Preliminary Mathematics for Quantum Computing
CS 151 - Quantum Computer Science

Prepared by: Elene Ivaniashvili
Course Instructor: Saeed Mehraban

January 30, 2024

Overview

This document provides an overview of the mathematical concepts that are fundamental for understanding and working with quantum systems. These notes summarise the required mathematical prerequisites for the course Quantum Computer Science (CS-151) at Tufts University. The document covers complex numbers and linear algebra, which are crucial tools for representing quantum states and operators in a mathematical framework.

The first part of the document introduces complex numbers and their properties, such as the complex conjugate and modulus. The second part of the document covers linear algebra basics, including vector spaces, basis vectors, and linear transformations. It explains how these concepts are used to represent quantum states and operators in a mathematical framework. The document also explains the concept of inner products, which are used to compute probabilities and measure the similarity between quantum states.

Overall, the document on preliminary mathematics in quantum computing provides a solid foundation for understanding the mathematical concepts and tools that are necessary for working with quantum systems. By covering complex numbers and linear algebra, the document provides readers with the essential mathematical background required for further study in quantum computing.

Contents

1 Complex Numbers

1.1 Complex Numbers

A complex number is a number of the form $z = a + bi$, where a and b are real numbers, and i is the imaginary unit, which has the property that $i^2 = -1$. The set of all complex numbers is denoted by $\mathbb{C}$.

1.1.1 Real and Imaginary Parts

For a complex number $z = a + bi$, the real part is denoted by $\mathrm{Re}(z) = a$, and the imaginary part is denoted by $\mathrm{Im}(z) = b$.

1.1.2 Complex Conjugate

The complex conjugate of a complex number $z = a + bi$ is the complex number $z^* = \bar{z} = a - bi$. The complex conjugate has the following properties:

- $(\bar{z})^* = z$
- $z\bar{z} = |z|^2$

1.1.3 Magnitude and Argument

The magnitude (or modulus) of a complex number $z = a + bi$ is denoted by $|z|$ and is defined as $|z| = \sqrt{a^2 + b^2}$.

The argument (or phase) of a complex number $z = a + bi$ is denoted by $\arg(z)$ and is defined as the angle θ such that $z = |z|(\cos(\theta) + i\sin(\theta))$. The argument is not unique, as it is defined modulo 2π.

1.1.4 Polar Form

A complex number $z = a + bi$ can be expressed in polar form as $z = r(\cos(\theta) + i\sin(\theta))$, where $r = |z|$ and $\theta = \arg(z)$.

1.1.5 Euler's Formula

Euler's formula states that for any real number θ,

$$e^{i\theta} = \cos(\theta) + i\sin(\theta) \tag{1}$$

Using Euler's formula, we can write the polar form of a complex number as $z = re^{i\theta}$.

1.2 Complex Number Arithmetic

1.2.1 Addition

The sum of two complex numbers is obtained by adding their real and imaginary parts separately:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \tag{2}$$

1.2.2 Subtraction

The difference of two complex numbers is obtained by subtracting their real and imaginary parts separately:

$$(a + bi) - (c + di) = (a - c) + (b - d)i \tag{3}$$

1.2.3 Multiplication

The product of two complex numbers is obtained by expanding and simplifying the terms:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \tag{4}$$

1.2.4 Division

The division of two complex numbers is obtained by multiplying both the numerator and the denominator by the complex conjugate of the denominator and simplifying:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} \tag{5}$$

1.2.5 Complex Exponentiation

Using Euler's formula, we can define the exponentiation of a complex number:

$$z^n = (re^{i\theta})^n = r^n e^{in\theta} = r^n(\cos(n\theta) + i\sin(n\theta)) \tag{6}$$

1.3 Complex Functions

In quantum computing, some important complex functions are used, such as complex exponential functions and complex trigonometric functions.

1.3.1 Complex Exponential Function

The complex exponential function is defined as:

$$f(z) = e^z = e^{a+bi} = e^a e^{bi} = e^a(\cos(b) + i\sin(b)) \tag{7}$$

1.3.2 Complex Trigonometric Functions

The complex sine and cosine functions are defined in terms of complex exponentials as:

$$\sin(z) = \frac{e^{iz} - e^{-iz}}{2i} = \sin(a)\cosh(b) + i\cos(a)\sinh(b) \tag{8}$$

$$\cos(z) = \frac{e^{iz} + e^{-iz}}{2} = \cos(a)\cosh(b) - i\sin(a)\sinh(b) \tag{9}$$

2 Bra-Ket Notation

2.1 Vectors in braket notation

In bra-ket notation, a column vector $\mathbf{v}$ is represented by a *ket*,

$$|\mathbf{v}\rangle. \tag{10}$$

For example, if $\mathbf{v}$ is a vector in $\mathbb{R}^3$, we can represent it in bra-ket notation as

$$|\mathbf{v}\rangle = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \tag{11}$$

where v_1, v_2, v_3 are the components of the vector in some chosen basis.

We can represent a row vector with *bra*, which is the conjugate transpose of the corresponding ket. The bra corresponding to the ket $|\mathbf{v}\rangle$ is denoted by $\langle\mathbf{v}|$ and is defined as

$$\langle\mathbf{v}| = |\mathbf{v}\rangle^\dagger = \begin{pmatrix} v_1^* & v_2^* & v_3^* \end{pmatrix} \tag{12}$$

where † denotes the Hermitian conjugate, which is the transpose of the matrix with complex conjugate entries.

The inner product of two vectors $|\mathbf{v}\rangle$ and $|\mathbf{w}\rangle$ is denoted by $\langle\mathbf{v}|\mathbf{w}\rangle$ and is defined as:

$$\langle\mathbf{v}|\mathbf{w}\rangle = \mathbf{v}^\dagger\mathbf{w} = \sum_{i=1}^{n} v_i^* w_i \tag{13}$$

where n is the dimension of the vectors. $|v\rangle$ and $|w\rangle$ are both in $\mathbb{C}^n$. i.e., they have same dimension. Note that the inner product of two vectors is a complex number.

The norm of a vector $|\mathbf{v}\rangle$ is denoted by $\||v\rangle\|$ and is defined as:

$$\||v\rangle\| = \sqrt{\langle\mathbf{v}|\mathbf{v}\rangle} = \sqrt{\sum_{i=1}^{n} |v_i|^2} \tag{14}$$

where $|v_i|$ denotes the absolute value of v_i.

2.2 Operators in bra-ket notation

An operator is a mathematical object that acts on a state vector to produce another state vector. Formally, if $\hat{A}$ is an operator and $|\psi\rangle$ is a state vector, then $\hat{A}|\psi\rangle = |\phi\rangle$ where $|\phi\rangle$ is another state vector. We can represent operators in bra-ket notation using a sum of outer products.

An operator is said to be Hermitian if it is equal to its own adjoint, i.e., $\hat{A}^\dagger = \hat{A}$. In braket notation, a Hermitian operator $\hat{A}$ is represented as:

A unitary operator is an operator that preserves the inner product of vectors, i.e., it satisfies the condition:

$$\langle u|U^\dagger U|v\rangle \tag{15}$$

for all vectors $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$. Equivalently, a unitary operator $\hat{U}$ is defined as satisfying

$$UU^\dagger = U^\dagger U = I \tag{16}$$

where I is the identity operator, and $U^\dagger$ is the conjugate transpose of U.

2.3 Examples

Here are some examples of how bra-ket notation is used in linear algebra:

- The projection operator onto a subspace V of a vector space W is given by:

  $$\hat{P_V} = \sum_{i=1}^{n} |v_i\rangle\langle v_i| \tag{17}$$

  where $|v_i\rangle$ are the basis vectors of V.

- The identity operator in a vector space is given by:

  $$\hat{I} = \sum_{i=1}^{n} |e_i\rangle\langle e_i| \tag{18}$$

  where $|e_i\rangle$ are a set of basis vectors of the vector space.

- The Pauli matrices in quantum mechanics are given by:

  $$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{19}$$

  $$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0| \tag{20}$$

  $$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{21}$$

3 Scalars, Vectors, and Matrices

3.1 Scalars

Scalars in quantum computing are complex numbers, denoted as $c \in \mathbb{C}$. Scalars are used to represent the probability amplitudes of quantum states and the elements of matrices that represent quantum operators. Complex numbers can be written in the form $c = a + bi$, where $a, b \in \mathbb{R}$ and i is the imaginary unit, satisfying $i^2 = -1$.

3.2 Vectors

Vectors in quantum computing are elements of a complex vector space. Quantum states are represented as column vectors called state vectors. For a quantum system with n basis states (e.g., qubits), the quantum state vector is an element of $\mathbb{C}^n$. The quantum states can be expressed as linear combinations of the orthonormal basis vectors:

$$|\psi\rangle = \sum_{i=1}^{n} c_i |\mathbf{e}_i\rangle \tag{22}$$

where $c_i \in \mathbb{C}$ are the complex coefficients, and $|\mathbf{e}_i\rangle$ are the basis vectors.

3.3 Matrices

Matrices in quantum computing are used to represent linear operators that act on quantum states. A quantum operator is represented by a square matrix $A \in \mathbb{C}^{n\times n}$, which acts on a quantum state vector $|\psi\rangle \in \mathbb{C}^n$ to produce a new quantum state vector $|\phi\rangle \in \mathbb{C}^n$:

$$|\phi\rangle = A|\psi\rangle \tag{23}$$

Quantum observables are represented by Hermitian matrices, which are matrices that are equal to their conjugate transpose. Unitary matrices are used to represent quantum gates and time evolution operators. A unitary matrix U satisfies $UU^\dagger = U^\dagger U = I$, where I is the identity matrix and $U^\dagger$ is the conjugate transpose of U.

3.3.1 Basic Matrix Operations

In this section, we briefly review some basic matrix operations that are important in quantum computing.

3.3.2 Matrix Addition and Subtraction

Two matrices of the same size can be added or subtracted element-wise:

$$(A \pm B)_{ij} = A_{ij} \pm B_{ij} \tag{24}$$

3.3.3 Matrix Multiplication

Matrix multiplication is a binary operation that takes a pair of matrices and produces another matrix. If $A \in \mathbb{C}^{n\times m}$ and $B \in \mathbb{C}^{m\times p}$, then their product $AB \in \mathbb{C}^{n\times p}$ is defined as:

$$(AB)ij = \sum k = 1^m A_{ik} B_{kj} \tag{25}$$

Matrix multiplication is associative but not, in general, commutative, meaning that $(AB)C = A(BC)$, but $AB \neq BA$ in general.

3.3.4 Conjugate Transpose

The conjugate transpose of a complex matrix $A \in \mathbb{C}^{n\times m}$, denoted as $A^\dagger$, is obtained by taking the transpose of the matrix and then taking the complex conjugate of each element:

$$A^\dagger_{ij} = \overline{A}_{ji} \tag{26}$$

where $\overline{A}ji$ is the complex conjugate of Aji.

3.4 Matrix representation of Quantum computations

Using the matrix representation of computations, we see that a classical state is a vector of zeros and ones such that one entry is 1 and the rest of zeros. We could view this as a vector of zeros and ones such that the sum of (squares) of entries is 1. We saw that a probability vector is a vector of non-negative numbers that sum to 1. Classical states were special cases of probability vectors. If we ask a state to have complex number square summing to 1 we get quantum states. Physically, we can encode a quantum bit within the degrees of freedom of a physical system: Electron spin up or down, photon polarization being clockwise or counter clockwise. Mathematically we have.

- Vector notation $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. E.g. $|0\rangle$ could mean spin up and $|1\rangle$ spin down.
- Superposition: $|\psi\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$.
- **Example:** $|+\rangle := \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ and $|-\rangle := \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
- Normalization $|\psi\rangle = \begin{pmatrix}\alpha_0\\\alpha_1\\\dots\\\alpha_{N-1}\end{pmatrix}$ then $\sum_i |\alpha_i|^2 = 1$

4 Vector Space

A vector space is a set of objects (vectors) that can be added together and multiplied by scalars (complex numbers in quantum computing), and it follows a set of rules called axioms. In quantum computing, vector spaces are used to represent the state space of quantum systems.

4.1 Hilbert Space

In quantum computing, a complex Hilbert space is used as the vector space to describe quantum states. A Hilbert space is a complex vector space equipped with an inner product, which allows us to define the distance and angle between vectors. It also has the property that it is complete, meaning that any Cauchy sequence of vectors in the space converges to a limit in the space.

4.2 Basis Vectors and Linear Combinations

A basis of a vector space is a set of linearly independent vectors that span the entire space. In other words, every vector in the space can be expressed as a unique linear combination of the basis vectors. For a quantum system with n basis states (e.g., qubits), the quantum state vector is an element of $\mathbb{C}^n$. The quantum states can be expressed as linear combinations of the orthonormal basis vectors:

$$|\psi\rangle = \sum_{i=1}^{n} c_i |\mathbf{e}_i\rangle \tag{27}$$

where $c_i \in \mathbb{C}$ are the complex coefficients, and $|\mathbf{e}_i\rangle$ are the basis vectors.

4.3 Superposition

Superposition is a fundamental concept in quantum mechanics, which is a direct consequence of the vector space structure of quantum states. Superposition states that a quantum system can exist in multiple states simultaneously. Mathematically, this means that a quantum state vector can be a linear combination of basis vectors:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \tag{28}$$

where $c_0, c_1 \in \mathbb{C}$ are probability amplitudes, and $|0\rangle$ and $|1\rangle$ are basis vectors.

4.4 Linear Combinations and Span

A linear combination of a set of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ is an expression of the form:

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_n\mathbf{v}_n \tag{29}$$

where $c_1, c_2, \ldots, c_n$ are scalars. The span of a set of vectors is the set of all possible linear combinations of those vectors:

$$\text{span}\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_n\mathbf{v}_n : c_1, c_2, \ldots, c_n \in \mathbb{F} \tag{30}$$

where $\mathbb{F}$ is the field of scalars (usually the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$). The span of a set of vectors is always a subspace of the vector space.

4.5 Linear Independence and Dependence

A set of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ is linearly independent if the only linear combination that equals the zero vector is the trivial linear combination (i.e., all coefficients are zero):

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_n\mathbf{v}_n = \mathbf{0} \implies c_1 = c_2 = \cdots = c_n = 0 \tag{31}$$

If there exists a non-trivial linear combination that equals the zero vector, the set of vectors is linearly dependent.

4.6 Basis and Dimension

A basis of a vector space is a set of linearly independent vectors that spans the vector space. In other words, every vector in the vector space can be uniquely expressed as a linear combination of the basis vectors.

The dimension of a vector space is the number of vectors in any basis of the vector space. The dimension is denoted as $\dim(V)$.

4.7 Orthogonality and Orthonormality

Two vectors are orthogonal if their dot product (inner product) is zero:

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i = 0 \tag{32}$$

A set of vectors is orthogonal if every pair of distinct vectors in the set is orthogonal.

A set of vectors is orthonormal if it is orthogonal and all the vectors in the set have a norm (magnitude) of 1.

An orthogonal basis is a basis in which all the basis vectors are orthogonal. An orthonormal basis is a basis in which all the basis vectors are orthonormal.

4.8 Gram-Schmidt Process

The Gram-Schmidt process is a method for orthogonalizing a set of vectors in an inner product space. It is commonly used in linear algebra and is particularly useful for constructing orthonormal bases.

4.8.1 Description

Given a set of n linearly independent vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ in an inner product space, the Gram-Schmidt process produces a set of n orthogonal vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$, where $\mathbf{u}_1 = \mathbf{v}_1$ and $\mathbf{u}_i$ is obtained by subtracting from $\mathbf{v}_i$ its projection onto the subspace spanned by $\mathbf{u}_1, \mathbf{u}2, \ldots, \mathbf{u}i - 1$ and then normalizing the result:

$$\mathbf{u}_1 = \mathbf{v}_1 \ \mathbf{u}_i \qquad\qquad = \mathbf{v}i - \sum j = 1^{i-1} \frac{\langle \mathbf{u}_j, \mathbf{v}_i \rangle}{\langle \mathbf{u}_j, \mathbf{u}_j \rangle} \mathbf{u}_j, \quad i = 2, 3, \ldots, n.$$

Here, $\langle \cdot, \cdot \rangle$ denotes the inner product, which is a bilinear form that satisfies certain properties, such as linearity in the first argument and conjugate symmetry.

After applying the Gram-Schmidt process, the resulting set of vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ is an orthonormal basis for the subspace spanned by the original set of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.

4.8.2 Instructions

To apply the Gram-Schmidt process to a set of vectors, follow these steps:

1. Start with the first vector $\mathbf{v}_1$ and set $\mathbf{u}_1 = \mathbf{v}_1$.

2. For $i = 2, 3, \ldots, n$, compute $\mathbf{u}_i$ using the formula above, where $\langle \cdot, \cdot \rangle$ denotes the inner product.

3. Normalize each $\mathbf{u}_i$ by dividing it by its norm: $\mathbf{u}_i = \frac{\mathbf{u}_i}{|\mathbf{u}_i|}$, where $|\cdot|$ denotes the norm induced by the inner product.

4. The resulting set of vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ is an orthonormal basis for the subspace spanned by the original set of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.

5 Inner Product, Norm, and Outer Product

5.1 Inner Product

The inner product is a function that takes two vectors as input and returns a scalar. In quantum computing, we deal with complex vector spaces, so the inner product is defined as follows:

$$\langle\psi|\phi\rangle = \sum_{i=1}^{n} \overline{c_i} d_i \tag{33}$$

where $|\psi\rangle = \sum_{i=1}^{n} c_i |\mathbf{e}_i\rangle$ and $|\phi\rangle = \sum_{i=1}^{n} d_i |\mathbf{e}_i\rangle$ are quantum states, and $\overline{c_i}$ is the complex conjugate of c_i.

The inner product has the following properties:

- Conjugate symmetry: $\langle\psi|\phi\rangle = \overline{\langle\phi|\psi\rangle}$
- Linearity: $\langle\psi|(a\phi_1 + b\phi_2)\rangle = a\langle\psi|\phi_1\rangle + b\langle\psi|\phi_2\rangle$
- Positivity: $\langle\psi|\psi\rangle \geq 0$
- Definiteness: $\langle\psi|\psi\rangle = 0$ if and only if $|\psi\rangle = 0$

5.2 Norm

The norm of a vector is a measure of its magnitude or length. In quantum computing, the norm of a quantum state vector $|\psi\rangle$ is given by the square root of the inner product of the vector with itself:

$$\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle} \tag{34}$$

A quantum state is said to be normalized if its norm is equal to 1. Normalized quantum states are important because their coefficients (probability amplitudes) can be used to compute probabilities of measurement outcomes.

5.3 Cauchy-Schwarz Inequality

The Cauchy-Schwarz inequality is an important result relating the inner product and the norm. It states that for any two vectors $\mathbf{u}$ and $\mathbf{v}$ in an inner product space:

$$|\langle\mathbf{u}|\mathbf{v}\rangle|^2 \leq |\mathbf{u}|^2|\mathbf{v}|^2 \tag{35}$$

5.4 Orthogonality

Two vectors are orthogonal if their inner product is zero:

$$\langle\mathbf{u}|\mathbf{v}\rangle = 0 \tag{36}$$

5.5 Projection

The projection of a vector $|u\rangle$ onto another vector $|v\rangle$ is defined as:

$$P_v(|u\rangle) = \frac{\langle \mathbf{v}|\mathbf{u}\rangle}{\langle v|v\rangle}|v\rangle \tag{37}$$

We can represent this projection operator using a matrix $P_v = \frac{|v\rangle\langle v|}{\langle v|v\rangle}$, such that $P_v(|u\rangle) = P_v|u\rangle$. In particular, if $|v\rangle$ is a unit vector, then P_v is the outer product $|v\rangle\langle v|$.

5.6 Outer Product

The outer product is a function that takes two vectors as input and returns a matrix. In quantum computing, the outer product of two quantum state vectors $|\psi\rangle$ and $|\phi\rangle$ is defined as:

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \psi_1\overline{\psi_1} & \psi_1\overline{\psi_2} & \cdots & \psi_1\overline{\psi_n} \\ \psi_2\overline{\psi_1} & \psi_2\overline{\psi_2} & \cdots & \psi_2\overline{\psi_n} \\ \vdots & \vdots & \ddots & \vdots \\ \psi_n\overline{\psi_1} & \psi_n\overline{\psi_2} & \cdots & \psi_n\overline{\psi_n} \end{pmatrix} \tag{38}$$

where $|\psi\rangle = \sum_{i=1}^{n} c_i|\mathbf{e}i\rangle$ and $|\phi\rangle = \sum i = 1^n d_i|\mathbf{e}_i\rangle$ are quantum states.
The outer product has the following properties:

- Linearity: $(a|\psi_1\rangle + b|\psi_2\rangle)\langle\phi| = a|\psi_1\rangle\langle\phi| + b|\psi_2\rangle\langle\phi|$
- Linearity: $|\psi\rangle\langle(a\phi_1 + b\phi_2)| = a|\psi\rangle\langle\phi_1| + b|\psi\rangle\langle\phi_2|$

6 Tensor Product

The tensor product, also known as the Kronecker product or the outer product, is an essential mathematical tool in quantum computing. It is used to describe the combined state of multiple qubits and to construct multi-qubit gates. In this document, we present the definition, properties, and applications of the tensor product in quantum computing.

6.1 Definition

Given two matrices A of size $m \times n$ and B of size $p \times q$, the tensor product of A and B, denoted by $A \otimes B$, is a matrix of size $(mp) \times (nq)$ defined as:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}. \tag{39}$$

6.2 Properties

The tensor product has several important properties, including:

1. **Bilinearity:** The tensor product is bilinear, meaning it is linear in both factors:

$$(A + A') \otimes B = A \otimes B + A' \otimes B \tag{40}$$

$$A \otimes (B + B') = A \otimes B + A \otimes B' \tag{41}$$

   for any matrices A, A', B, and B' of compatible dimensions.

2. **Associativity:** The tensor product is associative when applied to vector spaces, meaning:

$$(A \otimes B) \otimes C = A \otimes (B \otimes C) \tag{42}$$

   for any matrices A, B, and C of compatible dimensions. Note that this does not imply that the tensor product of matrices is associative.

3. **Distributivity over Matrix Multiplication:** The tensor product distributes over matrix multiplication:

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD) \tag{43}$$

   for any matrices A, B, C, and D of compatible dimensions.

4. **Identity:** The identity element for the tensor product is the 1×1 identity matrix I_1:

$$A \otimes I_1 = I_1 \otimes A = A \tag{44}$$

   for any matrix A.

5. **Transpose:** The transpose of a tensor product is given by:

$$(A \otimes B)^T = A^T \otimes B^T \tag{45}$$

for any matrices A and B.

6. **Conjugate:** The conjugate of a tensor product is given by:

$$(A \otimes B)^* = A^* \otimes B^* \tag{46}$$

for any matrices A and B.

7. **Adjoint:** The adjoint of a tensor product is given by:

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger \tag{47}$$

for any matrices A and B.

8. **Determinant:** The determinant of a tensor product of square matrices is given by:

$$\det(A \otimes B) = (\det(A))^m (\det(B))^n \tag{48}$$

where A is an $n \times n$ matrix, B is an $m \times m$ matrix, and both A and B have compatible dimensions.

9. **Trace:** The trace of a tensor product is given by:

$$\text{Tr}(A \otimes B) = \text{Tr}(A)\text{Tr}(B) \tag{49}$$

for any square matrices A and B of compatible dimensions.

6.3 Multi-Qubit States

In quantum computing, the tensor product is used to represent the combined state of multiple qubits. Given two qubits in states $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ and $|\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$, their combined state is described by the tensor product $|\psi\rangle \otimes |\phi\rangle$, which is a 4×1 column vector:

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} \tag{50}$$

For n qubits, the combined state is an $2^n \times 1$ column vector, which can be written as the tensor product of the individual qubit states. For example, for three qubits in states $|\psi\rangle$, $|\phi\rangle$, and $|\chi\rangle$, the combined state is:

$$|\psi\rangle \otimes |\phi\rangle \otimes |\chi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \otimes \begin{pmatrix} \epsilon \\ \zeta \end{pmatrix} = \begin{pmatrix} \alpha\gamma\epsilon \\ \alpha\gamma\zeta \\ \alpha\delta\epsilon \\ \alpha\delta\zeta \\ \beta\gamma\epsilon \\ \beta\gamma\zeta \\ \beta\delta\epsilon \\ \beta\delta\zeta \end{pmatrix} \tag{51}$$

6.4 Multi-Qubit Gates

The tensor product is also used to construct multi-qubit gates by combining single-qubit gates or other multi-qubit gates. For example, given two single-qubit gates U and V, their combined action on a two-qubit state can be represented as:

$$(U \otimes V)|\psi\rangle \otimes |\phi\rangle = U|\psi\rangle \otimes V|\phi\rangle. \tag{52}$$

As an example, the combined action of two Hadamard gates H on a two-qubit state is given by:

$$(H \otimes H)|\psi\rangle \otimes |\phi\rangle = H|\psi\rangle \otimes H|\phi\rangle. \tag{53}$$

For controlled gates, such as the CNOT gate, the tensor product is used to express the gate as a matrix that acts on the combined state of the control and target qubits:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

7 Matrix Operations

7.1 Matrix Addition and Subtraction

Matrix addition and subtraction are performed element-wise. If $A \in \mathbb{C}^{n \times m}$ and $B \in \mathbb{C}^{n \times m}$, then their sum $A + B$ and difference $A - B$ are given by:

$$(A \pm B)_{ij} = A_{ij} \pm B_{ij} \tag{54}$$

7.2 Matrix Multiplication

Matrix multiplication is the primary operation in quantum computing, as it is used to describe the action of quantum gates and operators. If $A \in \mathbb{C}^{n \times m}$ and $B \in \mathbb{C}^{m \times p}$, then their product $AB \in \mathbb{C}^{n \times p}$ is defined as:

$$(AB)_{ij} = \sum_{k=1}^{m} A_{ik} B_{kj} \tag{55}$$

Matrix multiplication is associative but not commutative, meaning that $(AB)C = A(BC)$, but $AB \neq BA$ in general.

7.3 Transpose

The transpose of a matrix A of size $m \times n$ is a matrix A^T of size $n \times m$, and its elements are defined as:

$$A^T_{ij} = A_{ji} \tag{56}$$

for all $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$.

The transpose operation has the following properties:

$$(A^T)^T = A \; (A + B)^T \qquad = A^T + B^T \; (cA)^T = c(A^T) \; (AB)^T \qquad = B^T A^T \tag{57}$$

7.4 Matrix Inversion

The inverse of a square matrix A of size $n \times n$ is a matrix A^{-1} of the same size, such that their product is the identity matrix I_n:

$$AA^{-1} = A^{-1}A = I_n \tag{58}$$

Not all matrices have an inverse; a matrix is called invertible or nonsingular if it has an inverse, and non-invertible or singular if it does not. If a matrix is invertible, its inverse is unique.

The matrix inversion operation has the following properties:

$$(A^{-1})^{-1} = A \; (AB)^{-1} \quad = B^{-1}A^{-1} \; (A^T)^{-1} = (A^{-1})^T \; (cA)^{-1} \quad = \frac{1}{c}A^{-1} \quad \text{for nonzero } c \tag{59}$$

7.5 Determinant

The determinant is a scalar function that takes a square matrix and returns a scalar value. The determinant of a 2 × 2 matrix A is defined as:

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21} \tag{60}$$

For an $n \times n$ matrix A, the determinant can be calculated using the Laplace expansion, which is a recursive formula:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) \tag{61}$$

where A_{ij} is the $(n-1) \times (n-1)$ matrix obtained by deleting the i-th row and j-th column of A.

The determinant has the following properties:

$$\det(A^T) = \det(A) \;\; \det(AB) \quad = \det(A)\det(B) \;\; \det(A^{-1}) = \frac{1}{\det(A)} \quad \text{if } A \text{ is invertible} \tag{62}$$

7.6 Trace

The trace of a matrix is an important concept with various applications. The trace of a square matrix A of size $n \times n$ is defined as the sum of its diagonal elements:

$$\text{Tr}(A) = \sum_{i=1}^{n} A_{ii}. \tag{63}$$

In the context of quantum mechanics, the trace often appears in calculations involving density matrices, which describe the state of a quantum system. For instance, the trace of a density matrix ρ is always equal to 1, representing the total probability of the system:

$$\text{Tr}(\rho) = 1. \tag{64}$$

Moreover, the trace operation is used to compute expectation values of observables, which are represented by Hermitian matrices. Given an observable O and a quantum state represented by a density matrix ρ, the expectation value of the observable is given by:

$$\langle O \rangle = \text{Tr}(O\rho). \tag{65}$$

7.7 Identity Matrix

The identity matrix $I \in \mathbb{C}^{n \times n}$ is a square matrix with ones on the diagonal and zeros elsewhere:

$$I_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases} \tag{66}$$

The identity matrix has the property that $AI = IA = A$ for any matrix $A \in \mathbb{C}^{n \times n}$.

7.8 Conjugate Transpose

The conjugate transpose of a complex matrix $A \in \mathbb{C}^{n \times m}$, denoted as $A^\dagger$, is obtained by taking the transpose of the matrix and then taking the complex conjugate of each element:

$$A^\dagger_{ij} = \overline{A}_{ji} \tag{67}$$

where $\overline{A}_{ji}$ is the complex conjugate of A_{ji}.

7.9 Hermitian Matrices

A Hermitian matrix $H \in \mathbb{C}^{n \times n}$ is a square matrix that is equal to its conjugate transpose:

$$H = H^\dagger \tag{68}$$

Hermitian matrices have real eigenvalues and play an important role in quantum mechanics, as they represent observable quantities in quantum systems.

8 Eigenvalues and Eigenvectors

Eigenvalues and eigenvectors are essential concepts in linear algebra that provide insight into the behavior of linear transformations. Given a square matrix A of size $n \times n$, a scalar λ is an eigenvalue of A if there exists a non-zero vector $\mathbf{v}$ such that:

$$A\mathbf{v} = \lambda\mathbf{v} \tag{69}$$

The vector $\mathbf{v}$ is called an eigenvector corresponding to the eigenvalue λ.

8.1 Characteristic Equation

To find the eigenvalues of a matrix A, we can rewrite the eigenvalue equation as follows:

$$(A - \lambda I_n)\mathbf{v} = \mathbf{0} \tag{70}$$

where I_n is the identity matrix of size $n \times n$. For a non-trivial solution $\mathbf{v}$, the matrix $(A - \lambda I_n)$ must be singular, which means that its determinant is zero:

$$\det(A - \lambda I_n) = 0 \tag{71}$$

This equation is called the characteristic equation of the matrix A. Solving it yields the eigenvalues of A.

8.2 Finding Eigenvectors

Once the eigenvalues have been found, the corresponding eigenvectors can be obtained by solving the following system of linear equations:

$$(A - \lambda I_n)\mathbf{v} = \mathbf{0} \tag{72}$$

for each eigenvalue λ.

8.3 Diagonalizing a matrix

Here is how you diagonalize a matrix: For a complex matrix $A \in \mathbb{C}^{d\times d}$ the eigenvalues of A are numbers λ such that $A - \lambda I$ is singular. That means $det(A - \lambda I) = 0$; that means you have to solve this equation for λ. For a 2×2 matrix, the determinant is the product of entries on the diagonal minus the product of off-diagonal entries. For instance in order to find the eigenvalues of X you should solve $det(X - \lambda I) = 0$ which gives you $(-\lambda)(-\lambda) - (1)(1) = 0$. Which gives you $\lambda = \pm 1$ as its solution.

Once you have found the eigenvalues, it is time to find eigenvectors. The eigenvector $|v\rangle$ corresponding to eigenvalue λ satisfies $(A - \lambda I)|v\rangle = 0$. You should write this as a system of equations. If λ is a unique eigenvalue, you will find the entries of $|v\rangle$ up to a free parameter.

You can set that free parameter to make $|v\rangle$ have a unit norm. For instance, in order to find the eigenvector corresponding to eigenvalue $+1$ for X, you have to solve

$$\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = 0$$

Solving this you will find that $a = b$, and in order to normalize the vector you can choose $a = b = 1/\sqrt{2}$.

The next step is to find a unitary matrix O that diagonalizes A, ie, $OAO^-1 = D$ where D is the diagonal matrix with the eigenvalues of A. If you think about it, O^{-1} needs to be a matrix that maps the basis A is defined to its eigenbasis. So to construct O, we place each eigenvector as its columns. For instance, in the case of X, the eigenvectors are $|+\rangle$ and $|-\rangle$. So

$$O = (|+\rangle|-\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Which is the Hadamard matrix, as we expected.

8.4 Eigenvalues and Matrix Powers

If a matrix A is diagonalizable, its powers can be computed easily using the diagonal form:

$$A^k = PD^kP^{-1} \tag{73}$$

for any positive integer k. This property is useful for computing the exponential of a matrix, which has applications in solving systems of linear differential equations.

9 Unitary Matrices

A unitary matrix $U \in \mathbb{C}^{n\times n}$ is a square matrix that satisfies the following condition:

$$UU^\dagger = U^\dagger U = I \tag{74}$$

where $U^\dagger$ denotes the conjugate transpose of U, and I is the identity matrix. Unitary matrices preserve the inner product and norms of vectors, making them essential for describing the evolution of quantum states in quantum computing.

Unitary matrices are the complex analogs of orthogonal matrices, which are matrices with real entries satisfying $A^TA = AA^T = I_n$. Unitary matrices preserve the inner product between vectors, which means that for any vectors $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$, the following holds:

$$\langle U\mathbf{v}, U\mathbf{w}\rangle = \langle \mathbf{v}, \mathbf{w}\rangle \tag{75}$$

where $\langle \cdot, \cdot \rangle$ denotes the inner product in the complex vector space $\mathbb{C}^n$.

9.1 Properties of Unitary Matrices

Unitary matrices have several important properties:

- The product of two unitary matrices is unitary:

$$(UV)^*UV = V^*U^*UV = V^*VU^*U = I_n \tag{76}$$

- The inverse of a unitary matrix is unitary:

$$(U^{-1})^*U^{-1} = U^*U = I_n \tag{77}$$

- The determinant of a unitary matrix is a complex number with absolute value 1:

$$|\det(U)| = 1 \tag{78}$$

- The eigenvalues of a unitary matrix are complex numbers with absolute value 1.

9.2 Hermitian Matrices

A square matrix A of size $n \times n$ with complex entries is called Hermitian if its conjugate transpose A^* (also denoted as $A^\dagger$) is equal to itself:

$$A^* = A \tag{79}$$

Hermitian matrices are the complex analogs of symmetric matrices, which are matrices with real entries satisfying $A^T = A$. The eigenvalues of a Hermitian matrix are always real.

9.3 Unitary Diagonalization

A Hermitian matrix A of size $n \times n$ can be diagonalized by a unitary matrix U:

$$A = UDU^* \tag{80}$$

where D is a diagonal matrix with the eigenvalues of A on its diagonal, and the columns of U are the eigenvectors of A corresponding to the eigenvalues in D. This process is called unitary diagonalization.

The diagonalization process can be summarized as follows:

1. Find the eigenvalues λ_i of the Hermitian matrix A.
2. For each eigenvalue λ_i, find a corresponding eigenvector $\mathbf{v}_i$ by solving the equation $(A - \lambda_i I_n)\mathbf{v}_i = 0$.
3. Normalize the eigenvectors and form the unitary matrix U with the normalized eigenvectors as its columns.
4. Form the diagonal matrix D with the eigenvalues λ_i on its diagonal.
5. Verify that $A = UDU^*$.

9.4 Unitary Transformations

Unitary matrices represent unitary transformations, which are linear transformations that preserve the inner product of vectors. Given two vectors $|\psi\rangle$ and $|\phi\rangle$ in a complex vector space, a unitary transformation U satisfies the following property:

$$\langle U\psi | U\phi \rangle = \langle \psi | \phi \rangle \tag{81}$$

Unitary transformations preserve the orthogonality and norms of vectors, ensuring that quantum states remain normalized after the application of quantum gates.

9.5 Unitary Matrices and Quantum Gates

In quantum computing, unitary matrices are used to represent quantum gates, which are the basic building blocks of quantum circuits. Quantum gates operate on quantum states, which are represented as unit vectors in a complex Hilbert space. Since unitary matrices preserve inner products and norms, they ensure that quantum gates maintain the normalization of quantum states.

A quantum gate U is a unitary matrix acting on a quantum state $|\psi\rangle$:

$$|\psi'\rangle = U|\psi\rangle \tag{82}$$

where $|\psi'\rangle$ is the resulting quantum state after applying the gate.

9.5.1 Examples of Quantum Gates

Some common quantum gates represented by unitary matrices include:

- Identity gate (I):

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{83}$$

- Pauli-X gate (X), also known as the NOT gate:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{84}$$

- Pauli-Y gate (Y):

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{85}$$

- Pauli-Z gate (Z):

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{86}$$

- Hadamard gate (H):

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{87}$$

10 Special Matrices in Quantum Computation

10.1 Pauli Matrices

The Pauli matrices are a set of three 2×2 matrices that are widely used in quantum computing. They are defined as follows:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{88}$$

The Pauli matrices have the following properties:

- They are Hermitian: $\sigma_x^\dagger = \sigma_x$, $\sigma_y^\dagger = \sigma_y$, $\sigma_z^\dagger = \sigma_z$.
- They are unitary: $\sigma_x^\dagger \sigma_x = \sigma_y^\dagger \sigma_y = \sigma_z^\dagger \sigma_z = I$.
- Their square is the identity matrix: $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$.
- They anti-commute: $\sigma_x \sigma_y \sigma_z = -\sigma_y \sigma_x \sigma_z = -\sigma_z \sigma_y \sigma_x = -\sigma_y \sigma_z \sigma_x = -\sigma_x \sigma_z \sigma_y = -\sigma_z \sigma_x \sigma_y$.

10.2 Hadamard Gate

The Hadamard gate is a 2×2 matrix that is used to create superpositions in quantum computing. It is defined as:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{89}$$

The Hadamard gate has the following properties:

- It is Hermitian: $H^\dagger = H$.
- It is unitary: $H^\dagger H = I$.
- Its square is the identity matrix: $H^2 = I$.

10.3 Phase Gates

Phase gates are a family of 2×2 matrices that introduce a relative phase between the basis states. The most common phase gates are the S and T gates, defined as:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \tag{90}$$

In general, a phase gate can be represented as:

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

where θ is the phase angle.

Phase gates have the following properties:

- They are Hermitian: $S^\dagger = S$, $T^\dagger = T$, and $P(\theta)^\dagger = P(\theta)$.
- They are unitary: $S^\dagger S = T^\dagger T = P(\theta)^\dagger P(\theta) = I$.
- The S and T gates satisfy: $S^2 = \sigma_z$, $T^4 = \sigma_z$, and $T^8 = I$.

10.4 Controlled Gates

Controlled gates act on two qubits and perform an operation on the target qubit if the control qubit is in the $|1\rangle$ state. The most common controlled gate is the Controlled-NOT (CNOT) gate, which is defined as:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The controlled version of a unitary matrix U is given by:

$$CU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

where C is the controlled gate.

Controlled gates have the following properties:

- They are unitary: $\mathrm{CNOT}^\dagger \mathrm{CNOT} = I$ and $\mathrm{C}(U)^\dagger \mathrm{C}(U) = I$.
- The CNOT gate can be expressed in terms of the Pauli matrices as $\mathrm{CNOT} = I \otimes \frac{1}{2}(\sigma_z + I) + \sigma_x \otimes \frac{1}{2}(\sigma_z - I)$.

10.5 SWAP Gate

The Swap gate exchanges the states of two qubits. It is represented by the following 4×4 matrix:

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

The Swap gate has the following properties:

- It is Hermitian: $\mathrm{SWAP}^\dagger = \mathrm{SWAP}$.
- It is unitary: $\mathrm{SWAP}^\dagger\mathrm{SWAP} = I$.
- Its square is the identity matrix: $\mathrm{SWAP}^2 = I$.

11 Measurements in Quantum Computing

Measurements play a crucial role in quantum computing as they extract information from quantum states, collapsing them into classical outcomes. This section presents a comprehensive and detailed overview of measurements in quantum computing, including the postulates of quantum mechanics, types of measurements, and the measurement process.

11.1 Postulates of Quantum Mechanics

Quantum mechanics is governed by a set of postulates that describe the behavior of quantum systems. The following postulates are relevant to measurements in quantum computing:

1. Quantum states are represented by vectors in a complex vector space called the Hilbert space. For a qubit, the Hilbert space is a two-dimensional complex vector space, and its state can be represented as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$.

2. Observables are represented by Hermitian operators acting on the Hilbert space. An observable $\hat{A}$ has a set of eigenvectors $\{|a_i\rangle\}$ and eigenvalues $\{a_i\}$, satisfying $\hat{A}|a_i\rangle = a_i|a_i\rangle$.

3. The outcome of a measurement is one of the eigenvalues of the observable being measured. The probability of obtaining a particular eigenvalue a_i when measuring the state $|\psi\rangle$ is given by $p(a_i) = |\langle a_i|\psi\rangle|^2$.

4. After a measurement yielding the outcome a_i, the quantum state collapses to the corresponding eigenvector $|a_i\rangle$.

11.2 Types of Measurements

In quantum computing, the most common type of measurement is the projective measurement, also known as the von Neumann measurement. This type of measurement is based on the eigenvalues and eigenvectors of the observable being measured. For qubits, the most common observables are the Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{91}$$

Other types of measurements include generalized measurements, such as positive operator-valued measures (POVMs), which allow for a more general description of the measurement process, including the effects of noise and decoherence.

11.3 Projective Measurements

Projective measurements are a specific type of measurement in quantum computing that project the measured quantum state onto one of the eigenvectors of the measurement operator. The outcome of a projective measurement is a classical bit of information, and the post-measurement state is one of the eigenvectors corresponding to the obtained classical outcome.

11.3.1 Mathematical Representation

A projective measurement is represented by a set of projectors $\{P_i\}$, where each projector P_i corresponds to a possible outcome i of the measurement. A projector is an idempotent, Hermitian operator, satisfying the following conditions:

$$P_i^\dagger = P_i \tag{92}$$

$$P_i^2 = P_i \tag{93}$$

The projectors must also be orthogonal and sum up to the identity operator:

$$P_i P_j = \delta_{ij} P_i \tag{94}$$

$$\sum_i P_i = I \tag{95}$$

where δ_{ij} is the Kronecker delta, and I is the identity operator.

11.3.2 Measurement Outcomes and Probabilities

When a quantum state $|\psi\rangle$ is measured using a set of projectors $\{P_i\}$, the probability of obtaining the outcome i is given by:

$$p(i) = \langle\psi|P_i|\psi\rangle \tag{96}$$

After the measurement, the quantum state collapses to the eigenvector corresponding to the outcome i. The post-measurement state $|\psi_i\rangle$ is given by:

$$|\psi_i\rangle = \frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}} \tag{97}$$

11.3.3 Example: Measurement in the Computational Basis

A common projective measurement in quantum computing is the measurement in the computational basis, which uses the standard basis vectors $|0\rangle$ and $|1\rangle$. The projectors for this measurement are:

$$P_0 = |0\rangle\langle 0| \tag{98}$$
$$P_1 = |1\rangle\langle 1| \tag{99}$$

Given a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the probabilities of obtaining the outcomes 0 and 1 are:

$$p(0) = |\alpha|^2 \tag{100}$$
$$p(1) = |\beta|^2 \tag{101}$$

The post-measurement states for the outcomes 0 and 1 are:

$$|\psi_0\rangle = \frac{|0\rangle\langle 0|(\alpha|0\rangle + \beta|1\rangle)}{\sqrt{|\alpha|^2}} = \frac{\alpha|0\rangle}{\sqrt{|\alpha|^2}} = |0\rangle\ |\psi_1\rangle \quad = \frac{|1\rangle\langle 1|(\alpha|0\rangle + \beta|1\rangle)}{\sqrt{|\beta|^2}} = \frac{\beta|1\rangle}{\sqrt{|\beta|^2}} = |1\rangle \tag{102}$$

11.3.4 Properties of Projective Measurements

Projective measurements have several important properties that are essential for quantum computing:

- **Irreversibility:** Projective measurements are inherently irreversible, meaning that once a quantum state has been measured, it is not possible to recover the original state. This property is a consequence of the projection postulate and the probabilistic nature of quantum mechanics.

- **Non-destructive Measurements:** Projective measurements can be non-destructive if the measured quantum state is already an eigenvector of the measurement operator. In this case, the state remains unchanged after the measurement. However, if the state is not an eigenvector, the measurement will collapse the state to one of the eigenvectors, destroying the original state in the process.

- **Measurement-induced Entanglement:** Projective measurements can induce entanglement between two or more quantum systems. This property is useful for preparing entangled states and implementing quantum algorithms that rely on entanglement.

- **No-cloning Theorem:** Due to the irreversibility of projective measurements, it is not possible to create a perfect copy of an unknown quantum state. This property, known as the no-cloning theorem, is a fundamental constraint in quantum information theory and has important implications for quantum cryptography and quantum error correction.

11.4 POVM Measurements

This section provides a detailed description of POVM (Positive Operator-Valued Measure) measurements in quantum computing. Unlike projective measurements, which are based on the eigenstates of a Hermitian operator, POVMs are a more general way to describe measurements in quantum mechanics. They can be applied to scenarios where the measurement process is not ideal or where the measurement outcomes are not orthogonal. This description covers the fundamentals of POVM measurements, their mathematical representation, and their properties. Unlike projective measurements, POVM measurements can describe non-orthogonal measurement outcomes and non-unitary measurement processes.

11.4.1 Mathematical Representation

A POVM measurement is represented by a set of positive semi-definite operators $\{E_i\}$, called POVM elements, which act on the quantum state space. These elements must satisfy the following conditions:

$$E_i \geq 0 \tag{103}$$

$$\sum_i E_i = I \tag{104}$$

where I is the identity operator.

11.4.2 Measurement Outcomes and Probabilities

When a quantum state $|\psi\rangle$ is measured using a POVM $\{E_i\}$, the probability of obtaining the outcome i is given by:

$$p(i) = \langle\psi|E_i|\psi\rangle \tag{105}$$

The post-measurement state $|\psi_i\rangle$ can be obtained by applying an appropriate quantum operation, which may be different for each outcome. However, unlike projective measurements, the post-measurement state is not uniquely determined by the POVM elements alone.

11.4.3 Properties of POVM Measurements

POVM measurements have several important properties that make them useful in quantum computing:

- **Generality:** POVM measurements are more general than projective measurements, as they can describe non-orthogonal measurement outcomes and non-unitary measurement processes. This makes them suitable for a wide range of scenarios, including open quantum systems, quantum error correction, and quantum cryptography.

- **Optimality:** In some situations, POVM measurements can provide optimal discrimination between non-orthogonal quantum states. This property is important for various quantum information processing tasks, such as quantum state discrimination, quantum cloning, and quantum communication.

- **Physical Realizability:** POVM measurements can be realized using a combination of unitary operations, ancillary quantum systems, and projective measurements. This makes them physically realizable in practice, which is essential for implementing quantum algorithms and protocols that rely on generalized measurements.

- **Connection to Projective Measurements:** Every projective measurement can be represented as a POVM measurement, making POVMs a natural generalization of projective measurements. In particular, a projective measurement can be described by a POVM with elements $E_i = P_i$, where P_i are the projectors corresponding to the measurement operator's eigenvectors.

11.5 Entangled States and Measurements

When measuring entangled states, the outcomes of the measurements on the individual qubits are correlated. For example, consider the Bell state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{106}$$

When measuring the σ_z observable on both qubits, the possible outcomes are:

- Both qubits yield $\lambda_0 = 1$ with probability $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$, resulting in the state $|00\rangle$.

- Both qubits yield $\lambda_1 = -1$ with probability $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$, resulting in the state $|11\rangle$.

Notice that the outcomes are perfectly correlated, i.e., if one qubit yields λ_0, the other qubit will also yield λ_0, and if one qubit yields λ_1, the other qubit will also yield λ_1. This correlation is a result of the entanglement between the qubits.