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

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:

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

Definition 1.2.2: Inner Product

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

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

Example 1.2.1 (Example: Inner Product)

Let $\mathbf{v} = \begin{bmatrix} 1+i \\ 2 \end{bmatrix}$ and $\mathbf{w} = \begin{bmatrix} 3 \\ i \end{bmatrix}$. Then:

$$\langle \mathbf{v}, \mathbf{w} \rangle = (1-i)(3) + (2)(i) = 3 - 3i + 2i = 3 - i.$$

Definition 1.2.3: 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:

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

Definition 1.2.4: Orthogonality

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

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

Example 1.2.2 (Example: Orthogonality)

Let $\mathbf{v} = \begin{bmatrix} 1 \\ i \end{bmatrix}$ and $\mathbf{w} = \begin{bmatrix} i \\ 1 \end{bmatrix}$. Then:

$$\langle \mathbf{v}, \mathbf{w} \rangle = (1)(i) + (i)(1) = i - i = 0.$$

Definition 1.2.5: 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**.

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:

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

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 1.3.1 (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 1: 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.

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