psi}\rangle \neq 0. \tag{3.4.6}$$

However, such an $\tilde{O}$ cannot have a corresponding O_A as this would automatically commute with $X_{\overline{A}}$, which contradicts 3.4.2.

(3) $\implies$ (4): Say $\tilde{O} \in M$, and $X_{\overline{A}}$ and Y_R are arbitrary operators on $\mathcal{H}_{\overline{A}}$ and $\mathcal{H}_R$ respectively. We then have:

$$\begin{aligned} \mathrm{Tr}_{R\overline{A}}(O_R \rho_{R\overline{A}}[\phi] X_{\overline{A}} Y_R) &= \langle \phi | X_{\overline{A}} Y_R O_R | \phi \rangle \\ &= \langle \phi | X_{\overline{A}} Y_R V \tilde{O} V^\dagger | \phi \rangle \\ &= \langle \phi | V \tilde{O} V^\dagger X_{\overline{A}} Y_R | \phi \rangle \\ &= \langle \phi | O_R X_{\overline{A}} Y_R | \phi \rangle \\ &= \mathrm{Tr}_{R\overline{A}}(\rho_{R\overline{A}}[\phi] O_R X_{\overline{A}} Y_R), \end{aligned} \tag{3.4.7}$$

where the first equality is by substituting in the definition of $\rho[\phi]$ and expanding, the second is by definition of O_R, the third is due to $V\tilde{O}V^\dagger$ commuting with Y_R trivially and with $X_{\overline{A}}$ by 3.4.3, and the last two by similar logic in reverse. This can only hold for arbitrary $X_{\overline{A}}$ and Y_R if $[O_R, \rho_{R\overline{A}}[\phi]] = 0$ as claimed.

(4) $\implies$ (1): Our basis $\{|\widetilde{\alpha, ij}\rangle_R\}$ for $\mathcal{H}_R$ gives a decomposition

$$\mathcal{H}_R = \oplus_\alpha (\mathcal{H}_{R_\alpha} \otimes \mathcal{H}_{\overline{R}_\alpha}) \tag{3.4.8}$$

and so $\mathcal{H}_{R\overline{A}} = \mathcal{H}_R \otimes \mathcal{H}_{\overline{A}}$ can be decomposed as

$$\mathcal{H}_{R\overline{A}} = \oplus_\alpha (\mathcal{H}_{R_\alpha} \otimes \mathcal{H}_{\overline{R}_\alpha} \otimes \mathcal{H}_{\overline{A}}). \tag{3.4.9}$$

From 3.4.4, we know that $[O_R, \rho_{R\overline{A}}[\phi]] = 0$ for all O_R as defined in 3.4.5. This means that $\rho_R[\phi] = I_R/|R|$ is the maximally mixed state on R. We therefore have that, in terms of this decomposition

$$\rho_{R\overline{A}}[\phi] = \oplus_\alpha \left[\frac{|R_\alpha||\overline{R}_\alpha|}{|R|} \left(\frac{I_{R_\alpha}}{|R_\alpha|} \otimes \rho_{\overline{R}_\alpha \overline{A}} \right) \right], \tag{3.4.10}$$

for some states $\rho_{\overline{R}_\alpha \overline{A}}$. The coefficient out the front can be computed by requiring that $\rho_{R\overline{A}}[\phi]$ is a valid density operator tracing to 1. Since $\rho_R[\phi] = I_R/|R|$, we must have also that $\mathrm{Tr}_{\overline{A}}(\rho_{\overline{R}_\alpha \overline{A}}) = I_{\overline{R}_\alpha}/|\overline{R}_\alpha|$.

By definition, $|\phi\rangle_{RA\overline{A}}$ is a purification of $\rho_{R\overline{A}}[\phi]$ on A, and in a purification the dimension of the purifying system is necessarily as big as the rank of the state being purified (this is immediate from the Schmidt decomposition). So, denoting $\mathrm{rank}(\rho_{\overline{R}_\alpha \overline{A}}) \equiv |\rho_{\overline{R}_\alpha \overline{A}}|$, we can write

$$\sum_\alpha |R_\alpha||\rho_{\overline{R}_\alpha \overline{A}}| \leq |A|. \tag{3.4.11}$$

This means that we can indeed decompose

$$\mathcal{H}_A = \oplus_\alpha (\mathcal{H}_{A_1^\alpha} \otimes \mathcal{H}_{A_2^\alpha}) \oplus \mathcal{H}_{A_3} \tag{3.4.12}$$

where $|A_1^\alpha| = |R_\alpha| = |L_\alpha|$ and $|A_2^\alpha| \geq |\rho_{\overline{R}_\alpha \overline{A}}|$ by long division. For each α, we can then purify $\rho_{\overline{R}_\alpha \overline{A}}$ on A_2^α; since $\mathrm{Tr}_{\overline{A}}(\rho_{\overline{R}_\alpha \overline{A}}) = I_{\overline{R}_\alpha}/|\overline{R}_\alpha|$, such a purification has the form

$$|\psi_\alpha\rangle_{\overline{R}_\alpha A_2^\alpha \overline{A}} = \frac{1}{\sqrt{|\overline{R}_\alpha|}} \sum_j |\alpha, j\rangle_{\overline{R}_\alpha} |\chi_{\alpha,j}\rangle_{A_2^\alpha \overline{A}}\,, \tag{3.4.13}$$

where the $|\chi_{\alpha,j}\rangle_{A_2^\alpha \overline{A}}$ are mutually orthonormal on $A_2^\alpha \overline{A}$. This means we can write a purification for $\rho_{R\overline{A}}$ on the full A system as

$$\begin{aligned} |\phi'\rangle &= \sum_{\alpha,i,j} \frac{1}{\sqrt{|R_\alpha|}} |\alpha, i\rangle_{R_\alpha} |\alpha, i\rangle_{A_1^\alpha} |\psi_\alpha\rangle_{\overline{R}_\alpha A_2^\alpha \overline{A}} \\ &= \frac{1}{\sqrt{|R|}} \sum_{\alpha,i,j} |\alpha, ij\rangle_R |\alpha, i\rangle_{A_1^\alpha} |\chi_{\alpha,j}\rangle_{A_2^\alpha \overline{A}}\,. \end{aligned} \tag{3.4.14}$$

Finally, since $|\phi\rangle$ and $|\phi'\rangle$ are two different purifications of $\rho_{R\overline{A}}[\phi]$ on A, they must differ by the action of some unitary U_A. We therefore have

$$\begin{aligned} (U_A \otimes I_{\overline{A}}) \left(\frac{1}{\sqrt{|R|}} \sum_{\alpha,i,j} |\alpha, ij\rangle_R \,(V\, |\widetilde{\alpha, ij}\rangle)_{A\overline{A}} \right) &= \frac{1}{\sqrt{|R|}} \sum_{\alpha,i,j} |\alpha, ij\rangle_R |\alpha, i\rangle_{A_1^\alpha} |\chi_{\alpha,j}\rangle_{A_2^\alpha \overline{A}} \\ \implies (U_A \otimes I_{\overline{A}}) V\, |\widetilde{\alpha, ij}\rangle &= |\alpha, i\rangle_{A_1^\alpha} \otimes |\chi_{\alpha,j}\rangle_{A_2^\alpha \overline{A}}\,, \end{aligned} \tag{3.4.15}$$

which finishes the proof. □

3.5 Holographic Properties of Erasure Codes

So far in this chapter, we have presented the three theorems of [5]. These are of increasing generality, and characterise the correctability of certain subsystems. However, we have yet to define what actually makes a code *holographic*. In high-energy physics, a holographic theory is one which posits a quantitative relationship between a gravitational theory and a non-gravitational theory 'on the boundary'. The most well known example of a holographic theory is the *AdS/CFT correspondence* [11], which describes a correspondence between a string theory on D-dimensional *anti-de Sitter space*, and a *conformal field theory* on its $D-1$-dimensional boundary. There is a so-called 'holographic dictionary', which precisely defines the links between objects in the gravitational bulk and the boundary CFT. One entry in this dictionary is the *Ryu-Takayanagi (RT) formula*, which describes the correspondence between the entropy of a boundary subregion A, and the entropy of the degrees of freedom in the gravitational bulk which are 'visible' from A:

$$S_A(\rho) = S_{\mathrm{bulk},A}(\rho) + \mathrm{Tr}(\mathcal{L}\rho). \tag{3.5.1}$$

Here, $\mathcal{L}$ is an operator acting on the bulk. It is this formula which can be interpreted in terms of quantum erasure correction. In fact, we can *define* what it means for an erasure correcting code to obey an RT formula as follows.

Definition 3.5.1. Say $V : \mathcal{H}_L \to \mathcal{H}$ is an encoding isometry, M is a von Neumann algebra on $\mathcal{H}_L$, and $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$ factorises. The triplet (V, A, M) has an RT formula if there exists an **area operator** $\mathcal{L} \in \mathcal{L}(\mathcal{H}_L)$ such that for any state ρ on $\mathcal{H}_L$:

$$S(\mathrm{Tr}_{\overline{A}}(V\rho V^\dagger)) = S(M, \rho) + \mathrm{Tr}(\rho\mathcal{L}). \tag{3.5.2}$$

Moreover, if $\mathcal{L} \propto I$, we say the RT formula is trivial.

It turns out that *any* operator-algebra erasure code obeying an additional condition called *complementary recovery* has an RT formula, with the converse also true. We say a triplet (V, A, M) has complementary recovery if not only does 3.4.2 hold for elements of M on $\mathcal{H}_A$, but also for elements of M' on $\mathcal{H}_{\overline{A}}$. That is, for any operator $\tilde{O}' \in M'$, there exists an operator $O_{\overline{A}}$ on $\mathcal{H}_{\overline{A}}$ such that for any state $|\tilde{\psi}\rangle \in \mathcal{H}_L$, we have

$$\begin{aligned} O_{\overline{A}} V |\tilde{\psi}\rangle &= V\tilde{O}' |\tilde{\psi}\rangle \\ O_{\overline{A}}^\dagger V |\tilde{\psi}\rangle &= V\tilde{O}'^\dagger |\tilde{\psi}\rangle \,. \end{aligned} \tag{3.5.3}$$

We can then state and prove the following theorem:

Theorem 3.5.1. *Say $V : \mathcal{H}_L \to \mathcal{H}$ is an encoding isometry, M is a von Neumann algebra on $\mathcal{H}$, and $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$ factorises. Also say that (V, A, M) has complementary recovery. Then, (V, A, M) and $(V, \overline{A}, M')$ both have an RT formula with the same area operator $\mathcal{L}$, and $\mathcal{L} \in Z_M$ is in the centre. Moreover, if (V, A, M) and $(V, \overline{A}, M)$ both have an RT formula with the same $\mathcal{L}$, then (V, A, M) have complementary recovery.*

To make the (rather dense) proof easier to follow, we present some initial lemmas first. The proofs of these are given in appendix A.

Lemma 3.5.1 (Uniqueness)**.** *Say V is an encoding isometry, and A is a subregion. Let $M \equiv V^\dagger(\mathcal{L}(\mathcal{H}_A) \otimes I_{\overline{A}})V$ be the image of operators on $\mathcal{H}_A$ projected onto $\mathcal{H}_L$. If M is a von Neumann algebra, then it is the unique von Neumann algebra for which complementary recovery is satisfied. If it is not, then no von Neumann algebra satisfying complementary recovery exists.*

Lemma 3.5.2. *To linear order, an arbitrary variation $\delta\rho$ satisfying $Tr\delta\rho = 0$ of the von Neumann entropy of a state σ satisfies*

$$\delta S(\rho) \equiv S(\sigma + \delta\rho) - S(\sigma) = -\,Tr\,(\delta\rho \log \sigma)\,. \tag{3.5.4}$$

Lemma 3.5.3. *To linear order, an arbitrary variation $\delta\rho$ satisfying $Tr\delta\rho = 0$ of the algebraic entropy of a state σ satisfies*

$$\delta S(\sigma, M) \equiv S(\sigma + \delta\rho, M) - S(\sigma, M) = -\sum_{\alpha} Tr\left(\delta\rho\left(\log\left(p_{\alpha}^{\{\sigma\}}\sigma_{L_\alpha}\right) \otimes I_{\overline{L}_\alpha}\right)\right). \tag{3.5.5}$$

The proof of 3.5.1 is then as follows.

Proof. ($\Longrightarrow$): Suppose M induces the decomposition $\mathcal{H}_L = \oplus_\alpha(\mathcal{H}_{L_\alpha} \otimes \mathcal{H}_{\overline{L}_\alpha})$, so M and M' have Wedderburn decompositions

$$M = \oplus_\alpha(\mathcal{L}(\mathcal{H}_{L_\alpha}) \otimes I_{\overline{L}_\alpha}), \quad M' = \oplus_\alpha(I_{L_\alpha} \otimes \mathcal{L}(\mathcal{H}_{\overline{L}_\alpha})). \tag{3.5.6}$$

Let $\{|\widetilde{\alpha, ij}\rangle\} = \{|\widetilde{\alpha, i}\rangle_{L_\alpha} \otimes |\widetilde{\alpha, j}\rangle_{\overline{L}_\alpha}\}$ be the basis of $\mathcal{H}_L$ which is compatible with M in the sense of 3.3.13. By the equivalence of 3.4.1 and 3.4.2 in theorem 3.4.1 and complementary recovery, we know there exist factorisations

$$\mathcal{H}_A = \oplus_\alpha(\mathcal{H}_{A_1^\alpha} \otimes \mathcal{H}_{A_2^\alpha}) \oplus \mathcal{H}_{A_3}, \quad \mathcal{H}_{\overline{A}} = \oplus_\alpha(\mathcal{H}_{\overline{A}_1^\alpha} \otimes \mathcal{H}_{\overline{A}_2^\alpha}) \oplus \mathcal{H}_{\overline{A}_3} \tag{3.5.7}$$

and unitaries $U_A \in \mathcal{L}(\mathcal{H}_A)$ and $U_{\overline{A}} \in \mathcal{L}(\mathcal{H}_{\overline{A}})$ such that

$$\begin{aligned} (U_A \otimes I_{\overline{A}})V\,|\widetilde{\alpha, i, j}\rangle &= |\alpha, i\rangle_{A_1^\alpha} \otimes |\chi_{\alpha,j}\rangle_{A_2^\alpha\overline{A}} \\ (I_A \otimes U_{\overline{A}})V\,|\widetilde{\alpha, i, j}\rangle &= |\overline{\chi}_{\alpha,i}\rangle_{A\overline{A}_2^\alpha} \otimes |\alpha, j\rangle_{\overline{A}_1^\alpha}. \end{aligned} \tag{3.5.8}$$

If we apply $(U_A \otimes I_{\overline{A}})$ and $(I_A \otimes U_{\overline{A}})$ sequentially, we see that

$$\begin{aligned} (I_A \otimes U_{\overline{A}})(U_A \otimes I_A)V\,|\widetilde{\alpha, i, j}\rangle &= |\alpha, i\rangle_{A_1^\alpha} \otimes (I_{A_2^\alpha} \otimes U_{\overline{A}})\,|\chi_{\alpha,j}\rangle_{A_2^\alpha\overline{A}} \\ (U_A \otimes I_A)(I_A \otimes U_{\overline{A}})V\,|\widetilde{\alpha, i, j}\rangle &= (U_A \otimes I_{\overline{A}_2^\alpha})\,|\overline{\chi}_{\alpha,i}\rangle_{A\overline{A}_2^\alpha} \otimes |\alpha, j\rangle_{\overline{A}_1^\alpha} \end{aligned} \tag{3.5.9}$$

In order for both of these to be true simultaneously, there therefore must exist states $|\chi_\alpha\rangle_{A_2^\alpha\overline{A}_2^\alpha}$ such that $(I_{A_2^\alpha} \otimes U_{\overline{A}})\,|\chi_{\alpha,j}\rangle_{A_2^\alpha\overline{A}} = |\chi_\alpha\rangle_{A_2^\alpha\overline{A}_2^\alpha} \otimes |\alpha, j\rangle_{\overline{A}_1^\alpha}$, which implies

$$(U_A \otimes U_{\overline{A}})V\,|\widetilde{\alpha, i, j}\rangle = |\alpha, i\rangle_{A_1^\alpha} \otimes |\chi_\alpha\rangle_{A_2^\alpha\overline{A}_2^\alpha} \otimes |\alpha, j\rangle_{\overline{A}_1^\alpha}. \tag{3.5.10}$$

This is the key fact which allows us to prove an RT formula.To do this, we suppose ρ is a state with support on $\mathcal{H}_L$, and we compute $S(M, \rho)$ and $S(\mathrm{Tr}_{\overline{A}}(V\rho V^\dagger))$ and take their difference.
Instead of considering $S(\mathrm{Tr}_{\overline{A}}(V\rho V^\dagger))$ we might as well consider $S(\mathrm{Tr}_{\overline{A}}(V\rho_M V^\dagger))$. To see why, set $O_A \in \mathcal{L}(\mathcal{H}_A)$, and compute

$$\mathrm{Tr}(O_A \cdot \mathrm{Tr}_{\overline{A}}(V\rho V^\dagger)) = \mathrm{Tr}((O_A \otimes I_{\overline{A}}) \cdot V\rho V^\dagger) = \mathrm{Tr}(V^\dagger(O_A \otimes I_{\overline{A}})V \cdot \rho). \tag{3.5.11}$$

by cyclicity of the trace. But $V^\dagger(O_A \otimes I_{\overline{A}})V \in M$ by uniqueness, and for any $\tilde{O} \in M$ we have $\mathrm{Tr}(\tilde{O}\rho) = \mathrm{Tr}(\tilde{O}\rho_M)$, we can just consider ρ_M in the above. Since the states $\mathrm{Tr}_{\overline{A}}(V\rho V^\dagger)$ and $\mathrm{Tr}_{\overline{A}}(V\rho_M V^\dagger)$ have the same expectation for all observables in M, they are the same state and so have the same entropy. Acting with a unitary on $\mathcal{H}_A$ and $\mathcal{H}_{\overline{A}}$ separately does not change the entropy, so we have:

$$S(\mathrm{Tr}_{\overline{A}}(V\rho_M V^\dagger)) = S(\mathrm{Tr}_{\overline{A}}((U_A \otimes U_{\overline{A}})V\rho_M V^\dagger(U_A \otimes U_{\overline{A}})^\dagger)). \tag{3.5.12}$$

The next step is to define isometries $\tilde{V}_\alpha : (\mathcal{H}_{L_\alpha} \otimes \mathcal{H}_{\overline{L}_\alpha}) \to (\mathcal{H}_{A_1^\alpha} \otimes \mathcal{H}_{\overline{A}_1^\alpha})$ using the states $|\alpha, i\rangle_{A_1^\alpha}$ and $|\alpha, j\rangle_{\overline{A}_1^\alpha}$:

$$\tilde{V}_\alpha |\widetilde{\alpha, i, j}\rangle \equiv |\psi_{\alpha,i}\rangle_{A_1^\alpha} \otimes |\alpha, j\rangle_{\overline{A}_1^\alpha}. \tag{3.5.13}$$

which is certainly an isometry since $|\alpha, i\rangle_{A_1^\alpha}$ and $|\alpha, j\rangle_{\overline{A}_1^\alpha}$ are orthonormal bases for $\mathcal{H}_{A_1^\alpha}$ and $\mathcal{H}_{\overline{A}_1^\alpha}$ respectively.
$\tilde{V}_\alpha$ then lets us rewrite 3.5.10 as

$$(U_A \otimes U_{\overline{A}})V |\widetilde{\alpha, i, j}\rangle = \tilde{V}_\alpha |\widetilde{\alpha, i, j}\rangle \otimes |\chi_\alpha\rangle_{A_2^\alpha \overline{A}_2^\alpha}. \tag{3.5.14}$$

which lets us further simplify $(U_A \otimes U_{\overline{A}})V\rho_M V^\dagger(U_A \otimes U_{\overline{A}})^\dagger$:

$$\begin{aligned}
&(U_A \otimes U_{\overline{A}})V\rho_M V^\dagger(U_A \otimes U_{\overline{A}})^\dagger) \\
&= \sum_\alpha p_\alpha \cdot (U_A \otimes U_{\overline{A}})V\rho_{L_\alpha}V^\dagger(U_A \otimes U_{\overline{A}})^\dagger \\
&= \sum_\alpha p_\alpha \cdot \frac{1}{p_\alpha}\sum_{i,j}\sum_{i',j'}(\rho_{\alpha\alpha})_{i,j,i',j'}(U_A \otimes U_{\overline{A}})V |\widetilde{\alpha, i, j}\rangle \langle\widetilde{\alpha, i', j'}| V^\dagger(U_A \otimes U_{\overline{A}})^\dagger \\
&= \sum_\alpha p_\alpha \cdot \frac{1}{p_\alpha}\sum_{i,j}\sum_{i',j'}(\rho_{\alpha\alpha})_{i,j,i',j'}\tilde{V}_\alpha |\widetilde{\alpha, i, j}\rangle \langle\widetilde{\alpha, i', j'}| \tilde{V}_\alpha^\dagger \otimes |\chi_\alpha\rangle\langle\chi_\alpha| \\
&= \sum_\alpha p_\alpha \cdot \tilde{V}_\alpha\rho_{L_\alpha}\tilde{V}_\alpha^\dagger \otimes |\chi_\alpha\rangle\langle\chi_\alpha|.
\end{aligned} \tag{3.5.15}$$

Here, the coefficients $(\rho_{\alpha\alpha})_{i,j,i',j'}$ are defined by the decomposition of ρ with respect to the Hilbert space decomposition of $\mathcal{H}_L$ written as

$$\rho = \sum_{\alpha,\alpha'}\sum_{i,j}\sum_{i',j'}(\rho_{\alpha\alpha})_{i,j,i',j'} |\widetilde{\alpha, i, j}\rangle \langle\widetilde{\alpha, i', j'}|. \tag{3.5.16}$$

Each of the states $\tilde{V}_\alpha\rho_{L_\alpha}\tilde{V}_\alpha^\dagger \otimes |\chi_\alpha\rangle\langle\chi_\alpha|$ are normalised and act on different blocks, so we can compute the entropy as

$$\begin{aligned}
S(\mathrm{Tr}_{\overline{A}}(V\rho V^\dagger)) &= -\sum_\alpha p_\alpha \log p_\alpha + \sum_\alpha p_\alpha S(\mathrm{Tr}_{\overline{A}}(\tilde{V}_\alpha\rho_\alpha\tilde{V}_\alpha^\dagger \otimes |\chi_\alpha\rangle\langle\chi_\alpha|)) \\
&= -\sum_\alpha p_\alpha \log(p_\alpha) + \sum_\alpha p_\alpha S(\mathrm{Tr}_{\overline{A}}(\tilde{V}_\alpha\rho_\alpha\tilde{V}_\alpha^\dagger)) + \sum_\alpha p_\alpha S(\mathrm{Tr}_{\overline{A}}(|\chi_\alpha\rangle\langle\chi_\alpha|)).
\end{aligned} \tag{3.5.17}$$

Now, since $|\alpha, j\rangle$ is independent of i, we further have that

$$S(\mathrm{Tr}_{\overline{A}}(\tilde{V}_\alpha \rho_{L_\alpha} \tilde{V}_\alpha^\dagger)) = S(\mathrm{Tr}_{\overline{A}_1^\alpha}(\tilde{V}_\alpha \rho_{L_\alpha} \tilde{V}_\alpha^\dagger)) = S(\mathrm{Tr}_{\overline{L}_\alpha}(\rho_{L_\alpha})) = S(\rho_{L_\alpha}). \tag{3.5.18}$$

Now, the first two terms of 3.5.17 are just $S(\rho, M)$, so we have

$$S(\mathrm{Tr}_{\overline{A}}(V\rho V^\dagger)) - S(\rho, M) = \sum_\alpha p_\alpha S(\mathrm{Tr}_{\overline{A}}(|\chi_\alpha\rangle\langle\chi_\alpha|)). \tag{3.5.19}$$

The RHS is linear in p_α, so must be linear in ρ also. This means there exists an area operator $\mathcal{L}$ such that the RHS can be written as $\mathrm{Tr}(\rho\mathcal{L})$. Explicitly, we define

$$\begin{aligned} I_\alpha &\equiv \sum_{i,j} |\widetilde{\alpha, i, j}\rangle\langle\widetilde{\alpha, i, j}| \\ \mathcal{L} &\equiv \sum_\alpha S(\mathrm{Tr}_{\overline{A}}(|\chi_\alpha\rangle\langle\chi_\alpha|)) \cdot I_\alpha \end{aligned} \tag{3.5.20}$$

which gives $\mathcal{L} \in M$, and so $\mathrm{Tr}(\rho\mathcal{L}) = \mathrm{Tr}(\rho_M\mathcal{L})$, and we can write

$$\begin{aligned} \mathrm{Tr}(\rho_M\mathcal{L}) &= \mathrm{Tr}\left(\sum_\alpha p_{L_\alpha}\rho_\alpha \cdot \sum_\alpha S(\mathrm{Tr}_{\overline{A}}(|\chi_\alpha\rangle\langle\chi_\alpha|)) \cdot I_\alpha\right) \\ &= \sum_\alpha p_\alpha S(\mathrm{Tr}_{\overline{A}}(|\chi_\alpha\rangle\langle\chi_\alpha|)) \cdot \mathrm{Tr}(\rho_{L_\alpha} I_\alpha) \\ &= S(\mathrm{Tr}_{\overline{A}}(V\rho V^\dagger)) - S(\rho, M), \end{aligned} \tag{3.5.21}$$

so (V, A, M) satisfy an RT formula with area operator $\mathcal{L}$, and $\mathcal{L} \in M$. We can do the same derivation for $(V, \overline{A}, M')$ with $i \leftrightarrow j$, and since $\mathcal{L} \in M'$, $\mathcal{L} \in Z_M$ as claimed.

($\Longleftarrow$): From lemmas 3.5.2 and 3.5.3, we know that for a state σ on $\mathcal{H}_L$ and arbitrary variation $\delta\rho$, we have

$$\begin{aligned} S\left(\mathrm{Tr}_{\overline{A}}\left(V(\sigma+\delta\rho)V^\dagger\right)\right) - S\left(\mathrm{Tr}_{\overline{A}}\left(V\sigma V^\dagger\right)\right) &= -\mathrm{Tr}\left(\mathrm{Tr}_{\overline{A}}\left(V\delta\rho V^\dagger\right)\log\mathrm{Tr}_{\overline{A}}\left(V\sigma V^\dagger\right)\right) \\ S(\sigma+\delta\rho, M) - S(\sigma, M) &= -\sum_\alpha \mathrm{Tr}\left(\delta\rho\left(\log\left(p_\alpha^{\{\sigma\}}\sigma_{L_\alpha}\right)\otimes I_{\overline{L}_\alpha}\right)\right) \end{aligned} \tag{3.5.22}$$

Also, recall the RT formula 3.5.2:

$$S\left(\mathrm{Tr}_{\overline{A}}\left(V\rho V^\dagger\right)\right) = S(\rho, M) + \mathrm{Tr}(\rho\mathcal{L}). \tag{3.5.23}$$

If the RT formula holds, for any state σ on $\mathcal{H}_L$ with small perturbation $\delta\rho$, we therefore have:

$$\begin{aligned} S\left(\mathrm{Tr}_{\overline{A}}\left(V(\sigma+\delta\rho)V^\dagger\right)\right) - S\left(\mathrm{Tr}_{\overline{A}}\left(V\sigma V^\dagger\right)\right) &= S(\sigma+\delta\rho, M) - S(\sigma, M) + \mathrm{Tr}((\sigma+\delta\rho)\mathcal{L}) - \mathrm{Tr}(\sigma\mathcal{L}) \\ \implies \mathrm{Tr}\left(\mathrm{Tr}_{\overline{A}}\left(V\delta\rho V^\dagger\right)\log\mathrm{Tr}_{\overline{A}}\left(V\sigma V^\dagger\right)\right) &= \sum_\alpha \mathrm{Tr}\left(\delta\rho\left(\log\left(p_\alpha^{\{\sigma\}}\sigma_{L_\alpha}\right)\otimes I_{\overline{L}_\alpha}\right) - \mathcal{L}\right). \end{aligned} \tag{3.5.24}$$

Both sides are linear in $\delta\rho$, and so we can integrate over all such perturbations to obtain

$$\mathrm{Tr}\left(\mathrm{Tr}_{\overline{A}}\left(V\rho V^{\dagger}\right)\log \mathrm{Tr}_{\overline{A}}\left(V\sigma V^{\dagger}\right)\right) = \sum_{\alpha} \mathrm{Tr}\left(\rho\left(\left(\log\left(p_{\alpha}^{\{\sigma\}}\sigma_{L_{\alpha}}\right)\otimes I_{\overline{L}_{\alpha}}\right)-\mathcal{L}\right)\right). \tag{3.5.25}$$

The next step is to calculate the relative entropy:

$$\begin{aligned} S\big(\mathrm{Tr}_{\overline{A}}\big(V\rho V^{\dagger}\big)\,|\mathrm{Tr}_{\overline{A}}\big(V\sigma V^{\dagger}\big)\big) &= \mathrm{Tr}\big(\mathrm{Tr}_{\overline{A}}\big(V\rho V^{\dagger}\big)\log\big(\mathrm{Tr}_{\overline{A}}\big(V\rho V^{\dagger}\big)\big)\big) - \mathrm{Tr}\big(\mathrm{Tr}_{\overline{A}}\big(V\rho V^{\dagger}\big)\log\big(\mathrm{Tr}_{\overline{A}}\big(V\sigma \\ &= -S\big(\mathrm{Tr}_{\overline{A}}\big(V\rho V^{\dagger}\big)\big) - \sum_{\alpha}\mathrm{Tr}\big(\rho\big(\big(\log\big(p_{\alpha}^{\{\sigma\}}\sigma_{L_{\alpha}}\big)\otimes I_{\overline{L}_{\alpha}}\big)-\mathcal{L}\big)\big) \\ &= -S(\rho, M) - \sum_{\alpha}\mathrm{Tr}\big(\rho\big(\big(\log\big(p_{\alpha}^{\{\sigma\}}\sigma_{L_{\alpha}}\big)\otimes I_{\overline{L}_{\alpha}}\big)\big)\big) \\ &= -S(\rho, M) - \sum_{\alpha}\mathrm{Tr}\big(p_{\alpha}^{\{\rho\}}\rho_{L_{\alpha}}\log\big(p_{\alpha}^{\{\sigma\}}\sigma_{L_{\alpha}}\big)\big) \\ &= S(\rho|\sigma, M), \end{aligned} \tag{3.5.26}$$

where we use 3.5.25 in the second line, and the RT formula in the third. We can perform the same argument with $A \leftrightarrow \overline{A}$ and $M \leftrightarrow M'$, and we find similarly that

$$S(\mathrm{Tr}_{A}(V\rho V^{\dagger})|\mathrm{Tr}_{\overline{A}}(V\sigma V^{\dagger})) = S(\rho|\sigma, M'). \tag{3.5.27}$$

These two conditions together in fact imply complementary recovery. Consider an arbitrary state $|\tilde{\psi}\rangle \in \mathcal{H}_L$, an arbitrary operator $X_{\overline{A}}$ on $\mathcal{H}_{\overline{A}}$, and an operator $\tilde{O} \in M$. von Neumann algebras are spanned by their Hermitian elements, so we can take $\tilde{O}$ to be Hermitian. Now, consider

$$\langle\tilde{\psi}|e^{-i\lambda\tilde{O}}V^{\dagger}X_{\overline{A}}Ve^{i\lambda\tilde{O}}|\tilde{\psi}\rangle = \langle\tilde{\psi}|e^{-i\lambda\tilde{O}}P_L V^{\dagger}X_{\overline{A}}VP_L e^{i\lambda\tilde{O}}|\tilde{\psi}\rangle\,. \tag{3.5.28}$$

We show that this is independent of λ. Define

$$|\tilde{\psi}(\lambda)\rangle \equiv e^{i\lambda\tilde{O}}\,|\tilde{\psi}\rangle\,, \tag{3.5.29}$$

and note that for any $\tilde{O}' \in M'$, we have that the expectation $\langle\tilde{\psi}(\lambda)|\tilde{O}'|\tilde{\psi}(\lambda)\rangle$ is independent of λ. Since for any state ρ, there is a corresponding $\rho_{M'}$ such that $\mathbb{E}_{\rho}(x') = \mathbb{E}_{\rho_{M'}}(x)$ for any $x' \in M'$, the state $(\tilde{\psi}(\lambda))_{M'}$ corresponding to $\tilde{\psi}(\lambda) \equiv |\tilde{\psi}(\lambda)\rangle\langle\tilde{\psi}(\lambda)|$ is also independent of λ. Therefore, for any two λ, λ', $(\tilde{\psi}(\lambda))_{M'} = (\tilde{\psi}(\lambda'))_{M'}$, which means

$$S(\tilde{\psi}(\lambda)|\tilde{\psi}(\lambda'), M') = 0. \tag{3.5.30}$$

So, from 3.5.27, we have

$$0 = S(\tilde{\psi}(\lambda)|\tilde{\psi}(\lambda'), M') = S(\mathrm{Tr}_{A}(V\tilde{\psi}(\lambda)V^{\dagger})|\mathrm{Tr}_{\overline{A}}(V\tilde{\psi}(\lambda')V^{\dagger})), \tag{3.5.31}$$

which further implies that $\mathrm{Tr}_A(V\tilde{\psi}(\lambda)V^\dagger)$ is independent of λ, which itself implies that $|\tilde{\psi}(\lambda)\rangle$ itself is independent of λ. Returning to 3.5.28, we see that it is independent of λ, and so in particular its first variation with respect to λ must vanish. This is proportional to $\langle\tilde{\psi}|[P_L V^\dagger X_{\overline{A}} V P_L, \tilde{O}]|\tilde{\psi}\rangle$, so we have

$$0 = \langle\tilde{\psi}|[P_L V^\dagger X_{\overline{A}} V P_L, \tilde{O}]|\tilde{\psi}\rangle = \langle\tilde{\psi}|[V^\dagger P_{\mathrm{code}} X_{\overline{A}} P_{\mathrm{code}} V, \tilde{O}]|\tilde{\psi}\rangle \tag{3.5.32}$$

which just implies 3.4.3 and hence 3.4.2. Since we can repeat this argument again with $M \leftrightarrow M'$ and $A \leftrightarrow \overline{A}$, we establish complementary recovery as claimed. □

Chapter 4

Approximate and Non-Isometric Codes

So far, we have discussed *exact* codes - ones which perfectly recover information. In practice, exact codes are almost impossible to implement, and some information will be lost in correcting errors. To talk about this precisely, we need the notion of *approximate error correction*.

4.1 Approximate and State Specific Codes

Consider the statement of theorem 3.1.1. In the language of density operators, this can be rewritten as saying that for all states $|\tilde{\psi}\rangle \in \mathcal{H}_L$, we have

$$\psi_{\overline{A}} \equiv \mathrm{Tr}_A \left(V |\tilde{\psi}\rangle \langle\tilde{\psi}| V^\dagger \right) = \chi_{\overline{A}}, \tag{4.1.1}$$

where $\chi_{\overline{A}} \equiv \mathrm{Tr}_A \left(|\chi\rangle \langle\chi|\right)$. The fact that $\chi_{\overline{A}}$ is fixed for *all* such states $|\tilde{\psi}\rangle$ is a reflection of the fact that for exact erasure correction, the $\overline{A}$ subsystem must know zero information about the A system. For approximate erasure correction, we need to be more careful. Suppose we replaced 4.1.1 with a directly approximate version[1]:

$$\|\psi_{\overline{A}} - \chi_{\overline{A}}\|_1 \leq \epsilon \tag{4.1.2}$$

for $\epsilon > 0$.

[1] Here, $\|X\|_1 \equiv \mathrm{Tr}\sqrt{X^\dagger X}$ is called the *trace norm*. We could equivalently replace it with e.g. fidelity.

Chapter 5

Conclusions

This is the place to put your conclusions about your work. You can split it into different sections if appropriate. You may want to include a section of future work which could be carried out to continue your research.

The conclusion section should be at least one page long, preferably 2 pages, but not much longer.

Appendix A

Quantum Mechanics and Information: Background and Conventions

In this appendix, I outline the background and conventions used for quantum mechanics and quantum information theory throughout this dissertation in detail. I mainly stick to the description of quantum mechanics as given in Nielsen and Chuang's textbook [13] and the notes of David Skinner, and supplement Nielsen and Chuang's description of quantum information and computing with notes by Richard Jozsa and John Preskill.

A.1 Quantum Mechanics

I begin with a discussion of the four defining postulates of quantum mechanics.

A.1.1 State Spaces

Postulate 1. Any isolated quantum system has an associated Hilbert space $\mathcal{H}$ called the *state space* of the system. The system is fully described by its *state vector* (or just *state*), which is a unit vector $|\psi\rangle \in \mathcal{H}$.

Note that this just tells us that the state space for a system exists, and not necessarily what the relevant Hilbert space is. The simplest example of a non-trivial system is that of the two-dimensional *qubit*, with state space denoted $\mathcal{H}_2$. An orthonormal basis of this space is given by the set $\{|0\rangle, |1\rangle\}$, so the state of a qubit can be written

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \quad a, b \in \mathbb{C} \tag{A.1.1}$$

with the condition that $|\psi\rangle$ is a unit vector (i.e. $\langle\psi,\psi\rangle = 1$) implying that $|a|^2 + |b|^2 = 1$. We say that $|\psi\rangle$ is in a *superposition* of $|0\rangle$ and $|1\rangle$, with *amplitudes* a and b, which generalises in the obvious way to arbitrary linear combinations of states.

A.1.2 Evolution of States

Postulate 2. The evolution in time of a *closed* quantum system is described by a unitary transformation. Explicitly, if $|\psi, t\rangle$ is the state of a system at time t, and $|\psi', t'\rangle$ is the state at time t', then the two states are related by some unitary operator $U(t, t')$ depending only on times t and t' such that

$$|\psi', t'\rangle = U(t, t')\,|\psi, t\rangle \tag{A.1.2}$$

Again, this does not tell us which unitary operators describe the dynamics of a real-world system. On a simple system such as a qubit, it turns out that any unitary operator can be realised. For example, the Pauli matrix X which takes $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$ is a unitary operator on a single qubit which can always be physically implemented. Note that this postulate generalises to the case of continuous time, whereupon evolution is governed by the Schrodinger equation, but this is less relevant for the case of quantum information.

A.1.3 Measurements

Postulate 3. A measurement of a quantum system is described by a set $\{M_m\}$ of *measurement operators*, which act on the state space of the system being measured. The index m labels the possible outcomes of the measurement. If the system is in state $|\psi\rangle$ immediately before the measurement is taken, the probability the measurement returns outcome m is given by

$$\mathbb{P}(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{A.1.3}$$

and the state of the system immediately after the measurement is

$$\frac{M_m\,|\psi\rangle}{\sqrt{\mathbb{P}(m)}}. \tag{A.1.4}$$

Since probabilities sum to 1, we can also derive that the measurement operators obey the *completeness relation*:

$$1 = \sum_m \mathbb{P}(m) = \langle\psi|\sum_m M_m^\dagger M_m|\psi\rangle\,,\ \forall\,|\psi\rangle \iff \sum_m M_m^\dagger M_m = I \tag{A.1.5}$$

which is a necessary condition for the measurement operators to obey.

Projective Measurements

In quantum information, a particularly important class of measurements are the *projective measurements.* These turn out to be exactly equivalent to the more general measurement postulate when augmented with the ability to perform unitary transformations as in postulate 2.

Definition A.1.1 (Projective measurement)**.** A projective measurement is described by a Hermitian operator (or *observable*) M acting on the state space of the system being measured. Since M is Hermitian, it has a spectral decomposition

$$M = \sum_m m P_m \tag{A.1.6}$$

where m indexes the eigenvalues, and P_m is the corresponding projector onto the m-eigenspace. The possible outcomes of the measurement correspond to the eigenvalues.

With this definition, we see that the probability of obtaining outcome m on measuring state $|\psi\rangle$ is

$$\mathbb{P}(m) = \langle\psi|P_m|\psi\rangle \tag{A.1.7}$$

and the state immediately after the measurement is

$$\frac{P_m |\psi\rangle}{\sqrt{\mathbb{P}(m)}}. \tag{A.1.8}$$

Projective measurements have all sorts of nice properties which general measurements do not. One notable such property is how *expectation values* in a probabilistic sense simplify. If we measure observable M on $|\psi\rangle$, the average outcome is

$$\begin{aligned} \mathbb{E}_\psi(M) &\equiv \sum_m m\mathbb{P}_\psi(m) \\ &= \sum_m m \langle\psi|P_m|\psi\rangle \\ &= \langle\psi| \sum_m mP_m|\psi\rangle \\ &= \langle\psi|M|\psi\rangle \end{aligned} \tag{A.1.9}$$

which can simplify many calculations. This is often denoted $\langle M\rangle_\psi \equiv \langle\psi|M|\psi\rangle$. In this dissertation, I use the convention where I define a projective measurement by just listing the set of projectors $\{P_m\}$ rather than the observable M, where it is implicit that $M = \sum_m mP_m$, $\sum_m P_m = 1$, and $P_m P_n = \delta_{mn} P_m$. I will also say '*perform a measurement in the* $|m\rangle$ *basis*', which refers to projective measurement with projectors $P_m = |m\rangle\langle m|$.

POVM measurements

In quantum mechanics, the post-measurement state is often not particularly relevant; the important item being the outcome probabilities instead, for example where a quantum circuit only performs a measurement at the end of the circuit. *POVM measurements* (standing for 'positive operator valued measure') are particularly well-suited for this sort of application. Suppose we perform a measurement $\{M_m\}$ on a state $|\psi\rangle$, so $\mathbb{P}(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. If we then define operators

$$E_m \equiv M_m^\dagger M_m, \tag{A.1.10}$$

then the E_m obey $\sum_m E_m = I$ and $\mathbb{P}(m) = \langle\psi|E_m|\psi\rangle$, and so the set $\{E_m\}$ alone is sufficient to determine the outcome probabilities. The operators E_m are called *POVM elements* for the measurement, and the set $\{E_m\}$ is simply called a POVM. It can be shown that any measurement where the measurement operators and the POVM operators are the same is a projective measurement, and moreover that for any POVM $\{E_m\}$, there exists a set of measurement operators $\{M_m\}$ describing an equivalent general measurement.

A.1.4 Composite Systems

Postulate 4. The state space of a composite system AB is the *tensor product* of the state spaces of the individual systems $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. More generally, if we have n systems indexed by i each prepared in the state $|\psi_i\rangle$, the joint state of the total system is $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$.

In practice, we often drop the tensor product symbol $\otimes$, and just write (for example) $|\psi\rangle_A \otimes |\phi\rangle_B \equiv |\psi\rangle_A |\phi\rangle_B$, where the subscript keeps track of which system each state refers to. We can also talk about the composition of operators. For example, if O_A and O_B are operators acting on systems A and B individually, the composition $O_A \otimes O_B$ acts on the joint state $|A\rangle|B\rangle$ as

$$(O_A \otimes O_B)|A\rangle|B\rangle \equiv O_A O_B |A\rangle|B\rangle = (O_A|A\rangle) \otimes (O_B|B\rangle). \tag{A.1.11}$$

We often wish to express operators and states explicitly in a basis. If $\{|a\rangle\}_{a=1}^n$ is an orthonormal basis for system A, then any operator O_A on $\mathcal{H}_A$ can be expressed as

$$O_A \equiv \sum_{ab} O_{ab} \left|a\right\rangle \left\langle b\right| = \begin{pmatrix} O_{11} & \dots & O_{1n} \\ \vdots & \ddots & \vdots \\ O_{n1} & \dots & O_{nn} \end{pmatrix}, \quad O_{ab} \in \mathbb{C}. \tag{A.1.12}$$

The composite operator $O_A \otimes O_B$ for some operator O_B on system B with state space $\mathcal{H}_B$ is then the block matrix

$$O_A \otimes O_B \equiv \begin{pmatrix} O_{11}O_B & \dots & O_{1n}O_B \\ \vdots & \ddots & \vdots \\ O_{n1}O_B & \dots & O_{nn}O_B \end{pmatrix}. \tag{A.1.13}$$

Note that this representation of an operator can be used to represent states as a specific case.

A.1.5 Density Operators

For some cases, the description of a state as being just a unit vector $\left|\psi\right\rangle$ is insufficient. This motivates the formalism of *density operators*, which find particular use in talking about subsystems of a composite system, systems which we may not know the state with certainty, and in statistical mechanics. Consider a system which is in the state $\left|\psi_i\right\rangle$ with probability p_i. The complete set $\{\left|\psi_i\right\rangle, p_i\}$ is known as an *ensemble* of pure states. The density operator for this system is then defined as

$$\rho \equiv \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|. \tag{A.1.14}$$

We can reformulate the postulates above in terms of density operators; we use them so frequently, that we do this explicitly.
For postulate 1, we note that the states $\left|\psi_i\right\rangle$ define a unique ρ and vice versa, so this remains unchanged. Similarly, the fourth postulate also remains unchanged since it does not explicitly refer to states in its statement. Consider postulate 2, and suppose we have a unitary U governing evolution of the system. ρ then evolves as

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \xrightarrow{U} \sum_i p_i U \left|\psi_i\right\rangle \left\langle\psi_i\right| U^\dagger = U\rho U^\dagger. \tag{A.1.15}$$

We can similarly reformulate the measurement postulate 3 for density operators. Suppose we perform a measurement with operators $\{M_m\}$. If our system happened to initially be in state $\left|\psi_i\right\rangle$, then the probability of outcome m is

$$\mathbb{P}(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \mathrm{Tr}(M_m^\dagger M_m \left|\psi_i\right\rangle \left\langle\psi_i\right|) \tag{A.1.16}$$

where the trace is taken over the entire state space. Therefore, the full probability of outcome m is

$$\mathbb{P}(m) = \sum_i \mathbb{P}(m|i)p_i = \sum_i p_i \mathrm{Tr}(M_m^\dagger M_m \left|\psi_i\right\rangle \left\langle\psi_i\right|) = \mathrm{Tr}(M_m^\dagger M_m \rho). \tag{A.1.17}$$

What is the density operator ρ immediately after the measurement returning m? If the initial state was $\left|\psi_i\right\rangle$, then we know that immediately after the measurement it is

$$\left|\psi_i^m\right\rangle = \frac{M_m \left|\psi_i\right\rangle}{\sqrt{\mathbb{P}(m|i)}}, \tag{A.1.18}$$

and so we now have an ensemble of states $\{\left|\psi_i^m\right\rangle, \mathbb{P}(i|m)\}$ immediately post-measurement. Therefore, ρ becomes

$$\rho_m \equiv \sum_i \mathbb{P}(i|m) \left|\psi_i^m\right\rangle \left\langle\psi_i^m\right|. \tag{A.1.19}$$

Probability theory states that $\mathbb{P}(i|m) = \mathbb{P}(m|i)p_i/\mathbb{P}(m)$, so we therefore find

$$\rho_m = \sum_i p_i \frac{M_m \left|\psi_i\right\rangle \left\langle\psi_i\right| M_m^\dagger}{\mathrm{Tr}(M_m^\dagger \rho)} = \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}(M_m^\dagger M_m \rho)}, \tag{A.1.20}$$

which completes the reformulation.
Density operators can also be axiomatised. Indeed, we can show that an arbitrary operator ρ is a density operator for some system if and only if both:

1. $\mathrm{Tr}(\rho) = 1$
2. ρ is a positive operator.

Before concluding, I'll introduce some nomenclature which is used to describe states quite often. A system which is known to be in state $\left|\psi\right\rangle$ exactly is called a *pure state*, and the density operator is $\rho = \left|\psi\right\rangle \left\langle\psi\right|$. If not, the state is said to be *mixed*, and the density operator can be written as in (A.1.14). A sufficient criterion for checking whether a state is pure or mixed is calculating $\mathrm{Tr}(\rho^2)$; if this is 1, then the state is pure, and if it is less than 1, it is mixed.

A.2 Quantum Information and Computation

This section will go through the basics of quantum information and computation. We discuss the definitions and conventions used for various distance measures for quantum information (with relevance to approximate error correction), entropy, as well as the basics of the circuit model of quantum computation.

A.2.1 Distance Measures

The point of quantum distance measures is to answer the question 'how close are two states?'. The two main distance measures are *trace distance* and *fidelity*. For our purposes, only fidelity is important, so we run through its definition and properties.

Definition A.2.1 (Fidelity)**.** Given two states (as density operators) ρ and σ, the **fidelity** between them is

$$F(\rho, \sigma) \equiv \mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}, \tag{A.2.1}$$

where $(\rho^{1/2})^2 = \rho$.

While fidelity is not formally a metric, it does give a useful notion of distance between states. Before going through its properties, we note two cases where fidelity simplifies. The first is when ρ and σ commute, so can be simultaneously diagonalised; in some basis $\{|i\rangle\}$ of the underlying Hilbert space, we have

$$\rho = \sum_i r_i |i\rangle \langle i|, \quad \sigma = \sum_i s_i |i\rangle \langle i|. \tag{A.2.2}$$

Then, we can compute the fidelity as

$$\begin{aligned} F(\rho, \sigma) &= \mathrm{Tr}\sqrt{\sum_i r_i s_i |i\rangle \langle i|} \\ &= \mathrm{Tr}\left(\sum_i \sqrt{r_i s_i} |i\rangle \langle i|\right) \\ &= \sum_i \sqrt{r_i s_i}. \end{aligned} \tag{A.2.3}$$

The second special case is the fidelity between a pure state $|\psi\rangle$ and arbitrary ρ. In this case, we have

$$F(|\psi\rangle, \rho) = \mathrm{Tr}\sqrt{|\psi\rangle \langle\psi|\rho|\psi\rangle \langle\psi|} = \sqrt{\langle\psi|\rho|\psi\rangle}, \tag{A.2.4}$$

so fidelity is just the square root of the overlap between $|\psi\rangle$ and ρ.

Properties

We now present some useful properties of fidelity.

Proposition 1. *Fidelity is invariant under unitary transformations; that is, for unitary U, we have*

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma). \tag{A.2.5}$$

Proof. For any positive operator A, we know that $\sqrt{UAU^\dagger} = U\sqrt{A}U^\dagger$. Density operators are positive, so

$$\begin{aligned} F(U\rho U^\dagger, U\sigma U^\dagger) &= \mathrm{Tr}\sqrt{(U\rho U^\dagger)^{1/2} U\sigma U^\dagger (U\rho U^\dagger)^{1/2}} \\ &= \mathrm{Tr}\sqrt{U\rho^{1/2}U^\dagger U\sigma U^\dagger U\rho^{1/2}U^\dagger} \\ &= \mathrm{Tr}\sqrt{U\rho^{1/2}\sigma\rho^{1/2}U^\dagger} \\ &= \mathrm{Tr}U\sqrt{\rho^{1/2}\sigma\rho^{1/2}}U^\dagger \\ &= F(\rho, \sigma). \end{aligned} \tag{A.2.6}$$

□

Fidelity can be characterised by a theorem called *Uhlmann's theorem.* Before presenting and proving this, we need two basic lemmas.

Lemma A.2.1. *Let A be an arbitrary operator, and U a unitary operator. Then*

$$|\mathit{Tr}(AU)| \leq \mathit{Tr}|A|, \tag{A.2.7}$$

with equality when $U = V^\dagger$, where $A = |A|V$ is the polar decomposition of A.

Proof. Equality is clear under the stated condition. We compute

$$|\mathrm{Tr}(AU)| = |\mathrm{Tr}(|A|VU)| = |\mathrm{Tr}(|A|^{1/2}|A|^{1/2}VU)|, \tag{A.2.8}$$

where we note that the trace term is just the Hilbert-Schmidt inner product $\langle |A|^{1/2}, |A|^{1/2}VU\rangle$. The Cauchy-Schwarz inequality then implies

$$|\mathrm{Tr}(AU)| \leq \sqrt{\mathrm{Tr}|A|\mathrm{Tr}(U^\dagger V^\dagger |A| VU)} = \mathrm{Tr}|A| \tag{A.2.9}$$

as required. □

Lemma A.2.2. *Suppose A and R are two quantum systems with the same Hilbert space, with bases $\{|i_A\rangle\}$ and $\{|i_R\rangle\}$ respectively. Define $|m\rangle = \sum_i |i_R\rangle |i_A\rangle$, and let P be an arbitrary operator on A and Q on R. Then*

$$\mathit{Tr}(Q^\dagger P) = \langle m|Q \otimes P|m\rangle \tag{A.2.10}$$

where the left hand side refers to matrix multiplication, and the matrix elements are taken with respect to the given bases.

Proof. We just compute:

$$\begin{aligned} \mathrm{Tr}(Q^\dagger P) &= \langle i_R|Q|j_R\rangle \langle i_A|P|j_A\rangle \\ &= \langle i_R| \langle i_A| (Q \otimes P) |j_R\rangle |j_A\rangle = \langle m|Q \otimes P|m\rangle , \end{aligned} \tag{A.2.11}$$

as required, where summation convention is implied. □

Theorem A.2.1 (Uhlmann's Theorem)**.** *Suppose ρ and σ are states of quantum system A. Introduce an auxiliary system R with $\mathcal{H}_R = \mathcal{H}_A$. Then:*

$$F(\rho, \sigma) = \max_{|\psi\rangle, |\phi\rangle} | \langle \psi|\phi\rangle |, \tag{A.2.12}$$

where the maximisation is taken over all purifications $|\psi\rangle$ of ρ and $|\phi\rangle$ of σ, both into RA.

Proof. Choose orthonormal bases $\{|i_A\rangle\}$ and $\{|i_R\rangle\}$ of A and R. Define $|m\rangle \equiv \sum_i |i_R\rangle |i_A\rangle$, and let $|\psi\rangle$ be an arbitrary purification of ρ. The Schmidt decomposition then implies that there exist some unitary operators U_A and U_R on A and R respectively such that

$$|\psi\rangle = (U_R \otimes \sqrt{\rho} U_A) |m\rangle . \tag{A.2.13}$$

We have an identical statement for some other unitaries V_A and V_R, and arbitrary purification $|\phi\rangle$ of σ. Taking an inner product then implies

$$| \langle \psi|\phi\rangle | = | \langle m|(U_R^\dagger V_R \otimes U_A^\dagger \sqrt{\rho}\sqrt{\sigma} V_A)|m\rangle |. \tag{A.2.14}$$

Using lemma A.2.2, we then have

$$| \langle \psi|\phi\rangle | = |\mathrm{Tr}(V_R^\dagger U_R U_A^\dagger \sqrt{\rho}\sqrt{\sigma} V_A)|. \tag{A.2.15}$$

So, defining $U \equiv V_A V_R^\dagger U_R U_A^\dagger$, we have

$$| \langle \psi|\phi\rangle | = |\mathrm{Tr}(\sqrt{\rho}\sqrt{\sigma} U)|. \tag{A.2.16}$$

Then, by lemma A.2.1, we have

$$| \langle \psi|\phi\rangle | \leq \mathrm{Tr}|\sqrt{\rho}\sqrt{\sigma}| = \mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}} = F(\rho, \sigma). \tag{A.2.17}$$

To attain equality, take the polar decomposition $\sqrt{\rho}\sqrt{\sigma} = |\sqrt{\rho}\sqrt{\sigma}|V$, and choose $U_A = U_R = V_R = I$ and $V_A = V^\dagger$, and we are done. □

While Uhlmann's theorem is not particularly useful in a computational sense, it shows us that the fidelity indeed has properties we would expect from a distance measure. It clearly implies symmetry of inputs $F(\rho, \sigma) = F(\sigma, \rho)$, and that it is bounded between 0 and 1, with equality with 1 if $\rho = \sigma$, and equality with 0 if and only if ρ and σ are supported on orthogonal subspaces. This would make sense: if two states are orthogonal, they are perfectly distinguishable, so we would expect minimum fidelity between them.

Fidelity is not a metric, but we can turn it into one. To do this, we make the following definition:

Definition A.2.2 (Angle)**.** Given two states ρ and σ, the **angle** between them is

$$A(\rho, \sigma) \equiv \arccos F(\rho, \sigma). \tag{A.2.18}$$

The motivation for this comes from the fact that the angle between two points on a sphere is a metric, and Uhlmann's theorem tells us that the fidelity between two states is the maximum possible inner product between purifications of these states. Clearly the angle is non-negative and symmetric in its inputs, and $A(\rho, \sigma) = 0 \iff \rho = \sigma$. The only property left to show angle is a metric is that it obeys the triangle inequality. To do this, consider three states ρ, σ, and τ. Choose purifications $|\phi\rangle$ of σ, $|\psi\rangle$ of ρ, and $|\gamma\rangle$ of τ such that

$$\begin{aligned} F(\rho, \sigma) &= \langle\psi|\phi\rangle \\ F(\sigma, \tau) &= \langle\phi|\gamma\rangle\,, \end{aligned} \tag{A.2.19}$$

and $\langle\psi|\gamma\rangle$ is real and positive. We have in general for arbitrary vectors that

$$\arccos(\langle\psi|\gamma\rangle) \leq \arccos(\langle\psi|\phi\rangle) + \arccos(\phi|\gamma) = A(\rho, \sigma) + A(\sigma, \tau), \tag{A.2.20}$$

but by Uhlmann's theorem, $F(\rho, \tau) \geq \langle\psi|\gamma\rangle$. Therefore $A(\rho, \tau) \leq \arccos(\langle\psi|\gamma\rangle)$. Together with (A.2.20), we then get the triangle equality, so angle is indeed a metric.

Fidelity is also monotonic under trace-preserving quantum operations.

Proposition 2. *Suppose $\mathcal{E}$ is a trace-preserving quantum operation, and ρ and σ are states of system A. Then*

$$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma). \tag{A.2.21}$$

Proof. Take purifications $|\psi\rangle$ and $|\phi\rangle$ of ρ and σ respectively onto a joint system AR such that $F(\rho, \sigma) = |\langle\psi|\phi\rangle|$. Introduce an environment E for the operation $\mathcal{E}$, which is initially in the state $|0\rangle_E$, and take it to interact with A via a unitary operation U. $U\left|\psi\right\rangle_{RA}\left|0\right\rangle_E$ is a purification of $\mathcal{E}(\rho)$, and similarly $U\left|\phi\right\rangle_{RA}\left|0\right\rangle_E$ is of $\mathcal{E}(\sigma)$. By Uhlmann's theorem, we therefore have

$$\begin{aligned} F(\mathcal{E}(\rho),\mathcal{E}(\sigma)) &\geq |\left\langle\psi\right|\left\langle 0|U^\dagger U|\phi\right\rangle\left|0\right\rangle| \\ &= |\left\langle\psi|\phi\right\rangle| \\ &= F(\rho,\sigma) \end{aligned} \tag{A.2.22}$$

as claimed. □

Our last property of fidelity is strong concavity.

Theorem A.2.2. *Let p_i and q_i be probability distributions indexed by i, and ρ_i and σ_i density operators also indexed by i. Then*

$$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq \sum_i \sqrt{p_iq_i}F(\rho_i,\sigma_i). \tag{A.2.23}$$

Proof. Choose purifications $\left|\psi_i\right\rangle$ and $\left|\phi_i\right\rangle$ of ρ_i and σ_i respectively such that $F(\rho_i,\sigma_i) = \left\langle\psi_i|\phi_i\right\rangle$. Introduce an ancillary system which has orthonormal basis $\{\left|i\right\rangle\}$, indexed by the same i as everything else. Define

$$\left|\psi\right\rangle \equiv \sum_i \sqrt{p_i}\left|\psi_i\right\rangle\left|i\right\rangle, \quad \left|\phi\right\rangle \equiv \sum_i \sqrt{q_i}\left|\phi_i\right\rangle\left|i\right\rangle. \tag{A.2.24}$$

Note that $\left|\psi\right\rangle$ purifies $\sum_i p_i\rho_i$ and $\left|\phi\right\rangle$ purifies $\sum_i q_i\sigma_i$, so by Uhlmann's theorem:

$$\begin{aligned} F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) &\geq |\left\langle\psi|\phi\right\rangle| \\ &= \sum_i \sqrt{p_iq_i}\left\langle\psi_i|\phi_i\right\rangle \\ &= \sum_i \sqrt{p_iq_i}F(\rho_i,\sigma_i) \end{aligned} \tag{A.2.25}$$

as claimed. □

Appendix B

Stuff that won't be read by anyone

Some people include in their thesis a lot of detail, particularly lots of tables containing raw results, figures of intermediate results, or computer code which no-one will ever read. You should be careful that anything like this you include should contain some element of uniqueness which justifies its inclusion.

Bibliography

[1] D. Aharonov and M. Ben-Or, *Fault-tolerant quantum computation with constant error rate*, SIAM Journal on Computing, 38 (2008), pp. 1207–1282.

[2] X. D. Ahmed Almheiri and D. Harlow, *Bulk locality and quantum error correction in ads/cft*, Journal of High Energy Physics, 163 (2015).

[3] C. Akers and G. Penington, *Quantum minimal surfaces from quantum error correction*, SciPost Phys., 12 (2022), p. 157.

[4] D. Deutsch and R. Jozsa, *Rapid solution of problems by quantum computation*, Proceedings of the Royal Society London, 439 (1992), pp. 553–558.

[5] D. Harlow, *The Ryu-Takayanagi Formula from Quantum Error Correction*, Communications in Mathematical Physics, 354 (2017), pp. 865–912.

[6] P. R. Jason Pollack and A. Rocchetto, *Understanding holographic error correction via unique algebras and atomic examples*, Journal of High Energy Physics, 56 (2022).

[7] V. F. R. Jones, *Von neumann algebras*. `https://math.berkeley.edu/~vfr/VonNeumann2009.pdf`, 2009.

[8] A. Kitaev, *Fault-tolerant quantum computation by anyons*, Annals of Physics, 303 (2003), pp. 2–30.

[9] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne, *Benchmarking quantum computers: The five-qubit error correcting code*, Phys. Rev. Lett., 86 (2001), pp. 5811–5814.

[10] E. Knill, R. Laflamme, and W. H. Zurek, *Resilient quantum computation*, Science, 279 (1998), pp. 342–345.

[11] J. M. Maldacena, *The Large N limit of superconformal field theories and supergravity*, Adv. Theor. Math. Phys., 2 (1998), pp. 231–252.

[12] L. A. L. T. e. a. Martín-López, E., *Experimental realization of shor's quantum factoring algorithm using qubit recycling*, Nature Photonics, 6 (2012), pp. 773–776.

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 10th ed., 2010.

[14] P. W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A, 52 (1995), pp. R2493–R2496.

[15] ——, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput., 26 (1997), p. 1484–1509.