

# 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] [14]

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

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Error Correction: An Introduction</b>	<b>4</b>
2.1	The Classical Bit-Flip . . . . .	4
2.2	The Quantum Bit-Flip . . . . .	5
2.3	Quantum Noise . . . . .	6
2.3.1	Quantum Operations . . . . .	6
2.3.2	Operator-Sum Representation . . . . .	7
2.3.3	Axiomatisation . . . . .	8
2.4	General Theory of Error Correction . . . . .	9
2.5	Quantum Erasure . . . . .	10
<b>3</b>	<b>Holographic Error Correction</b>	<b>12</b>
3.1	Conventional Erasure Correction . . . . .	12
3.2	Subsystem Error Correction . . . . .	17
3.3	Operator Algebra Error Correction . . . . .	18
3.3.1	von Neumann Algebras . . . . .	19
3.3.2	Classification of von Neumann Algebras . . . . .	20
3.3.3	Algebraic States and Entropy . . . . .	22
3.4	Operator-Algebra Error Correction . . . . .	24
3.5	Holographic Properties of Erasure Codes . . . . .	27
<b>4</b>	<b>Examples</b>	<b>32</b>

4.1	Codes with one term . . . . .	33
4.2	Codes with two terms . . . . .	36
4.3	A Complete Example . . . . .	39
<b>5</b>	<b>Conclusions</b>	<b>41</b>
<b>A</b>	<b>Quantum Information and Entropy</b>	<b>42</b>
A.1	Classical Information . . . . .	42
A.1.1	Shannon Entropy . . . . .	42
A.1.2	Relative Entropy . . . . .	43
A.2	Quantum Information . . . . .	44
A.2.1	von Neumann Entropy . . . . .	44
A.2.2	Relative Entropy . . . . .	46
A.2.3	Properties of von Neumann Entropy . . . . .	47
A.2.4	Entropy as a Measure of Entanglement . . . . .	47
<b>B</b>	<b>Quantum Circuit Notation</b>	<b>49</b>
B.1	Quantum Gates . . . . .	49
B.2	Quantum Circuits . . . . .	50

# 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 [17], 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 [13] - 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* [16]. 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 [10].

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][11][9] 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 holog-

raphy (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 [12]. 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 given purely for motivation.

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 [14]. Chapter 3 will present the main results and proofs of [5] - this paper is the primary reference for holographic error correction in general, describing 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 and expands on the examples of operator-algebra holographic codes in [6]. Finally, chapter 5 will present a summary of the project and suggestions as to future directions of study.

# Chapter 2

## Error Correction: An Introduction

In this chapter, we present the theory of quantum error correction. We begin with a discussion of a classical example to build 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 [14] and [5]. This chapter also assumes an understanding of quantum circuit notation. If this is not familiar, a brief summary of the salient features is presented in appendix B.

### 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, even if 1 bit flips, Bob will still 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

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

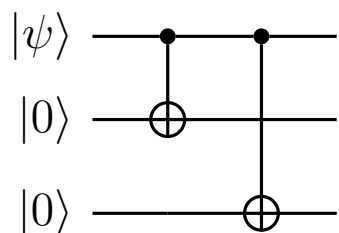
which is strictly less than  $p$  for  $0 < p < 1/2$ . Therefore so long as  $p$  is less than  $1/2$ , Bob has an increased chance of receiving Alice's intended message.

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 communication channel, 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  $|\psi\rangle$  to Bob. The quantum communications channel acts similarly 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  $|0\rangle \rightarrow |000\rangle$  and  $|1\rangle \rightarrow |111\rangle$ ; explicitly



$$(2.2.1)$$

Note in particular that the physical encoded state is **not** equal to three copies of the logical state:  $|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle \neq |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$ , 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

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

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  $\rho$ , 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  $\rho$  and evolves to state  $\rho'$ , 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  $\rho$ , and the environment is in  $\rho_{\text{env}}$ . 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

$$\rho \otimes \rho_{\text{env}} \rightarrow U(\rho \otimes \rho_{\text{env}})U^\dagger. \quad (2.3.2)$$

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

$$\mathcal{E}(\rho) = \text{Tr}_{\text{env}} [U(\rho \otimes \rho_{\text{env}})U^\dagger]. \quad (2.3.3)$$

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  $\rho_{\text{env}} = |e_0\rangle\langle e_0|$ . Then, we can rewrite 2.3.3 as

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

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  $\text{Tr}(\mathcal{E}(\rho)) = 1$ . Therefore

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

holds for all states  $\rho$ , and so

$$\sum_k E_k^\dagger E_k = I. \quad (2.3.6)$$

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.  $\text{Tr}(\mathcal{E}(\rho))$  is the probability that the process represented by  $\mathcal{E}$  occurs, so  $0 \leq \text{Tr}(\mathcal{E}(\rho)) \leq 1$ .
2.  $\mathcal{E}$  is *convex-linear*; that is, for a set of probabilities  $\{p_i\}$  and density matrices  $\{\rho_i\}$ , we have

$$\mathcal{E} \left( \sum_i p_i \rho_i \right) = \sum_i p_i \mathcal{E}(\rho_i). \quad (2.3.7)$$

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  $\text{Tr}(\mathcal{E}(\rho)) = 1$  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*

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

*for some set of operators  $E_i : \mathcal{H}_1 \rightarrow \mathcal{H}_2$ , 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, with operation elements*

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

*The action of this operation on a state  $\rho$  is therefore*

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

*It therefore ‘does nothing’ to  $\rho$  with probability  $1-p$ , and flips each basis element of  $\rho$  with probability  $p$ , exactly matching the bit-flip channel!*

## 2.4 General Theory of Error Correction

We now have the necessary theory to talk about the general theory behind quantum error-correction. A logical state  $\rho$  with support on a *logical space*  $\mathcal{H}_L$  is encoded by an *encoding isometry*  $V : \mathcal{H}_L \rightarrow \mathcal{H}$ , where the image of the isometry is called a *code subspace*  $\mathcal{H}_{\text{code}} \subseteq \mathcal{H}$ , and 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  $\mathcal{H}_{\text{code}} = \text{span}\{V|0\rangle, V|1\rangle\} = \text{span}\{|000\rangle, |111\rangle\}$ . After encoding, the state is subjected to noise (modelled by a quantum operation), a *syndrome measurement* is performed to diagnose whether an error occurred, and if so, what the error is, 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  $\mathcal{R}$ , both acting on the physical Hilbert space. For error correction to be deemed successful, we require that for any physical state  $\rho$  with support on  $\mathcal{H}_{\text{code}}$

$$(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho, \quad (2.4.1)$$

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

$$P_{\text{code}} E_i^\dagger E_j P_{\text{code}} = \alpha_{ij} P_{\text{code}} \quad (2.4.2)$$

where  $\alpha_{ij}$  are the elements of a complex hermitian matrix.

The proof of this can be found in [14]. 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 2.4.2.** *Suppose  $V : \mathcal{H}_L \rightarrow \mathcal{H}$  is an encoding isometry with image  $\mathcal{H}_{\text{code}}$ , 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*

$$F_i = \sum_j m_{ij} E_j \quad (2.4.3)$$

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

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

$$P_{\text{code}} \sigma_i^1 \sigma_j^1 P_{\text{code}} = \alpha_{ij} P_{\text{code}} \quad (2.4.4)$$

for the Pauli matrices  $\sigma_i^1 \in \{I, X, Y, Z\}$  acting on the first qubit, 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 [16] can do this, for example.

## 2.5 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** subsystem of

the physical space. Formally, we suppose that the physical space  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$  has a tensor product structure. One representation of the erasure channel is then

$$\mathcal{E}(\rho) = \text{Tr}_{\bar{A}}(\rho), \quad (2.5.1)$$

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  $\{|\bar{a}\rangle\}$  be orthonormal bases of  $\mathcal{H}_A$  and  $\mathcal{H}_{\bar{A}}$  respectively. We can then rewrite 2.5.1 as

$$\mathcal{E}(\rho) = \sum_{\bar{a}} \langle \bar{a} | \rho | \bar{a} \rangle, \quad (2.5.2)$$

from which we can read off operation elements

$$E_{\bar{a}} \equiv I_A \otimes \langle \bar{a} | = \sum_a |a\rangle \langle a| \otimes \langle \bar{a} |. \quad (2.5.3)$$

The natural question to ask is what the quantum error correction conditions 2.4.1 reduce to for erasures. To work this out, we can compute

$$E_{\bar{a}}^\dagger E_{\bar{b}} = (I_A \otimes |\bar{a}\rangle)(I_A \otimes \langle \bar{b}|) = I_A \otimes |\bar{a}\rangle \langle \bar{b}|, \quad (2.5.4)$$

and so 2.4.2 then reduces to

$$P_{\text{code}} |\bar{a}\rangle \langle \bar{b}| P_{\text{code}} = \alpha_{\bar{a}\bar{b}} P_{\text{code}} \quad (2.5.5)$$

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

$$P_{\text{code}} |\bar{a}\rangle \langle \bar{b}| P_{\text{code}} \propto P_{\text{code}}. \quad (2.5.6)$$

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

$$X_{\bar{A}} \equiv \sum_{\bar{a}, \bar{b}} x_{\bar{a}, \bar{b}} |\bar{a}\rangle \langle \bar{b}| \quad (2.5.7)$$

for some  $x_{\bar{a}, \bar{b}} \in \mathbb{C}$ . Therefore, if 2.5.5 holds, we have

$$P_{\text{code}} X_{\bar{A}} P_{\text{code}} \propto P_{\text{code}}. \quad (2.5.8)$$

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.

### 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  $V : \mathcal{H}_L \rightarrow \mathcal{H}$  be an encoding isometry, where  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ , and  $\mathcal{H}_{\text{code}} \subseteq \mathcal{H}$  is the image of  $V$ . Define an orthonormal basis  $\{|\tilde{i}\rangle\}$  of  $\mathcal{H}_L$ , and let  $|\phi\rangle \equiv \frac{1}{\sqrt{|R|}} |i\rangle_R (V |\tilde{i}\rangle)_{A\bar{A}}$ , 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  $|\chi\rangle_{A_2\bar{A}} \in \mathcal{H}_{A_2\bar{A}}$  such that

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

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

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

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

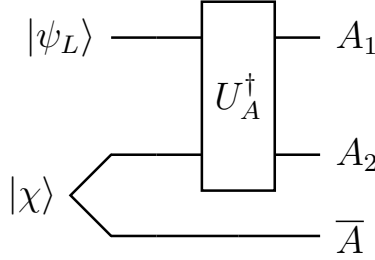
$$P_{\text{code}} X_{\bar{A}} P_{\text{code}} \propto P_{\text{code}} \quad (3.1.3)$$

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

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

$$\rho_{R\bar{A}}[\phi] = \rho_R[\phi] \otimes \rho_{\bar{A}}[\phi]. \quad (3.1.4)$$

Before proving this, let's go over some of the intuition behind each statement, and what all the objects in this theorem refer to.  $\bar{A}$  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  $U_A$  which does not need access to  $\bar{A}$  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  $\rho_{\bar{A}}[\phi]$  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 2.5.8; 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  $\bar{A}$  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  $\bar{A}$  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

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

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

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

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

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

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  $P_L V^\dagger X_{\bar{A}} V P_L \propto P_L$ . So suppose there was some  $X_{\bar{A}}$  such that  $P_L V^\dagger X_{\bar{A}} V P_L \not\propto P_L$ . 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  $V^\dagger X_{\bar{A}} V$  is not the identity, there must be some  $\tilde{O}$  on  $\mathcal{H}_L$  which doesn't commute with  $V^\dagger X_{\bar{A}} V$ , and some  $|\tilde{\psi}\rangle \in \mathcal{H}_L$  such that:

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

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  $X_{\bar{A}}$ ; if it had such an  $O_A$ , then  $\langle \tilde{\psi} | [V^\dagger X_{\bar{A}} V, \tilde{O}] | \tilde{\psi} \rangle = \langle \tilde{\psi} | [V^\dagger X_{\bar{A}} V, V^\dagger O_A V] | \tilde{\psi} \rangle = \langle \tilde{\psi} | V^\dagger [X_{\bar{A}}, O_A] V | \tilde{\psi} \rangle = 0$ , which is a contradiction.

(3)  $\implies$  (4): Consider arbitrary operators  $O_R$  on  $\mathcal{H}_R$  and  $X_{\bar{A}}$  on  $\mathcal{H}_{\bar{A}}$ . If we denote the constant of proportionality in 3.1.3 as  $\lambda \in \mathbb{C}$ , we have

$$P_{\text{code}} X_{\bar{A}} P_{\text{code}} = \lambda P_{\text{code}}, \quad (3.1.8)$$

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

$$\langle \phi | P_{\text{code}} X_{\bar{A}} P_{\text{code}} | \phi \rangle = \langle \phi | X_{\bar{A}} | \phi \rangle = \lambda \langle \phi | P_{\text{code}} | \phi \rangle = \lambda \langle \phi | \phi \rangle = \lambda, \quad (3.1.9)$$

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

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

since  $P_{\text{code}} | \phi \rangle = | \phi \rangle$ . Therefore, so long as  $\langle \phi | O_R | \phi \rangle$  and  $\langle \phi | X_{\bar{A}} | \phi \rangle$  are non-zero for any such  $O_R$  and  $X_{\bar{A}}$ , we have  $\rho_{R\bar{A}}[\phi] = \rho_R[\phi] \otimes \rho_{\bar{A}}[\phi]$ .

(4)  $\implies$  (1): First, note that by definition,  $| \phi \rangle$  is a purification of  $\rho_{R\bar{A}}[\phi] = \rho_R[\phi] \otimes \rho_{\bar{A}}[\phi]$  on subsystem  $A$ . Also note that  $| \phi \rangle$  maximally entangles  $R$  with  $A$ :

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

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

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

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  $| \chi \rangle_{A_2\bar{A}}$  to be an arbitrary purification of  $\rho_{\bar{A}}[\phi]$  on  $A_2$ . Note that the state

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

then purifies  $\rho_{R\bar{A}}[\phi]$  on  $A_1 A_2$ :

$$\begin{aligned}
\text{Tr}_{A_1 A_2} (| \Psi \rangle \langle \Psi |_{RA_1} \otimes | \chi \rangle \langle \chi |_{A_2\bar{A}}) &= \text{Tr}_{A_1} (| \Psi \rangle \langle \Psi |_{RA_1}) \text{Tr}_{A_2} (| \chi \rangle \langle \chi |_{A_2\bar{A}}) \\
&= \rho_R[\phi] \otimes \rho_{\bar{A}}[\phi].
\end{aligned} \tag{3.1.15}$$

Such a factorisation exists since the  $R$  and  $\bar{A}$  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  $\text{rank}(\rho_{\bar{A}}[\phi]) \leq |A_2|$ .

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:

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

as claimed.  $\square$

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

We now present 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

$$|\tilde{\psi}\rangle = \sum_{i=0}^2 a_i |\tilde{i}\rangle \quad (3.1.17)$$

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

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

Explicitly, the encoding isometry  $V$  can be written

$$V = |0\rangle \langle \tilde{0}| + |1\rangle \langle \tilde{1}| + |2\rangle \langle \tilde{2}|. \quad (3.1.19)$$

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

$$U_{12} \equiv |\tilde{00}\rangle\langle\tilde{00}| + |\tilde{01}\rangle\langle\tilde{11}| + |\tilde{02}\rangle\langle\tilde{22}| + |\tilde{12}\rangle\langle\tilde{01}| + |\tilde{10}\rangle\langle\tilde{12}| + |\tilde{11}\rangle\langle\tilde{20}| \\ + |\tilde{21}\rangle\langle\tilde{02}| + |\tilde{22}\rangle\langle\tilde{10}| + |\tilde{20}\rangle\langle\tilde{21}|, \quad (3.1.20)$$

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

$$|\tilde{11}\rangle \rightarrow |\tilde{01}\rangle \rightarrow |\tilde{12}\rangle \rightarrow |\tilde{10}\rangle \rightarrow |\tilde{22}\rangle \rightarrow |\tilde{02}\rangle \rightarrow |\tilde{21}\rangle \rightarrow |\tilde{20}\rangle \rightarrow |\tilde{11}\rangle. \quad (3.1.21)$$

We can then compute that

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

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

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

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

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

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

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

This is done by just defining

$$O_{12} \equiv U_{12}^\dagger \tilde{O} U_{12} \quad (3.1.26)$$

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  $\bar{A}$  is called *subsystem error correction*. This is theorem 2 of [5]. This theorem is as follows.

**Theorem 3.2.1.** *Let  $V : \mathcal{H}_L \rightarrow \mathcal{H}$  be an encoding isometry, where  $\mathcal{H}_L = \mathcal{H}_a \otimes \mathcal{H}_{\bar{a}}$  and  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ . Define orthonormal bases  $\{|\tilde{i}\rangle\}$  of  $\mathcal{H}_a$  and  $\{|\tilde{j}\rangle\}$  of  $\mathcal{H}_{\bar{a}}$ , and let  $|\phi\rangle \equiv \frac{1}{\sqrt{|R||\bar{R}|}} \sum_{i,j} |i\rangle_R |j\rangle_{\bar{R}} (V |\tilde{i}\tilde{j}\rangle)_{A\bar{A}}$  where  $R$  and  $\bar{R}$  are auxiliary systems with  $\mathcal{H}_R = \mathcal{H}_a$  and  $\mathcal{H}_{\bar{R}} = \mathcal{H}_{\bar{a}}$ . 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  $|\chi_j\rangle_{A_2\bar{A}} \in \mathcal{H}_{A_2\bar{A}}$  such that

$$(U_A \otimes I_{\bar{A}}) V |\tilde{i}\tilde{j}\rangle = |i\rangle_{A_1} \otimes |\chi_j\rangle_{A_2\bar{A}}, \quad (3.2.1)$$

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

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

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

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

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

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

$$\rho_{R\bar{R}A}[\phi] = \rho_R[\phi] \otimes \rho_{\bar{R}A}[\phi]. \quad (3.2.4)$$

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  $M = \langle x, y, \dots \rangle$  for the algebra generated by  $a, b, \dots$ .

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

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

**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

$$Z_M \equiv M \cap M'. \quad (3.3.2)$$

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

$$Z_M \equiv \langle I \rangle = \{\lambda I \mid \lambda \in \mathbb{C}\} \quad (3.3.3)$$

### 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  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$  such that  $M = \mathcal{L}(\mathcal{H}_A) \otimes I_{\bar{A}}$  and  $M' = I_A \otimes \mathcal{L}(\mathcal{H}_{\bar{A}})$ .*

In other words,  $M$  induces a tensor factorisation  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ , 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*

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

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

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

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*

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

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

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

and  $M$  has Wedderburn decomposition

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

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

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

such that  $M$  is the set of all operators which are block diagonal in  $\alpha$ , and acts as  $\tilde{O}_{L_{\alpha}} \otimes I_{\bar{L}_{\alpha}}$  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:

$$\tilde{O} = \begin{pmatrix} \tilde{O}_{L_1} \otimes I_{\bar{L}_1} & 0 & \dots \\ 0 & \tilde{O}_{L_2} \otimes I_{\bar{L}_2} & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}. \quad (3.3.10)$$

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

$$\tilde{O}' = \begin{pmatrix} I_{L_1} \otimes \tilde{O}'_{\bar{L}_1} & 0 & \dots \\ 0 & I_{L_2} \otimes \tilde{O}'_{\bar{L}_2} & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}. \quad (3.3.11)$$

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

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



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  $\mathcal{H}_{\bar{L}_\alpha}$  respectively; we use these to build a basis for the entire Hilbert space

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

### 3.3.3 Algebraic States and Entropy

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

$$\mathbb{E}_\rho(O) = \text{Tr}(O\rho). \quad (3.3.14)$$

In what follows, we will often wish to compute the expectation values of operators in a von Neumann algebra  $M$ . An arbitrary state  $\rho$  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  $\rho_M$ . 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  $\rho \in \text{End}(\mathcal{H})$  be a state. Then, there exists a unique state  $\rho_M \in M$  such that*

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

for all  $x \in M$ .

This theorem states that in computing expectation values of elements of  $M$ , we can replace  $\rho$  by  $\rho_M$ .

We can actually write down an explicit form for  $\rho_M$ . 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  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$  such that  $M = \mathcal{L}(\mathcal{H}_A) \otimes I_{\bar{A}}$ . Defining the reduced state

$$\rho_A \equiv \text{Tr}_{\bar{A}}\rho, \quad (3.3.16)$$

we see that the unique algebraic state obeying 3.3.3 is just

$$\rho_M \equiv \rho_A \otimes \frac{I_{\bar{A}}}{|\bar{A}|}. \quad (3.3.17)$$

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

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

in terms of which

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

Any state  $\rho$  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  $\rho$  will contribute to expectation values. We denote the  $\alpha\alpha'$ th block of  $\rho$  by  $\rho_{\alpha\alpha'}$ ; we can then define

$$p_{\alpha}\rho_{A_{\alpha}} \equiv \text{Tr}_{\bar{A}_{\alpha}}\rho_{\alpha\alpha}, \quad (3.3.20)$$

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

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

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  $\rho_M$  is equivalent to the von Neumann entropy of the reduced state  $\rho_A$ . This suggests that we should introduce a generalisation of the von Neumann entropy for a state  $\rho$  on an algebra  $M$ , which we define as follows:

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

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

where  $S(\rho_{A_{\alpha}}) \equiv -\text{Tr}_{A_{\alpha}}(\rho_{A_{\alpha}} \log \rho_{A_{\alpha}})$  is the von Neumann entropy of the reduced state  $\rho_{A_{\alpha}}$  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  $p_{\alpha}$ , and a quantum term associated to the von Neumann entropies of each diagonal block of  $\rho$ , 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  $p_{\alpha}$  vanishes.

We can also define the notion of *algebraic relative entropy*.

**Definition 3.3.6.** Given two states  $\rho, \sigma$  on  $M$ , the algebraic relative entropy between them is

$$\begin{aligned} S(\rho|\sigma, M) &= -S(\rho, M) - \text{Tr} \left( \oplus_{\alpha} [\log(p_{\alpha}^{\{\sigma\}}\sigma_{A_{\alpha}}) \otimes I_{\bar{A}_{\alpha}}] \rho \right) \\ &= \sum_{\alpha} p_{\alpha}^{\{\rho\}} \log \frac{p_{\alpha}^{\{\rho\}}}{p_{\alpha}^{\{\sigma\}}} + \sum_{\alpha} p_{\alpha}^{\{\rho\}} S(\rho_{A_{\alpha}}|\sigma_{A_{\alpha}}), \end{aligned} \quad (3.3.23)$$

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

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

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

Tracing out the corresponding blocks, we find

$$\rho_{A_1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \rho_{A_2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad (3.3.25)$$

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

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

## 3.4 Operator-Algebra Error Correction

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

**Theorem 3.4.1.** Let  $V : \mathcal{H}_L \rightarrow \mathcal{H}$  be an encoding isometry with image  $\mathcal{H}_{\text{code}} \subseteq \mathcal{H}$ , where  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ . Say we have a von Neumann algebra  $M$  on  $\mathcal{H}_L$ . Define orthonormal basis  $\{|\alpha, ij\rangle\}$  of  $\mathcal{H}_L$  as in 3.3.13, which is compatible with the decomposition  $\mathcal{H}_L = \oplus_\alpha (\mathcal{H}_{L_\alpha} \otimes \mathcal{H}_{\bar{L}_\alpha})$  induced by  $M$ . Let  $|\phi\rangle \equiv \frac{1}{\sqrt{|R|}} \sum_{\alpha, i, j} |\alpha, ij\rangle_R (V|\alpha, ij\rangle)_{A\bar{A}}$ , 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  $|\chi_{\alpha, j}\rangle_{A_2^\alpha \bar{A}} \in \mathcal{H}_{A_2^\alpha \bar{A}}$  such that

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

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

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

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

$$P_{\text{code}} X_{\bar{A}} P_{\text{code}} = V X' V^\dagger P_{\text{code}}, \quad (3.4.3)$$

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

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

$$[O_R, \rho_{R\bar{A}}[\phi]] = 0, \quad (3.4.4)$$

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

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

Similar to the last theorem, this characterises in some sense ‘how well’ a code subspace can correct a subalgebra  $M$  for the erasure of  $\bar{A}$ . 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  $P_{\text{code}} X_{\bar{A}} P_{\text{code}} = V x' V^\dagger P_{\text{code}}$ , 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

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

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

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

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

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  $X_{\bar{A}}$  by 3.4.3, and the last two by similar logic in reverse. This can only hold for arbitrary  $X_{\bar{A}}$  and  $Y_R$  if  $[O_R, \rho_{R\bar{A}}[\phi]] = 0$  as claimed.

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

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

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

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

From 3.4.4, we know that  $[O_R, \rho_{R\bar{A}}[\phi]] = 0$  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

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

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

By definition,  $|\phi\rangle_{RA\bar{A}}$  is a purification of  $\rho_{R\bar{A}}[\phi]$  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  $\text{rank}(\rho_{\bar{R}_\alpha \bar{A}}) \equiv |\rho_{\bar{R}_\alpha \bar{A}}|$ , we can write

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

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  $|A_2^\alpha| \geq |\rho_{\bar{R}_\alpha \bar{A}}|$  by long division. For each  $\alpha$ , we can then purify  $\rho_{\bar{R}_\alpha \bar{A}}$  on  $A_2^\alpha$ ; since  $\text{Tr}_{\bar{A}}(\rho_{\bar{R}_\alpha \bar{A}}) = I_{\bar{R}_\alpha}/|\bar{R}_\alpha|$ , such a purification has the form

$$|\psi_\alpha\rangle_{\bar{R}_\alpha A_2^\alpha \bar{A}} = \frac{1}{\sqrt{|\bar{R}_\alpha|}} \sum_j |\alpha, j\rangle_{\bar{R}_\alpha} |\chi_{\alpha, j}\rangle_{A_2^\alpha \bar{A}}, \quad (3.4.13)$$

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

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

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

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

which finishes the proof.  $\square$

## An Example

### 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* [12], 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  $A$ :

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

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  $V : \mathcal{H}_L \rightarrow \mathcal{H}$  is an encoding isometry,  $M$  is a von Neumann algebra on  $\mathcal{H}_L$ , and  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$  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  $\rho$  on  $\mathcal{H}_L$ :

$$S(\text{Tr}_{\bar{A}}(V\rho V^\dagger)) = S(M, \rho) + \text{Tr}(\rho\mathcal{L}). \quad (3.5.2)$$

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  $\mathcal{H}_{\bar{A}}$ . That is, for any operator  $\tilde{O}' \in M'$ , there exists an operator  $O_{\bar{A}}$  on  $\mathcal{H}_{\bar{A}}$  such that for any state  $|\tilde{\psi}\rangle \in \mathcal{H}_L$ , we have

$$\begin{aligned} O_{\bar{A}} V |\tilde{\psi}\rangle &= V \tilde{O}' |\tilde{\psi}\rangle \\ O_{\bar{A}}^\dagger V |\tilde{\psi}\rangle &= V \tilde{O}'^\dagger |\tilde{\psi}\rangle. \end{aligned} \quad (3.5.3)$$

We can then state and prove the following theorem:

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

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

$$M = \oplus_\alpha (\mathcal{L}(\mathcal{H}_{L_\alpha}) \otimes I_{\bar{L}_\alpha}), \quad M' = \oplus_\alpha (I_{L_\alpha} \otimes \mathcal{L}(\mathcal{H}_{\bar{L}_\alpha})). \quad (3.5.4)$$

Let  $\{\widetilde{|\alpha, ij\rangle}\} = \{|\alpha, i\rangle_{L_\alpha} \otimes |\alpha, j\rangle_{\bar{L}_\alpha}\}$  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

$$\mathcal{H}_A = \oplus_\alpha (\mathcal{H}_{A_1^\alpha} \otimes \mathcal{H}_{A_2^\alpha}) \oplus \mathcal{H}_{A_3}, \quad \mathcal{H}_{\bar{A}} = \oplus_\alpha (\mathcal{H}_{\bar{A}_1^\alpha} \otimes \mathcal{H}_{\bar{A}_2^\alpha}) \oplus \mathcal{H}_{\bar{A}_3} \quad (3.5.5)$$

and unitaries  $U_A \in \mathcal{L}(\mathcal{H}_A)$  and  $U_{\bar{A}} \in \mathcal{L}(\mathcal{H}_{\bar{A}})$  such that (dropping the tensor factors with identity operators)

$$\begin{aligned} U_A V |\widetilde{\alpha, i, j}\rangle &= |\alpha, i\rangle_{A_1^\alpha} \otimes |\chi_{\alpha, j}\rangle_{A_2^\alpha \bar{A}} \\ U_{\bar{A}} V |\widetilde{\alpha, i, j}\rangle &= |\bar{\chi}_{\alpha, i}\rangle_{A \bar{A}_2^\alpha} \otimes |\alpha, j\rangle_{\bar{A}_1^\alpha}. \end{aligned} \quad (3.5.6)$$

Applying  $U_{\bar{A}}$  to the first of these, and  $U_A$  to the second, we see

$$\begin{aligned} U_A U_{\bar{A}} V |\widetilde{\alpha, i, j}\rangle &= |\alpha, i\rangle_{A_1^\alpha} \otimes U_{\bar{A}} |\chi_{\alpha, j}\rangle_{A_2^\alpha \bar{A}} \\ U_A U_{\bar{A}} V |\widetilde{\alpha, i, j}\rangle &= U_A |\bar{\chi}_{\alpha, i}\rangle_{A \bar{A}_2^\alpha} \otimes |\alpha, j\rangle_{\bar{A}_1^\alpha} \end{aligned} \quad (3.5.7)$$

Equating the right hand sides, we see there must be states  $|\chi_\alpha\rangle_{A_2^\alpha \bar{A}_2^\alpha}$  and  $|\bar{\chi}_\alpha\rangle_{A_2^\alpha \bar{A}_2^\alpha}$  such that

$$\begin{aligned} U_{\bar{A}} |\chi_{\alpha, j}\rangle_{A_2^\alpha \bar{A}_2^\alpha} &= |\chi_\alpha\rangle_{A_2^\alpha \bar{A}_2^\alpha} \otimes |\alpha, j\rangle_{\bar{A}_1^\alpha} \\ U_A |\bar{\chi}_\alpha\rangle_{A_2^\alpha \bar{A}_2^\alpha} &= |\alpha, i\rangle_{A_1^\alpha} \otimes |\bar{\chi}_\alpha\rangle_{A_2^\alpha \bar{A}_2^\alpha}. \end{aligned} \quad (3.5.8)$$

However, the equality of the right hand sides of equation 3.5.7 tells us that  $|\chi_\alpha\rangle_{A_2^\alpha \bar{A}_2^\alpha} = |\bar{\chi}_\alpha\rangle_{A_2^\alpha \bar{A}_2^\alpha}$ . We therefore obtain that

$$U_A U_{\bar{A}} V |\widetilde{\alpha, i, j}\rangle = |\alpha, i\rangle_{A_1^\alpha} \otimes |\chi_\alpha\rangle_{A_2^\alpha \bar{A}_2^\alpha} \otimes |\alpha, j\rangle_{\bar{A}_1^\alpha}. \quad (3.5.9)$$

We can use this map to express any logical state  $\tilde{\rho}$  on  $\mathcal{H}_L$  as follows

$$U_A U_{\bar{A}} V \tilde{\rho} V^\dagger U_A^\dagger U_{\bar{A}}^\dagger = \bigoplus_{\alpha} \left[ p_{\alpha} \rho_{A_1^\alpha \bar{A}_1^\alpha} \otimes (\chi_{\alpha})_{A_2^\alpha \bar{A}_2^\alpha} \right]. \quad (3.5.10)$$

Here,  $\rho_{A_1^\alpha \bar{A}_1^\alpha}$  is a state acting on  $\mathcal{H}_{A_1^\alpha} \otimes \mathcal{H}_{\bar{A}_1^\alpha}$  in the same way as  $\tilde{\rho}_{L_\alpha \bar{L}_\alpha}$  does on  $\mathcal{H}_{L_\alpha} \otimes \mathcal{H}_{\bar{L}_\alpha}$  (recall that  $p_{\alpha} \rho_{L_\alpha \bar{L}_\alpha}$  are the diagonal blocks of  $\tilde{\rho}$  in  $\alpha$  with the  $p_{\alpha}$  chosen to ensure  $\text{Tr}(\rho_{L_\alpha \bar{L}_\alpha}) = 1$ ), and  $\chi_{\alpha} \equiv |\chi_{\alpha}\rangle \langle \chi_{\alpha}|$ . We therefore have that

$$\text{Tr}_{\bar{A}} \left( U_A U_{\bar{A}} V \tilde{\rho} V^\dagger U_A^\dagger U_{\bar{A}}^\dagger \right) = U_A \text{Tr}_{\bar{A}} (V \tilde{\rho} V^\dagger) U_A^\dagger = \bigoplus_{\alpha} \left[ p_{\alpha} \rho_{A_1^\alpha} \otimes (\chi_{\alpha})_{A_2^\alpha} \right]. \quad (3.5.11)$$

We then compute:

$$\begin{aligned} S(\text{Tr}_{\bar{A}} (V \tilde{\rho} V^\dagger)) &= -\text{Tr} \left[ \bigoplus_{\alpha} \left( p_{\alpha} \rho_{A_1^\alpha} \otimes (\chi_{\alpha})_{A_2^\alpha} \right) \log \bigoplus_{\alpha} \left( p_{\alpha} \rho_{A_1^\alpha} \otimes (\chi_{\alpha})_{A_2^\alpha} \right) \right] \\ &= -\sum_{\alpha} \text{Tr} \left[ p_{\alpha} \rho_{A_1^\alpha} \log (p_{\alpha} \rho_{A_1^\alpha}) \otimes (\chi_{\alpha})_{A_2^\alpha} + p_{\alpha} \rho_{A_1^\alpha} \otimes (\chi_{\alpha})_{A_2^\alpha} \log (\chi_{\alpha})_{A_2^\alpha} \right] \\ &= -\sum_{\alpha} \text{Tr}_{L_\alpha} [p_{\alpha} \tilde{\rho}_{L_\alpha} \log (p_{\alpha} \tilde{\rho}_{L_\alpha})] - \sum_{\alpha} p_{\alpha} \text{Tr} \left[ (\chi_{\alpha})_{A_2^\alpha} \log (\chi_{\alpha})_{A_2^\alpha} \right] \\ &= S(\tilde{\rho}, M) + \sum_{\alpha} p_{\alpha} S(\text{Tr}_{\bar{A}} (\chi_{\alpha})). \end{aligned} \quad (3.5.12)$$



On the first line, we use the fact that von Neumann entropy is invariant under unitary transformations and 3.5.11, the second uses that  $\log(O_A \otimes O_B) = \log(O_A) \otimes I_B + I_A \otimes \log(O_B)$ , and the third uses the fact that  $\rho_{A_1^\alpha}$  and  $\tilde{\rho}_{L_\alpha}$  have the same matrix elements on their corresponding Hilbert spaces. So, if we define

$$\mathcal{L} \equiv \oplus_\alpha S(\text{Tr}_{\bar{A}}(\chi_\alpha)) I_{L_\alpha \bar{L}_\alpha}, \quad (3.5.13)$$

we see that

$$\text{Tr}(\tilde{\rho} \mathcal{L}) = \text{Tr} \left( \bigoplus_\alpha [p_\alpha \tilde{\rho}_{L_\alpha} \otimes \tilde{\rho}_{\bar{L}_\alpha} S(\text{Tr}_{\bar{A}}(\chi_\alpha))] \right) = \sum_\alpha p_\alpha S(\text{Tr}_{\bar{A}}(\chi_\alpha)). \quad (3.5.14)$$

Therefore, we establish an RT formula

$$S(\text{Tr}_{\bar{A}}(V \tilde{\rho} V^\dagger)) = S(\tilde{\rho}, M) + \text{Tr}(\tilde{\rho} \mathcal{L}) \quad (3.5.15)$$

for  $(V, A, M)$ . Since we can repeat these arguments with  $A \leftrightarrow \bar{A}$  and  $M \leftrightarrow M'$  (i.e. with  $i \leftrightarrow j$ ), we see that complementary recovery holds. Moreover, since  $S(\text{Tr}_{\bar{A}}(\chi_\alpha)) = S(\text{Tr}_A(\chi_\alpha))$ , the area operator  $\mathcal{L}$  is indeed the same for both RT formulae; since it is in  $M$  and  $M'$ , it is in the centre as well.

( $\Leftarrow$ ): Recall the definition of algebraic relative entropy

$$S(\tilde{\rho}|\tilde{\sigma}, M) = -S(\tilde{\rho}, M) - \text{Tr}(\oplus_\alpha [\log(p_\alpha^{\{\tilde{\sigma}\}} \tilde{\sigma}_{L_\alpha}) \otimes I_{\bar{L}_\alpha}] \tilde{\rho}). \quad (3.5.16)$$

Consider taking a small perturbation  $\delta\tilde{\rho}$  about a state  $\tilde{\sigma}$ ; to first order in  $\delta\tilde{\rho}$ , we have that

$$S(\tilde{\sigma} + \delta\tilde{\rho}|\tilde{\sigma}, M) = 0. \quad (3.5.17)$$

We similarly find that

$$S(\text{Tr}_{\bar{A}}(V(\tilde{\sigma} + \delta\tilde{\rho})V^\dagger) | \text{Tr}_{\bar{A}}(V\tilde{\sigma}V^\dagger)) = 0 \quad (3.5.18)$$

to first order<sup>1</sup>. Using these facts, we take the same variation on 3.5.15:

$$\begin{aligned} S(\text{Tr}_{\bar{A}}(V(\tilde{\sigma} + \delta\tilde{\rho})V^\dagger)) &= S(\tilde{\sigma} + \delta\tilde{\rho}, M) + \text{Tr}((\tilde{\sigma} + \delta\tilde{\rho}) \mathcal{L}) \\ \implies \text{Tr}(\text{Tr}_{\bar{A}}(V\delta\tilde{\rho}V^\dagger) \log[\text{Tr}_{\bar{A}}(V\tilde{\sigma}V^\dagger)]) &= \sum_\alpha \text{Tr}(\delta\tilde{\rho}[(\log(p_\alpha^{\{\tilde{\sigma}\}} \tilde{\sigma}_{L_\alpha}) \otimes I_{\bar{L}_\alpha}) - \mathcal{L}]). \end{aligned} \quad (3.5.19)$$

Both sides of the equation are linear in  $\delta\tilde{\rho}$ , so we can integrate over all such perturbations:

$$\text{Tr}(\text{Tr}_{\bar{A}}(V\tilde{\rho}V^\dagger) \log[\text{Tr}_{\bar{A}}(V\tilde{\sigma}V^\dagger)]) = \sum_\alpha \text{Tr}(\tilde{\rho}[(\log(p_\alpha^{\{\tilde{\sigma}\}} \tilde{\sigma}_{L_\alpha}) \otimes I_{\bar{L}_\alpha}) - \mathcal{L}]). \quad (3.5.20)$$

---

<sup>1</sup>These can be proved by using the Baker-Campbell-Hausdorf formula, and noting that  $\text{Tr}(A[B, C]) = 0$  if  $A$  and  $B$  are simultaneously diagonalisable.

The next step is to calculate the relative entropy:

$$\begin{aligned}
S(\mathrm{Tr}_{\bar{A}}(V\tilde{\rho}V^\dagger)|\mathrm{Tr}_{\bar{A}}(V\tilde{\sigma}V^\dagger)) &= \mathrm{Tr}(\mathrm{Tr}_{\bar{A}}(V\tilde{\rho}V^\dagger) \log(\mathrm{Tr}_{\bar{A}}(V\tilde{\rho}V^\dagger))) \\
&\quad - \mathrm{Tr}(\mathrm{Tr}_{\bar{A}}(V\tilde{\rho}V^\dagger) \log(\mathrm{Tr}_{\bar{A}}(V\tilde{\sigma}V^\dagger))) \\
&= -S(\mathrm{Tr}_{\bar{A}}(V\tilde{\rho}V^\dagger)) - \sum_{\alpha} \mathrm{Tr}(\tilde{\rho}[(\log(p_{\alpha}^{\{\tilde{\sigma}\}}\tilde{\sigma}_{L_{\alpha}}) \otimes I_{\bar{L}_{\alpha}}) - \mathcal{L}]) \\
&= -S(\tilde{\rho}, M) - \sum_{\alpha} \mathrm{Tr}(\tilde{\rho}(\log(p_{\alpha}^{\{\tilde{\sigma}\}}\tilde{\sigma}_{L_{\alpha}}) \otimes I_{\bar{L}_{\alpha}})) \\
&= S(\rho|\sigma, M),
\end{aligned} \tag{3.5.21}$$

where we use 3.5.20 in the second line, and the RT formula in the third. We can perform the same argument with  $A \leftrightarrow \bar{A}$  and  $M \leftrightarrow M'$ , and we find similarly that

$$S(\mathrm{Tr}_A(V\rho V^\dagger)|\mathrm{Tr}_{\bar{A}}(V\sigma V^\dagger)) = S(\rho|\sigma, M'). \tag{3.5.22}$$

These two conditions together in fact imply complementary recovery. Consider an arbitrary state  $|\tilde{\psi}\rangle \in \mathcal{H}_L$ , an arbitrary operator  $X_{\bar{A}}$  on  $\mathcal{H}_{\bar{A}}$ , 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

$$\langle \tilde{\psi}|e^{-i\lambda\tilde{O}}V^\dagger X_{\bar{A}}V e^{i\lambda\tilde{O}}|\tilde{\psi}\rangle = \langle \tilde{\psi}|e^{-i\lambda\tilde{O}}P_L V^\dagger X_{\bar{A}}V P_L e^{i\lambda\tilde{O}}|\tilde{\psi}\rangle. \tag{3.5.23}$$

We show that this is independent of  $\lambda$ . Define

$$|\tilde{\psi}(\lambda)\rangle \equiv e^{i\lambda\tilde{O}}|\tilde{\psi}\rangle, \tag{3.5.24}$$

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  $\lambda$ . Since for any state  $\rho$ , 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  $\lambda$ . Therefore, for any two  $\lambda, \lambda'$ ,  $(\tilde{\psi}(\lambda))_{M'} = (\tilde{\psi}(\lambda'))_{M'}$ , which means

$$S(\tilde{\psi}(\lambda)|\tilde{\psi}(\lambda'), M') = 0. \tag{3.5.25}$$

So, from 3.5.22, we have

$$0 = S(\tilde{\psi}(\lambda)|\tilde{\psi}(\lambda'), M') = S(\mathrm{Tr}_A(V\tilde{\psi}(\lambda)V^\dagger)|\mathrm{Tr}_{\bar{A}}(V\tilde{\psi}(\lambda')V^\dagger)), \tag{3.5.26}$$

which further implies that  $\mathrm{Tr}_A(V\tilde{\psi}(\lambda)V^\dagger)$  is independent of  $\lambda$ , which itself implies that  $|\tilde{\psi}(\lambda)\rangle$  itself is independent of  $\lambda$ . Returning to 3.5.23, we see that it is independent of  $\lambda$ , and so in particular its first variation with respect to  $\lambda$  must vanish. This is proportional to  $\langle \tilde{\psi}|[P_L V^\dagger X_{\bar{A}} V P_L, \tilde{O}]|\tilde{\psi}\rangle$ , so we have

$$0 = \langle \tilde{\psi}|[P_L V^\dagger X_{\bar{A}} V P_L, \tilde{O}]|\tilde{\psi}\rangle = \langle \tilde{\psi}|[V^\dagger P_{\mathrm{code}} X_{\bar{A}} P_{\mathrm{code}} V, \tilde{O}]|\tilde{\psi}\rangle \tag{3.5.27}$$

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

# Chapter 4

## Examples

The notation in the previous chapter is rather dense and difficult to understand. We therefore present some simple examples to try and elucidate the structure of the proof of theorem 3.5.1. First, we recall some basic facts we've talked about so far to keep them all for easy reference.

We say a triplet  $(V, A, M)$  of an encoding isometry  $V : \mathcal{H}_L \rightarrow \mathcal{H} \cong \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ , a subregion  $A$ , and von Neumann algebra  $M$  on  $\mathcal{H}_L$  has an *RT formula* if

$$S(\text{Tr}_{\bar{A}}(V\rho V^\dagger)) = S(\rho, M) + \text{Tr}(\rho\mathcal{L}) \quad (4.0.1)$$

for any state  $\rho$  on  $\mathcal{H}_L$  and some *area operator*  $\mathcal{L} \in \mathcal{L}(\mathcal{H}_L)$ . The *algebraic entropy*  $S(\rho, M)$  is defined as

$$S(\rho, M) = - \sum_{\alpha} p_{\alpha} \log(p_{\alpha}) + \sum_{\alpha} p_{\alpha} S(\rho_{L_{\alpha}}). \quad (4.0.2)$$

In some sense, this splits the algebraic entropy into a ‘classical’ part  $S_c \equiv - \sum_{\alpha} p_{\alpha} \log(p_{\alpha})$  (which is just the Shannon entropy of a discrete probability distribution taking values  $\{p_{\alpha}\}$ ), and a ‘quantum’ part  $S_q \equiv \sum_{\alpha} p_{\alpha} S(\rho_{L_{\alpha}})$  (which is the sum of the von Neumann entropies of the reduced states  $\rho_{L_{\alpha}}$ , weighted by the probabilities  $p_{\alpha}$ ). Moreover, the left hand side of the RT formula is in some sense the von Neumann entropy of the state  $\rho$  on the subregion  $A$ , which we denote  $S_A$ . We therefore express the RT formula in full as

$$\underbrace{S(\text{Tr}_{\bar{A}}(V\rho V^\dagger))}_{S_A} = - \underbrace{\sum_{\alpha} p_{\alpha} \log(p_{\alpha})}_{S_c} + \underbrace{\sum_{\alpha} p_{\alpha} S(\rho_{L_{\alpha}})}_{S_q} + \text{Tr}(\rho\mathcal{L}). \quad (4.0.3)$$

Following [6], we present some examples of operator-algebra erasure codes which one, two, or all three of the classical, quantum, and area terms in their RT formula.

We express all the isometries as *quantum circuits*, and familiarity with these is assumed; for a summary, see appendix ????.

To analyse the codes, we need to make use of a uniqueness theorem of [6], which we state without proof.

**Theorem 4.0.1.** *Suppose  $V : \mathcal{H}_L \rightarrow \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$  is an encoding isometry, and  $A$  is a subregion. Let  $M \equiv V^\dagger(\mathcal{L}(\mathcal{H}_A) \otimes I_{\bar{A}})V$  be the image of operators on  $\mathcal{H}_A$  projected back onto  $\mathcal{H}_L$  under  $V$ . If  $M$  is a von Neumann algebra, then it is the **unique** von Neumann algebra such that  $(V, A, M)$  satisfy complementary recovery. If not, then no such von Neumann algebra exists.*

Combined with theorem 3.5.1, this gives a series of steps to compute the area operator of the RT formula for a given code. These are

1. Calculate  $M = V^\dagger(\mathcal{L}(\mathcal{H}_A) \otimes I_{\bar{A}})V$  and check it is a von Neumann algebra to verify that we have complementary recovery.
2. Compute the Wedderburn decomposition of  $\mathcal{H}_L$  induced by  $M$ , and follow 3.4.1 to define a basis  $|\widetilde{\alpha, i, j}\rangle$  which lines up with  $M$ .
3. Apply 3.4.1 twice to obtain unitaries  $U_A$  and  $U_{\bar{A}}$  such that  $U_A U_{\bar{A}} V |\widetilde{\alpha, i, j}\rangle = |\alpha, i\rangle \otimes |\chi_\alpha\rangle \otimes |\alpha, j\rangle$ .
4. Following theorem 3.5.1, obtain the states  $|\chi_\alpha\rangle$  and compute their entanglement entropies across  $A_2$  and  $\bar{A}_2$ ; these are the eigenvalues of  $\mathcal{L}$ .

## 4.1 Codes with one term

We start with some codes which have only a single term on the right hand side of the RT formula. To make sense of these, recall that the von Neumann algebra  $M$  on  $\mathcal{H}_L$  induces a decomposition

$$\mathcal{H}_L = \bigoplus_{\alpha} (\mathcal{H}_{L_\alpha} \otimes \mathcal{H}_{\bar{L}_\alpha}). \quad (4.1.1)$$

This expression takes into account the fact that the tensor factors  $\mathcal{H}_{L_\alpha}$  and  $\mathcal{H}_{\bar{L}_\alpha}$  may vary in dimensionality with  $\alpha$ . To keep these examples simple, we don't consider cases such as these. We therefore relabel

$$\mathcal{H}_{L_\alpha} \rightarrow \mathcal{H}_i, \quad \mathcal{H}_{\bar{L}_\alpha} \rightarrow \mathcal{H}_j, \quad (4.1.2)$$

so both of  $\mathcal{H}_i$  and  $\mathcal{H}_j$  are encoded by a qubit, or are not present at all. Moreover, we limit  $\alpha$  to take at most two values, so  $\alpha = 0$  or  $\alpha \in \{0, 1\}$  depending on

our specific example. When  $\alpha$  has two degrees of freedom, we encode it in its own Hilbert space  $\mathcal{H}_\alpha = \mathbb{C}^2$ , where each element of the computational basis keeps track of which  $\alpha$ -block of the decomposition we are in. Essentially, in this case we are expressing the Hilbert space isomorphism

$$\mathcal{H}_L = \bigoplus_{\alpha=0}^1 (\mathcal{H}_i \otimes \mathcal{H}_j) \cong \mathcal{H}_\alpha \otimes \mathcal{H}_i \otimes \mathcal{H}_j. \quad (4.1.3)$$

The benefit of doing this is that we can specify the encoding isometry  $V$  as quantum circuits as stated, acting on qubits.

### Example 1

In this example, we choose  $\mathcal{H}_i$  and  $\mathcal{H}_j$  to not be present, but allow  $\alpha \in \{0, 1\}$  to have its own qubit. The logical space is then

$$\mathcal{H}_L = \mathcal{H}_\alpha = \mathbb{C}^2. \quad (4.1.4)$$

Our encoding isometry is

$$V_1 \equiv \begin{array}{c} \alpha \text{ --- } \bullet \text{ --- } A \\ |0\rangle \text{ --- } \oplus \text{ --- } \bar{A} \end{array} \quad (4.1.5)$$

and we pick  $\mathcal{H}_A$  to be the first qubit on the right, and  $\mathcal{H}_{\bar{A}}$  to be the second. In terms of the computational basis  $\{|0\rangle, |1\rangle\}$ , we can write this algebraically as

$$V = |00\rangle_{A\bar{A}} \langle 0|_\alpha + |11\rangle_{A\bar{A}} \langle 1|_\alpha. \quad (4.1.6)$$

Following the uniqueness theorem, we compute the von Neumann algebra by calculating  $V^\dagger(\mathcal{L}(\mathcal{H}_A) \otimes I_{\bar{A}})V$ . We can express any operator  $O \in \mathcal{L}(\mathcal{H}_A) \otimes I_{\bar{A}}$  in terms of the Pauli matrices:

$$O = \alpha(I_A \otimes I_{\bar{A}}) + \beta(X_A \otimes I_{\bar{A}}) + \gamma(Y_A \otimes I_{\bar{A}}) + \delta(Z_A \otimes I_{\bar{A}}), \quad (4.1.7)$$

where  $\alpha, \dots, \delta \in \mathbb{C}$ , and then

$$V^\dagger O V = \alpha I + \delta Z. \quad (4.1.8)$$

$M$  is therefore the von Neumann algebra of diagonal operators on  $\mathcal{H}_\alpha$ . So, consider an arbitrary state  $\rho$  on  $\mathcal{H}_L$ . The algebraic state  $\rho_M$  is just the state consisting of the diagonal elements of  $\rho$

$$\rho_M = p_0 |0\rangle \langle 0| + p_1 |1\rangle \langle 1| \quad (4.1.9)$$

for some constants  $p_0$  and  $p_1$  summing to 1. Classically, we cannot say which of the two states the system is in, so observables in  $M$  can only measure a classical uncertainty in the state corresponding to the probabilities  $p_0$  and  $p_1$ , and cannot distinguish any superposition over  $\alpha$  from this. The algebraic entropy therefore reduces to just the classical term  $S(\rho, M) = S_c$ . Moreover, we calculate that  $\text{Tr}_{\bar{A}}(V\rho V^\dagger) = p_0 |0\rangle\langle 0| + p_1 |1\rangle\langle 1|$ . So the entropy  $S_A$  exactly matches  $S_c$ , and the full RT formula is just

$$S(\text{Tr}_{\bar{A}}(V\rho V^\dagger)) = - \sum_{\alpha=0}^1 p_\alpha \log p_\alpha. \quad (4.1.10)$$

This means we have a trivial area operator  $\mathcal{L} = 0$ . Interestingly,  $M$  is its own centre and is non-trivial, so even an algebra with a non-trivial centre can have a trivial area operator.

### Example 2

We now present a slightly degenerate example. We choose  $\mathcal{H}_i$  and  $\mathcal{H}_j$  to not be present again, but also restrict  $\alpha = 0$ . The logical Hilbert space is therefore one-dimensional, with  $\mathcal{H}_L = \mathbb{C}$ . We can still however define a single state:  $\rho = 1$ . Our encoding isometry is

$$V \equiv \begin{array}{c} |+\rangle \text{---} \bullet \text{---} A \\ |0\rangle \text{---} \oplus \text{---} \bar{A} \end{array} \quad (4.1.11)$$

which just prepares a Bell state:

$$V = |\Phi\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (4.1.12)$$

$S_A$  is therefore  $S(|\Phi\rangle\langle\Phi|) = \log 2$ , and the von Neumann algebra is just the set of scalars, so  $S(\rho, M) = 0$ . The RT formula is therefore achieved by choosing  $\mathcal{L} = \log 2$ , as then  $S_A = \log 2 = \text{Tr}(\rho\mathcal{L})$  as required.

### Example 3

In this example, we choose  $\alpha = 0$ , but allow each of  $\mathcal{H}_i$  and  $\mathcal{H}_j$  to be qubits, so  $\mathcal{H}_i = \mathcal{H}_j = \mathbb{C}^2$ . In full,  $\mathcal{H}_L = \mathcal{H}_i \otimes \mathcal{H}_j = \mathbb{C}^2 \otimes \mathbb{C}^2$ . Our encoding isometry is simply the identity

$$V \equiv \begin{array}{c} i \text{---} A \\ j \text{---} \bar{A} \end{array} \quad (4.1.13)$$

We have  $\mathcal{H}_i = \mathcal{H}_A$  and  $\mathcal{H}_j = \mathcal{H}_{\bar{A}}$ , so  $S_A = S(\text{Tr}_j(\rho))$  for arbitrary state  $\rho$ . Moreover,  $M = \mathcal{L}(\mathcal{H}_i) \otimes I_j$ , so the distribution over blocks is trivial with  $p_0 = 1$ , and the classical part of  $S(\rho, M)$  vanishes, leaving us with  $S(\rho, M) = S_q = S(\text{Tr}_j(\rho))$ . Therefore, we necessarily have  $\mathcal{L} = 0$  for the area operator.

## 4.2 Codes with two terms

In this section, we present some codes in which the RT formula has two terms on the right hand side. These examples are built up by combining the single term examples in various ways. There's a bit more complexity in the physical Hilbert space though, so we go through this first. Recall that in theorem 3.5.1,  $\mathcal{H}_A$  and  $\mathcal{H}_{\bar{A}}$  were decomposed into

$$\mathcal{H}_A = \bigoplus_{\alpha} (\mathcal{H}_{A_1^{\alpha}} \otimes \mathcal{H}_{A_2^{\alpha}}) \oplus \mathcal{H}_{A_3}, \quad \mathcal{H}_{\bar{A}} = \bigoplus_{\alpha} (\mathcal{H}_{\bar{A}_1^{\alpha}} \otimes \mathcal{H}_{\bar{A}_2^{\alpha}}) \oplus \mathcal{H}_{\bar{A}_3}. \quad (4.2.1)$$

As with the decomposition of  $\mathcal{H}_L$ , the  $\alpha$ -dependence allows dependence of dimensionality of the tensor factors on which  $\alpha$ -block we are in. In these examples, this is not the case. The presence of  $\mathcal{H}_{A_3}$  allows us to factor only the image of  $V$  in  $\mathcal{H}_A$  and  $\mathcal{H}_{\bar{A}}$ , which is what we do. Following what we did for  $\mathcal{H}_L$ , we therefore factorise as

$$\mathcal{H}_A = \mathcal{H}_{A_{\alpha}} \otimes \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}, \quad \mathcal{H}_{\bar{A}} = \mathcal{H}_{\bar{A}_{\alpha}} \otimes \mathcal{H}_{\bar{A}_1} \otimes \mathcal{H}_{\bar{A}_2}, \quad (4.2.2)$$

with the  $\mathcal{H}_{A_{\alpha}}$  and  $\mathcal{H}_{\bar{A}_{\alpha}}$  factors only present if we have an example with two  $\alpha$ -blocks. The fact that the  $\alpha$  degree of freedom is visible from both  $A$  and  $\bar{A}$  is where the pseudo-classical behaviour of the codes comes from. In these examples, we label the right hand side of our circuits with the associated decomposition of  $\mathcal{H}_A$  and  $\mathcal{H}_{\bar{A}}$  as well.

Recall as well in 3.5.1 that the decompositions above allowed us to show that there exist unitaries  $U_A$  and  $U_{\bar{A}}$  such that for codes with complementary recovery

$$U_A U_{\bar{A}} V |\alpha, i, j\rangle = |\alpha, i\rangle_{A_{\alpha} A_1} \otimes |\chi_{\alpha}\rangle_{A_2 \bar{A}_2} \otimes |\alpha, j\rangle_{\bar{A}_{\alpha} \bar{A}_1} \quad (4.2.3)$$

in our new notation. In our examples,  $U_A$  and  $U_{\bar{A}}$  will always be the identity.

#### Example 4

This example is perhaps the most intuitive so far, as all three of the tensor factors of  $\mathcal{H}_L = \mathcal{H}_\alpha \otimes \mathcal{H}_i \otimes \mathcal{H}_j$  are qubits. Our encoding isometry is the circuit

$$V = \begin{array}{ccc} \alpha & \text{---} \bullet & A_\alpha \\ i & \text{---} | & A_1 \\ |0\rangle & \text{---} \oplus & \bar{A}_\alpha \\ j & \text{---} & \bar{A}_1 \end{array} \quad (4.2.4)$$

We have chosen  $A$  to be the first two qubits, and  $\bar{A}$  to be the last two. We begin by computing  $M = V^\dagger(\mathcal{L}(\mathcal{H}_A) \otimes I_{\bar{A}})$ . Analogously to example 1,  $M$  has access to all diagonal operators on  $\mathcal{H}_\alpha$  (via  $\mathcal{H}_{A_\alpha}$ ), and analogously to example 3, it also has full access to all operators on  $\mathcal{H}_i$ .  $M$  also must necessarily act as the identity on  $\mathcal{H}_j$ . The centre  $Z_M$  is non-trivial: while it must act as the identity on  $\mathcal{H}_i$  and  $\mathcal{H}_j$ , it can act non-trivially on  $\mathcal{H}_\alpha$  as a diagonal operator.

Since we have decomposition  $\mathcal{H}_L = \mathcal{H}_\alpha \otimes \mathcal{H}_i \otimes \mathcal{H}_j$ , we note that the basis  $\{|\widetilde{\alpha, i, j}\rangle\}$  of  $\mathcal{H}_L$  which lines up with  $M$  is just  $|\widetilde{\alpha, i, j}\rangle = |\alpha\rangle |i\rangle |j\rangle$ . Considering how our isometry acts on such a basis element, we explicitly have

$$V |\widetilde{\alpha, i, j}\rangle = |\alpha\rangle_{A_\alpha} |i\rangle_{A_1} |\alpha\rangle_{\bar{A}_\alpha} |j\rangle_{\bar{A}_1}. \quad (4.2.5)$$

Comparing with 4.2.3, we see that we can clearly pick both unitaries  $U_A$  and  $U_{\bar{A}}$  to be identities, and the states  $|\alpha, i\rangle_{A_\alpha A_1} = |\alpha\rangle_{A_\alpha} |i\rangle_{A_1}$  and  $|\alpha, j\rangle_{\bar{A}_\alpha \bar{A}_1} = |\alpha\rangle_{\bar{A}_\alpha} |j\rangle_{\bar{A}_1}$  also factorise cleanly. We do not however have any  $|\chi_\alpha\rangle$  states (as we have no  $A_2$  and  $\bar{A}_2$  subsystems), so we see that  $\mathcal{L} = 0$  as it only has zero eigenvalues and the RT formula has no area term.

Now, the  $\alpha$  degree of freedom is visible from both  $A$  and  $\bar{A}$ , so acts as though it has been measured from the point of view of  $A$ , giving the classical term  $S_c$  on the right hand side. The  $i$  and  $j$  qubits may be entangled with  $\mathcal{H}_\alpha$ , so after measurement it will collapse to one of the  $\rho_\alpha$  states from the decomposition  $\rho_M = p_0 \rho_0 + p_1 \rho_1$ . The quantum term  $S_q$  then reduces to the probability  $p_\alpha$  corresponding to  $\rho_\alpha$ , multiplied by the von Neumann entropy of  $\rho_\alpha$  reduced to  $\mathcal{H}_i$ . In full, the RT formula is

$$S(\text{Tr}_{\bar{A}}(V \rho V^\dagger)) = - \sum_{\alpha} p_\alpha \log(p_\alpha) + \sum_{\alpha} p_\alpha S(\text{Tr}_j(\rho_\alpha)). \quad (4.2.6)$$



### Example 5

In this next code, we have the full  $\mathcal{H}_\alpha$  system, but no  $\mathcal{H}_i$  or  $\mathcal{H}_j$ . Our encoding isometry is

$$V = \begin{array}{c} \alpha \text{ --- } \bullet \text{ --- } \bullet \text{ --- } A_\alpha \\ |+\rangle \text{ --- } \bullet \text{ --- } A_2 \\ |0\rangle \text{ --- } \oplus \text{ --- } \bar{A}_\alpha \\ |0\rangle \text{ --- } \oplus \text{ --- } \bar{A}_2 \end{array} \quad (4.2.7)$$

As in example 1, the von Neumann algebra  $M$  is just the set of diagonal operators on  $\mathcal{H}_\alpha$ . The algebraic entropy  $S(\rho, M)$  will therefore again just be the classical Shannon entropy of the distribution  $\{p_\alpha\}$ .

We can actually be even more explicit with this example by considering a logical pure state  $|\psi\rangle = a|0\rangle + b|1\rangle$ , where  $|a|^2 = p_0$  and  $|b|^2 = p_1$ . We calculate  $V|\psi\rangle$  as

$$V|\psi\rangle = a|0+00\rangle + \frac{b}{\sqrt{2}}(|1010\rangle + |1111\rangle), \quad (4.2.8)$$

from which we can calculate the reduced state for the density operator  $\rho = |\psi\rangle\langle\psi|$  corresponding to our qubit:

$$\text{Tr}_{\bar{A}}(V\rho V^\dagger) = |a|^2|0+\rangle\langle 0+|_{A_\alpha A_2} + |b|^2\left(|1\rangle\langle 1|_{A_\alpha} \otimes \frac{I_{A_2}}{2}\right). \quad (4.2.9)$$

Therefore, the entropy  $S_A$  is

$$\begin{aligned} S_A &= -(|a|^2 \log |a|^2 + |b|^2 \log |b|^2) + |b|^2 S\left(\frac{I_{A_2}}{2}\right) \\ &= -\sum_{\alpha=0}^1 p_\alpha \log p_\alpha + \text{Tr}\left(\rho \begin{pmatrix} 0 & 0 \\ 0 & \log 2 \end{pmatrix}\right). \end{aligned} \quad (4.2.10)$$

So for this pure case, the area operator is explicitly  $\mathcal{L} = \log 2 \cdot |1\rangle\langle 1|$ . This matches what we expect: comparing with 4.2.3, we see that we have for this isometry

$$V|\widetilde{\alpha}, i, j\rangle = |\alpha\rangle_{A_\alpha} \otimes |\chi_\alpha\rangle_{A_2 \bar{A}_2} \otimes |\alpha\rangle_{\bar{A}_\alpha} \quad (4.2.11)$$

where  $|\chi_0\rangle = |00\rangle$  and  $|\chi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  is a Bell state. So since  $S(\text{Tr}_{\bar{A}}(|\chi_0\rangle\langle\chi_0|)) = 0$  and  $S(\text{Tr}_{\bar{A}}(|\chi_1\rangle\langle\chi_1|)) = \log 2$ ,  $\mathcal{L} = \sum_{\alpha=0}^1 S(\text{Tr}_{\bar{A}}(|\chi_\alpha\rangle\langle\chi_\alpha|)) \cdot I_\alpha$  matches what we found.

### Example 6

This example has  $\alpha = 1$ , and each of  $\mathcal{H}_i$  and  $\mathcal{H}_j$  are qubits. Our encoding isometry is

$$V = \begin{array}{c} i \text{ --- } A_1 \\ |+\rangle \text{ --- } A_2 \\ j \text{ --- } \bar{A}_1 \\ |0\rangle \text{ --- } \bar{A}_2 \end{array} \quad (4.2.12)$$

Analogously to example 3 again,  $M = \mathcal{L}(\mathcal{H}_i) \otimes I_j$ . Since there is only one value of  $\alpha$ , the classical part  $S_q = 0$ , and the only contribution to the algebraic entropy  $S(\rho, M)$  is the entropy of the reduced state on  $\mathcal{H}_i$ , so  $S(\text{Tr}_j(\rho))$ .

However, since there is a Bell state shared across  $A_2$  and  $\bar{A}_2$ , its entropy contributes to  $S_A$ . Explicitly, comparing with 4.2.3, we have

$$V |\widetilde{\alpha, i, j}\rangle = |i\rangle_{A_1} \otimes |\chi_0\rangle_{A_2 \bar{A}_2} \otimes |j\rangle_{\bar{A}_1}, \quad (4.2.13)$$

where  $|\chi_0\rangle$  is again a Bell state. We therefore have area operator  $\mathcal{L} = \log 2 \cdot I$ .

## 4.3 A Complete Example

We now present an example of a code in which *all* terms of the RT formula are present. All the terms in the decomposition  $\mathcal{H}_L = \mathcal{H}_\alpha \otimes \mathcal{H}_i \otimes \mathcal{H}_j$  are present, as are all terms in the decompositions of  $\mathcal{H}_A$  and  $\mathcal{H}_{\bar{A}}$ . The encoding isometry is given by

$$V = \begin{array}{c} \alpha \text{ --- } A_\alpha \\ i \text{ --- } A_1 \\ |+\rangle \text{ --- } A_2 \\ |0\rangle \text{ --- } \bar{A}_\alpha \\ j \text{ --- } \bar{A}_1 \\ |0\rangle \text{ --- } \bar{A}_2 \end{array} \quad (4.3.1)$$

Analogously to example 4,  $M$  has full access to operators on  $\mathcal{H}_i$  (via  $\mathcal{H}_{A_1}$ ); analogously to example 1, it has full access to diagonal operators on  $\mathcal{H}_\alpha$  (via  $\mathcal{H}_{A_\alpha}$ ); and it has no access to  $\mathcal{H}_j$ , so must act as the identity on it. The basis lining up with  $M$  therefore decomposes as  $|\widetilde{\alpha, i, j}\rangle = |\alpha\rangle |i\rangle |j\rangle$ . Applying the isometry to this basis state, we get the full form of 4.2.3

$$V |\widetilde{\alpha, i, j}\rangle = |\alpha, i\rangle_{A_\alpha A_1} \otimes |\chi_\alpha\rangle_{A_2 \bar{A}_2} \quad (4.3.2)$$

where  $|\alpha, i\rangle = |\alpha\rangle |i\rangle$ ,  $|\alpha, j\rangle = |\alpha\rangle |j\rangle$  both decompose, and the  $|\chi_\alpha\rangle$  are

$$|\chi_0\rangle_{A_2\bar{A}_2} = |+\rangle_{A_2} |0\rangle_{\bar{A}_2}, \quad |\chi_1\rangle_{A_2\bar{A}_2} = \frac{1}{\sqrt{2}}(|00\rangle_{A_2\bar{A}_2} + |11\rangle_{A_2\bar{A}_2}). \quad (4.3.3)$$

Following example 5, we see that we again prepare a Bell state on  $\mathcal{H}_{A_2} \otimes \mathcal{H}_{\bar{A}_2}$ , so the same calculation implies that the area operator is  $\mathcal{L} = \log 2 |1\rangle \langle 1|_\alpha$ . However, we also have all the pieces of example 4, so the algebraic entropy has both a classical and a quantum term, and so we have all three terms on the left hand side of the RT formula.

# 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 Information and Entropy

In this appendix, we present the necessary background in information theory to understand this dissertation. We will begin with some *classical* information theory to present the subject and build some intuition, before describing the quantum generalisations. We follow the textbook of Nielsen and Chuang[14] in presentation. Note that there are several other information-theoretic quantities which we don't describe here. We limit ourselves to only those definitions which are directly relevant to this dissertation.

### A.1 Classical Information

#### A.1.1 Shannon Entropy

The key concept of classical information theory is the *Shannon entropy* of a random variable  $X$ . Intuitively, this is a way of quantifying the information gained when we learn the value of  $X$ , or alternatively, the uncertainty about  $X$  before we learn its value. To define Shannon entropy, suppose we wish to quantify how much information is provided by an event  $E$  which may occur in a probabilistic experiment. To do this, we define an 'information function'  $I(E)$ , which we intuitively suppose should obey the following axioms:

1.  $I(E)$  is a function of the probability the event  $E$  occurs only, so we can write  $I = I(p)$ , where  $p \in [0, 1]$ .
2.  $I$  should be a smooth function of probability.

3. The information gained when two independent events occur with individual probabilities  $p$  and  $q$  should be equal to the sum of the information gained from each event alone; that is,  $I(pq) = I(p) + I(q)$ .

With these axioms, it's not hard to show that  $I(p) = k \log p$ , where  $k$  is a real constant. This therefore motivates the following definition of Shannon entropy.

**Definition A.1.1.** Suppose  $X$  is a discrete random variable, taking values  $x_n$  with probabilities  $p_n$ . The **Shannon entropy** of  $X$  is given by

$$H(X) \equiv - \sum_n p_n \log p_n. \quad (\text{A.1.1})$$

When Claude Shannon defined this, he chose the logarithm to be with base 2. This is arbitrary, and we choose the convention that the definition involves the *natural logarithm*, with base  $e$ .

**Example A.1.1** (Binary entropy). *Suppose  $X$  is a Bernoulli random variable, taking values  $x_0$  and  $x_1$  with probabilities  $p$  and  $1 - p$  respectively. The Shannon entropy of  $X$  is then*

$$H(X) \equiv H_{\text{bin}}(p) = -p \log p - (1 - p) \log (1 - p). \quad (\text{A.1.2})$$

*Note that this attains its maximum value for  $p = 1/2$ . This matches our intuition that entropy should be a measure of uncertainty in  $X$  before we measure it: if  $p = 1/2$ , we have maximum uncertainty as to whether a measurement of  $X$  will return  $x_0$  or  $x_1$ . To the contrary, if  $p = 0.999$ , even before measuring  $X$  we could say with some degree of certainty that  $X$  will return  $x_0$ .*

## A.1.2 Relative Entropy

The *relative entropy* is a measure of the ‘closeness’ of two probability distributions  $p(x)$  and  $q(x)$ , over the same index set  $x$ .

**Definition A.1.2.** Suppose  $p(x)$  and  $q(x)$  are two probability distributions, indexed over  $x$ . The **relative entropy** of  $p(x)$  to  $q(x)$  is given by

$$H(p(x) \| q(x)) \equiv \sum_x p(x) \log \frac{p(x)}{q(x)} = -H(X) - \sum_x p(x) \log q(x), \quad (\text{A.1.3})$$

where  $X$  is a random variable under probability distribution  $p$ .

It is not immediately obvious why this is a good definition for a distance between two distributions. The following theorem gives a starting point as to why this is the case.

**Theorem A.1.1.**  $H(p(x)||q(x)) \geq 0$ , so the relative entropy is non-negative, with equality if and only if  $p(x) = q(x)$  for all  $x$ .

**Example A.1.2.** Suppose  $X \sim p(x)$  is a random variable following discrete distribution  $p(x)$ , where the index set  $x$  takes  $d$  values. Set  $Y \sim q(x) \equiv 1/d$  to be the uniform distribution over  $x$ . Then:

$$H(p(x)||q(x)) = -H(X) - \sum_x p(x) \log \frac{1}{d} = \log d - H(X). \quad (\text{A.1.4})$$

Note that non-negativity therefore implies that  $H(X) \leq \log d$ ; an occasionally useful fact about entropy.

## A.2 Quantum Information

### A.2.1 von Neumann Entropy

Shannon entropy measures the uncertainty of random variables associated with classical probability distributions; quantum states are similarly associated with probabilities, with density operators replacing classical probability distributions. We therefore wish to define a similar measure of uncertainty for states. To motivate a definition, consider an ensemble of pure quantum states  $\{\rho_n\}$  occurring with corresponding probabilities  $\{p_n\}$ . The density operator for this system is then

$$\rho = \sum_n p_n \rho_n. \quad (\text{A.2.1})$$

If the set of states  $\{\rho_n\}$  are all orthogonal, this ensemble should behave exactly like a classical random variable following probability distribution  $\{p_n\}$ . A quantum measure of entropy should therefore reduce to  $H(p_n)$  in this case. With this idea in mind, we can define the so-called *von Neumann entropy*, which satisfies this intuition.

**Definition A.2.1.** Given a quantum state described by density operator  $\rho$  on  $\mathcal{H}$ , its **von Neumann entropy** is defined as

$$S(\rho) \equiv -\text{Tr}_{\mathcal{H}}(\rho \log \rho), \quad (\text{A.2.2})$$

where  $\log$  refers to the natural matrix logarithm.

The matrix logarithm is often quite computationally difficult to calculate. However, if we write  $\rho$  in terms of its eigenvectors  $\{|i\rangle\}$  and corresponding eigenvalues  $\{\eta_i\}$  as  $\rho = \sum_i \eta_i |i\rangle \langle i|$ , the von Neumann entropy is simply

$$S(\rho) = - \sum_i \eta_i \log \eta_i. \quad (\text{A.2.3})$$

**Example A.2.1.** *In this example, we consider two states in a two-state system with basis  $\{|0\rangle, |1\rangle\}$ . First, consider the state*

$$\rho = \frac{1}{2} (|0\rangle \langle 0| + |1\rangle \langle 1|) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (\text{A.2.4})$$

*The states  $|0\rangle \langle 0|$  and  $|1\rangle \langle 1|$  are orthogonal, so perfectly distinguishable; we therefore cannot say classically which of the two states the system is in, so we expect the von Neumann entropy to reduce to  $H_{\text{bin}}(1/2) = \log 2$ . This is exactly what we observe:*

$$S(\rho) = -\text{Tr}(\rho \log \rho) = -\frac{1}{2} \log \frac{1}{2} - \frac{1}{2} \log \frac{1}{2} = \log 2. \quad (\text{A.2.5})$$

*Alternatively, consider the state*

$$\sigma = \frac{1}{2} (|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| + |1\rangle \langle 1|) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}. \quad (\text{A.2.6})$$

*The von Neumann entropy is then*

$$S(\sigma) = -\text{Tr}(\sigma \log \sigma) = -1 \log 1 - 0 \log 0 = 0. \quad (\text{A.2.7})$$

*This vanishes because  $\sigma$  actually describes a pure state*

$$\sigma = \frac{1}{2} (|0\rangle + |1\rangle)(\langle 0| + \langle 1|), \quad (\text{A.2.8})$$

*so we can classically say the system described by  $\sigma$  is in the corresponding state with certainty.*

**Example A.2.2** (Quantum vs Classical Entropy). *Consider the density operator describing a superposition between two non-orthogonal states:*

$$\rho = p \underbrace{|0\rangle \langle 0|}_{\rho_0} + (1-p) \cdot \underbrace{\frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|)}_{\rho_1}. \quad (\text{A.2.9})$$

*This is a mixed state describing an ensemble of  $\rho_0$  and  $\rho_1$  with probabilities  $p$  and  $1-p$ . Classically, if this was the case the entropy of the ensemble would be given by*



$H_{bin}(p)$ . However, quantum effects mean that the lack of orthogonality between  $\rho_0$  and  $\rho_1$  generates cross terms in the density operator which modifies its eigenvalues. We can compute the eigenvalues of  $\rho$  as

$$\lambda_{\pm} \equiv \frac{1}{2} \left( 1 \pm \sqrt{1 - 2p(1-p)} \right), \quad (\text{A.2.10})$$

and so the von Neumann entropy is

$$S(\rho) = -\lambda_+ \log \lambda_+ - \lambda_- \log \lambda_- \neq H_{bin}(p). \quad (\text{A.2.11})$$

While this does not match the classical case, it does share some properties. They both vanish for  $p = 0, 1$ , which in the quantum case corresponds to there being no uncertainty in the system and  $\rho$  representing a pure state. They also both attain a maximum at  $p = 1/2$ , corresponding to the maximally mixed state.

## A.2.2 Relative Entropy

Similarly to the classical relative entropy measuring the distance between two probability distributions (without being a formal metric), there is a quantum relative entropy measuring the distance between two density operators without being a formal metric on the underlying Hilbert space. We define this as follows.

**Definition A.2.2.** Given two density operators  $\rho$  and  $\sigma$  on Hilbert space  $\mathcal{H}$ , the **relative entropy** between them is given by

$$S(\rho||\sigma) = -\text{Tr}_{\mathcal{H}} (\rho \log \rho - \rho \log \sigma) = -S(\rho) - \text{Tr}_{\mathcal{H}} (\rho \log \sigma). \quad (\text{A.2.12})$$

Once again, this is non-negative; a result called *Klein's inequality*

**Theorem A.2.1.** *The relative entropy is non-negative for any two states  $\rho$  and  $\sigma$ :*

$$S(\rho||\sigma) \geq 0. \quad (\text{A.2.13})$$

**Example A.2.3.** Suppose  $\rho$  and  $\sigma$  are states on a  $d$ -dimensional Hilbert space  $\mathcal{H}_d$ . Choose  $\sigma = I_d/d$  to be the maximally mixed state, proportional to the identity. Then, the relative entropy is given by

$$S(\rho||\sigma) = -S(\rho) - \text{Tr}_{\mathcal{H}_d} \left( \rho \log \frac{1}{d} \right) = -S(\rho) + \log d. \quad (\text{A.2.14})$$

Note then that non-negativity implies that  $S(\rho) \leq \log d$ .

### A.2.3 Properties of von Neumann Entropy

We now state some generic properties of von Neumann entropy, without proof. See [14] or any good set of notes on quantum information theory for proofs.

- $S(\rho) = 0$  if and only if  $\rho$  is a pure state.
- $S(\rho) = \log d$  is maximal for a  $d$ -dimensional Hilbert space if and only if  $\rho$  is a maximally mixed state (e.g.  $\rho$  is proportional to the identity).
- $S(\rho) = S(U\rho U^\dagger)$  is invariant under unitary transformations  $U$ ; this is just the statement that entropy is invariant under a change of basis.
- $S(\rho)$  is *concave*: given an ensemble of density operators  $\{\rho_i\}$  and probabilities  $\{p_i\}$ , we have

$$S\left(\sum_i p_i \rho_i\right) \geq \sum_i p_i S(\rho_i). \quad (\text{A.2.15})$$

- $S(\rho)$  satisfies the following bound, for the same set-up as the last property:

$$S\left(\sum_i p_i \rho_i\right) \leq \sum_i p_i S(\rho_i) - \sum_i p_i \log p_i = \sum_i p_i S(\rho_i) + H(p_i), \quad (\text{A.2.16})$$

with equality if the  $\rho_i$  are orthogonal.

- $S(\rho)$  is additive for independent systems. If  $\rho_A$  and  $\rho_B$  describe states in systems  $A$  and  $B$ , then

$$S(\rho_A \otimes \rho_B) = S(\rho_A) + S(\rho_B). \quad (\text{A.2.17})$$

- $S(\rho)$  is strongly subadditive: for any three systems  $A, B, C$ , we have

$$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{AC}). \quad (\text{A.2.18})$$

### A.2.4 Entropy as a Measure of Entanglement

Entanglement between quantum systems is notoriously a *very* hard quantity to quantify, particularly for more than two systems. However, for entanglement between precisely two systems, the von Neumann entropy can be used as a way to quantify the entanglement.

To build some intuition, suppose that we have a separable state of two systems

$A$  and  $B$ :  $|\Psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ . Consider the reduced density matrices on either system  $A$  or  $B$ :

$$\begin{aligned}\rho_A &= \text{Tr}_B (|\Psi_{AB}\rangle \langle \Psi_{AB}|) = |\psi_A\rangle \langle \psi_A| \\ \rho_B &= \text{Tr}_A (|\Psi_{AB}\rangle \langle \Psi_{AB}|) = |\psi_B\rangle \langle \psi_B|.\end{aligned}\tag{A.2.19}$$

Both of these are pure states, so  $S(\rho_A) = S(\rho_B) = 0$ . This is a result of our original state being separable;  $A$  and  $B$  were not entangled. Thus, we should expect that a non-zero von Neumann entropy for either of the reduced states to signify some degree of entanglement between  $A$  and  $B$ . We therefore take this as a definition of entanglement entropy.

**Definition A.2.3.** Suppose we have a quantum system of  $N$  particles, and a bipartition dividing it into a subsystem  $A$  of  $k$  particles and a subsystem  $B$  of  $l$  particles such that  $k + l = N$ . Suppose that the state of the system is described by  $\rho_{AB}$ . The *entropy of entanglement* for the bipartition is given by

$$S(\rho_A) = -\text{Tr}_A [\rho_A \log \rho_A] = -\text{Tr}_B [\rho_B \log \rho_B] = S(\rho_B),\tag{A.2.20}$$

where  $\rho_A = \text{Tr}_B (\rho_{AB})$  is the reduced state to subsystem  $A$  and similarly for  $\rho_B$ .

Note that this is not a unique definition of entanglement entropy. Some other common definitions include the *Renyi entanglement entropy*[15], or even simply relative entropy.

**Example A.2.4.** Consider the Bell state  $|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$ . This has density matrix

$$\rho_{AB} = \frac{1}{2} |\Psi\rangle \langle \Psi| = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},\tag{A.2.21}$$

which itself has zero entropy since it is a pure state. However, calculating the reduced density operators, we find

$$\begin{aligned}\rho_A &= \frac{1}{2}(|0\rangle \langle 0|_A + |1\rangle \langle 1|_A) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \rho_B &= \frac{1}{2}(|0\rangle \langle 0|_B + |1\rangle \langle 1|_B) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\end{aligned}\tag{A.2.22}$$

which have  $S(\rho_A) = S(\rho_B) = \log 2$ . This reflects the fact that the Bell states maximally entangle subsystems  $A$  and  $B$ .

# Appendix B

## Quantum Circuit Notation

In this appendix, we will introduce the graphical quantum circuit notation for quantum computations. This is adapted from Nielsen and Chuang[14]. We only describe the minimal set of features of a quantum circuit to understand our examples; for a more detailed explanation, we recommend consulting the above textbook.

### B.1 Quantum Gates

Generally, a quantum computation consists of taking a string of qubits  $|\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$  as an input, applying a series of unitary operators to specified qubits in turn, and outputting a string of qubits. In computing jargon, we call a unitary operator a *quantum gate* in this context. These can be as simple or as complex as we want; the *only* constraint is unitarity.

**Example B.1.1.** *Consider the qubit  $|\psi\rangle = a|0\rangle + b|1\rangle$ , with computational basis elements  $\{|0\rangle, |1\rangle\}$ . The quantum NOT gate, denoted  $X$ , is defined by its action on the computational basis as follows*

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle. \quad (\text{B.1.1})$$

*In matrix notation,  $X$  can be expressed as*

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (\text{B.1.2})$$

*Another quantum gate is the Hadamard gate, denoted  $H$ . This is defined by*

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle, \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle. \quad (\text{B.1.3})$$

In some sense, this rotates the computational basis elements by  $\pi/4$ . In matrix notation, it can be written

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (\text{B.1.4})$$

Both of these single-qubit gates are clearly unitary. However, gates don't have to act on only a single qubit. There are *multiple qubit gates*, which we give an example of too.

**Example B.1.2.** Consider the space of two qubits, with computational basis  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ . The *CNOT* (or controlled-*NOT*) gate is defined by

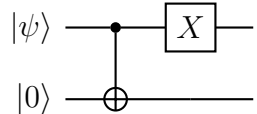
$$\begin{aligned} \text{CNOT} |00\rangle &= |00\rangle, & \text{CNOT} |10\rangle &= |11\rangle \\ \text{CNOT} |01\rangle &= |01\rangle, & \text{CNOT} |11\rangle &= |10\rangle. \end{aligned} \quad (\text{B.1.5})$$

This can be seen to act as a *NOT* gate on the second qubit if the first (or control) qubit is in the  $|1\rangle$  state, and as the identity if the control qubit is a  $|0\rangle$ . In matrix notation, it can be written as

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (\text{B.1.6})$$

## B.2 Quantum Circuits

Now we have defined a quantum gate, we can define a quantum circuit. Formally, a quantum circuit is an ordered sequence of quantum gates, measurements, and resets, all of which may be conditioned on the outcome of classical computations. In the simple examples in this dissertation, we do not consider any circuits involving measurements and resets; only quantum gates. Circuits are diagrammatically represented by quantum circuit notation, with the benefit being that it is far clearer to see which individual qubits a multiple-qubit gate may be acting on. The below diagram demonstrates a simple example.



$$\begin{array}{c} |\psi\rangle \\ |0\rangle \end{array} \begin{array}{c} \text{---} \bullet \text{---} \boxed{X} \text{---} \\ | \\ \oplus \end{array} \quad (\text{B.2.1})$$

We go through the pieces of this circuit step-by-step. The circuit takes an input state  $|\psi\rangle$  on the left, and adjoins on an ancillary qubit in the  $|0\rangle$  state. Moving to

the right, the symbol connecting the two wires signifies a  $CNOT$  gate, with the first qubit as control (denoted by the filled-in dot), and the second as the target (denoted by the circle with a cross). Finally, the  $X$  in a box signifies that the circuit acts on the first qubit with an  $X$  gate. We can be even more specific by considering the action of this circuit on an arbitrary input state  $|\psi\rangle = a|0\rangle + b|1\rangle$ . We have

$$a|0\rangle + b|1\rangle \xrightarrow{|0\rangle} a|00\rangle + b|10\rangle \xrightarrow{CNOT} a|00\rangle + b|11\rangle \xrightarrow{X_1} a|10\rangle + b|01\rangle. \quad (\text{B.2.2})$$

While this example doesn't really illustrate how powerful this notation is due to its simplicity, the salient features of a quantum circuit diagram are all present. Essentially, it is just a graphical notation for adjoining on ancillary qubits to a state, and then applying a series of unitary operators.

One gate which we haven't mentioned in our discussion is the *Toffoli gate*, which features in our examples. This is a three-qubit gate, which can be thought of as a "doubly controlled  $X$  gate". It acts as an  $X$  gate on the third qubit if and only if the first two qubits are in the  $|11\rangle$  state. In a quantum circuit diagram, this is denoted by the symbol


(B.2.3)

analogously to the  $CNOT$  gate.

# 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] R. JOZSA, *Quantum information and computation notes for part ii*. <https://www.qi.damtp.cam.ac.uk/files/PartIIIQC/Part%202%20QIC%20lecturenotes.pdf>, January 2019.
- [9] A. KITAEV, *Fault-tolerant quantum computation by anyons*, Annals of Physics, 303 (2003), pp. 2–30.
- [10] 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.

- [11] E. KNILL, R. LAFLAMME, AND W. H. ZUREK, *Resilient quantum computation*, Science, 279 (1998), pp. 342–345.
- [12] J. M. MALDACENA, *The Large  $N$  limit of superconformal field theories and supergravity*, Adv. Theor. Math. Phys., 2 (1998), pp. 231–252.
- [13] 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.
- [14] M. A. NIELSEN AND I. L. CHUANG, *Quantum Computation and Quantum Information*, Cambridge University Press, 10th ed., 2010.
- [15] A. RÉNYI, *On Measures of Entropy and Information*, Berkeley Symposium on Mathematical Statistics and Probability.
- [16] P. W. SHOR, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A, 52 (1995), pp. R2493–R2496.
- [17] —, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput., 26 (1997), p. 1484–1509.