COMP 458/558
Quantum Computing Algorithms

Micah Kepe

Contents

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 (adjoint) of a column vector:

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

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.

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.

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.

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.

Example 1.2.1 (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 $\lambda = 1 \pm i$.

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.

Definition 1.3.2: Classical Computing Paradigms

Quantum computing introduces a fundamentally different computational model:

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

Definition 1.3.3: 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 1.3.4: Basis States

Common qubit bases include:

- **Computational Basis:** $|0\rangle, |1\rangle$
- **Hadamard Basis:**
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
- **Circular Polarization Basis:**
$$|L\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad |R\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

Definition 1.3.5: Bloch Sphere

A geometric representation of a single qubit state:

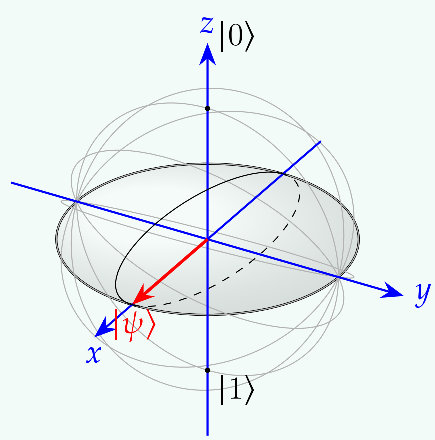
$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

Where:

- $\theta \in [0, \pi]$ is the polar angle
- $\phi \in [0, 2\pi)$ is the azimuthal angle
- Cartesian coordinates:
$$x = \sin\theta\cos\phi, \quad y = \sin\theta\sin\phi, \quad z = \cos\theta$$

Example 1.3.1 (Example Bloch Sphere Representation)

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



Definition 1.3.6: 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:
$$|\psi_{\text{new}}\rangle = \frac{|b\rangle\langle b|\psi\rangle}{\sqrt{P(b)}}$$

Example 1.3.2 (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:

$$\langle 0|1\rangle = 0$$
$$\langle 0|0\rangle = 1$$
$$\langle +|+\rangle = 1$$
$$\langle +|-\rangle = 0$$

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

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:

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

The computational basis states are represented as:

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

Definition 1.4.2: 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:

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

The post-measurement state is:

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

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

Definition 1.4.3: Important Quantum States

Several quantum states are particularly important in quantum computing:

- **Computational Basis States:** $|0\rangle$ and $|1\rangle$
- **Plus/Minus States:**
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
- **Complex Superposition States:**
$$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

Example 1.4.1 (Example: Equal Superposition State)
A qubit initially in state $|0\rangle$ is transformed into an equal superposition using the Hadamard gate:

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

Measuring this state results in either $|0\rangle$ or $|1\rangle$ with equal probability $P(0) = P(1) = \frac{1}{2}$.
Similarly, applying Hadamard to $|1\rangle$:

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

Definition 1.4.4: 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 1.4.5: Rotation Gates

Rotation gates rotate a qubit state around the Bloch sphere:

- **Rotation about X-axis:**
$$R_X(\omega) = \begin{bmatrix} \cos\frac{\omega}{2} & -i\sin\frac{\omega}{2} \\ -i\sin\frac{\omega}{2} & \cos\frac{\omega}{2} \end{bmatrix}$$
Effect: Rotates state by angle ω around X-axis
- **Rotation about Y-axis:**
$$R_Y(\omega) = \begin{bmatrix} \cos\frac{\omega}{2} & -\sin\frac{\omega}{2} \\ \sin\frac{\omega}{2} & \cos\frac{\omega}{2} \end{bmatrix}$$
Effect: Rotates state by angle ω around Y-axis
- **Rotation about Z-axis:**
$$R_Z(\omega) = \begin{bmatrix} e^{-i\omega/2} & 0 \\ 0 & e^{i\omega/2} \end{bmatrix}$$
Effect: Adds a relative phase between $|0\rangle$ and $|1\rangle$ components

Special cases:

- $R_X(\pi) = iX$
- $R_Y(\pi) = iY$
- $R_Z(\pi) = iZ$

Definition 1.4.6: 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: $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$

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

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

Definition 1.4.7: Additional Important Gates

- **Hadamard Gate (H):**
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$
Creates superposition states: $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$
- **Phase Gate (S):**
$$S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$$
Adds a $\pi/2$ phase to $|1\rangle$
- **T Gate:**
$$T = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$$
Adds a $\pi/4$ phase to $|1\rangle$

Definition 1.4.8: 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:

- **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)
- **Initial states:** Usually started in $|0\rangle$ unless specified otherwise

Example 1.4.2 (Example: Complex Circuit Analysis)
Consider the circuit applying the sequence HZH to $|0\rangle$:

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

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

Definition 1.4.9: Measurement in Quantum Circuits

Measurement collapses a quantum state to a basis state with probabilities determined by the squared magnitudes of its coefficients. For a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

- Probability of measuring $|0\rangle$: $P(0) = |\alpha|^2$
- Probability of measuring $|1\rangle$: $P(1) = |\beta|^2$
- Post-measurement state is the measured basis state
- Multiple measurements of identically prepared states give statistical distributions

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

Question 4: Exercise 2

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

Question 5: Exercise 3

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

Solution: Exercise 1 Solution:

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

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

1.5 Lecture 5: TBD

Chapter 2

Phase II: Fundamentals of Quantum Algorithms

Chapter 3

Phase III: Advanced Quantum Algorithms

Chapter 4

Phase IV: Special Topics in Quantum Computing

Chapter 5

Phase V: Concluding Lectures