Mathematical Foundation of Quantum Computing

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: December 21, 2023 Pranay Raja Krishnan

List of Notations

Unless explicitly defined the following notations are used.

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
$\mathbb{C}$	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 1.1: 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. conjugate-linear in first argument:
$\langle a\phi_1 + b\phi_2, \psi\rangle = \overline{a} \langle\phi_1, \psi\rangle + \overline{b} \langle\phi_2, \psi\rangle$
4. linear in second argument: $\langle\psi, a\phi_1 + b\phi_2\rangle = a \langle\psi, \phi_1\rangle + b \langle\psi, \phi_2\rangle$

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.

Note: We have set the inner product to be linear in the second argument and anti-linear in the first argument. This is to make later calculations easier. $\diamondsuit$

Definition 1.2: Given a matrix A, the **conjugate transpose** $A^\dagger$ is obtained by transposing A and applying the complex conjugate of each entry.

$A^\dagger = (\overline{A})^T = \overline{(A^T)}$ where $\overline{A}$ is the complex conjugate of A and A^T is the transpose of A.

Result 1.1: The conjugate transpose has the following properties:

- $(A + B)^\dagger = A^\dagger + B^\dagger$
- $(c \cdot A)^\dagger = \overline{c}A^\dagger$ for any $c \in \mathbb{C}$
- $(AB)^\dagger = B^\dagger A^\dagger$

- $(A^\dagger)^\dagger = A$

Definition 1.3: 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 axioms:

- 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
$\langle \psi, \phi \rangle = \begin{bmatrix} a \\ b \end{bmatrix}^\dagger \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \overline{a}c + \overline{b}d$ 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. They are empirical observations of the behaviour of quantum mechanical systems and will be considered as axioms in our abstract qubit system.

Definition 1.4: Any function $\phi : V \to \mathbb{F}$ from a vector space to its base field is called a **functional**.

Definition 1.5: 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 $v \in V$.

Result 1.2: A linear functional ϕ being bounded is equivalent to ϕ being continuous.

Definition 1.6: The set of all continuous linear functionals on a vector space V is known as the **continuous dual space** of V.

Result 1.3 (Riesz' representation theorem)**:** For any continuous linear functional ϕ on a Hilbert space $\mathcal{H}$, there exists a unique $u \in \mathcal{H}$ such that $\phi(v) = \langle u, v \rangle$ for all $v \in \mathcal{H}$.

In fact the converse is true as well.

Proposition 1.1: 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.

To verify f_ψ is continuous:
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 $|f_\psi| = |\langle \psi, \phi \rangle| \leq ||\psi||||\phi|| = M||\phi||$ where $M = ||\psi||$ is a fixed quantity for a fixed $\psi \in \mathcal{H}$, i.e. $|f_\psi|$ is bounded.

Hence f_ψ is continuous.

To verify f_ψ is unique:
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. $\square$

The above properties of Hilbert spaces justifies the **Dirac Bra/Ket Notation** which is widely used in quantum mechanics, and which we will follow in this paper.

Note: The **Dirac Bra/Ket Notation** is ubiquitously used in quantum mechanics and quantum information science. It allows vectors, continuous dual functions, and inner products to be represented conveniently.

Any vector $\psi \in \mathcal{H}$ will be written as $|\psi\rangle$ and is read *ket psi*.

The unique continuous linear functional f_ψ defined as $f_\psi(\phi) = \langle \psi, \phi \rangle$ for all $\phi \in \mathcal{H}$ and a fixed $\psi \in \mathcal{H}$ will be written as $\langle \psi|$ and is read *bra psi*.

The inner product $\langle \psi, \phi \rangle$ will then be written as $\langle \psi| |\phi\rangle$ or more simply as $\langle \psi|\phi\rangle$. $\diamondsuit$

Proposition 1.2: For any $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \in \mathcal{H}$, the linear functional $\langle \psi|$ has the matrix representation $\langle \psi| = |\psi\rangle^\dagger = \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix}$.

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 $\langle\psi| = f_{|\psi\rangle}(\phi) = |\psi\rangle^{\dagger} |\phi\rangle$ for all $|\phi\rangle \in \mathcal{H}$, i.e. $\langle\psi|$ is the linear functional which has matrix representation $|\psi\rangle^{\dagger}$. □

1.1 Superposition

Axiom 1.1 (Principle of Superposition)**:** Suppose $|\psi\rangle$ and $|\sigma\rangle$ are two mutually orthogonal vectors in a Hilbert space $\mathcal{H}$, and $a, b \in \mathbb{C}$.

Then $a|\psi\rangle + b|\sigma\rangle \in \mathcal{H}$ is a valid state vector of the state space of a qubit 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* to describe state vectors.

Proposition 1.3: Define $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ Then the set $\{ \ |0\rangle, |1\rangle \ \}$ is an orthonormal basis

Proof.

To verify linear independence:

Consider we set $a\,|0\rangle + b\,|1\rangle = 0_{\mathcal{H}}$ for some $a, b \in \mathbb{C}$ where $0_{\mathcal{H}} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ is the zero vector of $\mathcal{H}$.

Then $a\begin{bmatrix} 1 \\ 0 \end{bmatrix} + b\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0 \implies \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \implies a = 0$ and $b = 0$

To verify that $\{\ |0\rangle\,, |1\rangle\ \}$ *is a spanning set:*
The set is a linearly independent set of 2 vectors in a Hilbert space of dimension 2 $\implies$ it is a spanning set.

To verify orthonormality:
$\langle 0|0\rangle = \langle 0|\,|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1$ and $\langle 1|1\rangle = \langle 1|\,|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1$ Also,
$\langle 1|0\rangle = \langle 1|\,|0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = 0$ and $\langle 0|1\rangle = \overline{\langle 1|0\rangle} = 0.$ $\square$

Definition 1.7: 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 $|a|^2 + |b|^2 = 1.$

Proposition 1.4: Define $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$. Then the set $\{\ |+\rangle\,, |-\rangle\ \}$ is an orthonormal basis.

Proof.

To verify linear independence:

Consider we set $a\,|+\rangle + b\,|-\rangle = 0_{\mathcal{H}}$ for some $a, b \in \mathbb{C}$ where $0_{\mathcal{H}} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ is the zero vector of $\mathcal{H}$.

Then $a\,|+\rangle + b\,|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} a+b \\ a-b \end{bmatrix} = 0_{\mathcal{H}} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \implies a+b=0$ and $a-b=0 \implies a=0$ and $b=0$

To verify $\{\ |+\rangle\,, |-\rangle\ \}$ *spanning set:*
The set is a linearly independent set of 2 vectors in a Hilbert space of dimension 2 $\implies$ it is a spanning set.

To verify orthonormality:

$\langle +|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}^{\dagger}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2}\cdot 2 = 1$ and

$\langle -|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}^{\dagger}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{2}\cdot 2 = 1$

Also, $\langle +|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}^{\dagger}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = 0$ and
$\langle -|+\rangle = \overline{\langle +|-\rangle} = 0$

$\square$

Definition 1.8: 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 $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$

Axiom 1.2: 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, i.e. $|c| = 1$. Then $|\psi\rangle$ and $|\sigma\rangle$ represent the same state.

Therefore, not all choices of $a, b \in \mathbb{C}$ with $|a|^2 + |b|^2 = 1$ result in different quantum state vectors.

Definition 1.9: The multiple $c \in \mathbb{C}$ with $|c| = 1$ by which two vectors representing the same quantum state vector 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

Definition 1.10: Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be Hilbert spaces with orthonormal basis $\{|e_i\rangle\}_{i=1}^n$ and $\{|f_j\rangle\}_{j=1}^m$ respectively. The **tensor product** $\mathcal{H}_1 \otimes \mathcal{H}_2$ is an nm-dimensional Hilbert space with basis of the form $\{|e_i\rangle \otimes |f_j\rangle \mid 1 \leq i \leq n \text{ and } 1 \leq j \leq m\}$ where $\otimes$ denotes the tensor product operation which satisfies:

1. $(a\,|\psi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes (a\,|\phi\rangle) = a(|\psi\rangle \otimes |\phi\rangle)$
2. $a(|\psi\rangle \otimes |\phi\rangle) + b(|\psi\rangle \otimes |\phi\rangle) = (a+b)(|\psi\rangle \otimes |\phi\rangle)$
3. $(|\psi\rangle_1 + |\psi\rangle_2) \otimes |\phi\rangle = |\psi\rangle_1 \otimes |\phi\rangle + |\psi\rangle_2 \otimes |\phi\rangle$
4. $|\psi\rangle \otimes (|\phi\rangle_1 + |\phi\rangle_2) = |\psi\rangle \otimes |\phi\rangle_1 + |\psi\rangle \otimes |\phi\rangle_2$

for any $|\psi\rangle, |\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_1$, $|\phi\rangle, |\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}_2$ and $a, b \in \mathbb{C}$

For any two elements in $\mathcal{H}_1 \otimes \mathcal{H}_2$ of the form $|\psi_1\rangle \otimes |\phi_1\rangle$ and $|\psi_2\rangle \otimes |\phi_2\rangle$ for some $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_1$ and $|\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}_2$, we define the inner product $\langle\rangle : \mathcal{H}_1 \otimes \mathcal{H}_2 \to \mathbb{C}$ as $\langle\, |\psi_1\rangle \otimes |\phi_1\rangle \mid |\psi_2\rangle \otimes |\phi_2\rangle \,\rangle = \langle\psi_1|\psi_2\rangle_{\mathcal{H}_1} \langle\phi_1|\psi_2\rangle_{\mathcal{H}_2}$ and extend it to any pair of elements of $\mathcal{H}_1 \otimes \mathcal{H}_2$ using the linearity and conjugate linearity properties of the inner product.

Note: Given orthonormal basis $\{|e_i\rangle\}_{i=1}^n$ for $\mathcal{H}_1$ and $\{|f_j\rangle\}_{j=1}^m$ for $\mathcal{H}_2$, consider $|\psi\rangle \in \mathcal{H}_1, |\phi\rangle \in \mathcal{H}_2$ such that $|\psi\rangle = c_1\,|e_1\rangle + c_2\,|e_2\rangle + ... + c_n\,|e_n\rangle$ and $|\phi\rangle = d_1\,|f_1\rangle + d_2\,|f_2\rangle + ... + d_m\,|f_m\rangle$.

Then using the properties of the tensor product operation, $|\psi\rangle \otimes |\phi\rangle = (c_1\,|e_1\rangle + c_2\,|e_2\rangle + ... + c_n\,|e_n\rangle) \otimes (d_1\,|f_1\rangle + d_2\,|f_2\rangle + ... + d_m\,|f_m\rangle) = \sum_{i=1}^{n}\sum_{j=1}^{m} c_i d_j\,|e_i\rangle \otimes |f_j\rangle$.

The matrix multiplication rules for tensor product is defined analogously.

Let $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \in \mathcal{H}_1$ and $|\phi\rangle = \begin{bmatrix} c \\ d \end{bmatrix} \in \mathcal{H}_2$.

Then $|\psi\rangle \otimes |\phi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \begin{bmatrix} c \\ d \end{bmatrix} \\ b \begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$ ♢

Note: The notation for the tensor product $|\psi\rangle \otimes |\phi\rangle$ is often simplied as $|\psi\rangle |\phi\rangle$ or even $|\psi\phi\rangle$ ♢

Note: A more formal construction of the tensor product space can be found in Appendix B ♢

Axiom 1.3 (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.

Similarly, for a system of n interacting 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 qubits taken independently.

Proposition 1.5: For a 2 qubit system, the set $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is an orthonormal basis for the state space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$.

Proof.

To show $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ *is a basis:*
This follows from the definition of the tensor product space as $\{|0\rangle, |1\rangle\}$ is a basis for $\mathcal{H}_1$ and $\{|0\rangle, |1\rangle\}$ is a basis for $\mathcal{H}_2$.

To show $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ *is an orthonormal set*
$\langle |00\rangle \mid |00\rangle\rangle = \langle 0|0\rangle \langle 0|0\rangle = 1 \cdot 1 = 1$, $\langle |11\rangle \mid |11\rangle\rangle = \langle 1|1\rangle \langle 1|1\rangle = 1 \cdot 1 = 1$ and $\langle |00\rangle \mid |11\rangle\rangle = \langle 0|1\rangle \langle 1|1\rangle = 0 \cdot 1 = 0$

This shows that $|00\rangle$ is orthonormal to $|11\rangle$.

Similarly, taking the inner product for all combinations of basis elements in $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, we can see that it is an orthonormal set. □

Definition 1.11: The orthonormal basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ for $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is known as the **computational basis** for $\mathcal{H}$.

When there is no ambiguity, the elements of this basis are often represented by replacing the bit-string by the corresponding decimal value as:

- $|00\rangle = |0\rangle$
- $|01\rangle = |1\rangle$
- $|10\rangle = |2\rangle$
- $|11\rangle = |3\rangle$

Definition 1.12: For a system of two interacting qubits, the set $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ forms an orthonormal basis known as the **bell basis** where

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} \; |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} \; |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}$$

Definition 1.13: For a set of n interacting qubits the **computational basis** is given by $\{|\underbrace{00...0}_{n \text{ times}}\rangle, |\underbrace{00...0}_{n-1 \text{ times}}1\rangle, ..., |\underbrace{11...1}_{n \text{ times}}\rangle\} = \{|0\rangle, |1\rangle, ..., |2^n - 1\rangle\}$

Definition 1.14: A state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes ... \otimes \mathcal{H}_n$ is said to be **entangled** if it cannot be written as a simple tensor product of states $|v_1\rangle \in \mathcal{H}_1, |v_2\rangle \in \mathcal{H}_2, ..., |v_n\rangle \in \mathcal{H}_n$.

If we can write $|\psi\rangle = |v_1\rangle |v_2\rangle ... |v_n\rangle = |v_1 v_2 ... v_n\rangle$, the state is said to be **seperable**.

Example 1.1: The state $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$ of a 2-qubit system is seperable since we can write $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$

Example 1.2: The state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ of a 2-qubit system 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.

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.

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 1.1 (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 1.15: 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 1.2: The eigenvectors of an observable form an orthonormal basis for the Hilbert space.

Lemma 1.3: 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 1.4 (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 1.16: A **density operator** is a positive semi-definite operator on the Hilbert space whose trace is equal to 1.

Lemma 1.5: 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: $P(x_i) = \mathrm{tr}(\Pi_i \rho)$ 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 1.6: The expectation value of a quantum state ρ is $< A >= \mathrm{tr}(A\rho)$.

Definition 1.17: 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 1.4: 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 $|\psi\rangle = a|0\rangle + b|1\rangle$.

Note: 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 1.1: 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 1.2: 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 $|a_i\rangle \otimes |b_j\rangle$

Note: 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 1.18: 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 1.5: 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

Definition 1.19: A **unitary transformation** $U : \mathcal{H}_1 \to \mathcal{H}_2$ between two Hilbert space $\mathcal{H}_1$ and $\mathcal{H}_2$ is a isomorphism that preserves the inner product.

For a unitary transformation U on $\mathcal{H}$ we have $\langle U\psi|U\phi\rangle = \langle\psi|\phi\rangle$ for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$

Proposition 1.6: Unitary transformations map orthonormal bases to orthonormal bases.

Proof.

Consider an n dimensional Hilbert space $\mathcal{H}$ with orthonormal bases $\{|e_i\rangle\}_{i=1}^n$ and a unitary transformation U. Let $|f_i\rangle = U(|e_i\rangle)$ for all $1 \leq i \leq n$.

To show $\{|f_i\rangle\}$ *is a basis:*
Consider there are constants $c_1, c_2, ..., c_n$ such that $c_1 |f_1\rangle + c_2 |f_2\rangle + ... + c_n |f_n\rangle = 0_{\mathcal{H}}$.

Then $c_1 |f_1\rangle + c_2 |f_2\rangle + ... + c_n |f_n\rangle = 0_{\mathcal{H}} \implies$
$c_1 U(|e_1\rangle) + c_2 U(|e_2\rangle + ... + c_n U(|e_n\rangle) = 0_{\mathcal{H}} \implies$
$U(c_1 |e_1\rangle + c_2 |e_2\rangle + ... + c_n |e_n\rangle) = 0_{\mathcal{H}} \implies c_1 |e_1\rangle + c_2 |e_2\rangle + ... + c_n |e_n\rangle = 0_{\mathcal{H}}$.

The last implication follows from the fact that $\langle U\psi|U\phi\rangle = 0$ for all $|\psi\rangle \in \mathcal{H} \implies \langle\psi|\phi\rangle = 0$ for all $|\psi\rangle \in \mathcal{H} \implies |\phi\rangle = 0$

Since $\{|e_i\rangle\}_{i=1}^n$ is a basis, this implies $c_1 = c_2 = ... = c_n = 0 \implies \{|f_i\rangle\}_{i=1}^n$ is linearly independent.

Since $\{|f_i\rangle\}_{i=1}^n$ is a linearly independent set of n elements, it is a spanning set for the n-dimensional space $\mathcal{H}$.

To show $\{|f_i\rangle\}$ is orthonormal:
Then $\langle f_\alpha|f_\beta\rangle = \langle Ue_\alpha|Ue_\beta\rangle = \langle e_\alpha|e_\beta\rangle = \delta_{\alpha,\beta}$ since U is unitary.

This implies $\{|f_i\rangle\}_{i=1}^n$ is orthonormal. □

Definition 1.20: A unitary matrix U is called **unitary** if its conjugate transpose $U^\dagger$ is its inverse.

That is, a matrix is said to be unitary if $UU^\dagger = U^\dagger U = I$.

Theorem 1.1: A transformation is unitary if and only if its matrix representation U is a unitary matrix.

Proof.

Note that
$\langle U\psi|U\phi\rangle = \langle U\psi| |U\phi\rangle = |U\psi\rangle^\dagger |U\phi\rangle = |\psi\rangle^\dagger U^\dagger |U\phi\rangle = \langle\psi| U^\dagger U |U\phi\rangle$.

To show a unitary matrix U is a unitary transformation:
Let U be a unitary matrix with $U \dagger U = I$ and $|\psi\rangle, |\phi\rangle \in \mathcal{H}$.

Then $\langle U\psi|U\phi\rangle = \langle\psi| U^\dagger U |\phi\rangle = \langle\psi| |\phi\rangle = \langle\psi|\phi\rangle \implies$ the transformation is unitary.

To show a unitary transformation is represented by a unitary matrix:
Let U be a unitary transformation with $\langle U\psi|U\phi\rangle = \langle\psi|\phi\rangle$ for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$.

Then $\langle\psi| U^\dagger U |\phi\rangle = \langle\psi| |\phi\rangle$. Multiplying with $\langle\psi|^{-1}$ on the left of both sides and $|\phi\rangle^{-1}$ on the right of both sides we have the required equality $U^\dagger U = I$. □

Nature does not allow the state of qubits to evolve arbitrarily. Isolated quantum states which are not measured evolve unitarily.

Lemma 1.7 (Principle of Transformation)**:** In a quantum state space $\mathcal{H}$, every change of a quantum state over time that has not been caused by measurement is described by a unitary transformation.

If $|\psi\rangle_1$ is the quantum space at time t_1 and $|\psi\rangle_2$ is the quantum state space at time $t_2 > t_1$, then $|\psi\rangle_2$ is described by $|\psi\rangle_2 = U\,|\psi\rangle_1$ where U is a unitary transformation on the state space $\mathcal{H}$

Lemma 1.8: Quantum gates have the same number of inputs and outputs.

Lemma 1.9: Quantum Gates are reversible.

Proposition 1.7 (No Cloning Principle)**:**

Chapter 2

Gates and Circuits

Definition 2.1: A **quantum gate** is a function $U : \mathcal{H} \to \mathcal{H}$ such that $f(|\psi\rangle) = |\phi\rangle$ where $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ are valid quantum states in the state space $\mathcal{H}$ of n interacting qubits.

Definition 2.2: A **quantum circuit** is a sequence of quantum gates and measurement operators applied to an n-qubit register initialized to some known quantum state.

The following proposition is stated without proof.

Proposition 2.1 (Deferred Measurement Principle)**:** Every quantum circuit is equivalent to a circuit in which all measurements are made after all other computations.

This principle allows us to postpone any required measurements till after all quantum gates are applied on the circuit.

Proposition 2.2: Consider a quantum state space of a single qubit $\mathcal{H}$.. The transformation T which takes a quantum state $|\psi\rangle$ to another state $|\phi\rangle$ is described by the matrix $T = |\phi\rangle\langle\psi|$

Proof.

To show T takes $|\psi\rangle$ to $|\phi\rangle$:
Let $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ and $|\phi\rangle = \begin{bmatrix} c \\ d \end{bmatrix}$ with respect to the computational basis where $|a|^2 + |b|^2 = 1$ and $|c|^2 + |d|^2 = 1$.

Then $|\phi\rangle\langle\psi| = \begin{bmatrix} c \\ d \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}^{\dagger} = \begin{bmatrix} c \\ d \end{bmatrix} \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix} = \begin{bmatrix} c\overline{a} & c\overline{b} \\ d\overline{a} & d\overline{b} \end{bmatrix}$.

Applying this matrix to $|\psi\rangle$, we have $T(|\psi\rangle) = (|\phi\rangle\langle\psi|)|\psi\rangle =$
$\begin{bmatrix} c\overline{a} & c\overline{b} \\ d\overline{a} & d\overline{b} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} c\overline{a}a + c\overline{b}b \\ d\overline{a}a + d\overline{b}b \end{bmatrix} = \begin{bmatrix} c(|a|^2 + |b|^2) \\ d(|a|^2 + |b|^2 \end{bmatrix} = \begin{bmatrix} c \\ d \end{bmatrix} = |\phi\rangle$

□

Note: The transformation T need not be unitary, i.e. it may not be a valid quantum gate. ♢

Proposition 2.3: Let $\{|a\rangle, |b\rangle\}$ be an orthonormal basis for a qubit state space $\mathcal{H}$. Then the transformation U that takes $|0\rangle$ to $|a\rangle$ and $|1\rangle$ to $|b\rangle$ is given by $U = |a\rangle\langle 0| + |b\rangle\langle 1|$.

Further the transformation is unitary.

Proof.

To show U takes $|0\rangle$ to $|a\rangle$ and $|1\rangle$ to $|b\rangle$:
$U(|0\rangle) = (|a\rangle\langle 0| + |b\rangle\langle 1|)|0\rangle = (|a\rangle\langle 0|0\rangle + |b\rangle\langle 1|0\rangle) = |a\rangle$ since $\langle 0|0\rangle = 1$ and $\langle 1|0\rangle = 0$. Similarly, we can see $U(|1\rangle) = |b\rangle$.

To show U is unitary:

$$\begin{aligned}
U^{\dagger}U &= (|a\rangle\langle 0| + |b\rangle\langle 1|)^{\dagger}(|a\rangle\langle 0| + |b\rangle\langle 1|) \\
&= (|0\rangle\langle a| + |1\rangle\langle b|)(|a\rangle\langle 0| + |b\rangle\langle 1|) \\
&= |0\rangle\langle a||a\rangle\langle 0| + |0\rangle\langle a||b\rangle\langle 1| + |1\rangle\langle b||a\rangle\langle 0| + |1\rangle\langle 1||b\rangle\langle 1| = |0\rangle\langle 0| + |1\rangle\langle 1| \\
&= I \text{ since } \langle a||a\rangle = \langle b||b\rangle = 1 \text{ and } \langle a||b\rangle = \langle b||a\rangle = 0
\end{aligned}$$

□

Example 2.1: Consider the ordered basis $\{|1\rangle, |0\rangle\}$ for a qubit's state space $\mathcal{H}$.

Then the transformation that takes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$ is given by

$U = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}^{\dagger} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}^{\dagger} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} =$
$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Proposition 2.4: Let $\{|a\rangle, |b\rangle\}$ and $\{|c\rangle, |d\rangle\}$ be two orthonormal basis sets for a qubits state space $\mathcal{H}$. Then the transformation U that takes $|a\rangle$ to $|c\rangle$ and $|b\rangle$ to $|d\rangle$ is given by $|c\rangle\langle a| + |d\rangle\langle b|$.

Further, the transformation U is unitary.

Proof.

To show U takes $|a\rangle$ to $|c\rangle$:
$U|a\rangle = (|c\rangle\langle a| + |d\rangle\langle b|)|a\rangle = |c\rangle\langle a||a\rangle + |d\rangle\langle b||a\rangle = |c\rangle$ since $\langle a||a\rangle = \langle a|a\rangle = 1$ and $\langle b||a\rangle = \langle b|a\rangle = 0$ since $|a\rangle$ and $|b\rangle$ are orthogonal.

To show U takes $|b\rangle$ to $|d\rangle$:
$U|b\rangle = (|c\rangle\langle a| + |d\rangle\langle b|)|b\rangle = |c\rangle\langle a||b\rangle + |d\rangle\langle b||b\rangle = |d\rangle$ since $\langle b||b\rangle = \langle b|b\rangle = 1$ and $\langle a||b\rangle = \langle a|b\rangle = 0$ since $|a\rangle$ and $|b\rangle$ are orthogonal.

To show U is a unitary matrix:
Consider the transformation U_0 that takes $|0\rangle$ to $|a\rangle$ and $|1\rangle$ to $|b\rangle$. Then U_0 is a unitary transformation by Proposition 2.3, and therefore so is the inverse U_0^{-1} Let $U_1 = U_0^{-1}$. Then U_1 is a unitary transformation that takes $|a\rangle$ to $|0\rangle$ and $|b\rangle$ to $|1\rangle$.

Consider the transformation U_2 that takes $|0\rangle$ to $|c\rangle$ and $|1\rangle$ to $|d\rangle$. This is similarly a unitary transformation by Proposition 2.3.

Therefore $U = U_1 U_2$ is a transformation that takes $|a\rangle$ to $|c\rangle$ and $|b\rangle$ to $|d\rangle$ and it is unitary since composition of unitary tranformations is unitary. $\square$

2.1 Gates on a single Qubit

2.1.1 Pauli Gates

Definition 2.3 (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. $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\,\langle 0| - |1\rangle\,\langle 1|$

The Pauli X gate is also known as the **Quantum NOT gate** because its behaviour of sending $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$ resembles the effect of a classical NOT gate on bits 0 and 1.

2.1.2 Hadamard Gate

Definition 2.4 (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: 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 2.2: $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right) = \frac{1}{\sqrt{2}}(X+Z)$

2.1.3 Phase Gate

Definition 2.5: The z**-Phase Gate** R_z defines a rotation about the z-axis by an angle θ on the 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
$R_y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$

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

2.2 Gates on Multiple Qubits

2.2.1 CNOT Gate

Definition 2.6: 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 $\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} =$
$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$

The CNOT gate allows us to obtain an entangled state.

Example 2.2: The state $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ is seperable.

$\text{CNOT}\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ which is an entangled state.

The CNOT gate is its own inverse. This means it can also take an entangled state to a seperable one.

2.2.2 Hadamard Transform

Definition 2.7: Given a register of n qubits, the **Hadamard Transform** $H^{\otimes n}$ is the transformation that applies the Hadamard gate $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ on each of the n qubits.

Example 2.3: Consider the Hadamard transform applied on a n qubit register, where each qubit is in the $|0\rangle$ state, i.e. the register is in the state $|0^n\rangle$. Then

$$H^{\otimes n}|0^n\rangle = \frac{1}{2^{n/2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)...(|0\rangle\,|1\rangle) = \frac{1}{2^{n/2}}\sum_{j=0}^{2^n-1}|j\rangle$$

where $|j\rangle$ is the bitstring that represents j in binary.

Result 2.1: For any arbitrary state $|j\rangle$ in an n qubit registe ,

$$H^{\otimes n}|j\rangle = \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1}(-1)^{j.k}|k\rangle$$

where $j.k$ is the dot product of the bitstrings j and k.

Example 2.4:

$$H^{\otimes 5}|01011\rangle = \frac{1}{\sqrt{32}}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{\sqrt{32}}(|00000\rangle - |00001\rangle - |00010\rangle + |00100\rangle - ... + |11111\rangle)$$

2.2.3 Toffoli Gate

Definition 2.8: 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

Applications of Qubits

A circuit model for quantum computing describes all computations in terms of a circuit composed of simple gates followed by a sequence of measurements.

The standard circuit model for quantum computation uses gates from CNOT gate together with all single qubit transformations and its measurements as all single qubit measurements in the standard basis, i.e. all computations in the standard basis consist of a sequence of gates that are either CNOT or single-qubit gates followed by a sequence of single-qubit measurements.

In this paper, we will focus on the class of 'black box' algorithms.

3.1 Deutsch-Josza Algorithm

3.2 Simon's Algorithm

3.3 Grover's Search Algorithm

- Unlike Shor's does not have as impressive of an advantage over classical, but can be applied to a broader range of problems
- Simplest General problem which this can be applied to is search

- The problem of search is to find a string $x \in \{0,1\}^n$ such that $f(x) = 1$ or conclude that no such string exists (Note in this definition $N = 2^n$ as there are 2^n possibilities
- This problem is completely unstructured. There is no clever tricks we can use in the general case (e.g. binary search if it was ordered)
- Similar to Shor's and Simon's there will be some classical post-processing after the algorithm is run, perhaps multiple times
- First considered by Lov Grover
- Grover's algorithm in theory be applied to a broad range of problems (unlike Shor's) but there is question on how practical these implications are
- Solves a black box problem, and uses a black box similar to Deutsch, Deutsch-Jozsa and Simon's Algorithm
- One of the strengths of Grover's is that there does not need to be any promises on the black box
- Results in a $O(\sqrt{N})$ time complexity (calls to black box) where the best classical algorithms have $O(N)$ complexity (calls to black box)
- Depends on efficiency of black box
- $O(\sqrt{N})$ is provably optimal, no quantum algorithm can do better
- usually presented as a probabilistic algorithm that succeeds with high probability, but variants that do suceed with certainty are known
- Geometric Interpretation
- Problem Setup
- Oracle Setup
- Analysing Grover's Algorithm is more difficult than describing it, it will help to think about reflections and rotations in the plane
- Shor Notes, Grover Analysis

- Shor's Notes Lec 24 and 25
- Watrous Notes Lec 12 and 13

Example: Consider we have a an equation which has a finite set of possible solutions, each of which is numbered from 1 to N, and a black box which tells us whether a particular possible solution $i \in 1, ..., N$ is a solution. A classical naive algorithm will iterate over all possibilities, plugging them one after another into the black box, and determine the solution in $O(N)$ time.

The problem is captured in a black box that is described by a Boolean function, $P : \{0, ..., N-1\} \rightarrow \{0, 1\}$. The goal is to find a solution $x \in \{0, ..., N-1\}$ such that $P(x) = 1$. The predicate P is viewed as a black box, around which we will wrap a phase oracle. For a single solution case, even the best classical algorithms must inspect $N/2$ possiblities, i.e. $O(N)$.

We are given a phase oracle that tells us whether an input $x \in 1, ..., N-1$ is a solution.

Suppose we encode x in $N-1$ qubits as binary, i.e. the combination of $|0\rangle$ and $|1\rangle$ that results in $|x\rangle$ in binary. Assume that N is a power of 2 (we can do this by adding dummy search elements until we reach a power of 2).

Then the oracle O_p applied to $|x\rangle$ will give

$$O_p |x\rangle = \begin{cases} -|x\rangle & \text{if } x \text{ is a solution} \\ |x\rangle & \text{otherwise} \end{cases}$$

Show that it is unitary

Construct the above phase oracle transformation with Toffoli Gates, σ_x and σ_z gates.

Implementing this oracle: Start with a circuit that finds whether the input is a solution or not such that it sets the output qubit to $|0\rangle$ if the input is a solution and $|1\rangle$ on the output qubit if the input is not a solution. Apply σ_z to this output qubit and then uncompute everything to get $\pm |x\rangle$

The oracle can be described by the circuit: input:

$$\sum_x c_x |x\rangle |0\rangle$$

output:

$$\sum_x c_x |x\rangle |P(x)\rangle$$

Grovers algorithm iteratively increases the amplitudes c_x of each $|x\rangle$ with $P(x) = 1$ so that a final measurement will return a value of x of interest with high probability.

Grovers Algorithm starts with the superposition of every item in the search space, i.e. a superposition of $1, ..., N-1$, call this as $|\psi\rangle$, i.e.
$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle.$

Algorithm: Repeat a certain number of times:

1. Apply the oracle O_p
2. Apply the Hadamard transform $H^{\otimes n}$
3. Apply the gate $2|0\rangle\langle 0| - I$
4. Apply the Hadamard transform $H^{\otimes n}$

Refer to Shor, Lec 24 to see how to implement $2|0\rangle\langle 0| - I$ and its effect.

Grovers Initital Analysis:

Note: $H^{\otimes n}|0\rangle = |\psi\rangle$ This implies
$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|sigma\rangle\langle sigma| - I$ the above (last 3 steps of the algorithm) reflects all the amplitudes around their average value.

The first step O_p reflects each of the amplitudes around 0 and the last three steps reflects each of the amplitudes about their average value.

Marked state starts off with amplitude $\frac{1}{\sqrt{N}}$. First reflection about x axis takes it to $-\frac{1}{\sqrt{N}}$ and average is still $\frac{1}{\sqrt{N}}$.

After last 3 steps, marked state will be $\frac{3}{\sqrt{N}}$.

One more iteration of the algorithm gives, $\frac{5}{\sqrt{N}}$ and in general, the k-th iteration will have the marked state as $\frac{2k+1}{\sqrt{N}}$.

After $\frac{1}{2}\sqrt{N} \sim O(\sqrt{N})$ steps, almost all the amplitudes will be in the marked state, and we will have nearly a probability 1 of finding it.

Check Shor Lec 24 for textbook analysis of the algorithm

Appendix A

Geometric Representations of a Qubit

It is sometimes helpful to have a representation of the state-space of a qubit that corresponds with points in space.

A.1 Representation as the Extended Complex Plane

We can construct a mapping between the state space of a qubit $\mathcal{H}$ and the set of all complex numbers. For any state $|\psi\rangle \in \mathcal{H}$ with $|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$. Consider the map $f : \mathcal{H} \to \mathbb{C}$ defined as $f(|\psi\rangle) = f(a|0\rangle + b|1\rangle) = \frac{b}{a}$. We set $\alpha = \frac{b}{a}$.

Its inverse is given by $f^{-1}(\alpha) = \frac{1}{\sqrt{1+|\alpha|^2}}|0\rangle + \frac{\alpha}{\sqrt{1+|\alpha|^2}}|1\rangle$

To make f well-defined for $|1\rangle$ with $a = 0, b = 1$, we extend the complex plane by adding the point ∞ and define $f^{-1}(\infty) = |1\rangle$

We now have $|0\rangle \mapsto 0$, $|1\rangle \mapsto \infty$, $|+\rangle \mapsto +1$, $|-\rangle \mapsto -1$ under f.

A.2 Bloch Sphere

Once we have α in the previous representation, we can map each state onto the unit sphere. Say $\alpha = s + it$ for $s, t \in \mathbb{R}$. We define the map g as the standard stereographic projection onto the real unit sphere in 3 dimensions as $g(\alpha) = g(s + it) = \left(\frac{2s}{|\alpha|^2 + 1}, \frac{2t}{|\alpha|^2 + 1}, \frac{1 - |\alpha|^2}{|\alpha|^2 + 1} \right)$

In this representation $|0\rangle \mapsto (0, 0, 1)$, $|1\rangle \mapsto (0, 0, -1)$, $|+\rangle \mapsto (1, 0, 0)$, $|-\rangle \mapsto (-1, 0, 0)$.

The unit sphere is the image of all possible states of a qubit and is known as the **Bloch Sphere**.

On the Bloch sphere we have $|0\rangle \mapsto 0$, $|1\rangle \mapsto \infty$. $|+\rangle \mapsto +1$, $|-\rangle \mapsto -1$, $|i\rangle \mapsto i$, $|-i\rangle \mapsto -i$.

Appendix B

Construction of the Tensor Product Space

A general topological result is stated below.

Result B.1: Let $f : A \to B$ and $g : C \to D$ be continuous functions. Then the map $f \times g : A \times C \to B \times D$ given by $f \times g(axc) = f(a) \times g(c)$ for any $a \in A, c \in C$ is continuous.

Proposition B.1: Consider we have finite dimensional Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$.

For fixed vectors $|\psi\rangle \in \mathcal{H}_1$ and $|\phi\rangle \in \mathcal{H}_2$, define a functional $f_{\psi,\phi} : \mathcal{H}_1 \times \mathcal{H}_2 \to \mathbb{C}$ as $f_{\psi,\phi}(|\xi\rangle, |\eta\rangle) = \langle\xi|\psi\rangle_{\mathcal{H}_1} \langle\eta|\phi\rangle_{\mathcal{H}_2}$ for any $|\xi\rangle \in \mathcal{H}_1, |\eta\rangle \in \mathcal{H}_2$.

Then the functional $f_{\psi,\phi}$ is conjugate linear in both variables and continuous.

Proof.

To show $f_{\psi,\phi}$ is continuous:

From 1.1, we know that the inner products $\langle\xi|\psi\rangle_{\mathcal{H}_1}$ is a continuous function from $\mathcal{H}_1$ to $\mathbb{C}$. Similarly, $\langle\eta|\phi\rangle_{\mathcal{H}_2}$ is a continuous function from $\mathcal{H}_2$ to $\mathbb{C}$.

Using Result B.1, $f_{\psi,\phi}(|\xi\rangle, |\eta\rangle) = \langle\xi|\psi\rangle_{\mathcal{H}_1} \langle\eta|\phi\rangle_{\mathcal{H}_2}$ is continuous at all $|\xi\rangle \in \mathcal{H}_1, |\eta\rangle \in \mathcal{H}_2$

To show $f_{\psi,\phi}$ is conjugate linear in both variables:

Consider $|\xi_1\rangle, |\xi_2\rangle \in \mathcal{H}_1$ and $|\eta\rangle \in \mathcal{H}_2$.

$$\begin{aligned} \text{Then } f_{\psi,\phi}(|\xi_1\rangle + |\xi_2\rangle, |\eta\rangle) &= \langle \xi_1 + \xi_2 | \psi \rangle_{\mathcal{H}_1} \langle \eta | \phi \rangle_{\mathcal{H}_2} \\ &= (\langle \xi_1 | \psi \rangle_{\mathcal{H}_1} + \langle \xi_2 | \psi \rangle_{\mathcal{H}_1}) \langle \eta | \phi \rangle_{\mathcal{H}_2} \\ &= \langle \xi_1 | \psi \rangle_{\mathcal{H}_1} \langle \eta | \phi \rangle_{\mathcal{H}_2} + \langle \xi_2 | \psi \rangle_{\mathcal{H}_1} \langle \eta | \phi \rangle_{\mathcal{H}_2} \\ &= f_{\psi,\phi}(|\xi_1\rangle, |\eta\rangle) + f_{\psi,\phi}(|\xi_2\rangle, |\eta\rangle) \end{aligned}$$

Similarly, $f_{\psi,\phi}(|\xi\rangle, |\eta_1\rangle + |\eta_2\rangle) = f_{\psi,\phi}(|\xi\rangle, |\eta_1\rangle) + f_{\psi,\phi}(|\xi\rangle, |\eta_2\rangle)$ for any $|\xi\rangle \in \mathcal{H}_1$ and $|\eta_1\rangle, |\eta_2\rangle \in \mathcal{H}_2$

$$\begin{aligned} \text{Let } a \in \mathbb{C}. \text{ Then } f_{\psi,\phi}(|a\xi\rangle, |\eta\rangle) &= \langle a\xi | \psi \rangle \langle \eta | \phi \rangle \\ &= \langle a\xi | \, |\psi\rangle \langle \eta | \phi \rangle \\ &= |a\xi\rangle^\dagger |\psi\rangle \langle \eta | \phi \rangle \\ &= \overline{a} \, |\xi\rangle^\dagger |\psi\rangle \langle \eta | \phi \rangle \\ &= \overline{a} \, \langle \xi | \psi \rangle \langle \eta | \phi \rangle \end{aligned}$$

Similarly, $f_{\psi,\phi}(|\xi\rangle, a\,|\eta\rangle) = \overline{a} f_{\psi,\phi}(|\xi\rangle, |\eta\rangle)$ □

Note: In dirac's bra/ket notation, the functional $f_{\psi,\phi}$ is written as $|\psi\rangle \otimes |\phi\rangle$ where $|\psi\rangle \in \mathcal{H}_1$ and $|\phi\rangle \in \mathcal{H}_2$. For simplicity, we also write $|\psi\rangle \otimes |\phi\rangle$ as $|\psi\rangle |\phi\rangle$ or $|\psi\phi\rangle$. ♢

Proposition B.2: Given two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, consider the set $\mathcal{G}$ of all anti-linear and continuous functionals from $\mathcal{H}_1 \times \mathcal{H}_2$ to $\mathbb{C}$. Then $\mathcal{G} = \{g : \mathcal{H}_1 \times \mathcal{H}_2 \to \mathbb{C} \mid g \text{ is anti-linear and continuous }\}$ is a vector space over $\mathbb{C}$ with vector addition defined as $[g_1 + g_2](|\xi\rangle, |\eta\rangle) = g_1(|\xi\rangle, |\eta\rangle) + g_2(|\xi\rangle, |\eta\rangle)$ for any $g_1, g_2 \in \mathcal{G}$ and scalar multiplication is defined as expected.

Proof.

To show $\mathcal{G}$ has a zero vector:
Consider the function $0_{\mathcal{G}} : \mathcal{H}_1 \times \mathcal{H}_2 \to \mathbb{C}$ defined as $0_{\mathcal{G}}(|\xi\rangle, |\eta\rangle) = 0$

Then $0_{\mathcal{G}}$ is continuous since every constant function between topological spaces is continuous.

Consider $|\xi_1\rangle, |\xi_2\rangle \in \mathcal{H}_1$ and $|\eta\rangle \in \mathcal{H}_2$, $a, b \in \mathbb{C}$.

Also
$0_{\mathcal{G}}(a\left|\xi_1\right\rangle + b\left|\xi_2\right\rangle, \left|\eta\right\rangle) = 0 = (\overline{a}\cdot 0) + (\overline{b}\cdot 0) = \overline{a}\, 0_{\mathcal{G}}(\left|\xi_1\right\rangle, \left|\eta\right\rangle) + \overline{b}\, 0_{\mathcal{G}}(\left|\xi_2\right\rangle, \left|\eta\right\rangle)$
Similarly, $0_{\mathcal{G}}(\left|\xi\right\rangle, a\left|\eta_1\right\rangle + b\left|\eta_2\right\rangle) = \overline{a}0_{\mathcal{G}}(\left|\xi\right\rangle, \left|\eta_1\right\rangle) + \overline{b}0_{\mathcal{G}}(\left|\xi\right\rangle, \left|\eta_2\right\rangle)$ for any $\left|\xi\right\rangle \in \mathcal{H}_1$, $\left|\eta_1\right\rangle, \left|\eta_2\right\rangle \in \mathcal{H}_2$ and $a, b \in \mathbb{C}$.

This implies $0_{\mathcal{G}}$ is conjugate linear in both variables and is continuous
$\implies 0_{\mathcal{G}} \in \mathcal{G}$.

To show $\mathcal{G}$ is closed under vector addition:
Consider any two g_1, g_2 in $\mathcal{G}$.

$[g_1 + g_2](\left|\xi\right\rangle, \left|\eta\right\rangle) = g_1(\left|\xi\right\rangle, \left|\eta\right\rangle) + g_2(\left|\xi\right\rangle, \left|\eta\right\rangle)$
$\implies [g_1 + g_2]$ is continuous, since sum of continuous functions is continuous.

Also, consider $a \in \mathbb{C}$.

$$\begin{aligned}
\text{Then } [g_1 + g_2](a\left|\xi\right\rangle, \left|\eta\right\rangle) &= g_1(a\left|\xi\right\rangle, \left|\eta\right\rangle) + g_2(a\left|\xi\right\rangle, \left|\eta\right\rangle) \\
&= \overline{a}g_1(\left|\xi\right\rangle, \left|\eta\right\rangle) + \overline{a}g_2(\left|\xi\right\rangle, \left|\eta\right\rangle) \\
&= \overline{a}(g_1(\left|\xi\right\rangle, \left|\eta\right\rangle) + g_2(\left|\xi\right\rangle, \left|\eta\right\rangle)) \\
&= \overline{a}[g_1 + g_2](\left|\xi\right\rangle, \left|\eta\right\rangle) \\
&\implies [g_1 + g_2] \text{ is conjugate linear in first variable}
\end{aligned}$$

Similarly, $[g_1 + g_2]$ is also continuous in the second variable.

This implies $[g_1 + g_2]$ is continuous and conjugate linear in both variables
$\implies [g_1 + g_2] \in \mathcal{G}$.

To show $\mathcal{G}$ is closed under scalar multiplication
Consider $a \in \mathbb{C}$.

For any functional g in $\mathcal{G}$, $[a \cdot g](\left|\xi\right\rangle, \left|\eta\right\rangle) = a \cdot [g(\left|\xi\right\rangle, \left|\eta\right\rangle)]$ which is conjugate linear and continuous at every $\left|\xi\right\rangle \in \mathcal{H}_1, \left|\eta\right\rangle \in \mathcal{H}_2 \implies [a \cdot g] \in \mathcal{G}$ $\square$

Note: Consider the set $\mathcal{F} = \{\left|\psi\right\rangle \otimes \left|\phi\right\rangle \mid \left|\psi\right\rangle \in \mathcal{H}_1 \text{ and } \left|\phi\right\rangle \in \mathcal{H}_2\}$ where $\left|\psi\right\rangle \otimes \left|\phi\right\rangle$ is defined as previously.

Then any $\left|\psi\right\rangle \otimes \left|\phi\right\rangle \in \mathcal{F}$ is anti-linear and continuous which implies $\mathcal{F} \subseteq \mathcal{G}$.
$\diamondsuit$

Theorem B.1: Consider we have Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$.

Let $\{\left|e_i\right\rangle\}_{i=1}^{n}$ be an orthonormal basis for $\mathcal{H}_1$ and $\{\left|f_j\right\rangle\}_{j=1}^{m}$ be an orthonormal basis for $\mathcal{H}_2$.

Then $\{|e_i\rangle \otimes |f_j\rangle \, | 1 \leq i \leq n, 1 \leq j \leq m\}$ is an orthonormal basis for $\mathcal{G} = \{g : \mathcal{H}_1 \times \mathcal{H}_2 \to \mathbb{C} \mid g$ is conjugate linear and continuous $\}$

Proof.

Let $\mathcal{E} = \{|e_i\rangle \otimes |f_j\rangle\} | 1 \leq i \leq n, 1 \leq j \leq m\}$

To show $\mathcal{E}$ is a spanning set for $\mathcal{G}$:
Let $g \in \mathcal{G}$ and $|\xi\rangle \in \mathcal{H}_1, |\eta\rangle \in \mathcal{H}_2$

Since $\{|e_i\rangle\}_{i=1}^n$ is an orthonormal basis for $\mathcal{H}_1$,
$|\xi\rangle = c_1 |e_1\rangle + c_2 |e_2\rangle + ... + c_n |e_n\rangle$ for some $c_1, c_2, ..., c_n \in \mathbb{C}$.

Similarly, since $\{|f_j\rangle\}_{j=1}^m$ is an orthonormal basis for $\mathcal{H}_2$,
$|\eta\rangle = d_1 |f_1\rangle + d_2 |f_2\rangle + ... + d_n |f_n\rangle$ for some $d_1, d_2, ..., d_n \in \mathbb{C}$.

$$g(|\xi\rangle , |\eta\rangle) = g(\sum_{i=1}^n c_i |e_i\rangle , \sum_{j=1}^m d_j |f_j\rangle) = \sum_{i=1}^n \sum_{j=1}^m \overline{c_i}\overline{d_j} g(|e_i\rangle , |f_j\rangle).$$

Using the fact that $c_i = \langle e_i|\xi\rangle$ and $d_j = \langle f_j|\eta\rangle$,

$$g(|\xi\rangle , |\eta\rangle) = \sum_{i=1}^n \sum_{j=1}^m \overline{\langle e_i|\xi\rangle\langle f_j|\eta\rangle} g(|e_i\rangle , |f_j\rangle) =$$
$$\sum_{i=1}^n \sum_{j=1}^m \langle \xi|e_i\rangle \langle \eta|f_j\rangle g(|e_i\rangle , |f_j\rangle) = \sum_{i=1}^n \sum_{j=1}^m [|e_i\rangle \otimes |f_j\rangle](|\xi\rangle , |\eta\rangle) g(|e_i\rangle , |f_j\rangle) =$$
$$\sum_{i=1}^n \sum_{j=1}^m g_{ij} [|e_i\rangle \otimes |f_j\rangle](|e_i\rangle , |f_j\rangle)$$ where $g_{ij} = g(|e_i\rangle , |f_j\rangle)$.

Thus $g = \sum_{i=1}^n \sum_{j=1}^m g_{ij} |e_i\rangle \otimes |f_j\rangle$

$\implies$ every $g \in \mathcal{G}$ is a linear combination of functions in $\mathcal{E}$

To show $\mathcal{E}$ is a linearly independent set:
Consider $g \in \mathcal{G}$ such that $g = 0_{\mathcal{G}}$.

Then
$$g(|\xi\rangle , |\eta\rangle) = \sum_{i=1}^n \sum_{j=1}^m g_{ij} [|e_i\rangle \otimes |f_j\rangle](|\xi\rangle , |\eta\rangle) = \sum_{i=1}^n \sum_{j=1}^m g_{ij} \langle e_i|\xi\rangle \langle f_j|\eta\rangle = 0_{\mathcal{G}}.$$

Consider in particular, we take $|\xi\rangle$ and $|\eta\rangle$ from the set of basis vectors of $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, i.e. ($|\xi\rangle = |e_p\rangle$ and $|\eta\rangle = |f_q\rangle$ for some $1 \leq p \leq n, 1 \leq q \leq m$.

Then $g(|e_p\rangle, |e_q\rangle) = \displaystyle\sum_{i=1}^{n}\sum_{j=1}^{m} g_{ij} \langle e_i|e_p\rangle \langle f_j|f_q\rangle = g_{pq}$ since

$\langle e_i|e_p\rangle = \begin{cases} 1 & i = p \\ 0 & i \neq p \end{cases} = \delta_{i,p}$ and $\langle f_j|f_q\rangle = \begin{cases} 1 & j = q \\ 0 & j \neq q \end{cases} = \delta_{j,q}$.

$g = 0_{\mathcal{H}} \implies g(|e_p\rangle, |e_q\rangle) = 0 \implies g_{pq} = 0$ for any $1 \leq p \leq n, 1 \leq j \leq m$.
Therefore

$$g = 0_{\mathcal{H}} \implies \sum_{i=1}^{n}\sum_{j=1}^{m} g_{ij} |e_i\rangle \otimes |f_j\rangle = 0 \implies g_{ij} = 0 \;\; \forall \;\; 1 \leq i \leq n, 1 \leq j \leq m$$

$\implies \mathcal{E}$ is a linearly independent set.

To show $\mathcal{E}$ is orthonormal:
Consider any $|e_a\rangle \otimes |f_b\rangle, |e_c\rangle \otimes |f_d\rangle \in \mathcal{E}$ for some $1 \leq a, c \leq n, 1 \leq b, d \leq m$.

Then $\langle |e_a\rangle \otimes |f_b\rangle \mid |e_c\rangle \otimes |f_d\rangle\rangle = \langle e_a|e_c\rangle \langle f_b|f_d\rangle$

$$= \begin{cases} 0 & a \neq c \text{ or } b \neq d \\ 1 & a = b \text{ and } c = d \end{cases} = \delta_{a,c}\delta_{b,d}$$

$\implies \mathcal{E}$ is orthonormal □

Proposition B.3: Let $\{e_i\}_{i=1}^n$ be an orthonormal basis for $\mathcal{H}_1$ and $\{f_j\}_{j=1}^m$ be an orthonormal basis for $\mathcal{H}_2$.

For $\mathcal{G} = \{g : \mathcal{H}_1 \times \mathcal{H}_2 \to \mathbb{C} \mid g$ is conjugate linear and continuous $\}$ and $g_1, g_2 \in \mathcal{G}$ where $g_1 = \displaystyle\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij} |e_i\rangle \otimes |f_j\rangle$ and $g_2 = \displaystyle\sum_{i=1}^{n}\sum_{j=1}^{m} d_{ij} |e_i\rangle \otimes |f_j\rangle$,

the function $\langle g_1|g_2\rangle = \displaystyle\sum_{i=1}^{n}\sum_{j=1}^{m} \overline{c_{ij}} d_{ij}$ defines an inner product on $\mathcal{G}$.

Proof.

$$g_1 = \sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij} |e_i\rangle \otimes |f_j\rangle \text{ and } g_2 = \sum_{i=1}^{n}\sum_{j=1}^{m} d_{ij} |e_i\rangle \otimes |f_j\rangle$$

To show the function has conjugate symmetric property:

$$\langle g_1|g_2\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m}\overline{c_{ij}}d_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{m}(c_{ij}\overline{d_{ij}})^\dagger = (\sum_{i=1}^{n}\sum_{j=1}^{m}c_{ij}\overline{d_{ij}})^\dagger = \overline{\langle g_2|g_1\rangle}$$

To show the function has positive definite property:

$$\langle g_1|g_1\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m}\overline{c_{ij}}c_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{m}|c_{ij}|^2 \geq 0$$

If $\langle g_1|g_1\rangle = 0 \implies \sum_{i=1}^{n}\sum_{j=1}^{m}|c_{ij}|^2 = 0 \implies |c_{ij}|^2 = 0$ for all $1 \leq i \leq n, 1 \leq j \leq m \implies c_{ij} = 0$ for all $1 \leq i \leq n, 1 \leq j \leq m \implies g_1 = 0_{\mathcal{H}}$

Conversely, if

$g_1 = 0_{\mathcal{H}} \implies c_{ij} = 0$ for all $1 \leq i \leq n, 1 \leq j \leq m \implies \langle g_1|g_1\rangle = 0$

To show the function is conjugate linear in first variable:

Let $g_3 = \sum_{i=1}^{n}\sum_{j=1}^{m}a_{ij}\,|e_i\rangle \otimes |f_j\rangle$

$$g_1 + g_2 = \sum_{i=1}^{n}\sum_{j=1}^{m}(c_{ij}+d_{ij})\,|e_i\rangle \otimes |f_j\rangle$$

$$\implies \langle g_1+g_2|g_3\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m}[\overline{c_{ij}+d_{ij}}]a_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{m}[\overline{c_{ij}}+\overline{d_{ij}}]a_{ij} =$$
$$\sum_{i=1}^{n}\sum_{j=1}^{m}[\overline{c_{ij}}a_{ij}+\overline{d_{ij}}a_{ij}] = \langle g_1|g_3\rangle\,\langle g_2|g_3\rangle$$

Also,

$$\langle a\cdot g_1|g_2\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m}\overline{a\cdot c_{ij}}d_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{m}\overline{a}\,\overline{c_{ij}}d_{ij} = \overline{a}\sum_{i=1}^{n}\sum_{j=1}^{m}\overline{c_{ij}}d_{ij} = \overline{a}\,\langle g_1|g_2\rangle$$

To show the function is linear in the second variable

$\langle g_1|g_2+g_3\rangle = \langle g_1|g_2\rangle + \langle g_1|g_3\rangle$ can be shown similar to previous.

Also, $\langle g_1|ag_2\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m}\overline{c_{ij}}(a\cdot d_{ij}) = a\sum_{i=1}^{n}\sum_{j=1}^{m}\overline{c_{ij}}d_{ij} = a\,\langle g_1|g_2\rangle$

$\implies \langle g_1|g_2\rangle$ is an inner product on $\mathcal{G}$ $\square$

Definition B.1: Consider Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$.

The vector space
$\mathcal{G} = \{g : \mathcal{H}_1 \times \mathcal{H}_2 \to \mathbb{C} \mid g \text{ is conjugate linear and continuous } \}$ along with the inner product defined as previously is known as the **tensor product** of $\mathcal{H}_1$ and $\mathcal{H}_2$.

Proposition B.4: Consider $|\psi\rangle \in \mathcal{H}_1, |\phi\rangle \in \mathcal{H}_2$. The linear functional $|\psi\rangle \otimes |\phi\rangle$ defined as $[|\psi\rangle \otimes |\phi\rangle](|\xi\rangle, |\eta\rangle) = \langle\xi|\psi\rangle_{\mathcal{H}_1} \langle\eta|\phi\rangle_{\mathcal{H}_2}$ satisfies the following properties:

1. $(a\,|\psi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes (a\,|\phi\rangle) = a(|\psi\rangle \otimes |\phi\rangle)$
2. $a(|\psi\rangle \otimes |\phi\rangle) + b(|\psi\rangle \otimes |\phi\rangle) = (a+b)(|\psi\rangle \otimes |\phi\rangle)$
3. $(|\psi\rangle_1 + |\psi\rangle_2) \otimes |\phi\rangle = |\psi\rangle_1 \otimes |\phi\rangle + |\psi\rangle_2 \otimes |\phi\rangle$
4. $|\psi\rangle \otimes (|\phi\rangle_1 + |\phi\rangle_2) = |\psi\rangle \otimes |\phi\rangle_1 + |\psi\rangle \otimes |\phi\rangle_2$

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.