MERIDIAN INSTITUTE OF TECHNOLOGY

PHYS-4028: Quantum Information Theory

Lecture Notes — Autumn Semester 2026

Instructor: Dr. Julian Vance
Notes by: Arthur Pendelton
Affiliation: Vertex Quantum Research Center

Abstract

These lecture notes cover the theoretical foundations of quantum information theory and quantum computation. Topics include the mathematical structure of quantum mechanics, state space representation, projective and generalized measurements, multipartite entanglement, Bell's theorem, and foundational theorems such as the No-Cloning theorem. The notes are designed for advanced undergraduate and graduate students at the Meridian Institute of Technology, incorporating material from research conducted at Apex Quantum Labs and Synapse Research Group.

Contents

LECTURE 1

Quantum States and Superposition

We begin our exploration of quantum information theory by formalizing the mathematical representation of quantum states. Unlike classical states, which are represented by discrete variables (bits), quantum states reside in a complex vector space equipped with an inner product.

1.1 Hilbert Space and State Vectors

A physical system in quantum mechanics is associated with a **Hilbert Space** $\mathcal{H}$, which is a complete complex vector space with an inner product. We denote state vectors using Dirac's bra-ket notation.

Dirac notation was introduced by Paul Dirac in 1939. The ket $|\psi\rangle$ denotes a column vector, and the bra $\langle\psi|$ denotes its conjugate transpose (row vector).

Definition: Qubit

A qubit (quantum bit) is the fundamental unit of quantum information. Mathematically, it is a state vector $|\psi\rangle$ in a two-dimensional Hilbert space $\mathcal{H} \cong \mathbb{C}^2$, represented as a linear combination:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $\alpha, \beta \in \mathbb{C}$ are complex probability amplitudes satisfying the normalization condition:

$$|\alpha|^2 + |\beta|^2 = 1$$

The states $\{|0\rangle, |1\rangle\}$ form the computational basis.

1.2 The Superposition Principle

The linear structure of Hilbert space implies that quantum systems can exist in superpositions of basis states. This leads to the fundamental principle:

Theorem: Quantum Superposition

If $|\psi_1\rangle$ and $|\psi_2\rangle$ are two physically allowed states of a quantum system, then any normalized linear combination:

$$|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle$$

with $c_1, c_2 \in \mathbb{C}$, is also a physically allowed state of the system.

1.2.1 Bloch Sphere Representation

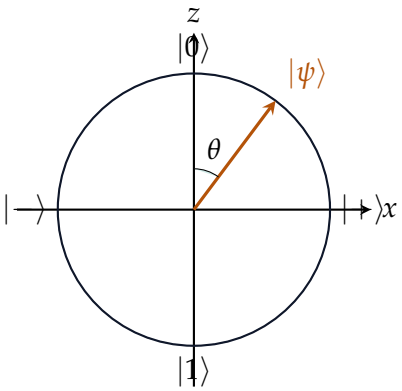
Ignoring the global phase, which has no observable consequences, any pure qubit state can be represented as a point on the surface of a three-dimensional unit sphere, known as the **Bloch Sphere**.

The parameters θ and ϕ represent the spherical coordinates of the state vector: $\theta \in [0, \pi]$ is the polar angle, and $\phi \in [0, 2\pi]$ is the azimuthal angle.

We express the state vector in terms of two angles, θ and ϕ:

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

We can visualize a slice of the Bloch sphere in the x-z plane (where $\phi = 0$):



In the next lecture, we will study how to extract information from these state vectors using quantum measurements.

LECTURE 2

Quantum Measurement and Observables

In classical mechanics, measuring a system does not affect its state. In quantum mechanics, however, measurements are active processes that alter the system's state and yield probabilistic outcomes.

2.1 Projective Measurements

A quantum measurement is described by an observable, which is a Hermitian operator A acting on the Hilbert space $\mathcal{H}$. Because A is Hermitian, it has a spectral decomposition:

$$A = \sum_i \lambda_i P_i$$

where λ_i are the real eigenvalues of A representing the possible measurement outcomes, and P_i are the orthogonal projection operators onto the corresponding eigenspaces.

Recall that a projection operator P_i satisfies $P_i^2 = P_i$ and $P_i^\dagger = P_i$. They are orthogonal: $P_i P_j = \delta_{ij} P_i$.

Definition: Projective Measurement

A projective measurement of a state $|\psi\rangle$ with respect to the observable A returns the outcome λ_i with probability given by the Born Rule:

$$p(\lambda_i) = \langle\psi|P_i|\psi\rangle$$

Immediately after the measurement, if the outcome λ_i is obtained, the state of the system collapses to:

$$|\psi'\rangle = \frac{P_i|\psi\rangle}{\sqrt{p(\lambda_i)}}$$

2.2 Expectation Value and Variance

The expected outcome of a measurement on a state $|\psi\rangle$ is the expectation value, defined as:

$$\langle A\rangle = \langle\psi|A|\psi\rangle = \sum_i \lambda_i p(\lambda_i)$$

The variance measures the uncertainty of the measurement outcome: $\Delta A^2 = \langle A^2\rangle - \langle A\rangle^2$.

To illustrate, consider the Pauli-Z operator $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, which has eigenvalues ± 1 corresponding to the states $\{|0\rangle, |1\rangle\}$. For a general qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$p(+1) = \langle\psi||0\rangle\langle 0||\psi\rangle = |\alpha|^2$$
$$p(-1) = \langle\psi||1\rangle\langle 1||\psi\rangle = |\beta|^2$$

The expectation value is:

$$\langle Z\rangle = (+1)|\alpha|^2 + (-1)|\beta|^2 = |\alpha|^2 - |\beta|^2$$

2.2.1 Comparison of Classical and Quantum Measurements

The table below contrasts the fundamental nature of measurements in the classical and quantum regimes.

Property	Classical Measurement	Quantum Measurement
Determinism	Completely deterministic in principle.	Inherently probabilistic (Born rule).
Disturbance	Measurement can be done without perturbing the state.	State collapses to an eigenstate of the observable.
Continuous Values	Measurable quantities have continuous, smooth values.	Physical quantities (like energy, spin) can be quantized.
Information	Infinite information can be stored and read.	Limited readable information per measurement (Holevo limit).

Table 2.1: Comparison of classical and quantum measurement regimes.

In the classical regime, we assume a objective state independent of our observation, whereas in the quantum regime, the observer and the observed system are intrinsically coupled during measurement.

LECTURE 3

Quantum Entanglement and Bell's Theorem

Perhaps the most counterintuitive feature of quantum mechanics is entanglement, which allows multiple particles to share a strong correlation that cannot be explained by any classical local theory.

3.1 Tensor Products and Composite Systems

To describe composite quantum systems, we use the tensor product of individual Hilbert spaces. If system A is in $\mathcal{H}_A$ and system B is in $\mathcal{H}_B$, the composite state space is $\mathcal{H}_A \otimes \mathcal{H}_B$.

If $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ are bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, then $\{|i\rangle_A \otimes |j\rangle_B\}$ forms a basis for the composite space.

Definition: Entanglement

A state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is called **separable** if it can be written as:

$$|\psi\rangle = |\phi\rangle_A \otimes |\chi\rangle_B$$

for some $|\phi\rangle_A \in \mathcal{H}_A$ and $|\chi\rangle_B \in \mathcal{H}_B$. Otherwise, $|\psi\rangle$ is called an **entangled state**.

The canonical example of a maximally entangled state of two qubits is the Bell state (or EPR pair):

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

where $|00\rangle \equiv |0\rangle \otimes |0\rangle$.

3.2 Bell's Theorem and the CHSH Inequality

In 1935, Einstein, Podolsky, and Rosen (EPR) argued that quantum mechanics was incomplete because it appeared to require "spooky action at a distance" to explain entanglement. They proposed that "local hidden variables" (LHVs) must exist to pre-determine measurement outcomes. In 1964, John Bell showed that EPR's assumption of local realism could be tested.

Theorem: Bell's Theorem

No physical theory of local hidden variables can reproduce all the statistical predictions of quantum mechanics.

To formalize this, consider the CHSH (Clauser-Horne-Shimony-Holt) inequality. Let Alice measure observables A or A', and Bob measure B or B', each with outcomes in $\{-1, +1\}$. Under any local hidden variable theory,

the expectation values of their joint measurements must satisfy:

$$S_{\text{LHV}} = \langle AB \rangle + \langle AB' \rangle + \langle A'B \rangle - \langle A'B' \rangle \leq 2$$

CHSH inequality. For a maximally entangled state $|\Phi^+\rangle$, with suitable choices of measurement angles, we can reach Cirel'son's bound: $S_{\text{QM}} = 2\sqrt{2} \approx 2.82 > 2$.

Quantum mechanics violates the

We present the proof that local realism bounds S to 2:

Proof

Let $a(\lambda), a'(\lambda) \in \{-1, 1\}$ be Alice's measurement outcomes, and $b(\lambda), b'(\lambda) \in \{-1, 1\}$ be Bob's, where λ is the hidden variable distributed according to a probability density $\rho(\lambda)$ with $\int \rho(\lambda) d\lambda = 1$. The expectation value is:

$$S = \int \left[a(\lambda)b(\lambda) + a(\lambda)b'(\lambda) + a'(\lambda)b(\lambda) - a'(\lambda)b'(\lambda) \right] \rho(\lambda) d\lambda$$

Rearranging the term in brackets:

$$a(\lambda) \left[b(\lambda) + b'(\lambda) \right] + a'(\lambda) \left[b(\lambda) - b'(\lambda) \right]$$

Since $b(\lambda), b'(\lambda) \in \{-1, 1\}$, either $b(\lambda) + b'(\lambda) = \pm 2$ and $b(\lambda) - b'(\lambda) = 0$, or vice versa. In either case, since $a(\lambda), a'(\lambda) \in \{-1, 1\}$, the absolute value of the bracket is exactly 2. Thus:

$$|S| \leq \int 2 \rho(\lambda) d\lambda = 2$$

This completes the proof.

□

This violation has been verified in numerous loop-hole-free experiments, showing that nature is fundamentally non-local or non-real.

LECTURE 4

Quantum Circuits and the No-Cloning Theorem

In this lecture, we introduce the circuit model of quantum computation and prove the No-Cloning Theorem, which highlights a key difference between classical and quantum information processing.

4.1 Quantum Gates and Unitary Operations

A quantum gate is a physical device that performs a unitary operation on one or more qubits. Since any quantum process must be reversible (excluding measurement), time evolution is represented by a unitary operator U, satisfying $U^\dagger U = I$.

Common single-qubit gates include the Hadamard gate H, which creates superpositions, and the Pauli gates X, Y, and Z.

The Hadamard gate is defined as:

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

It maps the basis states as follows:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle, \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$

4.2 The No-Cloning Theorem

In classical computing, copying information is trivial (e.g., copying a file or duplicating a bit). In quantum information, however, we cannot copy an arbitrary unknown quantum state. This is the celebrated **No-Cloning Theorem**, first proved by Wootters, Zurek, and Dieks in 1982.

Theorem: The No-Cloning Theorem

It is impossible to construct a unitary operator U that can clone an arbitrary unknown quantum state $|\psi\rangle$ onto a target state $|e\rangle$. That is, there exists no unitary U such that for all states $|\psi\rangle$:

$$U\left(|\psi\rangle \otimes |e\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$

This theorem is central to quantum cryptography: it prevents an eavesdropper from intercepting and copying quantum keys without leaving a trace. We prove this using the linearity of quantum mechanics.

Proof

Suppose there exists a unitary operator U that can clone any quantum state. Let $|\psi\rangle$ and $|\phi\rangle$ be two arbitrary states. By definition, U must satisfy:

$$U\left(|\psi\rangle \otimes |e\rangle\right) = |\psi\rangle \otimes |\psi\rangle \tag{4.1}$$
$$U\left(|\phi\rangle \otimes |e\rangle\right) = |\phi\rangle \otimes |\phi\rangle \tag{4.2}$$

Let us compute the inner product of the left-hand sides and the right-hand sides of these equations. Since U is unitary, it preserves the inner product:

$$\langle U(\psi \otimes e)|U(\phi \otimes e)\rangle = \langle \psi \otimes e|\phi \otimes e\rangle = \langle \psi|\phi\rangle\langle e|e\rangle = \langle \psi|\phi\rangle$$

On the other hand, the inner product of the right-hand sides is:

$$\langle \psi \otimes \psi|\phi \otimes \phi\rangle = \langle \psi|\phi\rangle\langle \psi|\phi\rangle = \left(\langle \psi|\phi\rangle\right)^2$$

For both calculations to be consistent, we must have:

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

This equation has only two possible solutions:

$$\langle \psi|\phi\rangle = 0 \quad \text{or} \quad \langle \psi|\phi\rangle = 1$$

This implies that $|\psi\rangle$ and $|\phi\rangle$ must be either identical or orthogonal. Therefore, the cloning machine can only clone states from a fixed set of mutually orthogonal states, and cannot clone an arbitrary unknown quantum state.

□

This completes the lecture series on the foundational aspects of quantum information theory. In subsequent courses, we will explore quantum algorithms such as Shor's factoring algorithm and Grover's search algorithm.

Bibliography

[1] Apex Quantum Labs. Quantum cryptography and communication security. Technical Report AQL-TR-2023-09, Nimbus Technology Institute, 2023.

[2] Synapse Research Group. Multi-party entanglement and its applications. *Journal of Vertex Science*, 42(3):201–218, 2024.

[3] Julian Vance and Arthur Pendelton. *Foundations of Quantum Informatics*. Meridian Academic Press, Meridian City, 2025.