Lecture 2
Postulates of Quantum Mechanics

Recall from last lecture that QC is linear. Today we discuss the notation we use in QC for linear algebra (Dirac notation) and formalize our notion of QC

(Ket) Let V be finite-dimensional vector space. We write $|v\rangle$ (or $|\psi\rangle$ or $|\varphi\rangle$ or $|a\rangle$...) to denote a vector of V. $|v\rangle$ is called a Ket.

(Bra) Given $|v\rangle \in V$, we write its dual or adjoint as $\langle v| : V \to \underbrace{F_V}_{\text{Field of } V}$. $\langle v|$ is called a Bra. For a complex vector space $\mathbb{C}^d$, $\langle v| = |v\rangle^{\dagger} = |v\rangle^{*}$ ← dagger which is the conjugate-transpose of $|v\rangle$

(Example) In $\mathbb{C}^2$, say $|v\rangle = \begin{bmatrix} 1 \\ i \end{bmatrix}$. Then $\langle v| = \begin{bmatrix} 1 & -i \end{bmatrix}$

In general, if $|v\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$, Then

$\langle v| = \begin{bmatrix} a^* & b^* \end{bmatrix}$ where $(c+di)^* = c-di$

(Inner products)

Recall that on $\mathbb{C}^d$, the inner product between $v = \begin{bmatrix} v_1 \\ \vdots \\ v_d \end{bmatrix}$ and $w = \begin{bmatrix} w_1 \\ \vdots \\ w_d \end{bmatrix}$ is

$$\langle v, w \rangle = \sum_i \bar{v}_i w_i$$

This is $\langle v| \cdot |w\rangle = [v_1^* \cdots v_d^*] \begin{bmatrix} w_1 \\ \vdots \\ w_d \end{bmatrix}$ and we denote this product by $\langle v|w\rangle$

(Bases)

i^{th} elementary vector $\begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \}i-1$

We denote e_i by the special ket $|i\rangle$ and call this the computational basis

Ex.

$$\begin{bmatrix} a \\ b \end{bmatrix} = a \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = a|0\rangle + b|1\rangle$$

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = a|0\rangle + b|1\rangle + c|2\rangle$$

Note:

$$\langle i|j\rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

(Unit vector)

A unit vector (in VS's we care about) is a vector v s.t. $\|v\| = \langle v|v\rangle^2 = 1$

Postulate #1 of QM

The state of an isolated physical system is a unit vector in a complex vector space $\mathbb{C}^d$, $d \geq 1$

We will almost exclusively use Qubit systems, which have state space $\mathbb{C}^2$ and computational basis $\{|0\rangle, |1\rangle\}$

(Notation)

We write the state of a qubit as

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

and say that $|\psi\rangle$ is in a superposition of states $|0\rangle$ and $|1\rangle$ with amplitudes a & b

(Tensor product)

Given two VS's V, W, the tensor product $V \otimes W$ of V & W is a VS with a bilinear map $\otimes : V \times W \longrightarrow V \otimes W$ which allows us to combine vectors $v \in V$, $w \in W$ into a single vector $v \otimes w \in V \otimes W$

(Abstract definition: $\otimes$ is the "free-est" possible bilinear map, so that all others "factor through" $\otimes$)

(Concrete defn for finite dimensions)

If V and W have bases $\{|e_i\rangle\}$ and $\{|f_j\rangle\}$, resp., then $V \otimes W$ has the basis

$$\{|e_i\rangle \otimes |f_j\rangle\}$$

and if $v = \sum_i a_i |e_i\rangle$, $w = \sum_j b_j |f_j\rangle$, then

$$v \otimes w = \sum_{ij} a_i b_j |e_i\rangle \otimes |f_j\rangle$$

Ex.

$\mathbb{C}^2 \otimes \mathbb{C}^2$ is a complex VS with basis

$$\{|0\rangle_1 \otimes |0\rangle_2,\ |0\rangle_1 \otimes |1\rangle_2,\ |1\rangle_1 \otimes |0\rangle_2,\ |1\rangle_1 \otimes |1\rangle_2\}$$

Note that $\mathbb{C}^2 \otimes \mathbb{C}^2$ has dim 4, and so

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \simeq \mathbb{C}^4$$

If we have $|\psi\rangle = a|0\rangle + b|1\rangle$, $|\varphi\rangle = c|0\rangle + d|1\rangle$, then

$$|\psi\rangle \otimes |\varphi\rangle = ac|0\rangle|0\rangle + ad|0\rangle|1\rangle + bc|1\rangle|0\rangle + bd|1\rangle|1\rangle$$

Note: we often drop $\otimes$ in Dirac notation

(Representation of $V \otimes W$ & Kronecker product)

In practice, we use the Kronecker product $\otimes$

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a\begin{bmatrix} c \\ d \end{bmatrix} \\ b\begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$$

And write vectors of $\mathbb{C}^n \otimes \mathbb{C}^m$ as vectors in $\mathbb{C}^{nm}$

Postulate #2 of QM

If two systems have state spaces V and W resp., their combined state ~~space~~ is a unit vector in $V \otimes W$

(Systems of qubits)

By postulate #2, a system of n qubits has state space $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} \cong \mathbb{C}^{2^n}$.

The computational basis of $\mathbb{C}^{2^n}$ has 2^n elements, which we denote by $|\vec{x}\rangle$, $\vec{x} \in \{0,1\}^n$

e.g. $|0001\rangle \in \mathbb{C}^{2^4}$, $|0111100\rangle \in \mathbb{C}^{2^7}$

This means a vector $|\psi\rangle \in \mathbb{C}^{2^n}$ is in a superposition of n-bit classical states

(Note)

The following are interchangeable:

$$|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle = |0\rangle$$
$$|0\rangle \otimes |1\rangle = |0\rangle|1\rangle = |01\rangle = |1\rangle$$
$$|1\rangle \otimes |0\rangle = |1\rangle|0\rangle = |10\rangle = |2\rangle$$

as numbers in binary

This coincides with the Kronecker product, since

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = e_2$$

(Product & entangled vectors)

$V \otimes W$ differs from $V \times W$ because not every element of $V \otimes W$ can be written as $v \otimes w$

Ex.

The vector $|\Phi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

cannot be written in the form $|\psi\rangle \otimes |\varphi\rangle$ for $|\psi\rangle, |\varphi\rangle \in \mathbb{C}^2$

This vector is called a Bell state

We call a state $|\psi\rangle$ a product state if it can be written as $|a\rangle \otimes |b\rangle$. Otherwise it is entangled

(linear operators)

A linear operator $A: V \to W$ between VS's V, W is a map which is linear, ie.

$$A(\alpha|\psi\rangle + \beta|\varphi\rangle) = \alpha A|\psi\rangle + \beta A|\varphi\rangle$$

Note: we often define a linear operator by giving its action on a basis $\{|e_i\rangle\}$ of V, e.g.

$$A: |0\rangle \mapsto |1\rangle \qquad \text{or just } A: |x\rangle \mapsto |\neg x\rangle,\ x \in \{0,1\}$$
$$\quad |1\rangle \mapsto |0\rangle$$

Boolean "Not"

This is valid since by linearity,

$$A\left(\textstyle\sum_i a_i |e_i\rangle\right) = \textstyle\sum_i a_i (A|e_i\rangle)$$

(matrix representations)

A linear operator $A: V \to W$ can be represented by a matrix $\{A_{ij}\} = \begin{bmatrix} A_{00} & \cdots & A_{n0} \\ \vdots & \ddots & \\ A_{0m} & & A_{nm} \end{bmatrix}$ over bases $\{|e_i\rangle\}$ and $\{|f_j\rangle\}$ of V, W resp. such that

$$A|e_i\rangle = \sum_j A_{ij} |f_j\rangle$$

Ex.

The matrix representation of the linear operator $A: |x\rangle \mapsto |\neg x\rangle$, $x \in \{0,1\}$ is

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

The matrix representation acts on a vector via matrix-vector multiplication. Ex.

$$A|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

(Outer products)

Another convenient way of describing an operator A is as a sum of outer products of basis vectors. Outer products are written in Dirac notation as $|\psi\rangle\langle\psi|$.

Ex. $|0\rangle\langle 1| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $|1\rangle\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Fact:

Given VS's V & W with orthonormal bases $\{|e_i\rangle\}$, $\{|f_j\rangle\}$, any linear operator $A: V \to W$ can be expressed as

$$A = \sum_{ij} A_{ij} |f_j\rangle\langle e_i|$$

Comes from completeness $\sum_i |e_i\rangle\langle e_i| = I = \sum_j |f_j\rangle\langle f_j|$

$$\begin{aligned} A &= I\,A\,I \\ &= \sum_{ij} |f_j\rangle\langle f_j| A |e_i\rangle\langle e_i| \\ &= \sum_{ij} (\langle f_j|A|e_i\rangle)\, |f_j\rangle\langle e_i| \end{aligned}$$

Classes of operators

- Normal: $AA^+ = A^+A$ ← conjugate transpose $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^+ = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$
- Unitary: $UU^+ = I = U^+U$ ← important
- Hermitian: $A = A^+$
- Projector: $P^2 = P$

  (Note: $|\psi\rangle\langle\psi|$ is the projector onto state $|\psi\rangle$. We often use projectors of the form $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$)
- Positive: $\langle\psi|A|\psi\rangle \geq 0 \quad \forall |\psi\rangle$

(Tensor products of operators)

As with states we can combine operators on different systems with the tensor product.

If $A: V \to W$ and $B: X \to Y$, then $A \otimes B: V \otimes X \to W \otimes Y$ and

$$(A \otimes B)(|\psi\rangle \otimes |\varphi\rangle) = A|\psi\rangle \otimes B|\varphi\rangle$$

As with states, we use the Kronecker product to represent a tensor product of operators as a matrix

$$\underbrace{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}_{= A} \otimes \underbrace{\begin{bmatrix} e & f \\ g & h \end{bmatrix}}_{= B} = \begin{bmatrix} aB & bB \\ cB & dB \end{bmatrix} = \begin{bmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{bmatrix}$$

Ex.

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, which swaps $|0\rangle \longleftrightarrow |1\rangle$

Then $A \otimes I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

Now $(A \otimes I)(|0\rangle \otimes |1\rangle) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |1\rangle \otimes |1\rangle$

In general, $A \otimes I$ "leaves the second system unchanged"

Properties of $\otimes$

1. $s(A \otimes B) = sA \otimes B = A \otimes sB$
2. $(A+B) \otimes C = A \otimes C + B \otimes C$
3. $A \otimes (B+C) = A \otimes B + A \otimes C$
4. $A \otimes (B \otimes C) = (A \otimes B) \otimes C$
5. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$
6. $(A \otimes B)(C \otimes D) = AC \otimes BD$

Postulate #3 of QM

The physical evolution of an isolated quantum system is represented by a unitary operator on the state space

(unitary operators satisfy $\| U|\psi\rangle \| = \| |\psi\rangle \|$ and hence take unit vectors to unit vectors)

Ex.

Common unitaries in QC include

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

(Pauli operators)

Also $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ (hadamard operator)

Note that

$$\underbrace{X : \begin{aligned} |0\rangle &\longmapsto |1\rangle \\ |1\rangle &\longmapsto |0\rangle \end{aligned}}_{\text{Bit flip}} \qquad \underbrace{Z : \begin{aligned} |0\rangle &\longmapsto |0\rangle \\ |1\rangle &\longmapsto \overset{\text{Phase}}{(-1)}|1\rangle \end{aligned}}_{\text{Phase flip}}$$

And also that

$$\begin{aligned} HXH &= \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= Z \end{aligned}$$

Postulate #4 of QM
(Measurement)

Let $\{M_m\}$ be a set of operators with associated outcomes m and such that

$$\sum_m M_m^\dagger M_m = I$$

Then the measurement of a state $|\psi\rangle$ with respect to $\{M_m\}$ produces outcome m with probability

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$$

and leaves the system in the state

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}} = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

Note: by linearity,

$$\begin{aligned}\sum_m p(m) &= \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle \\ &= \langle\psi|\left(\sum_m M_m^\dagger M_m\right)|\psi\rangle \\ &= 1\end{aligned}$$

Ex.

Recall that $|0\rangle\langle 0| + |1\rangle\langle 1| = I$

Measuring the state $|\psi\rangle = a|0\rangle + b|1\rangle$ w/t $\{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}$ produces outcome 0 with

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle$$
$$= |a|^2$$

The state after measurement is then

$$\frac{a}{|a|}|0\rangle$$

This is measurement in the computational basis

More generally, we can measure in any orthonormal basis $\{|e_i\rangle\}$ by setting $M_i = |e_i\rangle\langle e_i|$

projector onto $|e_i\rangle$

Measurement of $\{M_i\}$ will project or collapse a state onto this basis. We call this a projective or von Neumann measurement

Prop.

Any von Neumann measurement reduces to Unitary transformations and computational basis measurements

$U: |i\rangle \mapsto |e_i\rangle$ is unitary

Pf $M_i = |e_i\rangle\langle e_i| = U|i\rangle\langle i|U^\dagger$

$|\psi'\rangle = U^\dagger|\psi\rangle$

so $\langle\psi|M_i^\dagger M_i|\psi\rangle = \langle\psi|U|i\rangle\langle i|U^\dagger|\psi\rangle = \langle\psi'||i\rangle\langle i||\psi'\rangle$

and $M_i|\psi\rangle = U|i\rangle\langle i|U^\dagger|\psi\rangle = U(|i\rangle\langle i|\psi'\rangle)$

(Measurement of composite systems)

Often we want to only measure 1 system in a composite system. Here we can note that if $\sum_m M_m^\dagger M_m = I$, then

$$\begin{aligned}
\sum_m (M_m \otimes I)^\dagger (M_m \otimes I) &= \sum_m (M_m^\dagger \otimes I)(M_m \otimes I) && \text{(prop. of } \otimes) \\
&= \sum_m M_m^\dagger M_m \otimes I && \text{(prop. of } \otimes) \\
&= (\sum_m M_m^\dagger M_m) \otimes I && \text{(prop. of } \otimes) \\
&= I \otimes I \\
&= I
\end{aligned}$$

<u>Ex.</u>

Suppose we measure the state

$$|\psi\rangle = \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$$

w.r.t. the computational basis in the first qubit

$$\begin{aligned}
p(0) &= \langle\psi|(|0\rangle\langle 0| \otimes I)|\psi\rangle \\
&= \frac{1}{2}\langle\psi|(|00\rangle - |01\rangle) \\
&= \frac{1}{4}(\langle 00|00\rangle + \langle 01|01\rangle) \\
&= \frac{1}{2}
\end{aligned}$$

And the resulting state for outcome 0 would be

$$\frac{(|0\rangle\langle 0| \otimes I)|\psi\rangle}{\sqrt{1/2}} = \frac{\frac{1}{2}(|00\rangle - |01\rangle)}{\sqrt{1/2}}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$$

(Phase invariance)

Given states $|\psi\rangle$ and $|\psi'\rangle = e^{i\theta}|\psi\rangle$, we can note that the probability of measuring outcome m is the same for $|\psi\rangle$ and $|\psi'\rangle$:

$$\langle\psi'|M_m^\dagger M_m|\psi'\rangle = \langle\psi|e^{-i\theta}M_m^\dagger M_m e^{i\theta}|\psi\rangle$$
$$= \langle\psi|M_m^\dagger M_m|\psi\rangle$$

We call this a global phase and often ignore global phases since measurement can't observe them

Measurement can however detect relative phase

$$|\psi\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\psi'\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

by changing to an appropriate basis:

$$H|\psi\rangle = |0\rangle, \quad H|\psi'\rangle = |1\rangle$$

(Notation)

We denote $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = H|0\rangle = |+\rangle$

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = H|1\rangle = |-\rangle$

Observe that $\{|+\rangle, |-\rangle\}$ is a basis of $\mathbb{C}^2$