Foundations of Quantum Information & Computation

Undergraduate Thesis

Submitted in partial fulfillment of the requirements of
BITS F421T Thesis

By

Shantom Kumar Borah
ID No. 2016A3B50114P

Under the supervision of:

Dr. R.R. Mishra

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE PILANI, PILANI CAMPUS
November 2020

Declaration of Authorship

I, Shantom Kumar Borah, declare that this Undergraduate Thesis titled, 'Foundations of Quantum Information & Computation' and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: Shantom Borah

Date: 26/11/2020

Certificate

This is to certify that the thesis entitled, "*Foundations of Quantum Information & Computation*" and submitted by Shantom Kumar Borah ID No. 2016A3B50114P in partial fulfillment of the requirements of BITS F421T Thesis embodies the work done by him under my supervision.

Supervisor
Dr. R.R. Mishra
Faculty,
BITS-Pilani Pilani Campus
Date:

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE PILANI, PILANI CAMPUS

Abstract

Foundations of Quantum Information & Computation

by Shantom Kumar Borah

The objective of this thesis is to explore the fundamental concepts and theoretical framework associated with the fields of Quantum Information and Quantum Computation. The major areas covered in this work include the Theory of Quantum Channels, Unit Resource Theories and Quantum Shannon Theory. Apart from the theoretical studies that have been undertaken as part of this work, a certain amount of computational work has also been conducted in the form of simulations involving IBM's Qiskit Library. These include the simulation of a number of prominent Quantum Algorithms, including the HHL and QAOA algorithms, as well as an end-to-end simulation of a full Quantum Communication System.

Acknowledgements

I would like to express my most sincere appreciation and gratitude to all the people who have helped me directly or indirectly in the process of carrying out my undergraduate thesis work as part of my undergraduate degree at BITS Pilani.

I am deeply indebted to my thesis supervisor, Dr. R.R. Mishra, who has been a great mentor, and has been an invaluable source of support, in guiding me and in helping me navigate through the various aspects of Quantum Information Theory.

Lastly, I would like to express my sincere gratitude to my family members for providing me with a safe and peaceful working environment and for being a constant source of support during these difficult times of COVID-19.

Contents

List of Figures

Chapter 1

Introduction

1.1 Overview

The field of Quantum Computation & Quantum Information originally launched in the 1980's due to certain speculations by Richard Feynman, who noted that it seemed to be very difficult to simulate quantum mechanical systems on a classical computer, on account of the very large sizes of the Hilbert Spaces involved. The Hilbert Space corresponding to a many body system grows exponentially with the number of particles involved in the system and thus, as the size of the simulated system increases, a classical computer soon finds itself out of depth.

Following Feynman's speculations, pioneers of the field questioned whether it was possible to use this apparent difficulty to our advantage instead. That is, they questioned whether it was possible to design new, inherently quantum models of computation, that could solve certain problems much faster than the Classical Turing Machine. After all, quantum systems have no trouble simulating themselves! So, in a sense, they were already achieving an exponential speedup over classical computers.

Quantum Computers attempt to leverage this apparent difficulty to solve problems that were hitherto considered unsolvable on any practical classical computer. That is, Quantum Computers leverage inherently quantum properties of quantum systems, such as entanglement and superposition, to achieve super-polynomial or exponential speedups in the solution of certain specific problems.

The first quantum algorithms to be published were the Deutsch [3] and the Deutsch-Jozsa [4] algorithms. These algorithms conclusively addressed the questions discussed in the previous paragraphs in the affirmative. Although the specific problems being solved by these algorithms were not particularly useful. The first indications of practical utility of Quantum Computers came with Peter Shor's demonstration that Quantum Computers can be used to efficiently factorize

products of large prime numbers [13], and subsequently break the famous RSA encryption technology. At around the same time, Shor also demonstrated the existence of quantum error correcting codes [14]. Following these developments, the field of Quantum Computation has since blossomed into an active research area and has remained so in the past two decades.

While the advent of efficient Quantum Algorithms and research efforts into practical implementations of quantum computers are fairly new in the annals of history, the theory of Quantum Information can be traced much further back. The quantum Von Neumann Entropy, the central quantity of interest in quantum information theory was developed by Von Neumann [16] as far back as 1932, even before Claude Shannon's seminal paper on Classical Information Theory [12].

More recently, since the 1990s, researchers in the field have started exploring generalizations of Shannon's Information Theory to quantum communication systems. The famous Noiseless Coding Theorem [12] of Classical Information Theory has been successfully generalized to the Quantum Noiseless Coding Theorem by Ben Schumacher [11]. Generalization of the Noisy Coding Theorem has proven more difficult. A closed form expression for the Quantum Channel Capacity is not yet known, although a number of special cases have been investigated [15, 6].

1.2 Outline of the Thesis

This thesis aims to explore the fundamental mathematical framework underlying Quantum Information Theory and Quantum Computation. The major topics covered include the Theory of Quantum Channels, Quantum Resource Theories, Quantum Shannon Theory and Quantum Algorithms. The Thesis includes a Capstone Project, involving the end-to-end simulation of a quantum communication system using the IBM Qiskit Library. The organization of the thesis is given as follows:

- **Chapter 2** describes the theory of Quantum Channels. The major representations of quantum channels, viz, the Choi, Kraus and Stinespring representations are described. Kraus Operator descriptions of some typical noisy quantum channels are also described.
- **Chapter 3** describes the three unit quantum protocols in quantum communication, viz, entanglement distribution, super-dense coding and teleportation. Resource inequalities for these protocols are also described. Finally, the construction of arbitrary quantum protocols from the unit protocols is discussed.
- **Chapter 4** describes the generalization of Shannon's Information Theory to quantum channels. The concept of typicality and its application to the noiseless coding theorem is discussed. An overview of quantum channel capacities for certain special cases is also provided.

- **Chapter 5** includes the results of simulations of certain Quantum Algorithms using IBM Qiskit. A link to the Github repository for the code is provided, along with detailed descriptions of the HHL and QAOA algorithms.
- **Chapter 6** describes the final capstone project associated with the Thesis, which involves the end-to-end simulation of a quantum communication system.

The entire code for this work may be found in: https://github.com/Arkonaire/Quantum-Algorithms.

Chapter 2

Quantum Channels & Representations

Quantum Channels encompass the set of all physical operations that may be physically applied to a quantum system. The quantum system in question may be a part of a larger quantum system and may even be entangled with other quantum systems. We begin the chapter by reviewing the postulates of quantum mechanics under the density operator formalism. We then define the axiomatic concept of a quantum channel in terms of CPTP linear maps. Thereafter, we develop the Choi-Kraus theorem as well as the representations of a quantum channel in the Choi and Kraus forms. We then present the concept of purifications of a quantum channel in the form of the Stinespring Dilation. Finally, we provide the Kraus representations of a few typical noise models often used in the study of quantum information.

2.1 Postulates of Quantum Mechanics

In this section, we provide a brief review of the fundamental postulates of quantum theory. Because systems in quantum information are typically open quantum systems that are often entangled with the environment, we shall use the density operator formalism rather than the standard bra-ket formalism.

2.1.1 States

"Quantum Systems are represented by a Hilbert Space $\mathcal{H}$. The state of the system is represented by a density matrix $\rho \in \mathcal{L}(\mathcal{H})$"

In relation to the bra-ket picture, if a quantum system is known to be in a state $|\psi_i\rangle \in \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$, with respective probabilities $\{p_1, p_2, \ldots, p_n\}$, the density operator for the system is given by

$$\rho = \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i| \tag{2.1}$$

Thus, the density operator allows us to account for both classical as well as quantum probabilities in an ensemble. The density operator for any quantum system satisfies the following properties:

$$\rho = \rho^\dagger \tag{2.2}$$

$$Tr(\rho) = 1 \tag{2.3}$$

$$\langle\psi|\rho|\psi\rangle \geq 0 \quad \forall \quad |\psi\rangle \in \mathcal{H} \tag{2.4}$$

Thus, the density operator for any quantum system is Hermitian, has unit trace and is positive semidefinite. All of the above properties may easily be verified from Equation (2.1).

2.1.2 Evolution

"Time evolution of a quantum state ρ for an isolated quantum system is governed by a unitary operator U."

$$\rho(t) = U\rho(0)U^\dagger \tag{2.5}$$

The unitary operator U may be obtained from the system Hamiltonian H via the Schrodinger Equation

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle \tag{2.6}$$

Putting $|\psi(t)\rangle = U|\psi(0)\rangle$, we get

$$i\hbar\frac{\partial}{\partial t}U = HU \tag{2.7}$$

which can then be solved for the unitary operator U.

2.1.3 Measurement

"Measurement is described by a set of operators $\{M_m\}$, that satisfy the completeness relationship $\sum_m M_m^\dagger M_m = I$."

The probability of obtaining the m^{th} outcome is given by

$$p(m) = Tr(M_m \rho M_m^\dagger) \tag{2.8}$$

and the post measurement state of the quantum system is given by

$$\rho_m = \frac{M_m \rho M_m^\dagger}{Tr(M_m \rho M_m^\dagger)} \tag{2.9}$$

2.1.4 Composition

"For two uncorrelated quantum systems described by quantum states ρ_1 and ρ_2, the composite system may be described by the state $\rho = \rho_1 \otimes \rho_2$"

Here, $\otimes$ refers to the tensor product operation.The above postulates are generalizations of the corresponding postulates for pure state quantum mechanics. A more detailed exposition on how these may be derived from pure state quantum theory may be found in [9].

2.2 Quantum Channels

The postulates of quantum theory, discussed in the previous section seem to tell us that the only quantum operations that one may apply to a quantum system are unitary evolution and measurement. However, the postulates in the previous section are only valid for isolated quantum systems. In general, a number of other operations are possible on open quantum systems. Examples include:

- Adding another system, i.e., tensor product with an environment.
- Discarding a system, i.e., partial trace.
- Unitary evolution of a larger system of which the target system is a part.

Quantum Channels refer to the set of of all physical operations that can be physically applied to an open quantum system. More formally, a quantum channel is a linear map $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$ that satisfies the following properties:

- It is Linear.
- It is Trace Preserving.
- It is Completely Positive.

Linearity is an obvious requirement since operations on isolated systems (unitary evolution & measurement) form a subset of quantum channels and these are linear. The other two requirements stem from the requirement that the output of a quantum channel should be a valid

density matrix, when the input is a density matrix. Trace Preserving in the above context refers to the following equation being satisfied:

$$Tr[\mathcal{N}(X)] = Tr[X] \forall X \in \mathcal{L}(\mathcal{H}_A) \tag{2.10}$$

Positivity of a channel refers to the following condition:

$$X \geq 0 \implies \mathcal{N}(X) \geq 0 \tag{2.11}$$

However, the condition of positivity is not quite strong enough for quantum channels. Since the input to a quantum channel may be a part of a larger system, we require the map $id_R \otimes \mathcal{N}$ to be positive for all reference systems R. This condition is known as complete positivity. Thus, quantum channels may formally be defined as Completely Positive Trace Preserving (CPTP) maps.

2.3 The Choi-Kraus Theorem

The Choi-Kraus Theorem is one of the most important theorems in the theory of quantum channels, as it provides a neat mathematical way to represent CPTP maps. The resulting representation is known as the Kraus Operator Sum Representation (OSR).

A linear map $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is CPTP if and only if there exist a set of operators $\{V_l : \mathcal{H}_A \to \mathcal{H}_B\}$ such that

$$\mathcal{N}(X) = \sum_l V_l X V_l^\dagger \tag{2.12}$$

The operators $\{V_l\}$ are known as the Kraus operators for the channel $\mathcal{N}$, and they satisfy the completeness relation

$$\sum_l V_l^\dagger V_l = I \tag{2.13}$$

We shall not attempt to prove the Choi-Kraus Theorem here, but will instead refer the interested reader to [17].

2.4 Stinespring Dilation

While the Kraus OSR provides a neat way to mathematically represent quantum channels, it is imprtant to note that all quantum operations are after all manifestations of unitary evolution and measurement. These operations may be applied to a larger subsystem of which the target system forms a part, thus giving the impression of non unitary evolution. The Stinespring

representation emphasizes just this relation. Given a quantum channel with Kraus operators $\{V_l : \mathcal{H}_A \to \mathcal{H}_B\}$, let us define the following operator $U : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E\}$:

$$U = \sum_m V_m \otimes |m\rangle_E \tag{2.14}$$

Clearly, U is an operator from system A to the composition of systems B and E. It is easy to see that U is an isometry

$$U^\dagger U = \sum_{m,n} V_m^\dagger V_n \otimes \langle m|n\rangle_E = \sum_m V_m^\dagger V_m = I \tag{2.15}$$

The action of the quantum channel is then obtained by the following equation:

$$\mathcal{N}(\rho) = Tr_E[U\rho U^\dagger] \tag{2.16}$$

This is easily proven from the Choi-Kraus Theorem as follows

$$Tr_E[U\rho U^\dagger] = \sum_{m,n} V_m \rho V_n^\dagger Tr[|m\rangle\langle n|] = \sum_{m,n} V_m \rho V_n^\dagger \delta_{mn} = \sum_m V_m \rho V_m^\dagger \tag{2.17}$$

The above representation is referred to as the Stinespring Representation. Due to mathematical simplicity, the Kraus representation remains the most widely used representation. Although the Stinespring representation offers the valuable physical insight that all quantum operations are after all unitary evolutions or measurements on a larger quantum system.

2.5 Examples of Quantum Channels

In this section, we list a few common quantum channels, which are frequently used to model noise in quantum information theory.

2.5.1 Bit Flip Channel

The bit flip channel is a single qubit channel that flips the qubit with probability p and retains the qubit with probability $1 - p$. Its action is described as

$$\mathcal{N}(\rho) = pX\rho X^\dagger + (1-p)\rho \tag{2.18}$$

Kraus operators corresponding to this channel are

$$V_0 = \sqrt{p}X \tag{2.19}$$
$$V_1 = \sqrt{1-p}I \tag{2.20}$$

2.5.2 Phase Flip Channel

The phase flip channel is similar to the bit flip channel, except that the Pauli Z operator is applied instead of the Pauli X operator. Its action is described as

$$\mathcal{N}(\rho) = pZ\rho Z^\dagger + (1-p)\rho \tag{2.21}$$

Kraus operators corresponding to this channel are

$$V_0 = \sqrt{p}Z \tag{2.22}$$
$$V_1 = \sqrt{1-p}I \tag{2.23}$$

2.5.3 Depolarizing Channel

The depolarizing channel is a worst case noise scenario that is used when we have little to no knowledge of the quantum channel involved. This channel destroys the input and replaces it with the maximally mixed state with probability p. Its action is described as

$$\mathcal{N}(\rho) = \frac{pI}{2} + (1-p)\rho \tag{2.24}$$

Kraus operators corresponding to this channel are

$$V_0 = \sqrt{1-3p/4}I \tag{2.25}$$
$$V_1 = \sqrt{p}X \tag{2.26}$$
$$V_2 = \sqrt{p}Y \tag{2.27}$$
$$V_3 = \sqrt{p}Z \tag{2.28}$$

2.5.4 Amplitude Damping Channel

The amplitude damping channel is characterized by a damping parameter γ. Its action is described by two Kraus operators V_0 and V_1

$$\mathcal{N}(\rho) = V_0\rho V_0^\dagger + V_1\rho V_1^\dagger \tag{2.29}$$

where the Kraus operators corresponding to this channel are given by

$$V_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \tag{2.30}$$

$$V_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \tag{2.31}$$

2.5.5 Phase Damping Channel

The phase damping channel is characterized by a damping parameter λ. Its action is described by two Kraus operators V_0 and V_1

$$\mathcal{N}(\rho) = V_0 \rho V_0^\dagger + V_1 \rho V_1^\dagger \tag{2.32}$$

where the Kraus operators corresponding to this channel are given by

$$V_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix} \tag{2.33}$$

$$V_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix} \tag{2.34}$$

Chapter 3

Quantum Resources & Protocols

In this chapter, we present a discussion of Quantum Resource Theories. Such theories are typically concerned with inequalities involving inter-conversion among quantum communication resources. We introduce the unit quantum resources of Quantum Information Theory in the first section. We follow it up with the basic protocols involved in quantum communications and the associated resource inequalities. In the last section, we conclude with a discussion on the achievabilty of arbitrary resource inequalities.

3.1 Unit Quantum Resources

The following resources are typically classified as the unit quantum resources in Quantum Information Theory:

- Quantum Communication Channel: Measured in qubits (or qbits).
- Non Local Entanglement: Measured in ebits.
- Classical Communication Channel: Measured in cbits.

A single qbit of Quantum Communication is represented by the symbol $[q \to q]$. An ebit of Non Local Entanglement is represented as $[qq]$, while a cbit of classical communication is denoted by $[c \to c]$. Quantum Resource Theories are typically in the form of inequalities such as the following

$$[q \to q] \geq [c \to c] \tag{3.1}$$

Inequalities such as this state that there exists a communication protocol that consumes the resources on the left side of the inequality and produce the resources on the right. For example, the above inequality implies that there exists a protocol that consumes a qbit and produces a

cbit. In other words, quantum communication channels can simulate classical communication channels.

3.2 Unit Quantum Protocols

The following protocols are referred to as the unit quantum protocols in Quantum Information Theory:

- Entanglement Distribution.
- Superdense Coding.
- Quantum Teleportation.

These are described in detail below. In the following we shall refer to the transmitting agent as Alice and the receiving agent as Bob as is standard in Quantum Information.

3.2.1 Entanglement Distribution

The Entanglement Distribution Protocol achieves the following resource inequality

$$[q \to q] \geq [qq] \tag{3.2}$$

To start off, Alice takes two qubits in the standard state $|00\rangle$. Alice then applies a Hadamard transform on qubit 1 followed by a CNOT gate C_{10} on both qubits. Alice gets

$$C_{10}H_1|00\rangle = C_{10}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |0\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{3.3}$$

However, this is one bit of local entanglement and does not yet count as an ebit. To generate $[qq]$, Alice must consume one unit of $[q \to q]$, i.e., use a quantum communication channel, to send one of her qbits to Bob. This completes the Entanglement Distribution protocol.

3.2.2 Superdense Coding

Superdense Coding achieves the following resource inequality

$$[q \to q] + [qq] \geq 2[c \to c] \tag{3.4}$$

To achieve this, Alice and Bob start off with an entangled pair. Alice applies one of the operators in $\{I, X, Y, Z\}$ depending on whether she wants to encode 00, 01, 10 or 11 (thus, $2[c \to c]$). In each of the four cases, they get (up to global phase):

$$00 : I|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\phi^+\rangle \tag{3.5}$$

$$01 : X|\phi^+\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} = |\psi^+\rangle \tag{3.6}$$

$$10 : Y|\phi^+\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}} = |\psi^-\rangle \tag{3.7}$$

$$11 : Z|\phi^+\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} = |\phi^-\rangle \tag{3.8}$$

Alice then sends her share of the pair to Bob using one unit of $[q \to q]$. Since the above Bell states are orthonormal to each other, Bob can perform a Bell measurement to distinguish between them and thus acquire the 2 cbits sent by Alice.

3.2.3 Teleportation

Teleportation achieves the following resource inequality

$$2[c \to c] + [qq] \geq [q \to q] \tag{3.9}$$

Alice has a qbit in the state $\alpha|0\rangle + \beta|1\rangle$ that she needs to send to Bob. Both of them share an entangled pair in the state $|\phi^+\rangle$. The initial state of the system is

$$|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{3.10}$$

Here, qubits 2 and 1 are with Alice and qubit 0 is with Bob. Alice applies a H_2C_{21} operation on her share of the qubits. The state becomes

$$|\psi\rangle = H_2C_{21}\left[(\alpha|0\rangle + \beta|1\rangle) \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}\right] \tag{3.11}$$

$$= H_2\left[\alpha|0\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta|1\rangle \otimes \frac{|10\rangle + |01\rangle}{\sqrt{2}}\right] \tag{3.12}$$

$$= \alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{3.13}$$

$$= \frac{1}{2}(|00\rangle \otimes |\psi\rangle + |01\rangle \otimes X|\psi\rangle + |10\rangle \otimes Z|\psi\rangle + |11\rangle \otimes XZ|\psi\rangle) \tag{3.14}$$

Alice then measures her two qubits and sends the classical results of her measurement to Bob using $2[c \to c]$. Depending on what she gets, Bob's state collapses to either $|\psi\rangle$, $X|\psi\rangle$, $Z|\psi\rangle$ or

$XZ|\psi\rangle$. But because Alice sent him her 2 cbits, he knows exactly which one of the above occurred and is able to regenerate $|\psi\rangle$ by applying the necessary combination of X and Z operators.

3.3 The Unit Resource Capacity Region

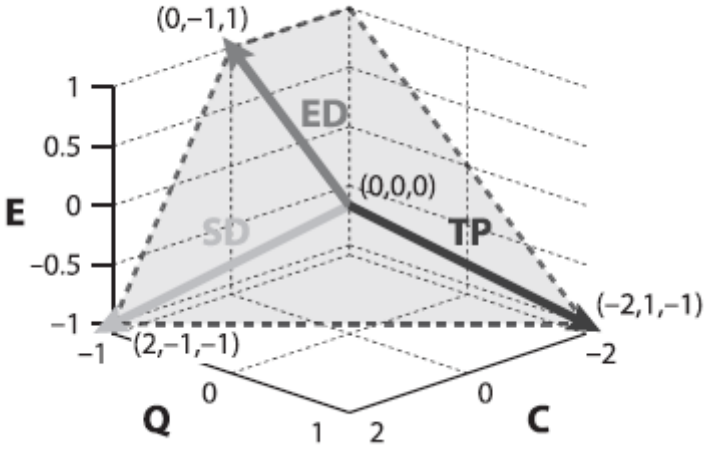

FIGURE 3.1: The Unit Resource Capacity Region. Source: [17]

We now describe a general scheme to construct any arbitrary achievable resource inequality. Consider a 3D space labelled by co-ordinates (C, Q, E). Each point in this space represents a resource inequality. C, Q, E here, respectively represents the amount of $[c \to c]$, $[q \to q]$ and $[qq]$ generated by the inequality. If the inequality consumes a given resource instead, it is designated with a negative sign. Thus, the three unit protocols are described by the following points in (C, Q, E) space:

- Entanglement Distribution: (0, -1, 1)
- Superdense Coding: (2, -1, -1)
- Quantum Teleportation: (-2, 1, -1)

Let P_1, P_2, P_3, represent the 3 unit quantum protocols in (C, Q, E) space. Then the set of all achievable protocols in (C, Q, E) space is given by all points in the set $\{\alpha P_1 + \beta P_2 + \gamma P_3 : \alpha, \beta, \gamma \geq 0\}$. This region corresponds to the Unit Resource Capacity Region shown in the Figure 3.1.

This theorem essentially says that all achievable protocols are linear combinations of the unit protocols. Hence, the name unit protocols. The proof of this theorem may be found in [17].

Chapter 4

Quantum Shannon Theory

In this chapter, we describe the generalization of Shannon's Information Theory to quantum channels. We start by defining the concept of Shannon Entropy for Classical Information and Von Neumann Entropy for Quantum Information. Then, we introduce the notion of typical sequences and discuss the Noiseless Coding Theorem. We then define the concept of channel capacity and review known special cases regarding the quantum channel capacity.

4.1 Shannon Entropy

Before we define the Shannon Entropy, we shall need to define the concept of a classical information source. A classical information source may be regarded as a random variable X that emits a sequence of symbols chosen from an alphabet $\mathcal{A}$. The symbols are emitted at random but are associated with a known probability distribution $p_X(x)$. We shall denote by x, a specific realization of the random variable X. Here, $x \in \mathcal{A}$. Each realization x of X, is associated with an information content $i_X(x)$, which we define as follows

$$i_X(x) = -log(p_X(x)) \tag{4.1}$$

Here, the logarithm is to the base 2. Clearly $i_X(x)$ measures the degree of uncertainty in x because less uncertainty is associated with the occurrence of a more probable x. The Shannon Entropy of the source is then, defined as

$$H(X) = E[i_X(x)] = -\sum_{x \in \mathcal{A}} p_X(x) log(p_X(x)) \tag{4.2}$$

Notice that the information content is a function of a realization of X, while the entropy is a function of the random variable. Similar to the information content, the entropy is a measure of the uncertainty associated with the source.

4.2 Von Neumann Entropy

Similar to a classical information source, a quantum information source is also a random variable. However, the realizations of the random variable in this case are quantum states $|\psi_i\rangle$ associated with probabilities p_i. Since such a ensemble is described by a density matrix ρ, the full description of a quantum source is a density matrix ρ The Von Neumann Entropy for this source is defined as

$$S(\rho) = -Tr[\rho \, log \, \rho] \tag{4.3}$$

4.3 Typical Sequences & Subspaces

4.3.1 The Classical Case

Let us now consider a sequence of n symbols emitted by a classical source X. The resulting random variable is denoted as X^n, and has realizations of the form $x^n = x_1 x_2 \dots x_n$, where all $x_i \in \mathcal{A}$. We shall assume all our sources to be independent and identically distributed (i.i.d.), so that

$$p_{X^n}(x^n) = p_X(x_1) p_X(x_2) \dots p_X(x_n) \tag{4.4}$$

We shall now define the concept of sample entropy. While the Entropy is a function of the random variable X, the sample entropy is a function of a particular realization x^n of X^n. While the entropy is the theoretical expectation value of the information content, the sample entropy $\tilde{H}(x^n)$ of a realization x^n, is the empirical mean of the information content

$$\tilde{H}(x^n) = \frac{1}{n} \sum_{j=1}^{n} i_X(x_j) = -\frac{1}{n} \sum_{j=1}^{n} log(p_X(x_j)) \tag{4.5}$$

By the law of large numbers, we expect the sample entropy to approach the Shannon entropy for large n. We now define the concept of a δ-typical sequence. A sequence x^n is said to be δ-typical if the following inequality holds

$$|\tilde{H}(x^n) - H(X)| \leq \delta \tag{4.6}$$

The set of all δ-typical sequences is denoted as $T_\delta^{X^n}$. We shall state, without proof, three important theorems regarding typical subspaces. The proofs may be found in [17].

Theorem 4.1:
For any positive ϵ, δ, no matter how small, there exists a sufficiently large n, such that

$$P[X^n \in T_\delta^{X^n}] \geq 1 - \epsilon \tag{4.7}$$

Theorem 4.2:
For any positive ϵ, δ and sufficiently large n, the size of the δ-typical set is bounded as follows

$$(1-\epsilon)2^{n(H(X)-\delta)} \leq |T_\delta^{X^n}| \leq 2^{n(H(X)+\delta)} \tag{4.8}$$

Theorem 4.3:
The probability of occurrence of a δ-typical sequence x^n is bounded as follows

$$2^{-n(H(X)+\delta)} \leq p_{X^n}(x^n) \leq 2^{-n(H(X)-\delta)} \tag{4.9}$$

The first of these theorems tells us that the δ-typical set for some small δ essentially contains all the probability for large n, i.e., the probability of occurrence of an x^n outside this set is highly improbable. The second theorem says that for large n, the size of the δ-typical set is approximately $2^{nH(X)}$, while the third tells us that within this set, the probability is almost uniform and is approximately $2^{-nH(X)}$.

4.3.2 The Quantum Case

For a quantum information source ρ, a sequence of symbols of length n is the density matrix $\rho^{\otimes n}$. To define the concept of quantum typicality, we shall first need to obtain the spectral decomposition of ρ as follows

$$\rho = \sum_x \lambda_x |x\rangle\langle x| \tag{4.10}$$

Since ρ is positive semidefinite and $Tr[\rho] = 1$, $p_X(x) = \lambda_x$ forms a valid probability distribution. In such a case, we may define a corresponding hypothetical classical source X associated with ρ via the probability distribution of its eigenvalues and the alphabet of its eigenvectors. Notice that for such X,

$$H(X) = S(\rho) \tag{4.11}$$

The sequence density matrix $\rho^{\otimes n}$ has a spectral decomposition

$$\rho = \sum_{all\ x^n} \lambda_{x_1}\lambda_{x_2}\ldots\lambda_{x_n} |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \otimes \cdots \otimes |x_n\rangle\langle x_n| \tag{4.12}$$

The completeness relation requires

$$I = \sum_{all\ x^n} |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \otimes \cdots \otimes |x_n\rangle\langle x_n| \tag{4.13}$$

Now corresponding to the classical source X, we can define the δ-typical set as in the previous section. If in the above equation, instead of all x^n, we choose to include only the δ-typical x^n in

the sum, we get a projection operator as follows

$$P_\delta = \sum_{x^n \in T_\delta^{X^n}} |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \otimes \cdots \otimes |x_n\rangle\langle x_n| \tag{4.14}$$

The subspace of the Hilbert Space $\mathcal{H}^{\otimes n}$, into which P_δ projects is the typical subspace for $\rho^{\otimes n}$, denoted as $\mathcal{H}_\delta$. We now present the generalizations of theorems 4.1-4.3 to the case of typical subspaces.

Theorem 4.4:
For any positive ϵ, δ, no matter how small, there exists a sufficiently large n, such that

$$Tr[P_\delta \rho^{\otimes n}] \geq 1 - \epsilon \tag{4.15}$$

Theorem 4.5:
For any positive ϵ, δ and sufficiently large n, the dimension of the δ-typical subspace is bounded as follows

$$(1-\epsilon)2^{n(S(\rho)-c\delta)} \leq Tr[P_\delta] \leq 2^{n(S(\rho)+c\delta)} \tag{4.16}$$

Theorem 4.6:
The eigenvalues of the projection of $\rho^{\otimes n}$ onto the typical subspace is bounded as follows

$$2^{-n(S(\rho)+c\delta)} P_\delta \leq P_\delta \rho^{\otimes n} P_\delta \leq 2^{-n(S(\rho)-c\delta)} P_\delta \tag{4.17}$$

4.4 The Noiseless Coding Theorem

The Noiseless Coding Theorem is essentially a statement of the maximal compression rate that is possible for a given information source under the assumption of a noiseless transmission channel. In the classical case, theorems 4.1-4.3 essentially tell us that we only need to consider the typical set of size approximately $2^{nH(X)}$, because a sequence outside this set is highly improbable. We can thus, encode the source in $nH(X)$ bits instead of n bits. Since for a 2 symbol alphabet, $0 \leq H(X) \leq 1$, data compression is achieved. Thus, data compression is achieved. Shannon's Noiseless Coding Theorem says that

The optimal rate of compression for an information source X is $H(X)$ bits per symbol

Similarly, for the quantum case, this is generalized by Schumacher's Noiseless Coding Theorem

The optimal rate of compression for an information source ρ is $S(\rho)$ bits per symbol

The noiseless coding theorems thus, provide an operational interpretation of the entropy as the maximal compressibility of an information source.

4.5 The Noisy Coding Theorem

Shannon's Noisy Coding theorem addresses the case of noisy communication channels. The Noisy Coding theorem essentially provides an expression for the channel capacity, which is the maximum number of bits per symbol at which information may be reliably be transmitted over a noisy channel. In the classical case, for an input X and output Y of the channel, the channel capacity is given as

$$\mathcal{C} = max[I(X:Y)] \tag{4.18}$$

where the maximization is over all possible probability distributions of the source and $I(X:Y)$ is the mutual information between X and Y, defined as follows

$$I(X:Y) = H(X) + H(Y) - H(XY) \tag{4.19}$$

Unfortunately, such an expression for the quantum case is not known in general. A number of special cases have been analyzed, the most prominent being the HSW theorem [7].

Chapter 5

The Qiskit Library

In this chapter, we shall outline the simulations of quantum algorithms that were conducted as part of the thesis work. We shall avoid detailed descriptions of the simulations involved. For the most part, we shall refer the reader to the Github repository for the code. We shall provide more detailed results for the more recent quantum algorithms, viz, the HHL and QAOA algorithms.

5.1 Quantum Algorithms in Qiskit

IBM Qiskit [1] is an open source python package for quantum computing applications. Qiskit contains multiple simulators for performing a variety of simulations related to quantum computing, and also provides cloud access to IBM's prototype quantum computers. The major circuit level simulators present in Qiskit are as follows:

- QASM Simulator
- Statevector Simulator
- Unitary Simulator

Qiskit also provides a variety of features such as addition of noise models to the simulations. The following algorithms were simulated using Qiskit.

- BB84 Protocol
- Bernstein-Vazirani Algorithm
- Deutsch Algorithm
- Deutsch-Jozsa Algorithm

- Grover's Algorithm
- Quantum Counting
- Quantum Phase Estimation
- Shor's Algorithm
- Simon's Algorithm
- Teleportation Protocol

We shall avoid providing detailed descriptions of these algorithms as such is already done in the associated Github repository: https://github.com/Arkonaire/Quantum-Algorithms

5.2 The HHL Algorithm

The HHL Algorithm [8] is a quantum algorithm for solving a system of linear equations. In this project, a simple version of the HHL algorithm, presented in [2] The circuit for this algorithm is shown in Figure 5.1.

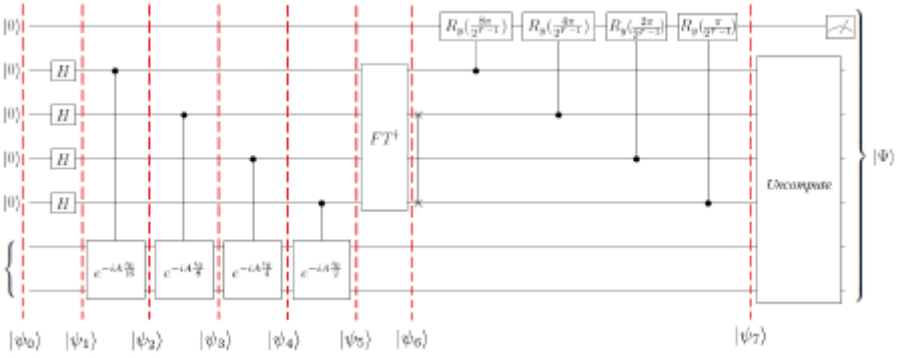

FIGURE 5.1: The HHL Algorithm Circuit. Source: [2]

The system of equations solved in this case is of the form $Ax = b$, where

$$A = \frac{1}{4}\begin{bmatrix} 15 & 9 & 5 & -3 \\ 9 & 15 & 3 & -5 \\ 5 & 3 & 15 & -9 \\ -3 & -5 & -9 & 15 \end{bmatrix} \qquad b = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \tag{5.1}$$

The solution is

$$x = \begin{bmatrix} -0.312 \\ 0.2188 \\ 0.3437 \\ 0.4062 \end{bmatrix} \tag{5.2}$$

which leads to the expected relative odds as

$$00 : 0.0029 \quad 01 : 0.1441 \quad 10 : 0.3559 \quad 11 : 0.4971 \tag{5.3}$$

Simulations were performed using Qiskit's QASM simulator. The results of the simulations are shown in Figure 5.2. We see that the results compare very well to the theoretical expectations.

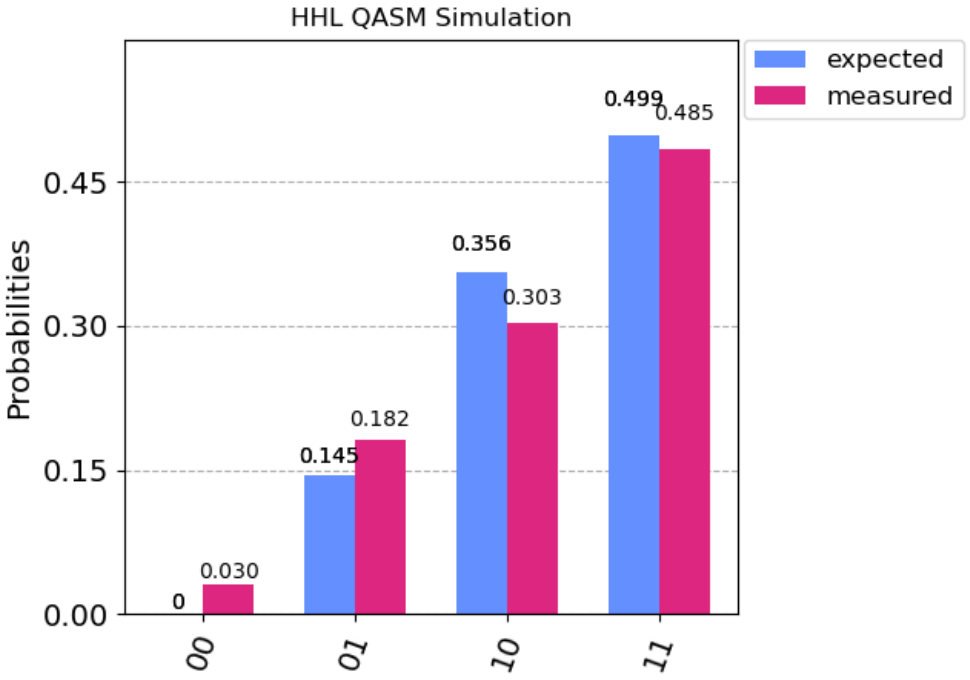

FIGURE 5.2: HHL Algorithm Simulation Results

5.3 The QAOA Algorithm

The QAOA Algorithm [5] is a hybrid classical-quantum algorithm for solving combinatorial optimization problems. In this case, a simulation of the QAOA algorithm for solving the max-cut problem was implemented. The variational circuit for the same is shown in Figure 5.3.

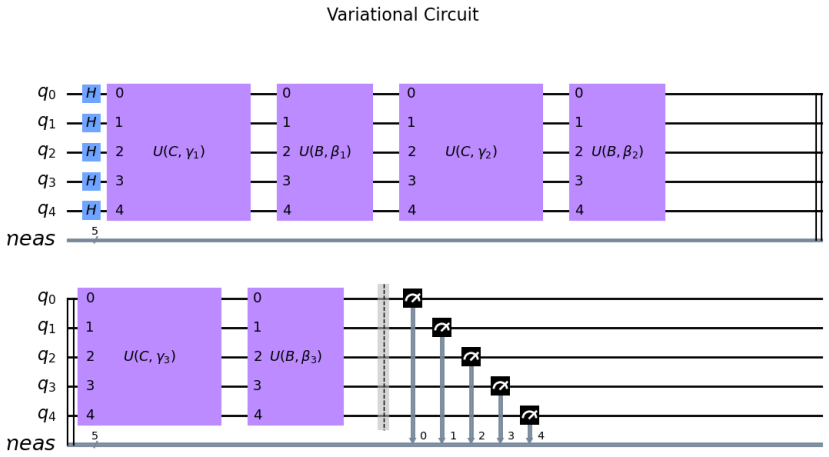

FIGURE 5.3: Quantum Circuit for QAOA Algorithm

It can be noted that the circuit has p (=3 in this case) repeating operators of the form $U(B, \beta_i)U(C, \gamma_i)$. The first operation is a Hadamard Transform that converts the input into a uniform superposition of all states. The U operators are defined as

$$U(A, \alpha) = e^{-i\alpha A} \tag{5.4}$$

Operators B is a series of X gates applied to all qubits while C is the cost function for the optimization problem.

$$B = \sum_{j=1}^{n} X_j \qquad C = \sum_{allz} C(z)|z\rangle\langle z| \tag{5.5}$$

Here, $C(z)$ is the max-cut cost function to be maximized. The circuit operation is fairly simple. The circuit above generates a quantum state $|\gamma, \beta\rangle$ parameterized by $2p$ parameters $\{\gamma_i, \beta_i\}_{i=1}^{p}$. The output is then measured multiple times to obtain the following expectation value

$$F = \langle\gamma, \beta|C|\gamma, \beta\rangle \tag{5.6}$$

The parameters are then optimized by a classical optimizer to maximize the value of F. Subsequent measurement leads to a value that is close to the optimizing value. For the max-cut problem simulated in this case, the results are shown in Figure 5.4.

As seen in the figure, the number of cuts obtained is 7. The optimal number is 8. As expected the result is approximately optimized, hence "Quantum Approximate Optimization Algorithm".

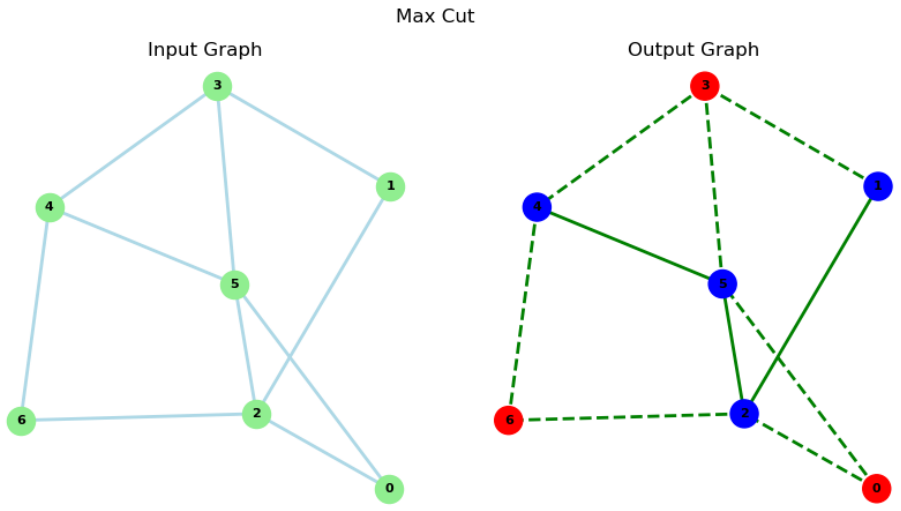

FIGURE 5.4: QAOA Algorithm for the MAX-CUT problem.

Chapter 6

Quantum Communication Systems

In this chapter, we outline the results of the end-to-end simulation of quantum communication system. The simulation is achieved in two stages. In the first stage the process of Schumacher Compression is demonstrated, under the assumption of a noiseless channel as well as its performance under a noisy channel is simulated. In the second stage, quantum error correcting codes have been implemented and channel performances are compared with and without error coding.

6.1 Schumacher Compression

We implement a Schumacher Compression scheme for a B92 ensemble of block length 3. The ensemble consists of 2 states $|0\rangle$ and $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ with equal probability 1/2. The density matrix for this state is given by

$$\rho = \begin{bmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{bmatrix} \tag{6.1}$$

The entropy of this ensemble is 0.6009. Thus the minimum number of qubits to be transmitted is approximately $0.6009 * 3$ 2. Following through the calculations given in [10], we expect the input to output fidelity to be 0.9234.

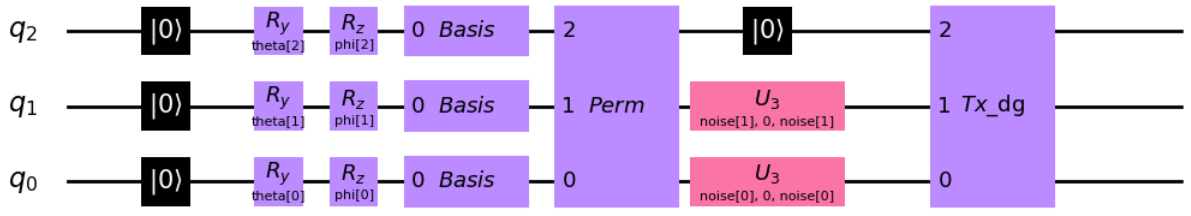

FIGURE 6.1: Schumacher Compression Circuit.

The associated circuit is shown in Figure 6.1. The first part of the circuit is a set of R_z and R_y operators that randomly sample a (θ, ϕ) from the B92 ensemble and prepare that state. The next part involves a basis transform to the eigenvectors of ρ. This is followed by a permutation operator to compress the more probable state to the least significant bits. The lower bits are transmitted to the receiver, which appends a 0 as the MSB for decoding and then performs the unitary inverse of the basis change and permutation operators to get back the input.

The input-output fidelities were measured in the noiseless case as well as with a bit-flip channel with $p = 0.1$. The results are in Figure 6.2. The noiseless fidelity is quite close to the theoretical value of 0.9234, while significant errors are observed in the noisy case as expected. This value is improved upon in the next section using error control coding.

```
D:\Operations\Anaconda3\envs\quantum_algorithms\python.exe "E:/Workshop/Github/Quantum-Algorithms/Schumacher Compression/compressor.py"
Noiseless System Fidelity:  0.915682126836385
Noisy (p = 0.1) System Fidelity:  0.8049182444583199

Process finished with exit code 0
```

FIGURE 6.2: Schumacher Compression Results.

6.2 Quantum Error Correction

We shall here analyze two separate cases:

- The 3-Qubit Code
- The 5-Qubit Code

The first one is capable of error correction against only single qubit bit flip errors. The latter is more powerful and can deal with general single qubit errors.

6.2.1 3 Qubit Error Correction

The 3 Qubit Error Correction Code Circuit is shown in Figure 6.3. It contains the following components from left to right:

- Encoder
- Noisy Channel
- Syndrome Measurement

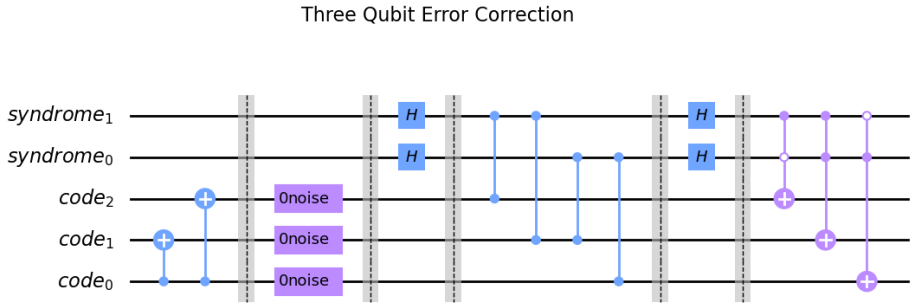

FIGURE 6.3: 3 Qubit Error Correction Circuit.

- Decoder

The performance was analysed using a bit-flip channel and a QASM simulation, the results of which are shown in Figure 6.4. As expected the qubits are one of 8 states due to errors on 3 qubits. But as the set represents only one logical qubit, we expect it to be in one of 2 states, as is the case with error correction enabled.

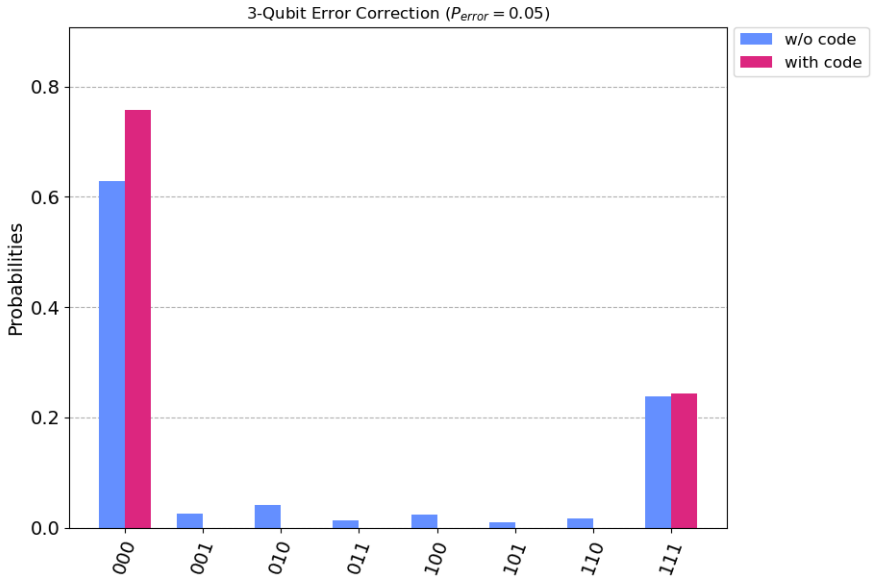

FIGURE 6.4: 3 Qubit Error Correction - QASM Simulation.

Finally, we vary the probability of error and plot the input-output fidelity as a function of the error probability in Figure 6.5. As expected, the fidelity decreases with increase in probability of error. The fidelity loss is much less with error correction than without. Although even with

error correction, perfect fidelity is not achieved. This is because only single qubit errors are corrected by the code.

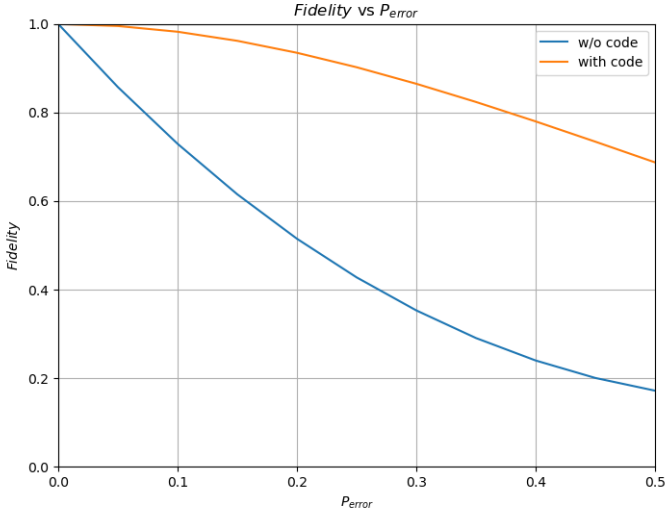

FIGURE 6.5: 3 Qubit Error Correction - Fidelity vs Probability of Error.

6.2.2 5 Qubit Error Correction

In this case, only a QASM simulation shall be possible because of the increased complexity of the circuit involved. The circuit in this case is shown in Figure 6.7. The QASM results for depolarizing noise are shown in Figure 6.6. As expected, only 2 states are observed with error correction as opposed to multiple states without.

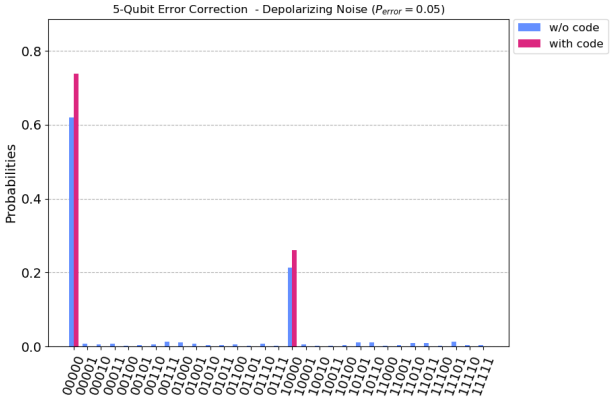

FIGURE 6.6: 5 Qubit Error Correction Circuit - QASM Simulation

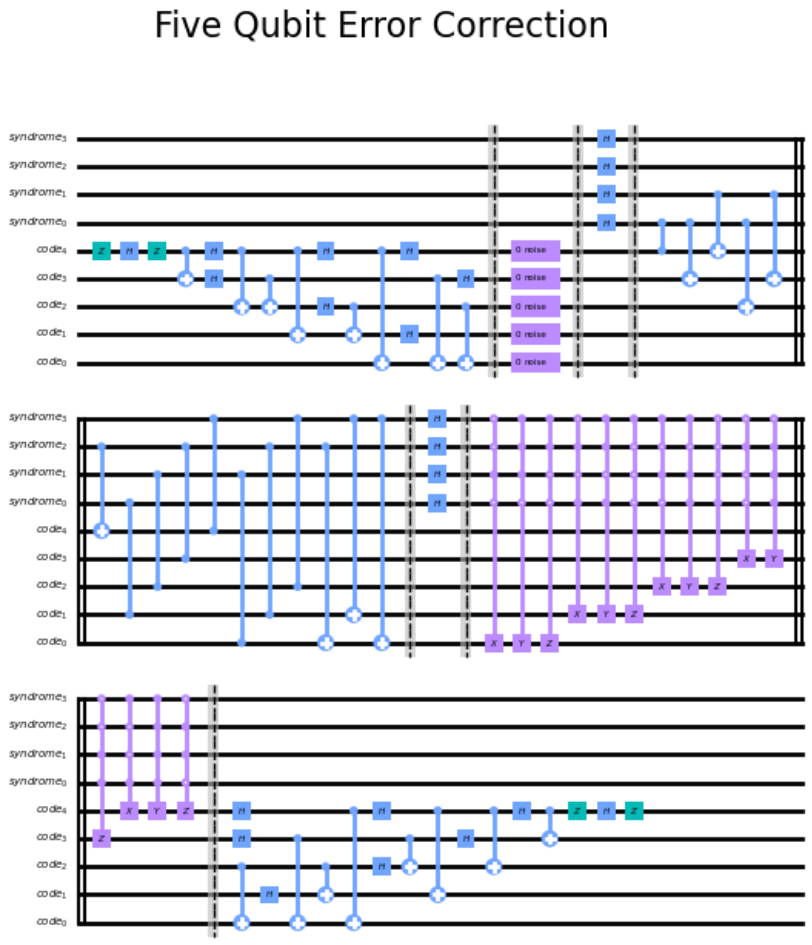

FIGURE 6.7: 5 Qubit Error Correction Circuit.

Chapter 7

Conclusions

The Thesis work described in this document has been intended to explore various aspects in the fundamentals of quantum information theory. Much of the work carried out in this regard has been theoretical reviews in regard to topics such as Quantum Channels, Resource Theories and Quantum Shannon Theory. Part of the work has been in the form of computational simulations involving the IBM Qiskit Library. The results of this review have been presented in this document, along with a discussion some of the major simulations carried out. The full code may be found in

https://github.com/Arkonaire/Quantum-Algorithms

Bibliography

[1] Héctor Abraham et al. *Qiskit: An Open-source Framework for Quantum Computing*. 2019. DOI: 10.5281/zenodo.2562110.

[2] Yudong Cao et al. "Quantum circuit design for solving linear systems of equations". In: *Molecular Physics* 110.15-16 (2012), pp. 1675–1680.

[3] David Deutsch. "Quantum theory, the Church–Turing principle and the universal quantum computer". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), pp. 97–117.

[4] David Deutsch and Richard Jozsa. "Rapid solution of problems by quantum computation". In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (1992), pp. 553–558.

[5] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. "A quantum approximate optimization algorithm". In: *arXiv preprint arXiv:1411.4028* (2014).

[6] Laszlo Gyongyosi, Sandor Imre, and Hung Viet Nguyen. "A survey on quantum channel capacities". In: *IEEE Communications Surveys & Tutorials* 20.2 (2018), pp. 1149–1205.

[7] Alexander S Holevo. "The capacity of the quantum channel with general signal states". In: *IEEE Transactions on Information Theory* 44.1 (1998), pp. 269–273.

[8] Seth Lloyd. "Quantum algorithm for solving linear systems of equations". In: *APS* 2010 (2010), pp. D4–002.

[9] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. USA: Cambridge University Press, 2011. ISBN: 1107002176.

[10] John Preskill. "Lecture notes for physics 229: Quantum information and computation". In: *California Institute of Technology* 16 (1998).

[11] Benjamin Schumacher. "Quantum coding". In: *Physical Review A* 51.4 (1995), p. 2738.

[12] Claude E Shannon. "A mathematical theory of communication". In: *The Bell system technical journal* 27.3 (1948), pp. 379–423.

[13] Peter W Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". In: *SIAM review* 41.2 (1999), pp. 303–332.

[14] Peter W Shor. "Scheme for reducing decoherence in quantum computer memory". In: *Physical review A* 52.4 (1995), R2493.

[15] Graeme Smith. "Quantum channel capacities". In: *2010 IEEE Information Theory Workshop*. IEEE. 2010, pp. 1–5.

[16] John Von Neumann. *Mathematical foundations of quantum mechanics: New edition*. Princeton university press, 2018.

[17] Mark M. Wilde. *Quantum Information Theory*. 1st. USA: Cambridge University Press, 2013. ISBN: 1107034256.