COMP 458/558
Quantum Computing Algorithms

Micah Kepe

Table of Contents

Chapter 1 **Phase I: Introduction and Background** Page 2

1.1 Lecture 1: Overview of Quantum Computing Concepts 2
1.2 Lecture 2: Review of Linear Algebra Concepts 3
1.3 Lecture 3: Quantum Bits and Quantum States 7
1.4 Lecture 4: Quantum Gates and Transformations 11
1.5 Lecture 5: Other Quantum Gates, Measurement, Multi-Qubit Systems 15
1.6 Lecture 6: Multi-Qubit Gates and Circuit Construction 18
1.7 Lecture 7: More Multi-Qubit Gates, Reversibility Property, No-Cloning Theorem 21

Chapter **Appendix** Page 27

Chapter 1

Phase I: Introduction and Background

1.1 Lecture 1: Overview of Quantum Computing Concepts

Definition 1.1.1: Quantum Computing

Quantum computing is a computational paradigm leveraging quantum mechanical principles such as superposition, entanglement, and interference to perform computations that can surpass the capabilities of classical systems for specific tasks.
[a]

[a] Superposition allows quantum bits (qubits) to exist in multiple states simultaneously, and entanglement enables correlations between qubits even at a distance.

Historical Development of Quantum Computing

- **1980s-1990s:** Conception of quantum computing, with foundational ideas like the quantum Turing machine and quantum gates.
- **1990s-2000s:** Demonstration of key building blocks, such as quantum algorithms (e.g., Shor's and Grover's algorithms).
- **2016:** Emergence of quantum computing clouds, enabling access to quantum hardware via the internet.
- **2019:** First claims of **quantum advantage**, showcasing tasks where quantum computers outperform classical counterparts.
- **2024:** Increasing qubit counts and improvements in quantum error correction techniques.

Applications of Quantum Computing

Quantum computing offers **speedup** in areas such as:

1. **Quantum Simulation:** Applications in chemistry, physics, and materials science, such as simulating molecular energy levels and drug discovery.
2. **Security and Encryption:** Developing quantum-safe cryptographic protocols and random number generation.
3. **Search and Optimization:** Enhancing solutions for weather forecasting, financial modeling, traffic planning, and resource allocation.

Example 1.1.1 (Example: Quantum Speedup in Drug Discovery)

Drug discovery benefits from quantum simulation by enabling more accurate modeling of molecular interactions, which classical computers struggle to achieve efficiently.

Classical vs. Quantum Computing Paradigms

- **Classical Computing:** Utilizes traditional processing units (CPU, GPU, FPGA) and executes deterministic computations.
- **Quantum Computing:** Employs quantum processing units (QPU) with probabilistic computation based on quantum states.

Note:-

Note: Classical computing paradigms still dominate in tasks that require precision and deterministic results. Quantum computing excels in probabilistic or exponentially large state-space problems.

1.2 Lecture 2: Review of Linear Algebra Concepts

Linear algebra provides the foundation for manipulating quantum states, which are represented using vectors and matrices in a complex vector space.

Definition 1.2.1: Vectors: Row and Column Vectors

A **vector** is an ordered list of numbers, which can be represented as either a row or column vector. The components of vectors in quantum computing belong to the field of complex numbers ($\mathbb{C}$).

Column Vectors

A column vector is a vertical arrangement of numbers:

$$\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}, \quad v_i \in \mathbb{C}.$$

Row Vectors

A row vector is the complex conjugate transpose **vector** of a column vector:

$$\mathbf{v}^\dagger = \begin{bmatrix} \overline{v_1} & \overline{v_2} & \dots & \overline{v_n} \end{bmatrix}.$$

The adjoint of a column vector is a row vector, and vice versa. We represent the adjoint of a vector using the dagger symbol (†).

Dirac Notation

In quantum computing, vectors are represented using **Dirac notation** (bra-ket notation):

- **Ket** $|v\rangle$: Represents a column vector.
- **Bra** $\langle v|$: Represents the adjoint (conjugate transpose) of the ket.
- Example: $|v\rangle = \begin{bmatrix} 1+i \\ 2 \end{bmatrix}, \quad \langle v| = \begin{bmatrix} 1-i & 2 \end{bmatrix}.$

Definition 1.2.2: Euler's Formula

Euler's formula relates complex exponentials to trigonometric functions:

$$e^{i\omega} = \cos(\omega) + i\sin(\omega)$$

This is fundamental in representing quantum states and transformations.

Definition 1.2.3: Inner Product

The **inner product** of two vectors $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$ is defined as:

$$\langle \mathbf{v}, \mathbf{w} \rangle = \mathbf{v}^\dagger \mathbf{w} = \sum_{i=1}^{n} \overline{v_i} w_i$$

which measures the overlap between two quantum states.

Example 1.2.1 (Inner Product Example)

Given two vectors:

$$\mathbf{v} = \begin{bmatrix} 1 \\ i \end{bmatrix}, \quad \mathbf{w} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

The inner product is:

$$\langle \mathbf{v}, \mathbf{w} \rangle = \begin{bmatrix} 1 & -i \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 2 - i$$

We also have the following property that the inner product is equivalent to the square of the Euclidean norm of a vector:

$$\langle \mathbf{v}, \mathbf{v} \rangle = \|\mathbf{v}\|^2$$

Definition 1.2.4: Outer Product

The **outer product** of two vectors $\mathbf{v} \in \mathbb{C}^m$ and $\mathbf{w} \in \mathbb{C}^n$ produces an $m \times n$ matrix:

$$\mathbf{v}\mathbf{w}^\dagger = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{bmatrix} \begin{bmatrix} \overline{w_1} & \overline{w_2} & \dots & \overline{w_n} \end{bmatrix}$$

This operation is useful for constructing quantum operators.

Definition 1.2.5: Tensor Product

The **tensor product** (or Kronecker product) allows us to describe multi-qubit systems. Given two vectors:

$$\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}, \quad \mathbf{w} = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$$

Their tensor product is:

$$\mathbf{v} \otimes \mathbf{w} = \begin{bmatrix} v_1 w_1 \\ v_1 w_2 \\ v_2 w_1 \\ v_2 w_2 \end{bmatrix}$$

The tensor product expands the state space, allowing representation of entangled states.

Orthagonality

Two vectors $v, w \in \mathbb{C}^n$ are **orthogonal** if their inner product is zero:

$$\langle \mathbf{v}, \mathbf{w} \rangle = 0$$

Orthogonal vectors are linearly independent and span a subspace of the vector space. As you might remember from linear algebra, a set of orthogonal vectors can be used to construct an orthonormal basis, and any vector can be expressed as a linear combination of the basis vectors.

This will be useful when we cover the quantum bases in section 1.3.

Definition 1.2.6: Adjoint of a Matrix

The **adjoint** (or Hermitian conjugate) of a matrix A is obtained by taking the transpose and complex conjugate of each entry:

$$A^\dagger = \overline{A^T}$$

If A is:

$$A = \begin{bmatrix} 1 & i \\ 2 & 3 \end{bmatrix}$$

Then its adjoint is:

$$A^\dagger = \begin{bmatrix} 1 & 2 \\ -i & 3 \end{bmatrix}$$

Definition 1.2.7: Unitary Matrix

A square matrix U is called **unitary** if its adjoint is equal to its inverse:

$$U^\dagger U = I$$

where I is the identity matrix. Unitary matrices preserve the norm of quantum states and represent reversible quantum operations. Example:

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad U^\dagger U = I$$

Definition 1.2.8: Hermitian Matrix

A square matrix H is called **Hermitian** if it is equal to its adjoint:

$$H = H^\dagger$$

Hermitian matrices represent observable quantities in quantum mechanics and have real eigenvalues. Example:

$$H = \begin{bmatrix} 2 & i \\ -i & 2 \end{bmatrix}$$

Since $H^\dagger = H$, it is Hermitian.

Note:-

Hermitian matrices **can't** have complex numbers in their diagonal General case illustration:

$$M = \begin{bmatrix} a+ib & c+id \\ e+if & g+ih \end{bmatrix} \quad \Rightarrow \quad M^\dagger = \begin{bmatrix} a-ib & e-if \\ c-id & g-ih \end{bmatrix} \quad \Rightarrow \quad M \neq M^\dagger$$

$\therefore$ Hermitian matrices have real diagonal elements.

Additionally, the general matrix M shown above is Hermitian iff. $c = e, d = -f$

Hermitian matrices are unitary, but unitary matrices are not necessarily Hermitian:

$$H \to U, \quad U \nrightarrow H$$

Definition 1.2.9: Eigenvalues and Eigenvectors

For a square matrix $A \in \mathbb{C}^{n \times n}$, a vector $\mathbf{v} \neq \mathbf{0}$ is an **eigenvector** if:

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

where $\lambda \in \mathbb{C}$ is the **eigenvalue**. Eigenvalues provide insight into the structure of linear transformations. In Braket notation, the eigenvalue equation is:

$$A|\mathbf{v}\rangle = \lambda|\mathbf{v}\rangle$$

Example 1.2.2 (Example: Eigenvalues)

For the matrix

$$A = \begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}$$

The characteristic equation is:

$$\det(A - \lambda I) = (1-\lambda)^2 + 1 = 0$$

Solving gives eigenvalues $\lambda = 1 \pm i$.

Definition 1.2.10: Quantum Bits/ Qubits

A **qubit** can be defined mathematically as follows:

$$|\psi\rangle = \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} \in \mathbb{C}^2$$

where:

$$\alpha_1, \alpha_2 \in \mathbb{C} \quad \text{and} \quad |\alpha_1|^2 + |\alpha_2|^2 = 1$$

The first property ensures that the qubit is normalized, while the second property ensures that the qubit is in a superposition of the basis states.

The first universal basis that we will look at is the computational basis, which consists of the states $|0\rangle$ and $|1\rangle$:

$$\text{Zero state} = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{One state} = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

A quantum state vector $|\psi\rangle$ can be expressed as a linear combination of the basis states:

$$|\psi\rangle = \alpha_1 |0\rangle + \alpha_2 |1\rangle$$

Note:-

Properties of the computational basis:

- **The computational basis states are orthogonal:**

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

- **The computational basis states are normalized:**

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

Question 1

Show that any unitary matrix preserves the inner product of two vectors.

Solution: Since a unitary matrix satisfies $U^\dagger U = I$, we have:

$$\langle U\mathbf{v}, U\mathbf{w}\rangle = \mathbf{v}^\dagger (U^\dagger U)\mathbf{w} = \mathbf{v}^\dagger \mathbf{w}$$

Thus, inner products are preserved.

1.3 Lecture 3: Quantum Bits and Quantum States

Definition 1.3.1: Qubit

A **qubit** is the fundamental unit of quantum information. Unlike a classical bit, which is either 0 or 1, a qubit can exist in a **superposition** of states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{where } \alpha, \beta \in \mathbb{C} \text{ and } ||\alpha||^2 + ||\beta||^2 = 1$$

Key features of qubits include:

- **Superposition:** A qubit can exist simultaneously in multiple basis states.
- **Complex Amplitudes:** Coefficients α and β are complex numbers carrying magnitude and phase information.
- **Interference:** Quantum states can interfere constructively or destructively.
- **Entanglement:** Qubits can be correlated in ways that classical bits cannot.

Classical Computing Paradigms

Quantum computing introduces a fundamentally different computational model. Here are some key paradigms in classical computing that quantum computing challenges:

- **Deterministic Computing:** Uses discrete states (0 or 1) with predictable transitions.
- **Analog Computing:** Uses continuous values susceptible to noise accumulation.
- **Probabilistic Computing:** Represents probabilistic mixtures of states.

In contrast, for quantum computing:

- **Quantum Computing:** Allows coherent superposition with complex amplitudes and quantum interference.

Definition 1.3.2: Dirac Notation

Quantum states are represented using **Dirac notation** (bra-ket notation):

- **Ket:** $|0\rangle, |1\rangle$ represent computational basis states
- Computational basis vectors:

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

- General state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Definition 1.3.3: Basis States

Common qubit bases include:

- **Computational Basis:** $|0\rangle, |1\rangle$
- **Hadamard Basis:**

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$$

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

- **Phase/ Circular Polarization Basis:**

$$|L\rangle = |+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$

$$|R\rangle = |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

Bloch Sphere Representation

Definition 1.3.4: Bloch Sphere

A geometric representation of a single qubit state:

$$|\psi\rangle = \left[\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right]e^{i\gamma}$$

Where:

- $\theta \in [0, \pi]$ is the polar angle
- $\phi \in [0, 2\pi)$ is the azimuthal angle
- γ is a global phase, often omitted since it cannot be represented on the Bloch sphere directly

Aside

Bloch Sphere Conversion to Cartesian Coordinates:

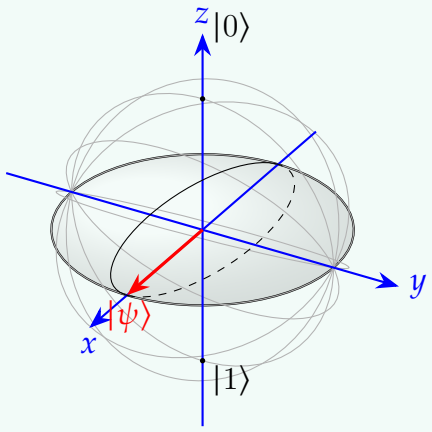
$$x = \sin\theta\cos\phi, \quad y = \sin\theta\sin\phi, \quad z = \cos\theta$$

Rearranging the Bloch sphere formula, we obtain that θ and ϕ can be expressed as:

$$\theta = 2\arccos(\alpha_1), \quad \phi = -i\ln\left(\frac{\alpha_2}{\sin\left(\frac{\theta}{2}\right)}\right)$$

Example 1.3.1 (Example Bloch Sphere Representation)

For the state $\theta = \frac{\pi}{2}, \phi = 0$:



Example 1.3.2 (Factoring Out the Global Phase)

Let's say that we have the following quantum state vector $|\psi\rangle$:

$$
\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2}}\left(i\,|0\rangle + |1\rangle\right) \\
&= \frac{i}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \\
&= \underbrace{i}_{\text{global phase}} \left(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\right)
\end{aligned}
$$

Quantum Measurement

When a qubit is measured:

- The quantum state *collapses* to an eigenstate
- Measurement probability depends on squared amplitude
- Computational basis measurement probabilities:

$$P(0) = |\alpha|^2, \quad P(1) = |\beta|^2$$

- Post-measurement state:

$$\boxed{|\psi_{\text{new}}\rangle = \frac{|b\rangle\langle b|\psi\rangle}{\sqrt{P(b)}}}$$

Example 1.3.3 (Measurement Example)

For the state $|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$:

- Probability of measuring $|0\rangle$: $P(0) = \frac{1}{3}$
- Probability of measuring $|1\rangle$: $P(1) = \frac{2}{3}$

Question 2: Orthonormality Check

Verify the inner products of basis states:

$$
\begin{aligned}
\langle 0|1\rangle &= 0 \\
\langle 0|0\rangle &= 1 \\
\langle +|+\rangle &= 1 \\
\langle +|-\rangle &= 0
\end{aligned}
$$

Solution: These relations hold due to the orthonormal nature of quantum basis states.

Note:-

Quantum Bases and Their θ and ϕ Values:

- **Computational Basis:** $|0\rangle \to \theta = 0, \phi = 0, \quad |1\rangle \to \theta = \pi, \phi = 0$
- **Hadamard Basis:** $|+\rangle \to \theta = \frac{\pi}{2}, \phi = 0, \quad |-\rangle \to \theta = \frac{\pi}{2}, \phi = \pi$
- **Phase Basis:** $|L\rangle = |+i\rangle \to \theta = \frac{\pi}{2}, \phi = \frac{\pi}{2}, \quad |R\rangle = |-i\rangle \to \theta = \frac{\pi}{2}, \phi = -\frac{\pi}{2}$

1.4 Lecture 4: Quantum Gates and Transformations

Quantum gates manipulate qubits through unitary transformations, preserving quantum information and enabling quantum computation. This section explores key quantum operations, their mathematical properties, and circuit representations.

Definition 1.4.1: Qubit Superposition and Hilbert Space

A **qubit** exists in a complex vector space called a **Hilbert space**. The state of a qubit is given by:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{where } \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1.$$

Measurement and Superposition Collapse

When a qubit is measured in the computational basis $\{|0\rangle, |1\rangle\}$, it collapses to one of the basis states with probability:

$$\boxed{P(0) = \|\alpha_1\|^2, \quad P(1) = \|\alpha_2\|^2.}$$

The post-measurement state is:

$$\boxed{|\psi_{\text{measurement}}\rangle = \frac{|b\rangle\langle b|\psi\rangle}{\sqrt{P(b)}}}$$

where $b \in \{0, 1\}$. This formula captures the quantum measurement postulate and ensures proper normalization of the post-measurement state.

In the computational basis, the probability of measuring $|b\rangle$ is:

$$\boxed{P(b) = \left\|\langle b|\psi\rangle\right\|^2}$$

Note:-

Probability Properties of Measurement:

$$P(0) = 1 - P(1)$$
$$P(+) = 1 - P(-)$$
$$P(+i) = 1 - P(-i)$$

Quantum Gates and Operations

Quantum gates are unitary matrices that transform qubits. A general qubit transformation is given by:

$$|\psi_{\text{final}}\rangle = U|\psi_{\text{initial}}\rangle$$

where U is a unitary matrix satisfying $U^\dagger U = I$. Key properties of quantum gates include:

- **Reversibility:** All quantum operations are reversible due to unitarity
- **Preservation of Norm:** The normalization condition $|\alpha|^2 + |\beta|^2 = 1$ is preserved
- **Linearity:** Gates act linearly on superposition states

Definition 1.4.2: Rotation Gates

Rotation gates rotate a qubit state around the Bloch sphere:

- **Rotation about X-axis:**

$$\boxed{R_X(\omega) = \begin{bmatrix} \cos\frac{\omega}{2} & -i\sin\frac{\omega}{2} \\ -i\sin\frac{\omega}{2} & \cos\frac{\omega}{2} \end{bmatrix}}$$

  Effect: Rotates state by angle ω around X-axis

- **Rotation about Y-axis:**

$$\boxed{R_Y(\omega) = \begin{bmatrix} \cos\frac{\omega}{2} & -\sin\frac{\omega}{2} \\ \sin\frac{\omega}{2} & \cos\frac{\omega}{2} \end{bmatrix}}$$

  Effect: Rotates state by angle ω around Y-axis

- **Rotation about Z-axis:**

$$\boxed{R_Z(\omega) = \begin{bmatrix} e^{-i\omega/2} & 0 \\ 0 & e^{i\omega/2} \end{bmatrix}}$$

  Effect: Adds a relative phase between $|0\rangle$ and $|1\rangle$ components

Definition 1.4.3: Pauli Matrices and Gates

The **Pauli matrices** define fundamental quantum operations:

- **Pauli-X (NOT Gate, Bit-Flip):**

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

  Effect: $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$

- **Pauli-Y (Combination of X and Z with phase):**

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

  Effect: $Y|0\rangle = i|1\rangle$, $Y|1\rangle = -i|0\rangle$

- **Pauli-Z (Phase-Flip Gate):**

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

  Effect: $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$

Aside

Each of these matrices is both **Hermitian** ($A = A^\dagger$) and **unitary** ($A^\dagger A = I$).

Important relationships:

- $X^2 = Y^2 = Z^2 = I$
- $XY = iZ$, $YZ = iX$, $ZX = iY$
- $YX = -iZ$, $ZY = -iX$, $XZ = -iY$

Circuit Notation

Quantum circuits visually represent quantum operations. Each qubit is represented as a horizontal line, and gates are applied sequentially from left to right. Important circuit elements include: [1]

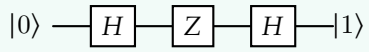
- **Single-qubit gates:** Represented as boxes with gate symbols
- **Measurements:** Depicted with a meter symbol
- **Time flow:** Left to right in circuits (***opposite of matrix multiplication order***) [2]

Example 1.4.1 (Example: Complex Circuit Analysis)
Consider the circuit applying the sequence HZH to $|0\rangle$:

[1] For rendering quantum circuits, consider using the `quantikz` package in LaTeX.
[2] Dor example, the circuit U_1U_2 corresponds to the matrix product U_2U_1.

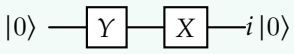
$$|\psi_1\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|\psi_2\rangle = Z|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$|\psi_3\rangle = H|\psi_2\rangle = |1\rangle$$

This sequence performs a NOT operation on $|0\rangle$ using only Hadamard and Phase-flip gates.



Example 1.4.2 (Another Circuit Example)

$$XY|0\rangle = X\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}$$
$$= \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0\\i\end{bmatrix}$$
$$= \begin{bmatrix}i\\0\end{bmatrix} = i|1\rangle$$



Question 3: Exercise 1

Apply the sequence SXH to $|0\rangle$ and calculate:

- The final state vector
- The probabilities of measuring $|0\rangle$ and $|1\rangle$
- The possible post-measurement states

Solution:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$XH|0\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$SXH|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$

Therefore:

- Final state: $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
- Measurement probabilities: $P(0) = P(1) = \frac{1}{2}$
- Post-measurement states: Either $|0\rangle$ or $|1\rangle$ with equal probability

Question 4: Exercise 2

Show that the Hadamard gate is its own inverse by calculating H^2.

Solution:

$$H^2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Question 5: Exercise 3

Calculate the effect of applying $R_Z(\pi/2)$ to the state $|+\rangle$.

Solution:

$$R_Z(\pi/2)|+\rangle = \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix} = |+i\rangle$$

1.5 Lecture 5: Other Quantum Gates, Measurement, Multi-Qubit Systems

Definition 1.5.1: Single-Qubit Gates

Quantum gates manipulate individual qubits. Single-qubit gates are represented by unitary matrices that operate on a single qubit.

The following are common single-qubit gates:

- **Hadamard Gate (H):**

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

Creates superposition: $\boxed{H|0\rangle = |+\rangle, H|1\rangle = |-\rangle}$

Properties:

  - Self-inverse: $H^2 = I$
  - Maps computational basis to $|\pm\rangle$ basis:

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

Note:-

$$H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle, \quad H|+\rangle = |0\rangle, \quad H|-\rangle = |1\rangle$$

- **Phase Gate (S):**

$$\boxed{S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}}$$

Adds a $\pi/2$ phase to $|1\rangle$, so it is also referred to as the "$\pi/4$ gate" due to $\theta/2$ term in the Bloch sphere equation.

Properties:

- **Unitary but not Hermitian**
- $S^2 = Z$
- Effect on $|+\rangle$: $\boxed{S|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)}$

- **T Gate:**

$$\boxed{T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}}$$

Adds a $\pi/4$ phase to $|1\rangle$, so it is also known as the "$\pi/8$ gate".

Properties:

- $T^2 = S$
- $T^4 = Z$
- Often used in quantum error correction

- **General Phase Gate** $P(\theta)$:

$$P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Generalizes S and T gates: $\boxed{S = P(\pi/2), T = P(\pi/4)}$

Example 1.5.1 (Example of Applying the Hadamard Gate)

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = |+\rangle$$

Note:-

The following properties arise from applying the Hadamard gate:

$$Z = HXH$$
$$X = HZH$$

Proof.

$$HXH = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$$

■

Back to Measurement

Measurement collapses quantum states to basis states with probabilities determined by amplitudes.

- **Z-basis:** Standard computational basis ($|0\rangle$, $|1\rangle$)

* For state $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$:

$$P(0) = ||\alpha||^2$$
$$P(1) = ||\beta||^2$$

- **X-basis:** Hadamard basis ($|+\rangle$, $|-\rangle$)
  * Measure in Z-basis after applying H gate
  * $P(+) = |\langle +|\psi\rangle|^2$
  * $P(-) = |\langle -|\psi\rangle|^2$
- **Y-basis:** Eigenstates of Y
  * $|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
  * $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

Multi-Qubit Systems

States for multiple qubits are represented as tensor products:

$$\boxed{\left|\psi\right\rangle = \sum_{k=0}^{k=2^n-1} \alpha_k \left|k\right\rangle, \quad \sum ||\alpha_k||^2 = 1}$$

Properties of tensor products:

- **Not commutative:** $(|0\rangle \otimes |1\rangle \neq |1\rangle \otimes |0\rangle)$
- Associative: $((|a\rangle \otimes |b\rangle) \otimes |c\rangle = |a\rangle \otimes (|b\rangle \otimes |c\rangle))$
- Distributive: $((\alpha|a\rangle + \beta|b\rangle) \otimes |c\rangle = \alpha(|a\rangle \otimes |c\rangle) + \beta(|b\rangle \otimes |c\rangle))$

Question 6: Exercise 1

Prove that the Hadamard gate is unitary and Hermitian.

Solution: To prove H is unitary and Hermitian:

$$H^\dagger = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = H$$
$$HH = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = I$$

Thus, H is both unitary ($HH^\dagger = I$) and Hermitian ($H = H^\dagger$).

Question 7: Exercise 2

For $\left|\psi\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, find measurement probabilities for $|00\rangle$ and $|11\rangle$.

Solution: For $\left|\psi\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

$$P(00) = |\langle 00|\,\psi\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$
$$P(11) = |\langle 11|\,\psi\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Question 8: Exercise 3

Determine if $U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$ is unitary.

Solution: To verify unitarity, compute $UU^\dagger$:

$$U^\dagger = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$$
$$UU^\dagger = \frac{1}{2}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\therefore$ U is unitary.

Question 9: Exercise 4

If we apply H $\otimes$ H to $|00\rangle$, what state do we get?

Solution:

$$\begin{aligned}(H \otimes H)\,|00\rangle &= (H\,|0\rangle) \otimes (H\,|0\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\end{aligned}$$

This creates an equal superposition of all two-qubit basis states.

1.6 Lecture 6: Multi-Qubit Gates and Circuit Construction

n-qubit gates are unitary transformations that operate on n qubits. This section explores key multi-qubit gates, their properties, and how to construct quantum circuits using these gates.

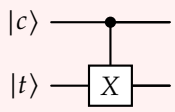
Controlled Gates

Definition 1.6.1: Controlled X Gate

(CNOT) is a two-qubit gate that flips the target qubit if the control qubit is in state $|1\rangle$, and does nothing if the control qubit is in state $|0\rangle$. The matrix representation of CNOT is given by:

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

Representing the gate in a circuit diagram:



The control qubit is denoted by $|c\rangle$ and the target qubit is denoted by $|t\rangle$.

Applying the CNOT gate to a two-qubit state $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$:

$$\begin{aligned} CX|00\rangle &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle \\ CX|01\rangle &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle \\ CX|10\rangle &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle \\ CX|11\rangle &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle \end{aligned} \tag{1.1}$$

Controlled-Z Gate

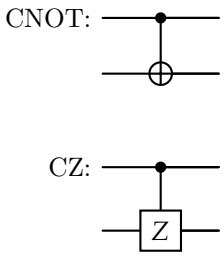
Definition 1.6.2: Controlled-Z Gate

(CZ) applies a phase flip if both qubits are in state $|1\rangle$:

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

Circuit Representations

The standard circuit representations for these multi-qubit gates are:



Tensor Product Ordering and Circuit Representations

When converting quantum circuits to mathematical expressions, it's important to understand that tensor products are not commutative: $A \otimes B \neq B \otimes A$ in general. However, we can modify the ordering of tensor products in our mathematical representation as long as we maintain the dependencies established by the circuit diagram. This leads to multiple valid mathematical representations of the same quantum circuit.

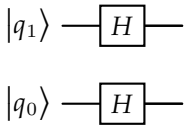
Definition 1.6.3: Bit Ordering Convention

Due to the non-commutativity of tensor products, we adopt the convention of representing qubits from most significant to least significant in our mathematical expressions. For an n-qubit system:

$$|q_{n-1}q_{n-2}...q_1q_0\rangle = |q_{n-1}\rangle \otimes |q_{n-2}\rangle \otimes ... \otimes |q_1\rangle \otimes |q_0\rangle$$

where q_0 is the least significant qubit.

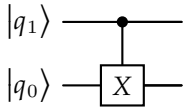
For example, consider a circuit with two Hadamard gates applied to different qubits:



This circuit can be represented mathematically in equivalent ways:

$$(H \otimes H)|q_1q_0\rangle = (H|q_1\rangle) \otimes (H|q_0\rangle) = H|q_1\rangle \otimes H|q_0\rangle$$

When gates have dependencies (like controlled operations), the ordering must respect these dependencies. For the CNOT gate:



The mathematical representation must preserve the control-target relationship, though intermediate calculations may use different but equivalent orderings:

$$CNOT_{1,0}|q_1q_0\rangle = CNOT(|q_1\rangle \otimes |q_0\rangle)$$

This flexibility in representation, while maintaining functional equivalence, is particularly useful when analyzing complex quantum circuits or optimizing quantum computations.

1.7 Lecture 7: More Multi-Qubit Gates, Reversibility Property, No-Cloning Theorem

Review Questions

Question 10: Number of Measurement Bases

How many different bases can we measure a n-qubit system in?

Solution: **Infinite**

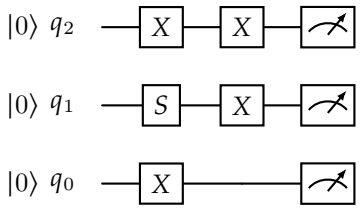
$$P(b) = \left\| \langle b|\psi\rangle \right\|^2$$

In quantum mechanics, a measurement basis for an n-qubit system is a set of orthonormal basis states in a 2^n-dimensional Hilbert space. The most common measurement basis is the **computational basis**, given by $\{|0\rangle, |1\rangle\}^{\otimes n}$. However, we can measure in **any** orthonormal basis.

The space of all possible measurement bases corresponds to the space of all possible orthonormal bases, which is parameterized by the unitary group $U(2^n)$. The set of all 2^n-dimensional orthonormal bases is described by the unitary group $U(2^n)$, modulo the global phase $U(1)$. Since this space is continuous and has infinitely many parameters, there exist an **infinite** number of measurement bases.

Question 11: Output of Quantum Circuit

What is the output quantum state of the following quantum circuit:



Solution: 011

- For q_2, the two X gates essentially cancel each other out as the gate is Hermitian ($XX = I$).
- For q_1, the S gate does not affect the starting state $|0\rangle$, and then the X gate flips the signal to $|1\rangle$.
- For q_0, the X gate simply flips the signal from $|0\rangle$ to $|1\rangle$.

Remembering that we read the diagram top-down as the most significant bit to the least significant bit, respectively, the output is 001.

More Multi-Qubit Gates

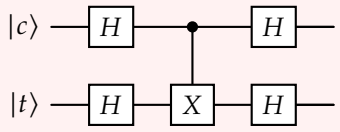
More 2-Qubit Gates

Definition 1.7.1: $CX(q_0 \to q_1)$ Gate

The control and target qubits of a CNOT gate can be swapped using Hadamard gates:

$$(H \otimes H) \cdot CNOT_{\text{control,target}} \cdot (H \otimes H) = CNOT_{\text{target,control}}$$

This transformation can be visualized in a circuit diagram:



The $CX(q_0 \to q_1)$ gate, also known as $CNOT_{target,control}$, is a variant of the CNOT gate where the control and target qubits are swapped. Its matrix representation is:

$$CNOT_{target,control} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

This gate flips the target qubit (q_1) if the control qubit (q_0) is in state $|1\rangle$.

Derivation of the $CX(q_0 \to q_1)$ Gate

The control and target qubits of a CNOT gate can be swapped using Hadamard (H) gates applied to both qubits. Mathematically, this operation is represented as:

$$(H \otimes H) \cdot \text{CNOT}_{\text{control,target}} \cdot (H \otimes H) = \text{CNOT}_{\text{target,control}}$$

The transformed CNOT gate is:

$$(H \otimes H) \cdot \text{CNOT} \cdot (H \otimes H).$$

Step 1: Compute CNOT $\cdot (H \otimes H)$
First, multiply the CNOT matrix with $H \otimes H$:

$$\text{CNOT} \cdot (H \otimes H) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

This results in:

$$\text{CNOT} \cdot (H \otimes H) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

Notice that the third and fourth rows of the matrix switch places due to the CNOT gate's effect.

Step 2: Multiply $(H \otimes H)$ to the Above Result
Now, multiply $H \otimes H$ from the left:

$$(H \otimes H) \cdot \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

Expanding this:

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \cdot \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

After computation, the resulting matrix is:

$$\text{CNOT}_{\text{target,control}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

This matrix corresponds to the CNOT gate with the control and target qubits swapped.

SWAP Gate

Definition 1.7.2: SWAP Gate

The SWAP gate exchanges the states of two qubits. Its matrix representation is:

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

The action of SWAP on basis states is given by:

$$SWAP\,|ab\rangle = |ba\rangle\,, \quad a, b \in \{0, 1\}$$

Effects of SWAP Gate The SWAP gate interchanges the states of two qubits. For any 2-qubit computational basis state, its action is:

Note:-

$$SWAP\ |00\rangle = |00\rangle\,,$$
$$SWAP\ |01\rangle = |10\rangle\,,$$
$$SWAP\ |10\rangle = |01\rangle\,,$$
$$SWAP\ |11\rangle = |11\rangle\,.$$

Thus, for any superposition of 2-qubit states, the SWAP gate exchanges the amplitudes corresponding to each qubit's position.

n-Qubit Gates

Before we just looked at the 2-qubit version of the Controlled X gate, but it extends to n-qubits.

Toffoli Gate

Definition 1.7.3: Toffoli Gate

(CCX) is a three-qubit gate with two control qubits and one target qubit. Its matrix representation is:

$$\textsc{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The Toffoli gate is Hermitian and only flips the target qubit if both control qubits are in state $|1\rangle$.

Effects of Toffoli Gate The Toffoli (CCX) gate acts on a 3-qubit system, where the first two qubits serve as control qubits and the third is the target. Its effect on the computational basis states is:

Note:-

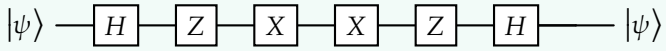
$$\begin{aligned} \text{Toffoli } |000\rangle &= |000\rangle\,, \\ \text{Toffoli } |001\rangle &= |001\rangle\,, \\ \text{Toffoli } |010\rangle &= |010\rangle\,, \\ \text{Toffoli } |011\rangle &= |011\rangle\,, \\ \text{Toffoli } |100\rangle &= |100\rangle\,, \\ \text{Toffoli } |101\rangle &= |101\rangle\,, \\ \text{Toffoli } |110\rangle &= |111\rangle\,, \\ \text{Toffoli } |111\rangle &= |110\rangle\,. \end{aligned}$$

In essence, the target qubit is flipped only when both control qubits are in the $|1\rangle$ state; otherwise, the state remains unchanged.

As you would expect, multi-controlled X gates are Hermitian.

Example 1.7.1 (Quantum Circuit Showing Hermitian Property)

A quantum circuit composed of Hermitian gates (e.g., X, Z, H) will cancel out when the circuit is reversed, resulting in the identity operation.



In this example, the quantum circuit consists of a sequence of Hermitian gates: the Hadamard (H), Pauli-Z (Z), and Pauli-X (X) gates. These gates satisfy the property:

$$H = H^\dagger, \quad X = X^\dagger, \quad Z = Z^\dagger$$

Since these gates are their own inverses (*i.e.,* $HH = I$, $XX = I$, and $ZZ = I$), if we apply the same sequence of gates in reverse order, they cancel out, leaving the identity operation.
The circuit above first applies H, then Z, then X twice (which cancels itself out), then Z again, and finally H again. This results in:

$$HZXXZH = I$$

Hence, the overall operation on the qubit is the identity transformation, meaning the final state remains the same as the initial state $|\psi\rangle$.

Definition 1.7.4: Reversibility Property of Quantum Computing

Quantum operations are inherently reversible due to the **unitary** nature of quantum gates. This means that any quantum circuit can be reversed by applying the inverse of each gate in the reverse order. Mathematically, if a quantum circuit is represented by a unitary matrix U, its reverse is represented by $U^\dagger$, and since quantum gates are unitary, they satisfy the property:

$$U^\dagger U = UU^\dagger = I$$

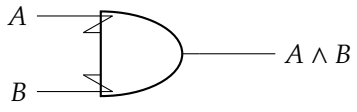
This reversibility is a fundamental difference between quantum and classical computing and is directly tied to the **no information loss** principle in quantum mechanics.

Why Reversibility is Important: In classical computing, operations such as the AND gate lose information. For example, given the output of an AND gate, we cannot uniquely determine the original input:

$$(0,0) \mapsto 0, \quad (0,1) \mapsto 0, \quad (1,0) \mapsto 0, \quad (1,1) \mapsto 1$$

Since multiple inputs can produce the same output, information is lost, making the operation **irreversible**.

Classical AND Gate (Irreversible)

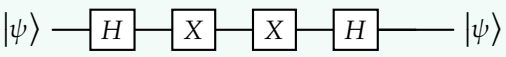


A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

This classical AND gate demonstrates information loss (irreversibility) because multiple distinct input states map to the same output state. As shown in the truth table, three different input combinations (0,0), (0,1), and (1,0) all produce the same output 0. Given only the output 0, it is impossible to determine which of these three input states generated it—this loss of information about the system's initial state makes the operation irreversible.

Quantum Reversibility: In contrast, **quantum gates are always unitary**, meaning they preserve the total amount of information. Given the final state of a quantum system, we can always determine its previous state by applying the inverse transformation. This is why quantum circuits must be composed of reversible operations.

Example 1.7.2 (Example of a Reversible Quantum Circuit:)



In this example, the quantum circuit consists of a sequence of unitary gates: the Hadamard (H) and the Pauli-X (X) gates. These gates satisfy:

$$H = H^\dagger, \quad X = X^\dagger$$

Since these gates are their own inverses (*i.e.*, $HH = I$ and $XX = I$), if we apply the same sequence of gates in reverse order, they cancel out, leaving the identity operation:

$$HXXH = I$$

Key Properties of Reversible Quantum Gates:

1. Every quantum gate U has an inverse $U^\dagger$, ensuring that no information is lost.

2. The composition of unitary gates remains unitary, preserving reversibility.
3. Classical **Toffoli and Fredkin gates** are reversible and can be used to construct reversible classical circuits, which is why they are also fundamental in quantum computing.
4. Measurement is **not** reversible, as it collapses the quantum state and introduces information loss.

The reversibility of quantum computing is crucial for error correction, fault-tolerant quantum computation, and simulating physical systems where information is conserved.

Example 1.7.3 (Example of Reversing a Quantum Circuit)
Consider a circuit composed of gates A, B, and C:

$$|\psi_{\text{final}}\rangle = CBA|\psi_{\text{initial}}\rangle.$$

The reverse circuit applies $C^\dagger$, $B^\dagger$, and $A^\dagger$ in reverse order:

$$|\psi_{\text{reversed}}\rangle = A^\dagger B^\dagger C^\dagger |\psi_{\text{final}}\rangle = A^\dagger B^\dagger C^\dagger CBA|\psi_{\text{initial}}\rangle = |\psi_{\text{initial}}\rangle.$$

Definition 1.7.5: Quantum No-Cloning Theorem

The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state. This result follows directly from the linearity of quantum mechanics.

Example 1.7.4 (Simple 2-Qubit Example)
Consider two qubits in states $|\psi\rangle$ and $|0\rangle$. The no-cloning theorem implies that there is no unitary operation U such that:

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle .$$

Proof. **Proof of the Quantum No-Cloning Theorem**
Assume a unitary operator U exists that can clone an arbitrary quantum state $|\psi\rangle$. Then, for two different states $|\psi\rangle$ and $|\phi\rangle$, we would have:

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle ,$$

$$U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle .$$

Now, consider the superposition state $|\xi\rangle = a|\psi\rangle + b|\phi\rangle$. Applying U to $|\xi\rangle \otimes |0\rangle$ should produce:

$$U(|\xi\rangle \otimes |0\rangle) = aU(|\psi\rangle \otimes |0\rangle) + bU(|\phi\rangle \otimes |0\rangle) = a(|\psi\rangle \otimes |\psi\rangle) + b(|\phi\rangle \otimes |\phi\rangle).$$

However, if U could clone $|\xi\rangle$, the result should be:

$$U(|\xi\rangle \otimes |0\rangle) = |\xi\rangle \otimes |\xi\rangle = (a|\psi\rangle + b|\phi\rangle) \otimes (a|\psi\rangle + b|\phi\rangle).$$

Expanding this, we get:

$$|\xi\rangle \otimes |\xi\rangle = a^2(|\psi\rangle \otimes |\psi\rangle) + ab(|\psi\rangle \otimes |\phi\rangle) + ab(|\phi\rangle \otimes |\psi\rangle) + b^2(|\phi\rangle \otimes |\phi\rangle).$$

Comparing the two expressions, we see that the terms $|\psi\rangle \otimes |\phi\rangle$ and $|\phi\rangle \otimes |\psi\rangle$ appear in the expanded $|\xi\rangle \otimes |\xi\rangle$, but they do not appear in $a(|\psi\rangle \otimes |\psi\rangle) + b(|\phi\rangle \otimes |\phi\rangle)$. This inconsistency demonstrates that a unitary operator U cannot clone an arbitrary quantum state, proving the no-cloning theorem. ■

Appendix

Bloch sphere, 9
  azimuthal angle, 9
  Cartesian coordinates conversion, 9
  global phase, 9
  polar angle, 9

Circuit notation, 13
  multi-qubit gates, 19
classical computing, 3, 8

Euler's formula, 3

matrix
  eigenvalue, 6
  eigenvalue equation, 6
  Hermitian, 6
  Pauli matrices, 12
  unitary, 5
multi-qubit systems, 17

quantum gates, 11
  n-qubit gates, 23
  multi-qubit gates, 18
    CNOT with swapped target and control, 22
    controlled gates, 19
    controlled-Z gate, 19
    SWAP gate, 23
    Toffoli gate, 23
  NOT gate, 13
  Pauli-Y gate, 13
  Phase-Flip gate, 13
  properties, 11
  rotation gates, 11
    X-axis, 12
    Y-axis, 12
    Z-axis, 12
  single-qubit gates, 15
    General Phase gate, 16
    Hadamard gate, 15
    Phase gate, 15
    T gate, 16
quantum measurement, 10, 16
  measurement bases, 16
  properties, 11
Quantum No-Cloning Theorem, 26
  proof, 26
qubit, 7
  properties, 7
  superposition, 11

Reversibility Property of Quantum Computing, 25

superposition, 2, 7

universal bases
  computational, 7, 8
    angles, 10
    properties, 7
  Hadamard basis, 8
    angles, 10
  phase basis, 8
    angles, 10
univesal basis
  computational
    measurement, 11

vector, 3
  adjoint, 3
  column, see ket 3
  dagger, see adjoint 3
  Dirac notation, 3, 8
    bra, 3
    ket, 3
  eigenvector, 6
  Euclidean norm, 4
  inner product, 4
  orthogonality, 4
  outer product, 4
  tensor product, 4
    properties, 17