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 2023-2024 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: October 7, 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

Qubits

The computers we use today are based on **bits** (binary digits) each of which can represent a 0 or 1 state. The rules governing these bits are laid out in classical information theory and these computers can be considered equivalent to a ideal abstract computational framework - the Turing Machine.

By exploiting certain phenomena observed in the working of quantum particles, we can derive a model of a computer which can achieve results that can not be replicated efficiently on a Turing Machine. In these quantum computers, the **qubit** (quantum bit) forms the foundational unit of computing.

Many different quantum particle effects have been used in labs - photon polarization, electron spin, the state of an atom in a cavity, and even defect centers in a diamond have been leveraged to created real life implementations of qubits. We will define a qubit as a mathematical object with a certain ruleset and expect that every real-world implementation follows the working of the abstract model.

Definition 1.0.1: A complex **Hilbert space** $\mathcal{H}$ is a vector space over $\mathbb{C}$ with a positive definite inner product $\langle\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ defined as $(\psi, \phi) \to \langle\psi, \phi\rangle$ such that for all $\phi, \phi_1, \phi_2, \psi \in \mathcal{H}$ and $a, b \in \mathbb{C}$ the inner product is:

1. conjugate symmetric: $\langle\psi, \phi\rangle = \overline{\langle\phi, \psi\rangle}$
2. positive definite: $\langle\psi, \psi\rangle \geq 0$ and $\langle\psi, \psi\rangle = 0 \iff \psi = 0$
3. linear in first argument: $\langle a\phi_1 + b\phi_2, \psi\rangle = a\langle\phi_1, \psi\rangle + b\langle\phi_2, \psi\rangle$
4. antilinear in second argument: $\langle\psi, a\phi_1 + b\phi_2\rangle = \overline{a}\langle\psi, \phi_1\rangle + \overline{b}\langle\psi, \phi_2\rangle$

and this inner product induces a norm $||.|| : \mathcal{H} \to \mathbb{R}$ defined as $\psi \to \sqrt{\langle\psi, \psi\rangle}$ in which $\mathcal{H}$ is complete.

Definition 1.0.2: A **qubit** is any quantum mechanical system whose state can be completely described by a unit vector in a 2-dimensional complex Hilbert space $\mathcal{H}$ and which follows these principles:

- Principle of Superposition
- Principle of Entanglement
- Principle of Measurement
- Principle of Transformation

The Hilbert space $\mathcal{H}$ is known as the **state space** and is equipped with the inner product $\langle\rangle$ which is defined as $\langle\psi, \phi\rangle = \overline{a}c + \overline{b}d$ for any $\psi = \begin{bmatrix} a \\ b \end{bmatrix}, \phi = \begin{bmatrix} c \\ d \end{bmatrix} \in \mathcal{H}$. Any unit vector of $\mathcal{H}$ is called a **state vector**.

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

Definition 1.0.3: Any function $\phi : V \to \mathbb{F}$ from a vector space to its base field is called a **functional**. A linear functional ϕ on a normed linear space V is said to be **bounded** if there exists some real M such that $||\phi(v)|| \leq M||v||$ for all $v \in V$. This is equivalent to ϕ being continuous.

Definition 1.0.4: The set of all continuous linear functionals on a vector space V is known as the **continuous dual space** of V.

Theorem 1.0.5 (Riesz' representation theorem)**:** For a continuous linear functional ϕ on a Hilbert space $\mathcal{H}$, there exists a unique $u \in \mathcal{H}$ such that $\phi(u, v) = \langle u, v \rangle$ for all $v \in \mathcal{H}$. This implies Hilbert spaces are conjugate isomorphic to their own conjugate dual spaces and there exists a bijection between a Hilbert space and its continuous dual space.

The above property of Hilbert spaces leads us to the **Dirac Bra/Ket Notation** which is widely used in quantum mechanics and quantum information theory, and which we will follow in the rest of this paper. The inner product on the quantum mechanical Hilbert space defined as $\langle \psi, \phi \rangle = \overline{a}c + \overline{b}d$ for any $\psi = \begin{bmatrix} a \\ b \end{bmatrix}, \phi = \begin{bmatrix} c \\ d \end{bmatrix} \in \mathcal{H}$.

Result 1.0.6: For a fixed $\psi \in \mathcal{H}$, consider a linear functional $f_\psi : \mathcal{H} \to \mathbb{C}$ such that $f_\psi(\phi) = \langle \psi, \phi \rangle$ for all $\phi \in \mathcal{H}$. Then f_ψ is continuous and unique.

Proof. f_ψ is continuous if and only if it is bounded. The Cauchy-Schwarz inequality for inner product tells us that $|\langle \psi, \phi \rangle| \leq ||\psi||||\phi||$. This implies $|f_\psi| = |\langle \psi, \phi \rangle| \leq M||\phi||$ where $M = ||\psi||$ is a fixed quantity, i.e. $|f_\psi|$ is bounded. Hence f_ψ is continuous.

Since f_ψ is a continuous linear functional, it is an element of the continuous dual space of $\mathcal{H}$ and is therefore unique by Riesz's representation theorem. □

Notation 1.0.7: Any $\psi \in \mathcal{H}$ will be written as $|\psi\rangle$. This is the notation for a vector in Dirac's bra/ket notation, and is read **ket psi**.

Consider f_ψ for a fixed $\psi \in \mathcal{H}$ as defined in the above result. We will write this unique f_ψ as $\langle \psi |$ and is read **bra psi**.

The linear functional $\langle \psi |$ applied on a vector $|\phi\rangle$ is written as $\langle \psi | \phi \rangle$ and $\langle \psi | \phi \rangle = f_\psi(\phi) = \langle \psi, \phi \rangle$ is the inner product of ψ and ϕ.

Result 1.0.8: If the inner product is defined as $\langle\psi|\phi\rangle = \overline{a}c + \overline{b}d$ for any $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, |\phi\rangle = \begin{bmatrix} c \\ d \end{bmatrix} \in \mathcal{H}$, then $\langle\psi|\phi\rangle = \langle\psi|\,|\phi\rangle = |\psi\rangle^\dagger\,|\phi\rangle$ where $|\psi\rangle^\dagger$ is the conjugate transpose of $|\psi\rangle$, i.e. $|\psi\rangle^\dagger = \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix}$. We denote $\langle\psi| = |\psi\rangle^\dagger$ and understand the operation $\langle\psi|\,|\phi\rangle$ to be that of matrix multiplication.

Proof. Consider $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, |\phi\rangle = \begin{bmatrix} c \\ d \end{bmatrix} \in \mathcal{H}$.

Then $|\psi\rangle^\dagger\,|\phi\rangle = \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \overline{a}c + \overline{b}d = \langle\psi|\phi\rangle = f_{|\psi\rangle}(|\phi\rangle)$ for some continuous linear functional $f_{|\psi\rangle} : \mathcal{H} \to \mathbb{C}$.

Since $f_{|\psi\rangle}$ is unique by Riesz's representation theorem, we can set $f_{|\psi\rangle}(\phi) = \psi^\dagger\phi$ for all $|\phi\rangle \in \mathcal{H}$. □

1.1 Superposition

Lemma 1.1.1 (Principle of Superposition)**:** Suppose $|\psi\rangle$ and $|\sigma\rangle$ are two mutually orthogonal vectors in the state space $\mathcal{H}$ of a quantum system, and $a, b \in \mathbb{C}$. Then $a\,|\psi\rangle + b\,|\sigma\rangle$ is a valid state vector of the quantum system when $a^2 + b^2 = 1$. The state of the system is completely defined by its state vector which is a unit vector in the systems' state space.

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. This leads to qubits being referred to as **two-state** quantum systems since its state is the linear combination of two orthogonal basis vectors. These orthogonal states act as the basis elements of the Hilbert space $\mathcal{H}$ modelling the qubit.

When working with Hilbert spaces associated with quantum systems, we normally use *orthonormal bases*.

Definition 1.1.2: The **computational basis** for the two dimensional complex vector space $\mathcal{H}$ is $\{|0\rangle, |1\rangle\}$ where $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

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 commonly used orthonormal basis for the Hilbert space $\mathcal{H}$ modelling a qubit is the Hadamard Basis.

Definition 1.1.3: The **Hadamard Basis** for the two dimensional complex vector space $\mathcal{H}$ is $\{|+\rangle, |-\rangle\}$ where
$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

Lemma 1.1.4: Consider a state $|\psi\rangle = a|0\rangle + b|1\rangle$ where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$ and a state $|\sigma\rangle = a'|0\rangle + b'|1\rangle$ where $a', b' \in \mathbb{C}$ and $|a'|^2 + |b'|^2 = 1$. Let $a|0\rangle + b|1\rangle = c(a'|0\rangle + b'|1\rangle)$ where $c \in \mathbb{C}$ is a complex number of modulus 1. Then $|\psi\rangle$ and $|\sigma\rangle$ represent the same state.

Definition 1.1.5: The multiple $c \in \mathbb{C}$ with $|c| = 1$ by which two vectors representing the same quantum state differ is called the **global phase**.

Global phases are artefacts of the mathematical framework we are using and have no physical meaning.

1.2 Entanglement

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.

Definition 1.2.1: Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be finite dimensional Hilbert spaces. The **tensor product** $\mathcal{H}_1 \otimes \mathcal{H}_2$ is a Hilbert space in which every element can be represented as $|v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle \otimes ... \otimes |v_k\rangle \otimes |w_k\rangle$ where $k = \min(n, m)$ and $|v_i\rangle \in \mathcal{H}_1, |w_i\rangle \in \mathcal{H}_2$ and $\otimes$ is the tensor product defined to satisfy the following properties:

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

If $|\psi\rangle = \alpha_1 |v_1\rangle + \alpha_2 |v_2\rangle + ... + \alpha_n |v_n\rangle$ and $|\phi\rangle = \beta_1 |w_1\rangle + \beta_2 |w_2\rangle + ... + \beta_m |w_m\rangle$, their tensor product is $|\psi\rangle \otimes |\phi\rangle = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_i \beta_j |v_i\rangle \otimes |w_j\rangle$

Notation 1.2.2: In dirac's bra/ket notation, the tensor product $|v\rangle \otimes |w\rangle$ of $|v\rangle \in \mathcal{H}_1$ and $|w\rangle \in \mathcal{H}_2$ is written as $|vw\rangle$ or $|v\rangle |w\rangle$

Proposition 1.2.3: Let $\{|v_i\rangle\} \subset \mathcal{H}_1$ be an orthonormal basis in $\mathcal{H}_1$ and $\{|w_j\rangle\} \subset \mathcal{H}_2$ be an orthonormal basis in $\mathcal{H}_2$. Then the set $\{|v_i w_j\rangle\}$ forms an orthonormal basis in $\mathcal{H}_1 \otimes \mathcal{H}_2$ and for finite-dimensional $\mathcal{H}_1$ and $\mathcal{H}_2$, $\dim(\mathcal{H}_1 \otimes \mathcal{H}_2) = \dim(\mathcal{H}_1)\dim(\mathcal{H}_2)$

Proof. □

Lemma 1.2.4 (Principle 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 computational 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 1.2.5: 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 1.2.6: Consider the state $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$. This state is seperable since we can write $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$

Example 1.2.7: Consider the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This is an entangled state. Assume that $|\psi\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ can be decomposed as

$|\psi\rangle = (\alpha_1|0\rangle_1 + \beta_1|1\rangle_1) \otimes (\alpha_2|0\rangle_2 + \beta_2|1\rangle_2) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$.

Equating the components, we find $\alpha_1\alpha_2 = \frac{1}{\sqrt{2}}$, $\alpha_1\beta_2 = 0$, $\beta_1\alpha_2 = 0$ and $\beta_1\beta_2 = \frac{1}{\sqrt{2}}$. These equations cannot be satisfied simulataneously as either one of α_1 or β_2 has to be 0.

Proposition 1.2.8: For Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ defining qubit systems, most states in the tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$ of the interacting qubit systems are entangled.

intuition. Consider a state $|\psi\rangle = a|0\rangle + b|1\rangle \in \mathcal{H}_1$, $a, b \in \mathbb{C}$. Since a and b are complex coefficients, we would have 4 degrees of freedom to assign a particular $|\psi\rangle$. However including the constraints that $a^2 + b^2 = 1$ and that multiplying by global phase leaves the state unchanged, we are effectively left with 2 degrees of freedom for assigning $|\psi\rangle$.

Similarly assigning $|\phi\rangle \in \mathcal{H}_2$ has 2 degrees of freedom.

Consider the 4-dimensional tensor space $\mathcal{H}_1 \otimes \mathcal{H}_2$. Since the state of any vector $|\omega\rangle$ in this space can be written as $|\omega\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$, where $a, b, c, d \in \mathbb{C}$ we have 8 degrees of freedom initially for assigning the vector $|\omega\rangle$. Including constraint $a^2 + b^2 + c^2 + d^2 = 1$ and that multiplying by global phase leaves the state unchanged, we have 6 degrees of freedom in assigning the value of $|\omega\rangle$ which is 2 degrees of freedom more than $4 = 2 \times 2$ from the individual qubits. □

1.3 Measurement

The principle of superposition might indicate that we can use the continuum state of 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 know 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*.

A naive version principle of measurement for a single qubit is stated below. We will formalize this notion and generalize it to multiple qubits.

Lemma 1.3.1 (Principle 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 $|b|^2$.
The process of measurement leads to the quantum state vector $|\psi\rangle$ undergoing a discontinuous change which leads to the collapse of the state vector onto one of the vectors in the preferred basis.

To formalize this notion, we have two main options: projection-valued measures (PVM) and positive-operator-valued measure (POVM). We will proceed to describe PVMs here.

Definition 1.3.2: An **observable** is a physically measurable quantity of a quantum system which is represented by a self-adjoint operator on the Hilbert space associated with the quantum system.

TODO: Add direct product in dirac notation

Lemma 1.3.3: The eigenvectors of an observable form an orthonormal basis for the Hilbert space.

Lemma 1.3.4: In a qubit represented by Hilbert space $\mathcal{H}$, the possible measurement values of an observable are given by the spectrum $\sigma(A)$ of the self adjoint operator A representing the observable.

The probability $p_\psi(\lambda)$ that a quantum system in the pure state $|\psi\rangle \in \mathcal{H}$ yields the eigenvalue λ of A upon measurement is given by the projection P_λ onto the eigenspace $\text{Eig}(A, \lambda)$ of λ as $p_\psi(\lambda) = ||P_\lambda |\psi\rangle ||^2$

Lemma 1.3.5 (Principle 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 $p_i = |\langle i|\psi\rangle|^2 = |c_i|^2$

Definition 1.3.6: A **density operator** is a positive semi-definite operator on the Hilbert space whose trace is equal to 1.

Lemma 1.3.7: For each measurement that can be defined, the probability distribution over the outcomes of the measurement can be computed from the density operator as defined by Born's rule: $P(x_i) = \text{tr}(\Pi_i \rho)$ where ρ is the density operator and Π_i is the projection operator onto the baiss vector corresponding to the measurement outcome x_i.

Lemma 1.3.8: The expectation value of a quantum state ρ is $< A >= \text{tr}(A\rho)$.

Definition 1.3.9: Let $\mathcal{H}$ be a Hilbert space. We call states $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle \in \mathcal{H}$ perfectly distinguishable if there exists a measurement system $\{M_i\}_{i=1}^m$ with $m \geq n$ such that $||M_j |\psi_1\rangle ||^2 = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$

Here *perfectly distinguishable* means that there is some experiment or experimental setup that can distinguish between these two states, atleast in theory.

Result 1.3.10: The states $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle$ are perfectly distinguishable if and only if they are orthogonal. This result is the reason we use orthogonal basis in quantum computing.

'TODO: Refer Nielsen, Chuang

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 1.3.11: 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.

Remark 1.3.12: 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 $|\psi\rangle = a|0\rangle + b|1\rangle = \langle 0|\psi\rangle|0\rangle + \langle 1|\psi\rangle|1\rangle$.

Remark 1.3.13: 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 $\langle\psi|\psi\rangle = \langle\psi|\,|\psi\rangle = \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = |a|^2 + |b|^2 = 1$

'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 1.3.14: 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'

Here *perfectly distinguishable* means that there is some experiment or experimental setup that can distinguish between these two states, atleast in theory.

Definition 1.3.15: Let $\mathcal{H}$ be a Hilbert space. We call states $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle \in \mathcal{H}$ perfectly distinguishable if there exists a measurement system $\{M_i\}_{i=1}^m$ with $m \geq n$ such that $||M_j |\psi_1\rangle||^2 = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$

Result 1.3.16: The states $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle$ are perfectly distinguishable if and only if they are orthogonal. This result is the reason we use orthogonal basis in quantum computing.

Positive-Operator-Valued Measures (POVMs) are a further generalization of the Projection-Valued Measure (PVMs) and are described in the appendix.

1.4 Transformation

Lemma 1.4.1 (Principle of Transformation)**:** Isolated Quantum states evolve unitarily, i.e. for an isolated system there exists a unitary matrix U_t such that $|\psi_t\rangle = U_t |\psi_0\rangle$ where $|\psi_0\rangle$ is the starting state and $|\psi_t\rangle$ is the state at time t.

Theorem 1.4.2: Any change applied to a quantum state can be represented by a unitary matrix M.

Proof. The initial state of the quantum state is a unit and so is the result state. This means we require that the transformation applied to the unit vector $M |\psi\rangle$ is a unit vector itself.

This will happen when $\langle M\psi|M\psi\rangle = 1$ for all quantum states $|\psi\rangle$

$\implies \langle\psi| M^\dagger M |\psi\rangle = 1 \implies M^\dagger M = I$ which is the condition for M being a unit vector. □

Definition 1.4.3: An observable is a physically measurable quantity of a quantum system which is represented by a self-adjoint operator on a Hilbert space.

Definition 1.4.4: A matrix is said to be **unitary** if and only if one of the following conditions hold:

1. $U^\dagger U = I$
2. $UU^\dagger = I$
3. the columns of U are orthonormal vectors
4. the rows of U are orthonormal vectors

'Alternate from Scherer'

Definition 1.4.5: An operator U on H is called **unitary** if
$\langle U\psi|U\phi\rangle = \langle\psi|\phi\rangle$ for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$

Lemma 1.4.6: The operator that takes $|a_1\rangle \to |b_1\rangle$ and $|a_2\rangle \to |b_2\rangle$ is obtained by the operation: $|b_1\rangle |b_1\rangle + |b_2\rangle \langle a_2|$.

Lemma 1.4.7: Quantum gates have the same number of inputs and outputs.

Lemma 1.4.8: Quantum Gates are reversible.

Chapter 2

Gates

Proposition 2.0.1: Gates are described by unitary matrices.

Proof. Let M be a transformation of a quantum qubit state $|\psi\rangle$. Physics says that the evolution of an isolated quantum system is linear, so the transformation M can be described by a matrix.

For any state $|\psi\rangle$, $M|\psi\rangle$ has to be a unit vector.
If $M|\psi\rangle$ is a unit vector, the inner product with itself is 1.
$\implies \langle\ (M|\psi\rangle)\ |\ (M|\psi\rangle)\ \rangle = 1$
$\implies \langle\psi|\, M^\dagger M\, |\psi\rangle = 1$
$\implies M^\dagger M = I$ where I is the identity matrix
$\implies M$ is unitary

□

Example 2.0.2: Verify that the Hadamard gate is unitary and find its eigenvalues, eigenvectors.

Since $UU^\dagger = I$, we can conclude that every unitary matrix is invertible. This leads to the following result:

Result 2.0.3: Only reversible gates can be implemented in quantum computing and any reversible gate has a quantum analog.

This shows us that the classical NOT gate has a quantum analog but NAND does not.

Any unitary 2×2 matrix is a valid gate but only a few are used in practice.

'TODO Notation $|\rangle \langle|$'

2.1 Gates on a single Qubit

Definition 2.1.1 (Pauli Gates)**:** I, X, Y, Z are known as the Pauli gates and are defined as:

1. $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = |0\rangle \langle 0| + |1\rangle \langle 1|$
2. $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |1\rangle \langle 0| + |0\rangle \langle 1|$
3. $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i\,|1\rangle \langle 0| - i\,|0\rangle \langle 1|$
4. $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle \langle 0| - |1\rangle \langle 1|$

'TODO: Effect of the Pauli Gates on the Bloch Sphere'

Definition 2.1.2 (Hadamard Gate)**:** The **Hadamard Gate** is the transformation $H : \mathcal{H} \to \mathcal{H}$ such that
$H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$ $H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$. It is defined by the matrix $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = |0\rangle \langle +| + |1\rangle \langle -|$

The Hadamard gate allows us to obtain a superposition state.

Remark 2.1.3: The Hadamard gate is its own inverse.
$H^2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I$

Remark 2.1.4: $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right) = \frac{1}{\sqrt{2}}(X + Z)$

Definition 2.1.5: The z**-Phase Gate** R_z defines a rotation about the z-axis by an angle θ on the Bloch sphere. 'TODO: Bloch Sphere'
It is given by $R_z = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} = |0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|$

The y**-Phase Gate** defines a rotation about the y axis and is defined by
$\begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$
The x**-Phase Gate** defines a rotation about the x axis and is defined by
$\begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$

2.2 Gates on Multiple Qubits

Definition 2.2.1: The **CNOT gate** is a gate that acts on 2 qubits which flips the second bit if the first bit is in the $|1\rangle$ state.
It is defined by the matrix $\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$

The CNOT gate allows us to obtain an entangled state.

Definition 2.2.2: The **Toffoli gate** is a gate that acts on 3 qubits that flips the third bit if the first two are in the $|1\rangle$ state.

Depending on the input the Toffoli gate can function as an AND, NOT and NAND gate. Since the NAND gate is universal, the Toffoli is as well. The Toffoli gate is also unitary which means it is a valid quantum gate. This shows that every classical circuit can be implemented as a quantum circuit.

Chapter 3

Algorithms

Definition 3.0.1: Test

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.