Mathematics of Quantum Computing

(Tentative Title)

A report submitted in partial fulfillment
of the requirement for the degree of

MASTER OF SCIENCE
IN
MATHEMATICS

by

Pranay Raja Krishnan
22MMT002

Under the guidance of

Dr. Trivedi Harsh Chandrakant

Department of Mathematics
The LNM Institute of Information Technology,
Rupa ki Nangal, Post-Sumel, Via-Jamdoli, Jaipur,
Rajasthan 302031 (INDIA).

Abstract

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

CERTIFICATE

This is to certify that the dissertation entitled **Mathematics of Quantum Computing (Tentative Title)** submitted by **Pranay Raja Krishnan** (22MMT002) towards the partial fulfillment of the requirement for the degree of Master of Science (M.Sc) is a bonafide record of work carried out by him at the Department of Mathematics, The LNM Institute of Information Technology, Jaipur, (Rajasthan) India, during the academic session 2018-2019 under my supervision and guidance.

Dr. Trivedi Harsh Chandrakant
Assistant Professor
Department of Mathematics
The LNM Institute of Information Technology, Jaipur

Acknowledgements

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Date: August 25, 2023 Pranay Raja Krishnan

List of Notations

Unless explicitly defined the following notations are used.
TODO: Add Required Notation

Symbol	Meaning
$\subseteq$	subset or equal to
$\not\subset$	not subset
$\supseteq$	superset or equal to
$\emptyset$	empty set
$\in$	belongs to
$\notin$	does not belong to
$\prod_{i \in I}$	product over index set I
$\mathbb{C}$	the set of real numbers
$\mathbb{R}$	the set of real numbers
$\mathbb{N}$	the set of natural numbers

Contents

Chapter 1

A brief history of Quantum Computing

In the last decades of the twentieth century, certain scientists sought to combine two recent theories that were highly influential: **Information Theory** and **Quantum Mechanics**.

- **1984:** Charles Bennet and Gilles Brassad published a quantum key distribution protocol now called **BB84**, allowing two parties to establish an absolutely secure secret key.

- **1980s:** Feynman recognized that a system of n-particle quantum systems could not be simulated efficiently by a Turing machine, seemingly requiring time/space that is exponential in n. He proposed that computers based on quantum systems could simulate quantum processes with more efficiency. This led to the question: If simluating quantum problems was more efficient on a quantum computer, would there be other problems that would run more efficiently on a quantum computer?

- **1994:** Peter Shor found the famous **Shor's Algorithm** for a quantum computer which could factors n-digit integers into primes with n^2 efficiency (with high probability). The fastest known algorithm for factoring n-digit integers in classical computing is of efficiency around $2^{n^{1/3}}$

Chapter 2

Qubits

2.1 Setting up the Qubit

The computers we use today rely on classical information theory, which are based on **bits** (binary digits) which can represents a 0 or 1 state. These **classical computers**) are equivalent to a Turing Machine in computational efficiency.

On a quantum computer the **qubit** (quantum bit) is the basic unit of information. On a real-life quantum computer, a qubit can be implemented using a variety of quantum phenomena. In labs, qubits have been implemented using photon polarization, electron spin, the ground/excited state of an atom in a cavity, and even defect centers in a diamond. While there could be many such real-life realizations of qubits, in this paper, we are not concerned with the specific implementation as long as they follow certain abstract rules.

Definition 2.1.1 (Qubit)**.** *A* ***qubit*** *is any quantum mechanical system which is associated with* 2*-dimensional complex Hilbert space* $\mathcal{H}$ *(known as the* ***state space*** *and follows the below postulates:*

- *Postulate of Superposition*
- *Postulate of Measurement*
- *Postulate of Projection 'TODO: Refer Scherer, P37'*
- *Postulate of Entanglement*
- *Postulate of Transformation*

A given state of the system is completely described by a unit vector $|\psi\rangle$*, which is called the* ***state vector*** *(or wave function) on the Hilbert Space*

The postulates in the above definition will be elaborated on in the upcoming sections.

Notation 2.1.2. *Observe above that we have written the vector* $\vec{\psi} \in \mathcal{H}$ *as* $|\psi\rangle$*. This is the notation for a vector in* Dirac's bra/ket notation*, and is read* ***ket psi***

When working with Hilbert spaces associated with quantum systems, we normally use *orthogonal bases.* The **computational basis** of the two dimensional complex vector space $\mathcal{H}$ is

$|0\rangle, |1\rangle$ where $|0\rangle = \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ \\ 1 \end{bmatrix}$

This is because these orthogonal bases represent perfectly distinguishable states.

TODO: refer Shor's Notes, Lec 02

Lemma 2.1.3 (Postulate of Superposition)**.** *With respect to the computational basis* $\{|0\rangle, |1\rangle\}$*, the state of the qubit can be described as*

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \\ b \end{bmatrix} = \begin{bmatrix} a \\ \\ b \end{bmatrix} \textit{ where } a, b \in \mathbb{C} \textit{ and } a^2 + b^2 = 1.$$

Another common basis for the Hilbert space $\mathcal{H}$ modelling a qubit is the **Hadamard Basis** $\{|+\rangle, |-\rangle\}$ where

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

The principle of superposition says that the state of a qubit can be modelled with a 2-dimensional Hilbert space. This leads to qubits being referred to as **two-state** quantum systems. This does not mean that this system has only two states, but rather that all possible states exist as a linear combination of just two states.

Like qubits are modelled by 2-dimensional Hilbert spaces, there could be quantum systems whose states are modelled as vectors in 3-dimensional vector spaces, these are called **qutrits**. Similarly, quantum systems whose states are modelled with n-dimensional vector spaces are called **qudits**. A result shows that a system of qutrits or qudits can be reduced to a system of multiple qubits that has similar efficiency, so these systems are rarely used.

Bibliography

[1] Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris.

[2] Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus.

[3] Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis.

[4] Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices.

[5] Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl.

[6] Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante.