Quantum measurement—Postulate 3:

In a quantum measurement, the different possible measurement outcomes (labeled $1, 2, \ldots, m$) are each associated with a projector $P_j$, where the projectors form an orthogonal decomposition of the identity:

$$P_i = P_i^+, \quad P_i^* P_j = \delta_{ij} P_i, \quad \sum_{i=1}^m P_i = I$$

The probabilities $p_1, \ldots, p_m$ of the outcomes are given by the Born rule:

$$p_j = \langle \psi \mid P_j \mid \psi \rangle = \langle \langle \psi \rangle \overline{\langle \psi \rangle} \rangle$$

and if the measurement is ideal (non-demolition) the state of the system changes:

$$|\psi\rangle \rightarrow |\psi_j\rangle = P_j |\psi\rangle / \sqrt{p_j}$$

We can associate these projectors with the eigenspaces of a Hermitian operator:

$$0 = 0^+ = \sum_{j=1}^m \lambda_j P_j \quad \text{projectors onto eigenspaces of real eigenvalues, all distinct}$$
The eigenvalues \( \hat{A}_j \) represent the values of some physical quantity being measured. Such a Hermitian operator \( \hat{A} \) is called an observable.

If \( |\Psi\rangle \) is an eigenstate of \( \hat{A} \), then one measurement outcome (say \( A \)) has prob. 1, and all the others 0. We say that \( |\Psi\rangle \) has a "well-defined" value of \( \hat{A} \). Because most Hermitian matrices do not commute, \( |\Psi\rangle \) cannot simultaneously have well-defined values of every observable. Noncommuting observables are called complementary.

The expectation value of an observable is the average over all measurement outcomes:

\[
\sum_j P_j \hat{A}_j = \sum_j \hat{A}_j \langle \Psi | P_j | \Psi \rangle = \sum_j \langle \Psi | \hat{A}_j P_j | \Psi \rangle = \langle \Psi | \hat{A} | \Psi \rangle = \langle \hat{A} \rangle.
\]

The variance of an observable \( \langle \Delta \hat{A}^2 \rangle \) is

\[
\langle \Psi | (\hat{A} - \langle \hat{A} \rangle)^2 | \Psi \rangle = \langle \Psi | (\hat{A}^2 - 2\hat{A} \langle \hat{A} \rangle + \langle \hat{A} \rangle^2) | \Psi \rangle
\]

\[
= \langle \Psi | \hat{A}^2 | \Psi \rangle - 2\langle \Psi | \hat{A} | \Psi \rangle \langle \hat{A} \rangle + \langle \Psi | \langle \hat{A} \rangle^2 | \Psi \rangle
\]

\[
= \langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2.
\]
complementary observables obey uncertainty principles. These give lower bounds on the variances. The most famous is Heisenberg's:

\[ \langle 4x^2 \rangle \langle 4p^2 \rangle \geq \frac{\hbar^2}{4} \]

Similar bounds can be written for any pair of complementary variables (though the r.h.s. may depend on the state).

Two observables that commute are called compatible. If two observables have the same spectral decomposition (but different eigenvalues) they are equivalent.

In this class we rarely care about the eigenvalues \( \{ \psi_j \} \). So we will usually specify a measurement just in terms of the projectors \( \{ P_j \} \).

Note an important special case. If \( \{ \psi_j \} \) is an orthonormal basis, then the projectors \( P_j = |\psi_j\rangle \langle \psi_j| \) form a measurement. We can write any state \( |\psi\rangle \) in terms of this basis:

\[ |\psi\rangle = \sum_j \alpha_j |\psi_j\rangle \Rightarrow P_j = |\psi_j\rangle \langle \psi_j| \]

Such a measurement—where all the projectors are rank 1—is called complete.
Postulate 4: Composite Systems

For a composite system—comprising 2 or more subsystems—the joint Hilbert space is the tensor product of the Hilbert spaces of the subsystems.

\[ d_1 = \dim \mathcal{H}_1, \quad d_2 = \dim \mathcal{H}_2 \Rightarrow \dim \mathcal{H}_1 \otimes \mathcal{H}_2 = d_1 d_2. \]

If we have a basis \( \{ |\psi_i\rangle \} \) for \( \mathcal{H}_1 \), and a basis \( \{ |\phi_j\rangle \} \) for \( \mathcal{H}_2 \), then \( \{ |\psi_i\rangle \otimes |\phi_j\rangle \} \) is a basis for \( \mathcal{H}_1 \otimes \mathcal{H}_2 \), \( i, j = 1, 2, \ldots \).

For qubits, we can use the \( \{ |0\rangle, |1\rangle \} \) basis.

2 qubits have 4 basis vectors:

\[ \begin{align*}
&|00\rangle, \quad |10\rangle, \quad |01\rangle, \quad |11\rangle, \\
&|10\rangle \otimes |11\rangle, \quad |01\rangle \otimes |11\rangle, \quad |11\rangle \otimes |10\rangle, \quad |11\rangle \otimes |11\rangle,
\end{align*} \]

\( \{ |0x\rangle \}_{x=0,1,2,3} \)

\( \text{Here we've combined } i \& j \text{ into a single index:} \)

\( |ij\rangle \rightarrow |12i+j\rangle. \)

Similarly, for 3 qubits there are 8 basis vectors:

\[ \begin{align*}
&|000\rangle, \quad |001\rangle, \quad \ldots, \quad |111\rangle, \\
&|100\rangle, \quad |110\rangle, \quad \ldots, \quad |111\rangle.
\end{align*} \]

\( \text{For } k \text{ qubits} \)

\( 0 \leq x \leq 2^k - 1 \)
If subsystem 1 is in state \( |\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle \) and "2" "2" \( |\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle \), then the joint system is in state

\[
|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle.
\]

These are \textit{product states}. But note that \textit{most states are not product}:

\[
|\psi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle.
\]

A state of a composite system that is not a product is called \textit{entangled}.

Entanglement is a central concept of this course. The first thing to note is that, if a system is in an \textit{entangled state} then measurements on the 2 subsystems are generally \textit{correlated}. (In product states they are \textit{independent}.) In fact, as we will see shortly, they are in a certain sense more strongly \textit{correlated} than is possible classically.

Let's see how postulates \# 2 and 3 apply to composite systems.
Evolution Reversible evolution is still described by unitary transformations. If $|\Psi\rangle$ is a state of 2 qubits, then

$$|\Psi\rangle \rightarrow U|\Psi\rangle$$

4x4 unitary $UU^+=U^+U=I$.

What if we apply a unitary transformation just to one subsystem? On the joint system this is written as $U \otimes I$ or $I \otimes U$

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\Rightarrow U \otimes I = \begin{pmatrix} aI & bI \\ cI & dI \end{pmatrix} = \begin{pmatrix} a0 & b0 \\ 0c & 0d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}$$

$$I \otimes U = \begin{pmatrix} U & 0 \\ 0 & U \end{pmatrix} = \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}$$

If a joint unitary $U$ can be factorized

$$U = U_A \otimes U_B$$

then $A \& B$ are evolving independently. Otherwise $A \& B$ are interacting. Physically, most interactions are local: that is, the subsystems must be close together in space.

Note that, just like states, most operators are not products: $\hat{O} \neq \hat{A} \otimes \hat{B}$. But any operator can be written as a linear combination of products:

$$\hat{O} = \sum_k A_k \otimes B_k.$$
Measurement

If $\hat{O}$ is an observable on one subsystem, then the observable on the joint system is $\hat{O} \otimes I$ or $I \otimes \hat{O}$. The projectors take the form $P_j \otimes I$ or $I \otimes P_j$, respectively.

It is also possible to do joint measurements on more than one subsystem at a time. Then the joint observable acts nontrivially on both subsystems.

E.g., $\hat{O} = X \otimes X$. The eigenvalues are $\pm 1$, and the eigenvectors are

$$+1 \begin{cases} 1++> \\ 1--> \end{cases}, \quad -1 \begin{cases} 1+-> \\ 1-+-> \end{cases}$$

Note that even though this observable is a product, this is not a product of two measurements.

Generally, to do a joint measurement one must bring the subsystems physically together. But there are tricks using entangled ancillas that allow one to do joint measurements on physically separated subsystems (as we shall see).
Quantum circuits

Circuits are a handy graphical representation of a quantum protocol, analogous to logical circuit diagrams. Qubits are represented as wires, with time going left to right:

$$|\psi_0\rangle$$

$$|\psi_1\rangle$$

$$+ \rightarrow$$

Classical info is written w/ double or thick lines:

$$\pm 1$$

There are three main elements to a circuit. First are state preparations:

$$|\psi\rangle$$

$$|\Phi^+\rangle$$

Next, there are unitary transformations.

[Diagrams of various quantum gates]

Finally, there are measurements:

Sometimes we explicitly include the classical output.

$$Z = \pm 1$$
When we have multiple, spatially separated parties we generally segregate them vertically:

\[
\text{Alice} \begin{cases} 14^A > \\ 10^A > \\ 10^A > \\ \end{cases} \quad \text{U}_E \quad \text{N} \quad \text{Bob} \begin{cases} 10^B > \\ \end{cases}
\]

So, for example, to remotely measure Bob\'s state, we can use the following circuit:

\[
\text{Alice} \quad 14^A > \quad \text{U}_Z \quad \text{Z}_A \oplus \text{Z}_B \quad \text{Bob} \quad 14^B >
\]

where \( \text{1} \Phi_+ > = \frac{1}{\sqrt{2}} (100^A + 111^A) \) is a maximally-entangled pair or ebit.

We\'ll see more tricks with entanglement next time, and throughout the course.