# QUANTUM COMPUTER EMULATED ON FPGA

A dissertation submitted to the Department of Electrical Engineering,
UNIVERSITY OF CAPE TOWN, in fulfilment of the requirements for the degree of

**BSc(Eng) Electrical and Computer Engineering**

*at* the

**University of Cape Town**

*by*

**Bonga Njamela**

**Supervised by :**
DR SIMON WINBERG



August 21, 2024

# Declaration

I know the meaning of plagiarism and declare that all the work in this dissertation, save for that which is properly acknowledged and referenced, is my own. It is being submitted for the degree of **Master of Science** in Electrical Engineering at the University of Cape Town. This work has not been submitted before for any other degree or examination in any other university.

Signature of Author:

August 21, 2024

Bonga Njamela

Date

University of Cape Town
Cape Town

# ABSTRACT

This MSc project focuses on .. describe the system.

Can provide a few paragraphs, want around 300 - 600 words.

# ACKNOWLEDGEMENTS

I would like to gladly express my gratitude to

# CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

- **ADC** – Analogue to Digital Converter
- **ASIC** – Application-specific Integrated Circuit

# NOMENCLATURE

Comment: you do not need to have both nomenclature and abbreviations it tends to be redundant.

- **Analogue to digital Converter (ADC):** an electronic device that converts data from its analogue format to its digital form.
- **Very High Speed Integrated Circuits Hardware Description Language (VHDL):** a hardware description language used in electronic design automation to describe digital and mixed-signal systems such as FPGA.

CHAPTER 1

# INTRODUCTION

Computational capabilities of classical computers that use binary to describe information are limited by physical constraints of power consumption and the amount of physical space that each element of information occupies. Moore's Law accurately predicted the exponential increase in transistors on integrated circuit chips, however, James R. Powell indicated that a persuasive argument from quantum mechanics based on the Heisenberg principle, defines an eventual limit to the miniaturization of transistors that can be achieved [9]. On the contrary, quantum mechanics also provides advantages that can be exploited to improve the computational capabilities by employing principles of superposition and quantum entanglement to represent different states of information.

Using the quantum state of particles to represent information forms the basis of quantum computing - a computing paradigm that uses the principles of quantum physics to represent and compute information as *qubits*. From the principle of superposition, qubits can be in a state of 0 and 1 simultaneously, unlike classical bits which can only be in a state of 0 or 1, and not both at the same time. Additionally, quantum entanglement allows qubits to be manipulated simultaneously, whereas classical bits can only be manipulated individually per operation. Exploiting these principles gives quantum computing a computational advantage where multiple instances of data can be manipulated simultaneously, thereby reducing the size of the instruction set as part of the architecture of a quantum computer. Another advantage of quantum computers is that, since qubits can exist in multiple states at the same time, the number of qubits required to perform a computation is exponentially smaller than the number of bits that would be required to perform the same operation using classical bits. These benefits account for the growing interest in quantum computing as means to overcome the limits of transistor growth as predicted by Moore's Law. Consequently, the use of quantum computer can reduce the time complexity of many processes that require exceptional performance to execute tasks. The following paper describes the design and emulation of a quantum computer on a field programmable logic gate array (FPGA) to simulate quantum acceleration of a classical computer.

The quantum computer emulator aims to model a heterogeneous processing framework for accelerating MRI image reconstruction by mapping the k-space of an image to spatial information using a 2D Fourier Transform. By accelerating the image reconstruction process, image acquisition and processing can be expedited to significantly decrease the amount of time that a patient spends the consisting of a central processsing unit (CPU) and a quantum com FPGAs are the current industry choice for hardware accelerators because they contain millions of reconfigurable logical elements, embedded memory blocks, and high speed transceivers. Each logical element is surrounding by a flexible interconnect that can be used to perform any Boolean operations on multiple bits, making them highly preferred for customizing hardware.

## 1.1 BACKGROUND

Further blurb

## 1.2 Problem Description

## 1.3 Focus

## 1.4 Objectives

## 1.5 Methodology Overview

## 1.6 Scope and Limitations

## 1.7 Plan of Development

**Chapter 2** presents a Literature Review of the underlying theory etc etc

**Chapter 3** outlines the requirements analysis and methodology

**Chapters 4** discusses design

**Chapters 5** presents results of testing

**Chapter 6** presents the conclusions for this work and discusses the extent to which objectives are satisfied

CHAPTER 2

# THEORETICAL FRAMEWORK

Quantum computer is a relatively new approach to computing. In 1982, Physicist Richard Feynman, set an inquiry on whether a classical computer could reasonably simulate a quantum physics. This is because classical computers-which are based on the Turing Machine-depends on discrete set of instructions that cannot represent the intrinsic continuous and analog properties of quantum particles. Consequently, sampling quantum information in discrete time intervals would introduce errors to the system. The following section develops a theoretical framework for quantum computing knowledge that forms the basis of the design of the FPGA-emulated quantum computer.

## 2.1 QUANTUM MECHANICS

### 2.1.1 Postulates of Quantum Mechanics

Quantum computing is based on the underlying principles of information theory and quantum mechanics. While this is also true for classical computers in that quantum mechanics principles govern the flow of electrons in the transistors contained in classical semiconductor chips, the influence of quantum mechanics in quantum computing extends beyond low-level implementation to the domain of computation and communication [10]. This applicability of the subject of quantum mechanics in both quantum computing and classical computing is because the subject seeks to describe the behaviour of atomic and subatomic particles, or quantum particles, such as electrons, protons and photons.

Classical mechanics fails to fully describe the behaviour of quantum particles. Consider a system of localised particles with a mass $m_i$, where $i$ is the index of the $i$-th particle. At any given time $t$, the state of the system of particles can be described by a set of position vectors, $\mathbf{r}_i$, and linear momenta $\mathbf{p_i}$. Given that the mass, position and momentum of each particle can be measured with high precision, the principles of classical mechanics suggest that progression of the state of the system can be determined with *certainty* since the set of trajectories can be retrieved from an application of Newton's equation of motion which is defined by an initial value system of differential equations

$$\mathbf{F}_i = m_i \frac{d^2\mathbf{r}_i}{dt^2} = \frac{d}{dt}\mathbf{p}_i \tag{2.1}$$

where $F_i$ is the force experience by particle $i$ at time $t$.

The implication that the universe is deterministic that stems from an interpretation of Netwon's equations of motion pointed to many deficiencies in classical mechanics. The first deficiency in classical mechanics that is addressed in quantum mechanics involves the *uncertainty* in measurements. Using a thought experiment, Max Born highlighted that there is an inherent uncertainty in determining the position of an electron through a microscope due to optics. There is also an inherent uncertainty about the momentum of the electron since the photon which is released by the electron and observed through the microscope lens because of there is an uncertainty in the directional component. The relationship between the uncertainty in the position and the momentum of the particle expounded by the *Heisenberg's Uncertainty Principle* which states that given an uncertainty in position, $\Delta x$, and an uncertainty in

the momentum, $\Delta p$, the inequality

$$\Delta x \Delta p \geq \hbar \tag{2.2}$$

where $\hbar = h/2\pi$ (and $h$ is Planck's constant). Intuitively, this inequality implies that the position and momentum of a quantum particle cannot be known exactly. Gaining information about the position of a quantum particle introduces uncertainties in the momentum. Conversely, gaining information about the momentum of a particle in a quantum system leads to uncertainties in the position of that particle.

Another discrepancy in the application of classical mechanics to quantum particles arises when considering the atomic model. From the perspective of classical mechanics, an electron in a hydrogen atom would lose kinetic energy as its orbitals collapses into a spiral that terminates at the nucleus of the atom. In other words, classical mechanics suggests that the energy of the electron is continuous. However, quantum mechanics suggests that quantum particles have discrete amounts of energy in each atomic orbital.

Quantum mechanics also addresses classical mechanic's inability to elucidate the duality of quantum particles. Young's double slit experiment and known phenomena, such as the photoelectric effect and Compton scattering, expose the wave-particle nature of photons and electrons that allows them behave like waves or particles, depending on the experiment.

### 2.1.2 **Quantum States**

To reconcile with the Heisenberg's Uncertainty Principle, energy quantisation, and wave-particle duality, quantum mechanics associates a particle with a probability wave denoted by $\psi$. Born postulated that the probability, $P(x, y, z, t)dxdydz$, of finding a particle in the infinitesimal volume, $dxdydz$, at time $t$, is proportional to the magnitude of the state function $\psi$. This state function $\psi$, or *quantum state*, contains all of the information that describes the quantum system. A quantum state must satisfy the normalisation property which states that

$$\int_{\tau} \psi^*(\mathbf{r}, t)\psi(\mathbf{r}, t) = 1 \tag{2.3}$$

where $\tau$ is the domain in which measurements of the state are taken.

In this paper, a quantum system is regarded as a system consisting of a one or more quantum particles that is fully defined by the quantum state function $\psi$. To define the quantum state of a particle more succinctly, consider the case where a single photon that is projected through a polarising gradient. The circular polarisation of the photon is considered to be the state of the quantum system. The state of a quantum system can be in a *superposition* of the vertical polarisation, $|\uparrow\rangle$, and the horizontal polarisation, $|\rightarrow\rangle$. By expressing each polarisation state as a unit vector, the measurement of a quantum state $\psi$ can be written as a linear combination of the horizontal and vertical bases, $|\uparrow\rangle$ and $|\rightarrow\rangle$, respectively, as

$$|\psi\rangle = \alpha\,|\uparrow\rangle + \beta\,|\rightarrow\rangle \tag{2.4}$$

where the coefficients $\alpha$ and $\beta$ are complex amplitudes of the state that satisfy the property

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.5}$$

The measured quantum state $\psi$ can be mapped to a unit circle where the angle subtended by the horizontal polarisation direction and the state unit vector corresponds to the measured polarisation angle. The quantum state of the photon can be illustrated as shown in figure 2.1 and is said to be in *superposition* if the amplitude coefficients are both non-zero, i.e. the photon is polarised horizontally and vertically simultaneously. If the preferred axis of the polarising gradient is $|\rightarrow\rangle$, the photon is absorbed with a probability of $|\alpha|^2$ and passes through with a probability of $|\beta|^2$. Therefore, the probability that the photon passes through the polariser is the square of the magnitude of the amplitude coefficients in the direction of the preferred axis [10].

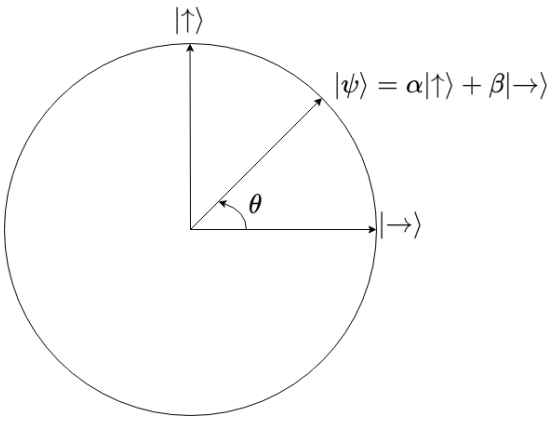



Figure 2.1: A photon can be polarised vertically with probability $\alpha$ or horizontally with probability $\beta$.

### 2.1.3 Unitary Operations on Quantum States

The analysis of the polarisation state of the quantum system with a single photon explored above can be extended to quantum systems that can be in $N$ different, mutually exclusive classical states. In this case, a quantum state is a superposition of classical states in the form

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + ... + \alpha_{N-1} |N-1\rangle \tag{2.6}$$

Superposition implies that state $|\psi\rangle$ is in each state $|i\rangle$ with amplitude $\alpha_i$. The vector space $\{|0\rangle, |1\rangle, ..., |N-1\rangle\}$ of states consists of unit vectors that are orthogonal to each other and therefore forms an $N$-dimensional orthonormal basis of a *Hilbert space*, i.e. the vector space of quantum states has an inner product [1]. Thus, a quantum state $\psi$ is a vector in Hilbert space, herein expressed as an $N$-dimensional column vector

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} \tag{2.7}$$

with the conjugate transpose

$$\langle\psi| = (\alpha_0^*, \alpha_1^*, \ldots, \alpha_{N-1}^*) \tag{2.8}$$

Suppose that the state unit vectors $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ form the orthonormal basis of the Hilbert space $\mathcal{H}_A$, and $|0\rangle, |1\rangle, \ldots, |M-1\rangle$ form an orthonormal basis $\mathcal{H}_B$. The Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ can be combined using in a tensor product Hilbert space $\mathcal{H}$, defined as

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \tag{2.9}$$

The output tensor product space has $N \cdot M$ dimensions spanned by the set of states $S_{\mathcal{H}}$, given by

$$S_{\mathcal{H}} = \{|a\rangle \otimes |b\rangle \mid a \in \{0, 1, \ldots, N-1\}, b \in \{0, 1, \ldots, M-1\}\} \tag{2.10}$$

Thus, any quantum state $|\psi\rangle_{\mathcal{H}}$ in the combined Hilbert space $\mathcal{H}$ can be expressed as the sum

$$|\psi_{\mathcal{H}}\rangle = \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \alpha_{ij} |a_i\rangle \otimes |b_j\rangle \tag{2.11}$$

called a *bipartite* quantum state [1]. Although there are higher dimensional tensor products Hilbert space of multiple states, this paper focuses on the operation and simulation of bipartite states.

A linear operation can be performed on a state $|\psi\rangle$ to change it to a different state, $\phi$, Applying the $N \times N$ complex-valued *unitary operation* $U$ on the vector space of the state $|\psi\rangle$ maps it to the space of state $|\phi\rangle$. Formally, a unitary operator is a bounded linear mapping

$$U : \mathcal{H} \to \mathcal{H} \tag{2.12}$$

on the Hilbert Space $H$ that preserves the norm, and satisfies

$$U^*U = UU^* = I \tag{2.13}$$

where $U^*$ is the Hermitian adjoint of $U$, and $I$ is the identity operator. The corollary is that a matrix $U$ is *unitary* if

$$U^{-1} = U^* \tag{2.14}$$

,i.e. if the inverse of $U$ is equal to the complex adjoint of $U$. The linear operator $U$ on the Hilbert space $\mathcal{H}$ defines a Hermitian adjoint operator $U^*$ on the space that obeys the rule

$$\langle Ux, y\rangle = \langle x, U^*y\rangle \tag{2.15}$$

where $\langle \cdot, \cdot \rangle$ is the inner product on $\mathcal{H}$. Another property of the unitary matrix that can be derived from its definition is that the determinant of $U$ is can be mapped to a unit circle in the complex plane, i.e.

$$|det(U)| = 1 \tag{2.16}$$

Given an outcome state

$$\phi = \beta_0 |0\rangle + \beta_1 |1\rangle + \ldots + \beta_{N-1} |N-1\rangle \tag{2.17}$$

with a probability constraint

$$\sum_{j=0}^{N-1} |\beta_j|^2 = 1 \tag{2.18}$$

the unitary transformation $U$ that is applied to $\psi$ can be expressed as the matrix multiplication

$$|\phi\rangle = U |\psi\rangle$$
$$|\phi\rangle = \begin{pmatrix} u_{11} & u_{12} & \ldots & u_{1N} \\ u_{21} & u_{22} & \ldots & u_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ u_{N1} & u_{N2} & \ldots & u_{NN} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{N-1} \end{pmatrix} \tag{2.19}$$

Since the unitary operator is linear and always has an inverse, it follows that operations performed on a quantum state are reversible. That is, the initial state $|\psi\rangle$ can be retrieved by applying the inverse operator $U^{-1}$ to the state $|\phi\rangle$.

## 2.2 QUANTUM STATES AND QUBITS

Quantum computing extends the principles of quantum mechanics to the domain of computation. Where a classical bit is a unit of information that can be 0 or 1, a *quantum bit* or *qubit*, is a unit of information that can be in a superposition of 0 and 1, corresponding to a quantum state $|\psi\rangle$ of a Hilbert space with two basis states, $|0\rangle$ and $|1\rangle$.

The basis states are associated with two orthogonal vectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.20}$$

such that, at a given time $t$, a qubit in quantum state $|\psi\rangle$ can be expressed as the superposition

$$|\psi\rangle = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.21}$$

that satisfies the normalisation constraint

$$|\alpha_0|^2 + |\alpha_1| = 1 \tag{2.22}$$

This implies that when a qubit in superposition is measured, it collapses with to the state $|0\rangle$ or $|1\rangle$, with a probability of $|\alpha_0|^2$ and $|\alpha_1|^2$, respectively.

### 2.2.1 Qubit Entanglement

Quantum systems of multiple qubits exist in two-dimensional complex Hilbert space as described in section 2.1.2 for quantum states of $N$ particles. The $N$-dimensional tensor product space of the system contains a set of basis states with a cardinality of $2^N$, i.e. a system with $n$ qubits has $2^n$ basis states, each of the form

$$|q_1\rangle \otimes |q_2\rangle \otimes \ldots \otimes |q_n\rangle \tag{2.23}$$

with $q_i \in \{0, 1\}$. In this paper, basis states are abbreviated as $|q_1 q_2 q_3 \ldots q_n\rangle$ or written in decimal form as $|1\rangle$, $|2\rangle, \ldots, |2^n - 1\rangle$, depending on the computation. A quantum system with multiple qubits is referred to as a *quantum register* of $n$ qubits and is considered to be in any superposition of the $n$ states represented in decimal form as

$$\psi_{qr} = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle + \cdots + \alpha_{2^n-1} |2^{n-1}\rangle \tag{2.24}$$

for

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1 \tag{2.25}$$

Composite systems consist of two or more quantum subsystems. Statistical ensembles of pure quantum subsystem spaces show non-classical correlations between basis states, known as *quantum entanglement*. Qubits in composite quantum systems can leverage quantum *entanglement* to facilitate linear operations and classical communications (LOCC). Formally, a pure quantum state $|\psi\rangle$ is said to be entangled if it is not *separable*. A separable pure state $|\xi\rangle$, in a tensor product Hilbert space $\mathcal{H}_{nm} = \mathcal{H}_n \otimes \mathcal{H}_m$, can be written as the tensor product of states $\psi \in \mathcal{H}_n$ and $\phi \in \mathcal{H}_m$, i.e.

$$|\xi\rangle = |\psi\rangle \otimes |\phi\rangle \tag{2.26}$$

Consider the pure bipartite state

$$|\psi^+\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \tag{2.27}$$

from the tensor product space $\mathcal{H}_{22} = \mathcal{H}_2 \otimes \mathcal{H}_2$. It can be shown that this bipartite state $|\psi\rangle^+$, known as an EPR-pair, is indeed entangled. Let

$$|\psi_1\rangle = \alpha |0\rangle + \beta |1\rangle$$
$$|\psi_2\rangle = \gamma |0\rangle + \delta |1\rangle$$

be pure states from the two-dimensional Hilbert space where

$$|\alpha|^2 + |\beta|^2 = 1$$
$$|\gamma|^2 + |\delta|^2 = 1$$

If the state $|\psi\rangle^+$ is separable, it can be written as

$$\begin{aligned} |\psi\rangle^+ &= |\psi_1\rangle \otimes |\psi_2\rangle \\ &= (\alpha |0\rangle + \beta |1\rangle) \otimes (\gamma |0\rangle + \delta |1\rangle) \end{aligned}$$

From the property of distributivity of the tensor product and the assumption of separability, the bipartite state $\psi^+$ the product above can be expanded to

$$\begin{aligned}|\psi\rangle^+ &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle\end{aligned}$$

For the assumption of separability to hold true, the state amplitudes must satisfy

$$\alpha\delta = \beta\gamma = 0$$
$$\alpha\gamma = \beta\delta = \frac{1}{\sqrt{2}}$$

Since there are no values such that these statements are true, it must be that

$$|\psi\rangle^+ \neq |\psi_1\rangle \otimes |\psi_2\rangle$$

Hence, the pure state $|\psi^+\rangle$ is entangled [7]. Similarly, it can be shown that the state $|\psi^-\rangle$ defined by

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|00\rangle$$

is an entangled state. Initially, both $|\psi_1\rangle$ and $|\psi_2\rangle$ are in a superposition of the $|0\rangle$ and $|1\rangle$ basis states. The state of the qubit collapses to $|00\rangle$ when state $|\psi_1\rangle$ is measured and $|0\rangle$ is observed. Therefore, an observation of the eigenstate $|\psi_1\rangle$ is correlated to the eigenstate $|\psi_2\rangle$ of the second qubit that was not observed. The states $|\psi^+\rangle$ and $|\psi^-\rangle$ belong to a set of four orthogonal eigenvectors of entangled states, namely

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}|00\rangle \pm \frac{1}{\sqrt{2}}|11\rangle \tag{2.28}$$
$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}|01\rangle \pm \frac{1}{\sqrt{2}}|10\rangle \tag{2.29}$$

Entanglement in bipartite state quantum systems can be exploited using non-local quantum unitary operations. These operations are independent of the distance between entangled qubits, since information about one state in an entangled 2-qubit system simultaneously reveals information about an associated, non-classically correlated state.

The degree of qubit entanglement is quantified by the *Schmidt number* whose logarithm corresponds to the zero-error entanglement cost of generating a given quantum state using LOCC [3]. Quantum information theory also uses *von Neumann entropy* to quantify the extent of entangle of qubits. This is because for an system of entangled states, von Neumann entropy of a joint Hilbert space $\mathcal{H}_{nm}$ can be smaller than the entropy of its subsystems. To define von Neumann entropy, a density operator $\rho$ is assigned to a quantum system with pure state and is given by

$$\rho = |\psi\rangle\langle\psi| \tag{2.30}$$

A mixed state is a statistical ensemble of density operators of pure states, where each density operator $\rho$ is a Hermitian projection operator which satisfies $\rho^2 = \rho$. The von Neumann entropy $\mathcal{E}$ is then defined as

$$\mathcal{E}(\rho) = -\text{tr}(\rho\log\rho) \tag{2.31}$$

The von Neumann entropy of a pure quantum state is equal to 0, and the entropy of a maximally mixed state is equal to

$$\mathcal{E}(\rho) = -\sum_{i=0}^{n}\frac{1}{n}\log\frac{1}{n} = \log n \tag{2.32}$$

Similarly, it can be shown that if $\rho_n$, $\rho_m$ and $\rho_{nm}$ are the density operators of quantum systems $\mathcal{H}_n$, $\mathcal{H}_m$, and composite system $\mathcal{H}_n m$, then the joint von Neumann entropy of the system must satisfy

$$\mathcal{E}(\rho_n, \rho_m) = \mathcal{E}(\rho_{nm}) \tag{2.33}$$

More intuitively, the von Neumann entropy is a measure of the stability of a measurement on a quantum system. A measure of entanglement $E$ must satisfy LOCC monoticity in that it cannot increase under LOCC operations. That is to say, when all operations are performed locally on the respective subsystem and information between subsystems is transmitted using classical communication channels, the measure of entanglement $E$ must be invariant under local unitary operations. Other measures, such as the *entanglement cost*, give information about how expensive it is to create an entangled state with density operator $\rho$, using LOCC operations in a bipartite entangled state [7]. For pure states, von Neumann entropy suffices as an entanglement measure.

## 2.3 Quantum Gates and Quantum Circuits

Complex operations on classical computers are completed using primitive logic gates such as `NOT`, `AND`, `OR`, `NOR`, `NAND` and `XNOR` gates. Analogously, quantum state transformations on an $n$ qubit system can be executed by an application simple unitary operations on one- and two-qubit quantum systems. Quantum state transformations that act on a finite number of qubits are called *quantum gates*. A collection or sequence of quantum gates is referred to as a *quantum circuit*.

### 2.3.1 Bloch Sphere Representation of Qubits

The quantum state $|\psi\rangle$ in equation 2.21 with complex amplitudes $\alpha$ and $\beta$, can be written in the polar form

$$|\psi\rangle = r_\alpha e^{i\theta_\alpha} |0\rangle + r_\beta e^{i\theta_\beta} |1\rangle \tag{2.34}$$

to expose the phase of a qubit. The *relative phase* $\phi_r$ of the system is defined as the angle between the state vectors in a Hilbert space. More concisely,

$$\phi_r = \theta_\alpha - \theta_\beta \tag{2.35}$$

Changing the relative phase of a qubit is equivalent to performing a rotation of the state vector in Hilbert space. Unlike the relative phase, *global phase* $\gamma_g$ is arbitrary and does not have any physical meaning, therefore, multiplying the state $|\psi\rangle$ by an arbitrary global phase does not change the state in a meaningful manner, i.e.

$$|\psi\rangle = e^{i\gamma_g} |\psi\rangle \tag{2.36}$$

This property of the global phase also implies that multiplication of the wave function represented by $\alpha |0\rangle$ with a global phase rotation does not have an effect on the state, therefore

$$|\psi\rangle = \alpha |0\rangle + e^{i\gamma_g}\beta |1\rangle$$

Let $\gamma_g = \phi_r$ be the global phase. From the property of the global phase, the quantum state $|\psi\rangle$ can be expressed such that the only unknown is the relative phase $\phi_r$,

$$|\phi\rangle = \alpha |0\rangle + e^{i\phi_r}\beta |1\rangle \tag{2.37}$$

The normalisation constraint on the state requires that

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.38}$$

which represents an unit circle in the complex plane. By setting

$$\alpha = \cos\theta \tag{2.39}$$
$$\beta = \sin\theta \tag{2.40}$$

where $\theta \in \mathbb{R}$ is the *absolute phase*, the normalisation constraint holds and a qubit can be represented using a *Bloch sphere* diagram which maps the state vector to a spherical 3D Hilbert subspace to represent information about the relative phase of the state and the argument of the amplitudes as illustrated in figure 2.2. The Bloch sphere is centred at the origin with a radius of 1. The absolute phase $\theta$ is taken with respect to the $\hat{z}$-axis corresponding to the orthogonal basis vectors, $|0\rangle$ and $|1\rangle$, of the state space. The relative phase $\phi$ is considered with respect to the

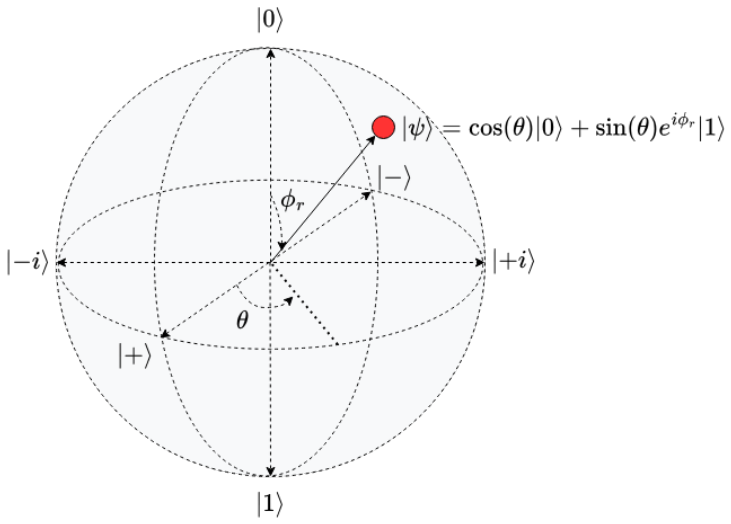



Figure 2.2: Showing a Bloch sphere diagram where relative phase is mapped to the vertical rotation around the $xy$-plane and $\theta$ corresponds the angle of the horizontal rotation of the qubit around the $\hat{z}$-axis.

$\hat{x}$-axis. Generally, each axis of the 3D plane represents two counter states. The states on the $\hat{z}$-axis correspond to the basis vectors,

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

The $\hat{x}$-axis represents the EPR-pair, or Bell states, namely,

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Similarly, the $\hat{y}$-axis represents the imaginary part of the state vector, or mathematically,

$$|+i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{i}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$|-i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{i}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

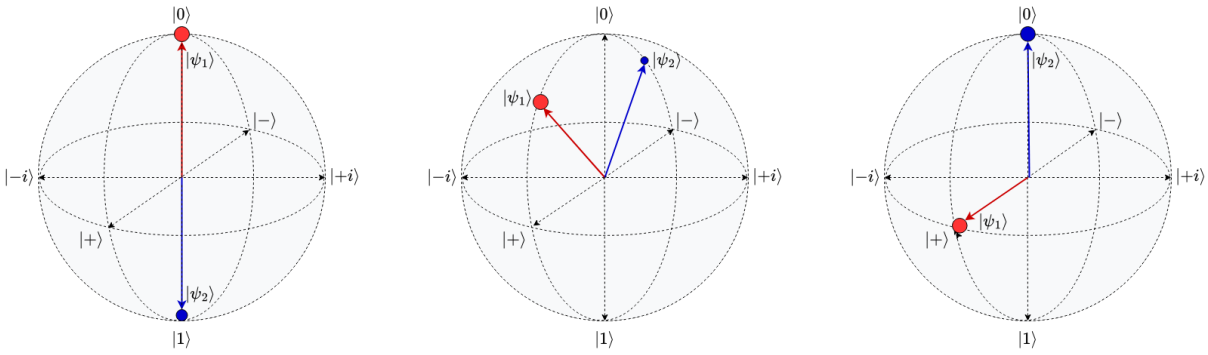
Every point on the surface of a Bloch sphere represents a quantum state. This makes Bloch sphere diagrams a very powerful tool for representing quantum gate transformations applied to a qubit.

### 2.3.2 Quantum Gates Operations

Applications of quantum information processing employs single qubit gates as more of a mathematical abstraction compared to realisable classical logic gates. Quantum gates are not always physically but are extensively used in analysing quantum computing algorithms. From a mathematical point of view, quantum gates are unitary transformations on a small number of qubits. Typically, quantum gates work with up to 3 qubits.

Single qubit gates correspond to unitary operations known as *Pauli* matrices, I, X, Y, and Z. The Pauli $X$ gate is analogous to a classical `NOT` gate in that it performs a qubit flip transformation. For example, given an initial observation of the state $\psi$ which is specified by normalised amplitudes $\alpha$ and $\beta$, the $X$ gate acts linearly to interchange the amplitude of the coefficients that define the superposition by the transformation

$$X : |\psi\rangle \rightarrow |\psi'\rangle \tag{2.41}$$




(a) Pauli-$X$ gate. (b) Pauli-$Z$ gate. (c) Hadamard gate.

Figure 2.3: Three Bloch spheres representing important single-qubit quantum gate operations. The initial state is in red and the final measured state is blue. The $X$ gate is analogous to a classical `NOT` gate and the $Z$ gate changes the phase of the qubit.

for

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$
$$|\psi'\rangle = \alpha\,|1\rangle + \beta\,|0\rangle \tag{2.42}$$

The unitary matrix representing the X gate transformation is written as

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.43}$$

Thus, given a qubit in Hilbert space $H_2$ with normalised amplitudes $\alpha$ and $\beta$, the output of the $X$ gate unitary operator is

$$X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \tag{2.44}$$

This transformation can also be illustrated on a Bloch sphere as shown in figure 2.3a where the initially measured state of the qubit, $|\psi_1\rangle$, is rotated around the $\hat{x}$-axis by $\pi$ rad to obtain $|\psi_2\rangle$. Since the quantum gate is a unitary operator, it maintains the condition of normalisation on the Hilbert space [8]. Other Pauli gate matrices are expressed in equation 2.45 where it can be shown that for each unitary matrix $U$, $UU^\dagger = I$, where $U^\dagger$ is the adjoint of $U$. This implies that the identity matrix $I$, operates in a manner that is analogous to a classical circuit buffer which has the same bit at input and output. Applying the an identity gate is equivalent to measuring the same state at the start and end of a computation, the input state of the quantum system is the same as the output state.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.45}$$

The $X$ gate is one of three physically realisable single-qubit gates that are considered in this research. The other two gates that are of significance to quantum information processing are the Pauli-$Z$ gate and the *Hadamard* gate $H$ - illustrated using Bloch diagrams as shown in figure 2.3b and 2.3c, respectively. Equation 2.45 shows that the $Y$ gate performs rotations through the $\hat{y}$-axis which corresponds to the complex plane and is therefore not physically realisable. The $Z$ gate is a special case of the *phase gate*,

$$R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \tag{2.46}$$

which rotates the state vector of a qubit through the $\hat{z}$-axis by $\phi = \pi$ rad, effectively negating the amplitude of the $|1\rangle$ basis state and leaving the $|0\rangle$ basis state unchanged. The Hadamard gate $H$ rotates the qubit by $\pi/2$ rad through the $\hat{y}$-axis and by $\pi$ rad in the $\hat{x}$-axis. This implies that, given an initial state $|0\rangle$ to which the Hadamard

gate is applied, there is an equal probability of observing $|0\rangle$ or $|1\rangle$ [1]. When a Hadamard gate is applied to the $|+\rangle$ state, the output is derived from

$$\begin{aligned} H|+\rangle &= H\left[\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}\right] \\ &= \frac{1}{\sqrt{2}}H\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{\sqrt{2}}H\begin{pmatrix}0\\1\end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix} + \frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix}\frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix} \end{aligned}$$

which gives the state $|0\rangle$. This derivation of the Hadamard operation exposes the phenomenon of *interference* that qubits experience due to their wave nature. This occurs when the $|1\rangle$ and $-|1\rangle$ states cancel each other out, corresponding to an overlap in the peaks and troughs of the qubit waveforms that are in a superposition of states.

### 2.3.3 Multiple-Qubit Gates

Multiple-qubit gates can be realised by performing a sequence of single-qubit gate transformations. Constructing a multiple-qubit gate from two single-qubit systems given by matrix $U$ and matrix $V$ equivalent to taking the tensor product of the matrices, i.e. $U \otimes V$. In some cases, multiple-qubit gates can transform the system such that qubits become entangled. Generally, these type of gates cannot be decomposed into a tensor product of single-bit transformation. An example of a 2-qubit gate is the *controlled*-NOT (CNOT) gate which is defined as the sum of tensor products of the identity matrix $I$ and the $X$ gate with the standard basis inputs $|0\rangle$ and $|1\rangle$, i.e.,

$$\texttt{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \tag{2.47}$$

Equivalently, the unitary matrix representation of the CNOT gate is

$$\texttt{CNOT} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \tag{2.48}$$

Given a standard basis input, the CNOT gate has four possible outputs, namely,

$$\texttt{CNOT} \;: \begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{cases} \tag{2.49}$$

The CNOT gate is particularly important for applications in quantum information processing due to its capability to change the entanglement between input qubits [10]. For example, given the separable 2-qubit input state $|\psi_1\rangle$ where

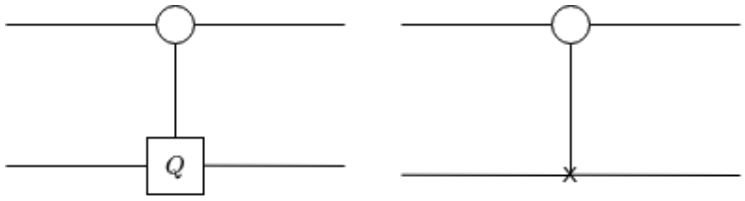
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle \tag{2.50}$$

the CNOT gate converts unentangled input state to an entangled Bell state

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

The generalised CNOT gate consists of gates that perform a single-qubit transformation $Q$ on the second qubit in the input when the first input is the basis state $|1\rangle$ and leave it unchanged when the first input is $|0\rangle$. The first input is called the *control qubit* and the second qubit is called the *target qubit*. Formally, the generalised CNOT gate can be expressed as

$$\Lambda Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q \tag{2.51}$$




Generalised $\Lambda Q$ CNOT gate. $\Lambda X$ CNOT gate.

Figure 2.4: The $\Lambda X$ gate is a 2-qubit gate which is a special case of the generalised 2-qubit $\Lambda Q$ CNOT gate.

where $Q$ is a $2 \times 2$ matrix. Thus, the $4 \times 4$ matrix representation of the generalised CNOT gate is

$$\Lambda Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q_{11} & q_{12} \\ 0 & 0 & q_{21} & q_{22} \end{pmatrix} \tag{2.52}$$

where each $q_{ij}$, for $i = 1, 2$ and $j = 1, 2$, is an element of the single-qubit gate $Q$. The graphical representation of the generalised CNOT gate and the special case of the CNOT which uses the $X$ gate is shown in figure 2.4. Note that the control qubit of the CNOT gate does not change and the target qubit changes depending on the state of the control qubit. This operation is analogous to the operation of the XOR gate, since the unitary transformation can also be expressed algebraically as

$$\texttt{CNOT} : |A, B\rangle \rightarrow |A, B \oplus A\rangle \tag{2.53}$$

where $\oplus$ represents the direct sum of the basis sets $A$ and $B$ that produces a vector space with basis $A \cup B$.

### 2.3.4 Quantum Circuits

Illustrations of the CNOT gate as shown in figure 2.4 form an essential part of representing and interpreting quantum computations. A sequence of quantum gates forms a *quantum gate array*, also known as a *quantum circuit*. In a quantum circuit, single-qubit gates are represented using block diagram notation as depicted in figure 2.5. There are infinitely many $2 \times 2$ unitary matrices so there are also infinitely many single-qubit gates and quantum circuits. In quantum circuit representations, time progresses from the left, at the input of the quantum circuit, to the right, at

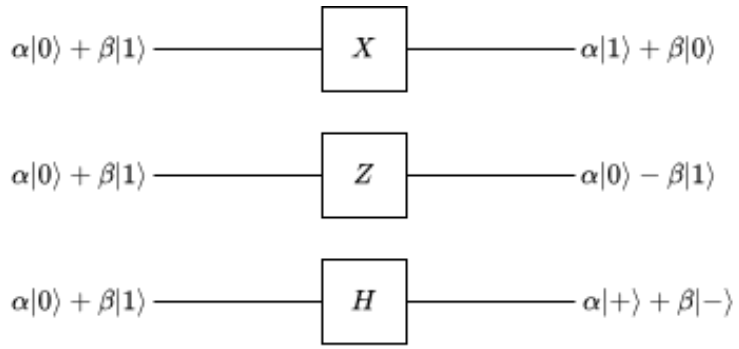



Figure 2.5: Quantum circuit gate component representations of the Pauli-$X$, Pauli-$Z$ and $H$ single-qubit logic gates.

the output of the quantum circuit. Each line in the quantum circuit represents a wire, which in turn, represents the passage of time from left to right or a qubit of information as it is translated in Hilbert space. By convention, it is assumed that the multiple-qubit input to a circuit is the state consisting of a sequence of $|0\rangle$ basis states. It is crucial to note that the final state of an input qubit cannot be determined by only looking at the wire corresponding to that

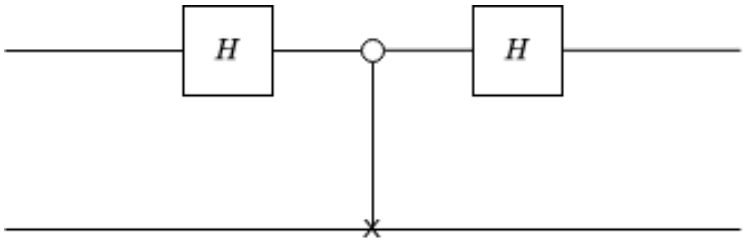



Figure 2.6: Demonstrating a quantum circuit that consists of two series $H$ gates on the control line of the $\Lambda X$ gate.

qubit. For example, from the circuit in figure 2.6, it might appear that the first qubit's state would remain the same since $H^2 = I$, however, given the input state $|00\rangle$, the state of the output is defined by the unitary transformation

$$U : |00\rangle \rightarrow \frac{1}{2}\left(|00\rangle + |10\rangle + |01\rangle - |11\rangle\right)$$

which is not obvious by focusing on the control line of the circuit [10]. Figure 2.7 shows another example of a quantum circuit known as a *swap gate* which contains three `CNOT` gates. Since the swap gate uses `CNOT` gates, it follows a sequence of transformations on a basis state $|\psi_a, \psi_b\rangle$ that involves direct sums of vector states that produces an output where the qubit states are interchanged. The swap gate uses both qubits as the control to perform the operation

$$\begin{aligned} |\psi_a, \psi_b\rangle &\rightarrow |\psi_a, \psi_a \oplus \psi_b\rangle \\ &\rightarrow |\psi_a \oplus (\psi_a \oplus \psi_b), \psi_a \oplus \psi_b\rangle \\ &= |\psi_b, \psi_a \oplus \psi_b\rangle \\ &\rightarrow |\psi_b, (\psi_a \oplus \psi_b) \oplus \psi_b\rangle \\ &= |\psi_b, \psi_a\rangle \end{aligned} \tag{2.54}$$

The swap gate is also equivalent to applying the transformation $U$, given by,

$$U : |\psi_a\rangle \langle\psi_a| \otimes X + |\psi_b\rangle \langle\psi_b| \otimes X \tag{2.55}$$

which applies a tensor product of the Pauli-$X$ gate to each qubit in the system. Quantum circuits are said to be

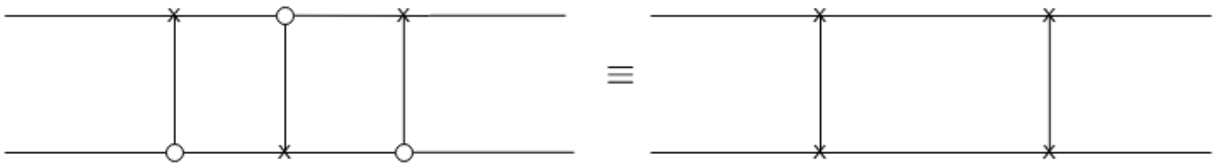



Figure 2.7: Quantum circuit of a swap gate that interchanges the input state from $|\psi_a, \psi_b\rangle$ to $|\psi_b, \psi_a\rangle$.

*acyclic* in that feedback from one part of the circuit to another is prohibited [10]. This is contrary to classical electronic circuits which employ feedback to control the stability of classical systems. Another contradiction between quantum circuits and classical circuits is that quantum circuit wires cannot be joined together to perform an operation that is analogous to a classical `OR` gate operation. Furthermore, most quantum circuit operations are reversible since they use unitary operations, however, qubits cannot be cloned, which means that copy operations at the output of a quantum circuit are prohibited.

Quantum circuit outputs are measured to collapse the single qubit state $|\psi\rangle$ with basis states $|0\rangle$ and $|1\rangle$ to a classical bit $\sigma$ where the probability of obtaining 0 is $|\alpha|^2$ and the probability of obtaining 1 is $|\beta|^2$, such that the normalisation condition is satisfied. The symbol for a measurement in a quantum circuit is shown in figure 2.8 where $\sigma$ is represented by a double-line wire.


Figure 2.8: Quantum circuit measurement symbol.

## 2.4 CONCLUSION

Quantum gates are unitary operations on vector states that transform the properties of qubits. This mathematical definition of quantum gates is useful in interpreting vector transformations, however, the structures represented in by the mathematics may not always be realisable. For that reason, this paper focuses on quantum gates that are realisable such as the Pauli-$X$, Pauli-$Z$, $H$, and `CNOT` gates. For solid state or optical quantum computers, these unitary transformations on qubits can be physical operations such as the application of a magnetic field to particles in NMR and laser pulses in ion trap implementations[10]. Performing quantum computation can be difficult due to the probabilistic behaviour of qubits, thus, modelling systems that are costly to achieve with current technology can be useful. The theoretical framework formulated in this section forms the foundation to the concepts used to design and emulate a quantum information processing system on FPGA.

CHAPTER 3

# LITERATURE REVIEW

Integrating quantum computers to current classical systems has proven to be a difficult endeavour because of the differences between classical bits and qubits. Properties of qubits such as superposition and entanglement also make it difficult to construct heterogeneous edge computing systems consisting of quantum processing units (QPUs), classical central processing units (CPUs), and graphical processing units (GPUs). This chapter presents a review of existing literature on modelling quantum computer architecture on a classical machine. The study focuses on previous implementations and simulations of interfaces between quantum and classical computers in heterogeneous computing systems. Furthermore, guidelines for conducting accurate FPGA-based quantum computer emulations are discussed with respect to quantum algorithm implementation and communicating the output from a quantum computer as bits to a classical computer. From this context, the paper investigates bit encoding methodologies, quantum algorithm and quantum circuit implementations in engineering applications, qubit decoding, as well as different types of quantum computer architectures that exist.

The chapter begins by discussing applications of quantum circuit theory and implementations in quantum computing algorithms that can be performed on a FPGA-based emulated quantum computer. Then, the study investigates quantum computing architectures, communication protocols and interfaces for transmitting data between classical and quantum computers. In particular, the use of data encoding methods that have been previously implemented in engineering are discussed. The review terminates with a discourse into the overall integration and accurate simulation of heterogeneous systems containing QPUs.

## 3.1 MODELLING QUANTUM GATES AND THE QUANTUM FOURIER TRANSFORM (QFT)

Quantum circuits are in important tool for describing quantum algorithms that employ physical properties of qubits such as superposition and entanglement. Some of the physical properties of qubits make it difficult to implement quantum computations at a large scale. For instance, qubits undergo *quantum decoherence* which is a process where a quantum system's interaction with its surroundings leads to a loss of information. To develop and implement quantum algorithms while compensating for the costs in achieving stable quantum systems, Khalid et al., describe the emulation of quantum circuits in FPGAs which can map the parallel tasks more efficiently than software simulations [5]. In their approach, quantum circuits are modelled using VHDL and synthesized in hardware to achieve the performance that is required for practical applications.

Khalid et al. implement a qubit by storing values of the state amplitudes $\alpha$ and $\beta$ for a state vector with the standard basis set $\{|0\rangle, |1\rangle\}$. The amplitudes were processed using a fixed point scheme. The reason for opting for a fixed point scheme instead of using floating-point representations was because of $\alpha$ and $\beta$ having a decimal part of 0 or 1 only [5]. Their approach to quantum gates was to introduce an input error $\delta$ that is propagated and augmented with discretisation error $\epsilon$ in the coefficients of the quantum gate's unitary matrix. An expanded error model includes multiple errors that are added linearly to the qubit transformation as illustrated in figure 3.1.

These errors arise when performing quantum measurements according the Heisenberg's Uncertainty Principle, and affect the probability of the qubit being in the $|0\rangle$ or $|1\rangle$ state [5]. Using the Bloch sphere representation to

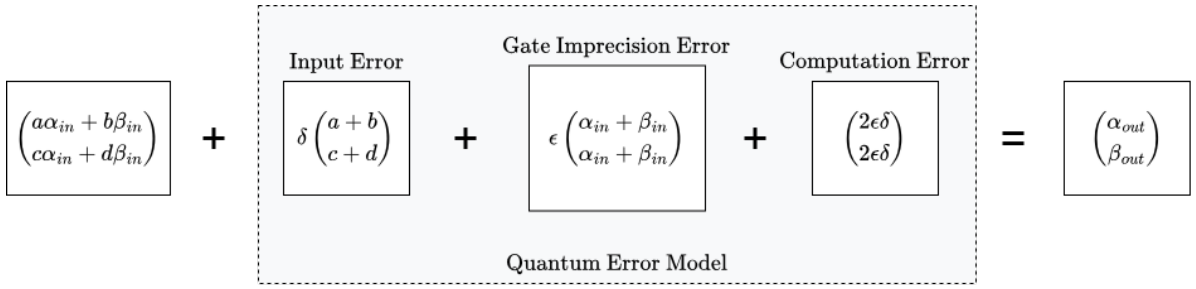



Figure 3.1: Quantum gate model accounting for input errors, gate imprecision errors and computation errors that affect the output of a quantum algorithm.

illustrate the state of the qubit where the desired state vector is $(\alpha, \beta)^T$ and the actual, measured state vector is $(\alpha + \alpha_\epsilon, \beta + \beta_\epsilon)$, as shown in figure **??**, Khalid et al. define the the absolute error in the measurement as the distance $E$ between the actual state values and the measured state values.

Khalid et al. considered errors when mapping quantum gate transformations to VHDL code and showed that an $n$-qubit gate is represented by a $2^n \times 2^n$ matrix [5]. For controlled gates, variables were passed as a parameter to a code generating script which automated the construction of an arbitrary size quantum gates [5]. Immediate registers, called *quantum state registers* (QSRs), were used to hold the qubit values after each gate in a quantum circuit, as depicted in figure 3.2.

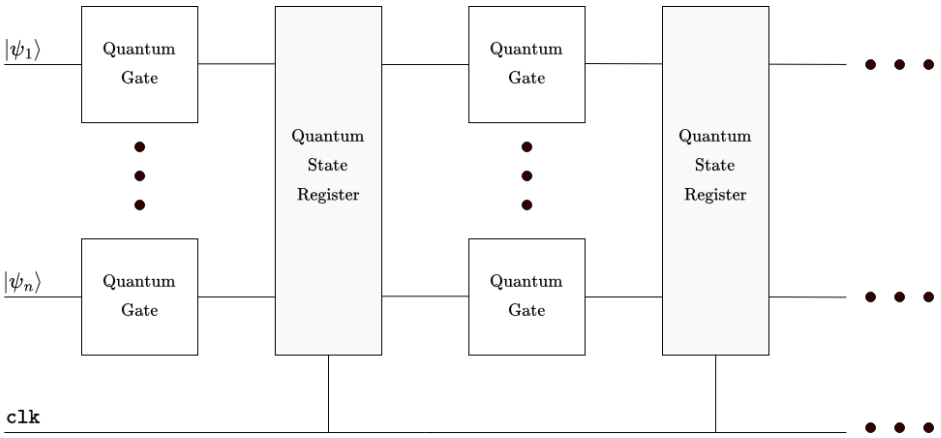



Figure 3.2: Emulated quantum circuit uses quantum state registers to hold qubit values at the output of each quantum gate in a quantum circuit.

Since time flows from left to right in the quantum circuit diagram, each quantum register is equivalent to a representation of the state of the entire 3-qubit quantum system [5].

In a similar implementation of the FPGA-based emulated quantum computer, Silva and Zabaleta use a single matrix to model quantum gates [12]. The justification for using a single matrix was to use a fewer memory resources in the FPGA and emulate transformations of greater input vectors [12]. Another difference between Khalid et al. and Silva and Zabaleta's implementations is that the latter wrote the unitary matrix in C++ and used directives to convert the code to a hardware description language. In both implementations, however, the chosen quantum circuit for performing quantum algorithms on FPGA was the quantum Fourier transform (QFT).

In the analysis of linear time-dependent classical systems, the Fourier transform is harnessed as a reversible tool that transforms a signal from the time domain to the frequency domain and vice versa. In the discrete time domain, the Fast Fourier transform (FFT) is performed to reduce the computational complexity by decomposing the Discrete Fourier transform (DFT) of a signal into two half-point transforms. Silva and Zabaleta approach the QFT circuit as the quantum counterpart of FFT algorithms by exploiting advantages of quantum parallelism to transform data

in the time domain to frequency domain [12]. However, in 2015, Khalil et al. noted that the QFT does not speed up the computational time of the Fourier transform on classical data due to the property of qubits that prohibits parallel read out of state amplitudes [6]. In 2010, Nielsen and Chuang defined the 3-qubit QFT as an efficient quantum circuit for performing the Fourier transform on quantum amplitudes, as seen in figure 3.3 below [8]. The corresponding matrix for the `QFT` gate described by the 3-qubit quantum circuit is written explicitly, using $\omega = e^{2\pi/8}$, as

$$\texttt{QFT} = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \tag{3.1}$$

The 3-qubit QFT circuit proposed by Nielsen and Chuang uses a sequence of $H$ gates, $R_\phi$ phase gates, and a special case of the phase gate known as the $T$ gate which rotates a state vector by $\phi = \pi/8$ rad. For an $n$-qubit system, a total of $n(n+1)/2 + n/2$ gates are required to perform the QFT [8].

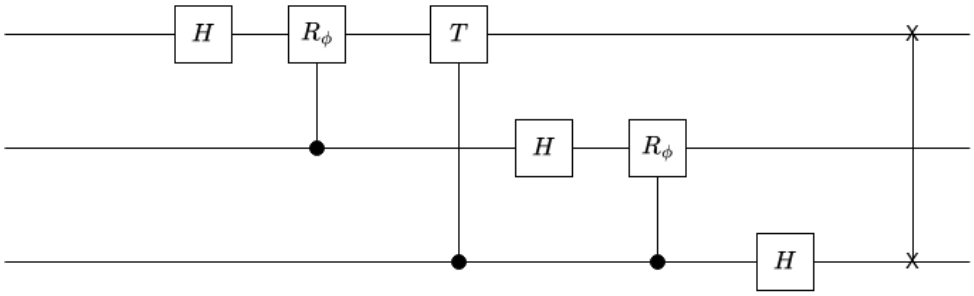



Figure 3.3: An explicit quantum circuit for the 3-qubit Quantum Fourier Transform which uses the Hadamard gate, $H$, phase gate, $R_\phi$, and the $\pi/8$ gate, $T$.

Nielsen and Chuang further elaborated that the advantage of using the QFT is that is allows for *phase estimation*, approximation of the eigenvalues of a unitary operator [8]. Additionally, the QFT provides an algorithm of $\mathcal{O}(n^2)$ on a quantum computer, compared to the FFT which requires $\mathcal{O}(n2^n)$ gates to computer the DFT on a classical computer [8]. The QFT is similar to the FFT in that it is invertible by reversing the circuit. Using this property of the circuit, the QFT can be employed to solve many of the computational problems that are explored in the following section.

## 3.2 Applications of Quantum Algorithms

According to Nielsen and Chuang, phase estimation should be approached as modular part of an algorithm that, when combined with other subroutines, can perform quantum parallel tasks [8]. Phase estimation uses black boxes, or *oracles* which is capable of preparing a quantum state and performing a controlled-gate operation. This procedure uses two registers, one containing $t$ bits that are initially in the state $|0\rangle$ and a second register which begins in the state $|u\rangle$, and contains as many qubits as is necessary to store the state $|u\rangle$. In the first stage of the procedure, a Hadamard gate is applied to the first register, followed by an application of controlled-gate operations on the second register such that the ancillary matrix of the controlled-gate is raised to successive powers of two [8]. In the second stage of phase estimation, the inverse QFT is applied on the first register. The state of this register is read out in the third and final stage of the phase estimation procedure to produce a good estimation of the phase in the oracle.

In a 1994 seminal paper, Shor introduced quantum order-finding algorithms as an effective means for solving discrete logarithms and factoring problems [11]. Most applications of Shor's algorithm involve the use the QFT

circuit in combination with other gates such as the Hadamard gate [13, 4]. The algorithm that was proposed by Shor has been extensively researched for its ability to crack the public key encryption method, known as the RSA cryptosystem. In a 2019 study that focused on the quantum Shor algorithm simulated on FPGA, Zhang et al. employed Shor's findings to factor a large integer $N$ which satisfies $N = p \times q$, where $p$ and $q$ are prime numbers [13]. Zhang et al. divided the algorithm into a quantum part and classical part, then simulated the execution of the quantum part on FPGA as a heterogeneous device for offloading inefficient work from a CPU host [13]. The communication interface between the heterogeneous quantum device and the CPU for executing both parts of the divided algorithm was modelled through PCIe [13]. Zhang et al. performed the experiment on the CPU using the C programming language while the hardware architecture was implemented on Intel Arria 10 GX 1150 device using OpenCL to simulate three quantum registers with a maximum length of 17 qubits [13]. The use of 17 qubits to perform Shors algorithm in factoring the integer $(327)_{10}$, required 102796 adaptive lookup tables (ALUTs), 157446 registers, and a total of 1846 RAM blocks on the FPGA [13]. Zhang et al. found that the number of RAM blocks double for every qubit that is added [13]. Additionally, the study showed that the execution time increases exponentially with the qubit number such that the algorithm's time complexity is linear with the number of qubits, $n$ [13].

## 3.3 Quantum Processing Unit Architectures

In a similar 2021 study, Hlukhov, approaches a quantum computer as a heterogeneous device that consists of a classical control computer and its quantum accelerator, i.e. a digital quantum coprocessor [4]. The study focuses on implementing the digital quantum coprocessor on FPGA to factorise the integer $(15)_{10}$ using Shor's algorithm. Unlike the implementation of this quantum algorithm by Zhang et al., Hlukhov introduced a model of digital quantum gate that includes an ALU, a comparator and a pipeline register as seen in figure 3.4 [4].

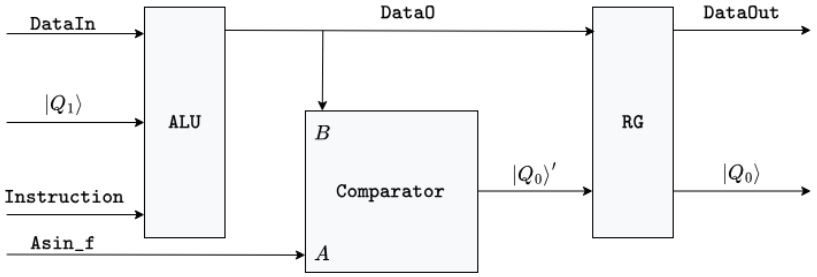



Figure 3.4: Model of a digital quantum gate that includes an ALU, a comparator and a pipeline.

In the digital quantum gate model, the output of the gate is represented by the qubit state code `DataOut` and the measured state $|Q_0\rangle$ of a qubit is taken from the pipeline register [4]. An intermediate status code, `DataO`, is evaluated in the comparator with the random variable `Asin_f` to obtain the measured state $|Q_0\rangle'$. This quantum coprocessor architecture also positions both oscillators and transformers near the digital quantum gates inside the digital qubits [4]. The design for the implementation of the quantum part of Shor's algorithm used 8 digital qubits in a quantum register where each qubit was a byte [4].

## 3.4 Quantum Communication Interfaces and Protocols

## 3.5 Heterogeneous Computing Systems with Quantum Computers

## 3.6 Quantum Computer Model Accuracy

CHAPTER 4

# METHODOLOGY

## 4.1 USER REQUIREMENTS

CHAPTER 5

# DESIGN OF SPECIAL SYSTEM

## 5.1 SYSTEM DESIGN

CHAPTER 6

# RESULTS AND DISCUSSION

## 6.1 SUBSECTION NAME

# BIBLIOGRAPHY


[1] DE WOLF, R. Quantum computing: Lecture notes.

[2] DESIGN, AND REUSE. Free ip cores projects. `http://www.design-reuse.com/download/sip/`. Accessed: 2015-03-03.

[3] GUPTA, M., AND NENE, M. J. Quantum Computing: An Entanglement Measurement. In *Proceedings of IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation, ICATMRI 2020* (12 2020), Institute of Electrical and Electronics Engineers Inc.

[4] HLUKHOV, V. Implementation of Shor's Algorithm in a Digital Quantum Coprocessor. In *International scientific and practical conference:{Intellectual systems and information technologies}* (2021).

[5] KHALID, A. U., ZILIC, Z., AND RADECKA, K. FPGA Emulation of Quantum Circuits, 2004.

[6] KHALIL-HANI, M., LEE, Y., AND MARSONO, M. An Accurate FPGA-Based Hardware Emulation on Quantum Fourier Transform.

[7] KURZYK, D. Introduction to Quantum Entanglement. *Theoretical and Applied Informatics 24* (08 2012), 135–150.

[8] NIELSEN, M. A., AND CHUANG, I. L. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[9] POWELL, J. R. The Quantum Limit to Moore's Law. *Proceedings of the IEEE 96*, 8 (2008), 1247–1248.

[10] RIEFFEL, E. G., AND POLAK, W. H. *Quantum Computing: A Gentle Introduction*. MIT Press, 2011.

[11] SHOR, P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *35TH ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE, PROCEEDINGS* (LOS ALAMITOS, 1994), IEEE Comput. Soc. Press, pp. 124–134.

[12] SILVA, A., AND ZABALETA, O. G. FPGA Quantum Computing Emulator Using High Level Design Tools. In *2017 8th Argentine Symposium and Conference on Embedded Systems, CASE 2017* (11 2017), Institute of Electrical and Electronics Engineers Inc., pp. 19–24.

[13] ZHANG, X., ZHAO, Y., LI, R., LI, X., GUO, Z., ZHU, X., AND DONG, G. The Quantum Shor Algorithm Simulated on FPGA. In *2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)* (2019), pp. 542–546.

APPENDIX A

# ADC/DAC CORE

## A.1 A USEFUL SUB APPENDIX

Put your appendix stuff here.