CS 599 P1: Introduction to Quantum Computation — Boston University, Fall 2025
Instructor: Alexander Poremba — **Scribe:** *Selene Wu*

LECTURE #3: PRINCIPLES OF QUANTUM INFORMATION

Date: 9/9/25

The goal of this lecture is to introduce you to the *mathematical formalism* of quantum information. This formalism provides the precise language in which quantum states, transformations, and measurements are described, allowing us to reason about quantum systems in a rigorous way.

We will begin with three fundamental axioms, which are derived from the quantum mechanics of **closed quantum systems**. Such systems are isolated from their environment and are represented by *pure* quantum states, typically expressed as vectors in a Hilbert space. The evolution of these states is governed by unitary transformations, and their measurement outcomes are described by the *Born rule*. Later in the course, we will extend this framework to **open quantum systems**, which inevitably interact with their surroundings. These are more generally described by *mixed* quantum states, represented not by vectors but by density operators. This generalization will allow us to account for noise, decoherence, and statistical uncertainty, which are unavoidable features of real quantum mechanical systems.

1 Quantum states.

Let us begin with the mathematical representation of quantum states.

Axiom 1 (States)

A state is a complete description of a physical system. In quantum mechanics, a state is described by a "ray" in Hilbert space.

There are two things we need to unpack here: first, what is a *Hilbert space* and, second, why do we refer to a quantum state as a "ray" and not as a vector?

Hilbert Spaces. A d-dimensional Hilbert space $\mathcal{H}$ (for our purposes) is a *finite-dimensional* complex vector space, $\mathbb{C}^d$, which is equipped with an inner product $\langle \cdot | \cdot \rangle$. When $d = 2$ we call these states qubits, when $d > 2$ we call these states "qudits" (d-dimensional analogs of qubits).

Because a d-dimensional Hilbert space is a complex vector space $\mathbb{C}^d$, it admits an orthonormal basis $\{|b_0\rangle, |b_1\rangle, \ldots, |b_{d-1}\rangle\}$; a convenient choice is the canonical basis $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ with

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \cdots \quad , \quad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Dirac notation. In quantum mechanics, we make use of the so-called *Dirac notation*, which is also known as "bra-ket" notation, to denote quantum states.

1. A "ket vector" $|\psi\rangle \in \mathcal{H}$ corresponds to a d-dimensional complex **column** vector. We can write it in terms of the standard basis as

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{d-1} |d-1\rangle .$$

   Because it is a column vector, we can alternatively think of $|\psi\rangle$ as a $(d \times 1)$ complex matrix.

2. A "bra vector" $\langle\psi| \in \mathcal{H}^*$ with $\langle\psi| \coloneqq (|\psi\rangle)^\dagger$ is a d-dimensional complex **row** vector, where $\mathcal{H}^*$ is the *dual* complex vector space; note that $\mathbf{v}^\dagger$ is the complex adjoint of $\mathbf{v}$ (the vector we get by taking the transpose and complex conjugate of $\mathbf{v}$). We can write it in terms of the standard basis as

$$\langle\psi| = \overline{\alpha_0} \langle 0| + \overline{\alpha_1} \langle 1| + \cdots + \overline{\alpha_{d-1}} \langle d-1| .$$

   Because it is a row vector, we can alternatively think of $\langle\psi|$ as a $(1 \times d)$ complex matrix.

Adjoints of Complex Matrices

Let $A, B \in \mathbb{C}^{d\times d}$ be arbitrary complex matrices. Then, the adjoint has the following properties:

- (Addition:) $(A + B)^\dagger = A^\dagger + B^\dagger$.
- (Multiplication:) $(A \cdot B)^\dagger = B^\dagger \cdot A^\dagger$.

Notice the ordering of the matrices in the case of multiplication. The above properties also apply to ket and bra vectors, as these correspond to $(d \times 1)$ and $(1 \times d)$ dimensional matrices, respectfully.

Inner products. As mentioned above, a Hilbert space $\mathcal{H}$ is equipped with an inner product between states,

$$\langle\cdot|\cdot\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}, \quad (|\psi\rangle, |\phi\rangle) \mapsto \langle\psi|\phi\rangle .$$

To define the action of the inner product, let us consider two d-dimensional quantum states,

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{d-1} |d-1\rangle$$

as well as

$$|\phi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle + \cdots + \beta_{d-1} |d-1\rangle .$$

Then, the inner product $\langle\psi|\phi\rangle$ is essentially a $(1 \times d)$ by $(d \times 1)$ matrix multiplication given by

$$\begin{aligned}
\langle\psi|\phi\rangle &:= (|\psi\rangle)^\dagger \cdot |\phi\rangle = \langle\psi| \cdot |\phi\rangle \\
&= (\overline{\alpha_0} \langle 0| + \overline{\alpha_1} \langle 1| + \cdots + \overline{\alpha_{d-1}} \langle d-1|) \cdot (\beta_0 |0\rangle + \beta_1 |1\rangle + \cdots + \beta_{d-1} |d-1\rangle) \\
&= \overline{\alpha_0}\beta_0 \langle 0|0\rangle + \overline{\alpha_1}\beta_1 \langle 1|1\rangle + \cdots + \overline{\alpha_{d-1}}\beta_{d-1} \langle d-1|d-1\rangle \\
&= \overline{\alpha_0}\beta_0 + \overline{\alpha_1}\beta_1 + \cdots + \overline{\alpha_{d-1}}\beta_{d-1}.
\end{aligned}$$

Here, we crucially used the fact that $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ is an orthonormal basis of $\mathcal{H}$; meaning that $\langle i|j\rangle = \delta_{i,j}$ where $\delta_{i,j}$ is the Kronecker delta, which is equal to 1, if $i = j$, and 0, if $i \neq j$.
Let us now review some of the *properties* of the inner product.

- **Positivity:** For all nonzero $|\psi\rangle \in \mathcal{H}$,
$$\langle\psi|\psi\rangle > 0.$$
- **Conjugate symmetry:** For all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$,
$$\langle\psi|\phi\rangle = \overline{\langle\phi|\psi\rangle}.$$
- **Linearity in the first argument:** For all $|\psi_1\rangle, |\psi_2\rangle, |\phi\rangle \in \mathcal{H}$ and $\alpha, \beta \in \mathbb{C}$,
$$(\alpha |\psi_1\rangle + \beta |\psi_2\rangle)^\dagger |\phi\rangle = \overline{\alpha} \langle\psi_1|\phi\rangle + \overline{\beta} \langle\psi_2|\phi\rangle .$$
- **Linearity in the second argument:** For all $|\phi_1\rangle, |\phi_2\rangle, |\psi\rangle \in \mathcal{H}$ and $\alpha, \beta \in \mathbb{C}$,
$$\langle\psi| (\alpha |\phi_1\rangle + \beta |\phi_2\rangle) = \alpha \langle\psi|\phi_1\rangle + \beta \langle\psi|\phi_2\rangle .$$

Wait, didn't you say ray not vector? Quantum states that only differ by a scalar turn out to be physically indistinguishable, so we technically work with *equivalence classes* of vectors. Concretely,

$$|\psi\rangle \equiv \alpha |\psi\rangle , \ \forall \alpha \in \mathbb{C} \setminus \{0\}.$$

This means that $|\psi\rangle$, $2|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ all correspond to the same quantum state as they point towards the same direction in Hilbert space, for any $\theta \in [0, 2\pi]$. Because we only care about the "direction" of complex vectors, we refer to them as "rays" in Hilbert space. We appear to mostly call them vectors anyways. Generally we use the normalized vector as the *canonical representation* of these equivalence classes, and we say that two states are the same if they differ by a global complex phase.

2 Evolution of a Closed Quantum System

To enable quantum information processing, we need to ensure that we can apply a transformations to a given state. How do states of quantum mechanical systems *evolve* in time?

Axiom 2 (Evolution)

The evolution of a closed quantum system is described by a unitary linear operator.

Unitary transformations. When we transform a quantum state such that

$$|\psi\rangle \quad \mapsto \quad U|\psi\rangle$$

we want to preserve the property that the norm of our state vectors remains 1; this is clearly desirable if we want to preserve the probabilistic interpretation of quantum mechanics, where the squared ampltidudes of quantum states correspond to probabilities. If we consider the norm of our final state, we notice that

$$\|U|\psi\rangle\| = \sqrt{\langle\psi| U^\dagger U |\psi\rangle}.$$

If it were the case that $U^\dagger = U^{-1}$, then we could ensure that

$$\|U|\psi\rangle\| = \sqrt{\langle\psi| U^\dagger U |\psi\rangle} = \sqrt{\langle\psi|\psi\rangle} = \||\psi\rangle\| = 1$$

as desired. A linear operator U that satisfies such a property is called a **unitary** operator; concretely, it has the defining property that

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

where I is the identity matrix. A unitary operator takes orthogonal quantum states to orthogonal quantum states, and can therefore be thought of as a *change of basis* in Hilbert space.

A unitary operator also comes with a natural physical interpretation: the evolution of a quantum system is fundamentally *reversible*; and, the information in the system is *conserved*. Later, when we introduce the mixed state formalism, we will see that this is not the case for open quantum systems; these systems evolve according to the more general notion of a quantum channel.

3 Composite Quantum Systems

In this section, we will introduce the mathematical formalism to describe multiple quantum systems.

As a warm-up, let us first consider the case of two single-qubit systems. Recall that a single qubit lives in the two-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$, with computational basis

$$\{|0\rangle, |1\rangle\}.$$

If we have two qubits, say in system A and system B, we need a Hilbert space that can describe all possible joint states of A and B. For instance, the state $|0\rangle_A |1\rangle_B$ should represent the situation in which A is in $|0\rangle$ and B is in $|1\rangle$. In addition, we also want the formalism to apply to superpositions: if system A is in the state $|0\rangle$ and system B is in the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, then we also want to consider joint states of the form

$$|0\rangle_A \left(\frac{|0\rangle_B + |1\rangle_B}{\sqrt{2}} \right) = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |0\rangle_A |1\rangle_B) \,,$$

where the right-hand side describes all possible configurations one may observe in the joint system AB; in particular, we are equally like to observe the outcome $(0, 0)$ and $(0, 1)$. Therefore, we are looking for a mathematical description that respects *linearity*: if we fix the outcome in one system, say A, then the operation should be *linear* with respect to superpositions in the second system, say B, and vice versa.

The correct mathematical operation for combining two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ with such a property is the so-called *tensor product* Hilbert space, and it is denoted by

$$\mathcal{H}_A \otimes \mathcal{H}_B.$$

As it turns out, the tensor product is a *bi-linear* operation between vectors, and thus acts exactly as required.

To illustrate what the operation looks like, let us go back to the example of two-qubit systems, which come with an orthonormal basis $\{|0\rangle, |1\rangle\}$. To construct a basis of the joint two-qubit system, we will use the *tensor product* to combine the underlying single-qubit bases. Concretely, when representing vectors as columns, the tensor product of the basis vectors is computed using the *Kronecker product*:

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \otimes \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \\ b_1 \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_1 a_2 \\ a_1 b_2 \\ b_1 a_2 \\ b_1 b_2 \end{pmatrix}.$$

In the case of two qubits, each qubit state $|\psi\rangle, |\phi\rangle \in \mathbb{C}^2$ combines to form a joint state $|\psi\rangle \otimes |\phi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, which can be thought of as a vector in $\mathbb{C}^4$. The standard basis for this composite space is

$$\{|0\rangle \otimes |0\rangle,\ |0\rangle \otimes |1\rangle,\ |1\rangle \otimes |0\rangle,\ |1\rangle \otimes |1\rangle\},$$

which is often abbreviated as

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \quad \text{or} \quad \{|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle\}.$$

This leads us to the third axiom.

Axiom 3 (Composition of Hilbert spaces)

If the Hilbert space of a quantum system A is $\mathcal{H}_A$, and the Hilbert space of another quantum system B is $\mathcal{H}_B$, then the Hilbert space of their composition AB is given by $\mathcal{H}_A \otimes \mathcal{H}_B$.

Next, we are going to introduce important characteristics of tensor product spaces, as well as the mathematical properties behind the tensor product itself.

Properties of composite systems. Suppose $\mathcal{H}_A$ has dimension d_A with orthonormal basis

$$\{|a_i\rangle\}_{i=0,\ldots,d_A-1}$$

and $\mathcal{H}_B$ has dimension d_B with orthonormal basis

$$\{|b_j\rangle\}_{j=0,\ldots,d_B-1}.$$

Then, the following properties hold for the tensor product system $\mathcal{H}_A \otimes \mathcal{H}_B$:

- **Dimension:** $\mathcal{H}_A \otimes \mathcal{H}_B$ has dimension $d_A d_B$, and not $d_A + d_B$ as one might first guess.
- **Orthonormal basis:** An orthonormal basis of $\mathcal{H}_A \otimes \mathcal{H}_B$ takes the form

$$\left\{|a_i\rangle_A \otimes |b_j\rangle_B \;\middle|\; i = 0, \ldots, d_A - 1,\ j = 0, \ldots, d_B - 1\right\}.$$

- **States:** Any state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be written as

$$|\psi\rangle_{AB} = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} \alpha_{ij}\ |a_i\rangle_A \otimes |b_j\rangle_B.$$

Properties of the tensor product. For any vectors $|\psi\rangle, |\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_A$, $|\phi\rangle, |\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}_B$, and scalars $\alpha, \beta \in \mathbb{C}$, the tensor product $\otimes$ satisfies:

- **Linearity in the first argument:**

$$(\alpha |\psi_1\rangle_A + \beta |\psi_2\rangle_A) \otimes |\phi\rangle_B = \alpha |\psi_1\rangle_A \otimes |\phi\rangle_B + \beta |\psi_2\rangle_A \otimes |\phi\rangle_B.$$

- **Linearity in the second argument:**

$$|\psi\rangle_A \otimes (\alpha |\phi_1\rangle_B + \beta |\phi_2\rangle_B) = \alpha |\psi\rangle_A \otimes |\phi_1\rangle_B + \beta |\psi\rangle_A \otimes |\phi_2\rangle_B.$$

- **Scalars factor out:**

$$(\alpha |\psi\rangle_A) \otimes |\phi\rangle_B = \alpha (|\psi\rangle_A \otimes |\phi\rangle_B).$$

- **Zero vector identity:**

$$\mathbf{0}_A \otimes |\phi\rangle_B = \mathbf{0}_{AB} = |\psi\rangle_A \otimes \mathbf{0}_B.$$

Notational remark. When we write $\alpha \left|\psi\right\rangle_A \otimes \left|\phi\right\rangle_B$, we mean $\alpha \left(\left|\psi\right\rangle_A \otimes \left|\phi\right\rangle_B\right)$. By linearity, this is equal to $\left(\alpha \left|\psi\right\rangle_A\right) \otimes \left|\phi\right\rangle_B$, so parentheses are usually omitted without ambiguity.

Inner product on the tensor product space. The composite space $\mathcal{H}_A \otimes \mathcal{H}_B$ is itself a Hilbert space, and thus is naturally equipped with an inner product.

We describe the action of the inner product using a concrete example. Suppose that

$$\left|\psi\right\rangle_{AB} = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} \alpha_{ij} \left|a_i\right\rangle_A \otimes \left|b_j\right\rangle_B, \quad \left|\phi\right\rangle_{AB} = \sum_{k=0}^{d_A-1} \sum_{\ell=0}^{d_B-1} \beta_{k\ell} \left|a_k\right\rangle_A \otimes \left|b_\ell\right\rangle_B.$$

Then, the inner product is given by

$$\begin{aligned}
\left\langle\psi|\phi\right\rangle &= \left(\sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} \overline{\alpha}_{ij} \left\langle a_i\right|_A \otimes \left\langle b_j\right|_B \right) \left(\sum_{k=0}^{d_A-1} \sum_{\ell=0}^{d_B-1} \beta_{k\ell} \left|a_k\right\rangle_A \otimes \left|b_\ell\right\rangle_B \right) \\
&= \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} \sum_{k=0}^{d_A-1} \sum_{\ell=0}^{d_B-1} \overline{\alpha}_{ij} \beta_{k\ell} \left\langle a_i|a_k\right\rangle_A \left\langle b_j|b_\ell\right\rangle_B \\
&= \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} \overline{\alpha}_{ij} \beta_{ij}.
\end{aligned}$$

Here we used orthonormality: $\left\langle a_i|a_k\right\rangle = \delta_{i,k}$ and $\left\langle b_j|b_\ell\right\rangle = \delta_{j,\ell}$.

4 Operations on composite quantum systems

Recall that linear operators are completely specified by their action on a *basis*. Suppose $\mathcal{H}_A$ has dimension d_A with orthonormal basis $\{\left|a_i\right\rangle\}_{i=0,\ldots,d_A-1}$ and $\mathcal{H}_B$ has dimension d_B with orthonormal basis $\{\left|b_j\right\rangle\}_{j=0,\ldots,d_B-1}$. Then the basis of the tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$ is

$$\left\{ \left|a_i\right\rangle_A \otimes \left|b_j\right\rangle_B \;\middle|\; i = 0, \ldots, d_A - 1,\ j = 0, \ldots, d_B - 1 \right\}.$$

Multi-system operators. Suppose M_A is a linear operator acting on $\mathcal{H}_A$ and N_B is a linear operator acting on $\mathcal{H}_B$. Then their tensor product $M_A \otimes N_B$ acts as

$$(M_A \otimes N_B)(\left|a_i\right\rangle_A \otimes \left|b_j\right\rangle_B) = (M_A \left|a_i\right\rangle_A) \otimes (N_B \left|b_j\right\rangle_B).$$

In particular, for a general state

$$\left|\psi\right\rangle_{AB} = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} \alpha_{ij} \left|a_i\right\rangle_A \otimes \left|b_j\right\rangle_B,$$

we have

$$(M_A \otimes N_B) \left|\psi\right\rangle_{AB} = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} \alpha_{ij} \left(M_A \left|a_i\right\rangle_A\right) \otimes \left(N_B \left|b_j\right\rangle_B\right).$$

Let's consider a simple example on two qubits.

Example: Two-qubit operations

Let X be the Pauli X gate on system A and let H be the Hadamard gate on system B. Then,

$$\begin{aligned}(X_A \otimes H_B)\left(|0\rangle_A \otimes |1\rangle_B\right) &= |1\rangle_A \otimes \left(\frac{|0\rangle_B - |1\rangle_B}{\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2}}(|1\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B)\end{aligned}$$

Note that we often drop the system labels for convenience; for example,

$$(X \otimes H)\left(|0\rangle \otimes |1\rangle\right) = \frac{1}{\sqrt{2}}(|1\rangle |0\rangle - |1\rangle |1\rangle).$$