Lecture 1: Historical Context and the Single Qubit

Mathematical Foundations

Moody T. Chu

NC State University

Lecture Overview

The Convergence of Disciplines

Quantum information science sits at the intersection of four major fields:

- **Quantum Mechanics:** The underlying physics governing behavior at the atomic and subatomic scale.
- **Computer Science:** The theory of computation, complexity, and algorithms.
- **Information Theory:** Mathematical limits of communication, compression, and noise.
- **Cryptography:** The science of secure communication and privacy.

Together these fields give rise to fundamentally new models of computation that exploit quantum phenomena.

The Birth of Quantum Mechanics

Classical physics broke down at the turn of the 20th century:

- The **ultraviolet catastrophe** (Rayleigh–Jeans law) predicted infinite energy radiated by a blackbody — clearly unphysical.
- Planck (1900) resolved this by postulating that energy is emitted in discrete quanta: $E = h\nu$.
- Einstein's photoelectric effect (1905) confirmed that light itself is quantized.
- Bohr, Heisenberg, Schrödinger, and Dirac developed the full mathematical framework in the 1920s.

The result: nature is *fundamentally probabilistic* at small scales, described by *state vectors* and *linear operators*, not classical trajectories.

The Qubit: A Mathematical Definition

- A **qubit** is the fundamental unit of quantum information — the quantum analogue of a classical bit.
- Mathematically, it is a *unit vector* in a two-dimensional complex Hilbert space $\mathbb{C}^2$.
- We designate two special orthonormal vectors as the **computational basis states**:

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

- These satisfy $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = 0$.

The Hilbert Space $\mathbb{C}^2$

- $\mathbb{C}^2$ is equipped with the standard complex inner product:

$$\langle u|v\rangle = \bar{u}_1 v_1 + \bar{u}_2 v_2,$$

  where $\bar{u}_i$ denotes complex conjugation.
- The inner product induces a norm: $\| \, |\psi\rangle \, \|^2 = \langle\psi|\psi\rangle$.
- A qubit state must be **normalized**: $\langle\psi|\psi\rangle = 1$.
- The computational basis $\{|0\rangle, |1\rangle\}$ is *orthonormal* and *complete*: every qubit state is a linear combination of these two vectors.

Quantum Superposition

The most general (normalized) qubit state is:

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

- α and β are called **probability amplitudes**.
- A qubit is not "secretly" in state $|0\rangle$ or $|1\rangle$: it genuinely exists in a *superposition* of both until measured.
- This is not classical uncertainty — it is a fundamental feature of quantum mechanics with measurable physical consequences (e.g., interference).

The Postulate of Measurement (Born Rule)

When we *measure* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the computational basis:

- We obtain outcome 0 with probability $P(0) = |\alpha|^2$.
- We obtain outcome 1 with probability $P(1) = |\beta|^2$.
- Note $P(0) + P(1) = |\alpha|^2 + |\beta|^2 = 1$. ✓
- After measurement, the state **collapses** irreversibly into the corresponding basis state ($|0\rangle$ or $|1\rangle$).

This *collapse* is what makes quantum measurement fundamentally different from classical observation: it **disturbs** the system.

Bits vs. Qubits

Feature	Classical Bit	Qubit
State space	$\{0, 1\}$	Unit vector in $\mathbb{C}^2$
General state	0 or 1	$\alpha \|0\rangle + \beta \|1\rangle$
Observation	Deterministic	Probabilistic (Born rule)
Post-measurement	Unchanged	State collapses
Copying	Unrestricted	No-Cloning Theorem

- The **No-Cloning Theorem** states that an unknown quantum state $|\psi\rangle$ *cannot* be perfectly copied — a profound departure from classical information.

From Four Real Parameters to Two

A general state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ involves two complex numbers α, β, hence *four* real parameters. Two constraints reduce this to *two*:

1. **Normalization:** $|\alpha|^2 + |\beta|^2 = 1$ removes one degree of freedom.
2. **Global phase:** $e^{i\varphi}\,|\psi\rangle$ and $|\psi\rangle$ are physically *identical* (no observable differs), so we can always choose $\alpha \in \mathbb{R}$, $\alpha \geq 0$.

Writing $\alpha = c_1 \in \mathbb{R}$ and $\beta = \gamma \in \mathbb{C}$, the state becomes:

$$|\psi\rangle = c_1\,|0\rangle + \gamma\,|1\rangle\,, \quad c_1 \geq 0,\; c_1^2 + |\gamma|^2 = 1.$$

This leaves exactly **two** independent real parameters.

The Bloch Sphere: Concept

- Since only two real parameters determine the state, every pure qubit state corresponds to a point on a **unit sphere** in $\mathbb{R}^3$ — the **Bloch sphere**.
- We use **angular (spherical) coordinates** (θ, ϕ) rather than the triple (c_1, c_2, c_3):
  - $\theta \in [0, \pi]$: polar angle from the $+Z$ axis.
  - $\phi \in [0, 2\pi)$: azimuthal angle around the Z axis.
- The **north pole** $(\theta = 0)$ represents $|0\rangle$; the **south pole** $(\theta = \pi)$ represents $|1\rangle$.
- Every point on the *surface* is a valid pure state; points *inside* the sphere correspond to mixed states (introduced later).

The Bloch Sphere: Parametrization

Setting $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$, the general qubit state is:

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

where $0 \leq \theta \leq \pi$ and $0 \leq \phi < 2\pi$.

- **Why $\theta/2$?** θ ranges over $[0, \pi]$ so that $\cos(\theta/2)$ and $\sin(\theta/2)$ are both non-negative and cover the full normalization circle. Using θ directly would only cover half the sphere.
- The Bloch vector $\mathbf{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ gives the corresponding point on S^2.
- Global phase $e^{i\varphi}$ is unobservable, so only the *relative* phase ϕ matters.

Common Qubit States on the Bloch Sphere

Beyond the computational basis, we frequently use the eigenstates of the Pauli X and Y operators:

- $|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}} \quad (\theta = \pi/2,\ \phi = 0)$: positive X-axis.
- $|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (\theta = \pi/2,\ \phi = \pi)$: negative X-axis.
- $|+i\rangle = \dfrac{|0\rangle + i\,|1\rangle}{\sqrt{2}} \quad (\theta = \pi/2,\ \phi = \pi/2)$: positive Y-axis.
- $|-i\rangle = \dfrac{|0\rangle - i\,|1\rangle}{\sqrt{2}} \quad (\theta = \pi/2,\ \phi = 3\pi/2)$: negative Y-axis.

Exercise: Verify these Bloch sphere coordinates using the parametrization on the previous slide.

Summary of Lecture 1

- Quantum information science bridges physics, computer science, information theory, and cryptography.
- A **qubit** is a unit vector in $\mathbb{C}^2$; the computational basis is $\{|0\rangle, |1\rangle\}$.
- **Superposition** $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a genuine quantum phenomenon, not classical ignorance.
- **Measurement** (Born rule): outcome probabilities are $|\alpha|^2$ and $|\beta|^2$; measurement collapses the state.
- The **Bloch sphere** parametrizes all pure single-qubit states by two angles (θ, ϕ), after removing the global phase freedom.

Looking Ahead: Lecture 2

In the next session, we will build the mathematical language more rigorously:

- **Hilbert spaces** and the axioms of the inner product.
- **Dirac notation**: bras, kets, and the dual space.
- **Linear operators**, adjoints, and the spectral theorem.
- **Orthonormal bases** and the completeness relation.

These tools will give us the precise language needed to state the *postulates of quantum mechanics* in Lecture 3.