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 28, 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 text, 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*
$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix}a\\0\end{bmatrix} + \begin{bmatrix}0\\b\end{bmatrix} = \begin{bmatrix}a\\b\end{bmatrix}$ *where $a, b \in \mathbb{C}$ 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.
The state of a qubit is a continuum which might indicate that we can use a single qubit to store an infinite amount of information. However, a principal of quantum mechanics states that we cannot interact with the qubit without fundamentally altering its state. To work with the state stored in a qubit, we must perform a measurement which forces the state of the qubit to "collapse" into one of two *preferred states*.

Lemma 2.1.4 (Postulate of Measurement)**.** *Any measurement device that interacts with the qubit will be calibrated with a pair of orthonormal vectors called the* ***preferred basis****, say*
$|u\rangle, |v\rangle$*. If the state of the qubit with respect to the preferred basis is* $|\psi\rangle = a|u\rangle + b|v\rangle$*, then measurement of the qubit will yield either* $|u\rangle$ *with a probability of* $|a|^2$ *or* $|v\rangle$ *with a probability* $|b|^2$*.*
After measurement, the state of the qubit itself will be changed to the output of the measurement.

This behaviour is an axiom of quantum mechanics substantiated by empirical observations from experiments over the last hundred years.

This property limits the amount of information that can be extracted from a qubit: a measurment yields atmost a single classical bit worth of information. In most cases, we also cannot make more than one measurement of original state of the qubit. On measurement, we have two possibilities, each corresponding to a probability of $|a|^2$ and $|b|^2$, then the total probability of the whole space will be $|a|^2 + |b|^2 = 1$, which is valid for unit vectors $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$.

Notation 2.1.5. *When* $|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$, *then* $\langle\psi|$ *is the conjugate transpose of* $|\psi\rangle$ *and is read as* ***bra psi****,* $\langle\psi| = \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix}$

This lets us write the inner product for $\mathcal{H}$ as: For any $|v\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, |w\rangle = \begin{bmatrix} c \\ d \end{bmatrix} \in \mathcal{H}$, the operation $\langle v|w\rangle = \langle v|\,|w\rangle = \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \overline{a}c + \overline{b}d$
We will consider the inner product as being linear in the second variable and conjugate-linear in the first variable.
If $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$, then we can show $\langle 0|\psi\rangle = a$, $\langle 1|\psi\rangle = b$. Therefore we can write $|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \langle 0|\psi\rangle\,|0\rangle + \langle 1|\psi\rangle\,|1\rangle$. The standard inner product of the $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ with itself in the Hilbert space $\mathcal{H}$ can therefore be written as $\langle\psi|\psi\rangle = \langle\psi|\,|\psi\rangle = \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = |a|^2 + |b|^2$

Lemma 2.1.6 (Postulate of Measurement)**.** *Any physical observable is associated with a self-adjoint operator* $\mathcal{A}$ *on the Hilbert space* $\mathcal{H}_S$*. The possible outcome of a measurement of the observable* $\mathcal{A}$ *is one of the eigenvalues of the operator* $\mathcal{A}$*.*
Writing the eigenvalues equation, $\mathcal{A}\,|i\rangle = a_i\,|i\rangle$ *where* $|i\rangle$ *is an orthonormal basis of eigenvectors of the operator* $\mathcal{A}$*, and* $|\psi\rangle = \sum_i c_i\,|i\rangle$*, then the probability that a measurement of the observable* $\mathcal{A}$ *results in the outcome* a_i *is given by* $p_i = |\,\langle i|\psi\rangle\,|^2 = |c_i|^2$

'TODO: Proof that self-adjoint matrices represent measurement operators'
'TODO: Relation of POVM and matrices'

Let $\mathcal{H}_1$ be an n-dimensional vector space with basis $\alpha = \{|a_1\rangle, |a_2\rangle, ..., |a_n\rangle\}$ and $\mathcal{H}_2$ be an m-dimensional vector space with basis $\beta = \{|b_1\rangle, |b_2\rangle, ..., |b_n\rangle\}$, then the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ is an nm-dimensional space with basis elements of the form $|a_i\rangle \otimes |b_j\rangle$

Notation 2.1.7. *In dirac's bra/ket notation, the tensor product of* $|v\rangle \in \mathcal{H}_2, |w\rangle \in \mathcal{H}_2$ *is* $|vw\rangle = |v\rangle |w\rangle = |v\rangle \otimes |w\rangle$

The tensor product is defined to satisfy the following properties:

1. $(|v_1\rangle + |v_2\rangle) |w\rangle = |v_1\rangle |w\rangle + |v_2\rangle |w\rangle$
2. $|v\rangle (|w_1\rangle + |w_2\rangle) = |v\rangle |w_1\rangle + |v\rangle |w_2\rangle$
3. $(a \cdot |v\rangle) |w\rangle = |v\rangle (a \cdot |w\rangle) = a \cdot (|v\rangle |w\rangle)$

Every element $|\sigma\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ can be written as a superposition of elements of the basis $\{|a_i\rangle |bj\rangle\}$ as $|\sigma\rangle = \alpha_{11} |a_1 b_1\rangle + \alpha_{12} |a_1 b2\rangle + ... + \alpha_{nm} |a_n b_m\rangle$.
Most elements $|\sigma\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ *cannot* be decomposed to $|\sigma\rangle = |v\rangle |w\rangle$ where $v \in \mathcal{H}_1, w \in \mathcal{H}_2$. 'TODO: Check proof'
As we have observed, a single qubit only gives us one classical bit worth of information. This equivalence diverges once we include *multiple* interacting qubits in the system. A system of n classical bits will have one degree of freedom for each bit, resulting in a state-space of n dimensions, i.e. classical systems are linear in n. In quantum systems, however, a system of n qubits will result in a state space of 2^n dimensions. This is because of the quantum property of *entanglement* which describes how quantum systems interact with each other.

Lemma 2.1.8 (Postulate of Entanglement)**.** *When we have two qubits being treated as a combined system, the state space of the combined system is the tensor product* $\mathcal{H}_1 \otimes \mathcal{H}_2$ *of the state spaces* $\mathcal{H}_1, \mathcal{H}_2$ *of the component qubit subsystems. If the first qubit is in state* $|\psi\rangle$ *and the second in state* $|\sigma\rangle$*, then the combined system of two interacting qubits is in state* $|\psi\sigma\rangle = |\psi\rangle |\sigma\rangle$*. Similarly, for a system of n qubits, the state space is the tensor product* $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes ... \otimes \mathcal{H}_n$ *of the state spaces of the n independent qubits.*

The most natural basis for $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is constructed from the tensor products of the basis vectors of $\mathcal{H}_1$ (say $\{|0\rangle_1, |1\rangle_1\}$ and of $\mathcal{H}_2$ (say $\{|0\rangle_2, |1\rangle_2\}$), then a basis for $\mathcal{H}$ is given by $\{|0\rangle_1 |0\rangle_2, |0\rangle_1 |1\rangle_2, |1\rangle_1 |0\rangle_2, |1\rangle_1 |1\rangle_2\}$
$= \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

We will often this basis as $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ when the context is unambiguous. So an arbitary state $|\psi\rangle \in \mathcal{H}$ can be described as $|\psi\rangle = c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle = c_0 |0\rangle + c_1 |1\rangle + c_2 |2\rangle + c_3 |3\rangle$.

Definition 2.1.9. *A state $|\psi\rangle$ is said to be **entangled** if it cannot be written as a simple tensor product of states $|v\rangle \in \mathcal{H}_1$ and $|w\rangle \in \mathcal{H}_2$. If we can write $|\psi\rangle = |v\rangle |w\rangle$, the state is said to be **seperable**.*

Example 2.1.10. *Consider the state $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We can show this is entangled. 'TODO'*

Example 2.1.11. *Consider the state $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$. We can show this is seperable since we can write $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$*

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.