Last class we learned about quantum states and measurement. As a recap,

\[
\text{States}: \sum_{i=0}^{d-1} a_i |i\rangle \in \mathbb{C}^d, \quad \sum_{i=0}^{d-1} |a_i|^2 = 1
\]

\[
\text{Measurement}: \sum_{i=0}^{d-1} a_i |i\rangle \xrightarrow{\text{measurement}} |i\rangle
\]

Today we’ll learn about gates, or unitary transformations, the main way we compute in QC.

Unitary transformations arise as a natural consequence of the fact that states are unit vectors. Much like stochastic matrices and probability vectors, unitary operations assure that we don’t “break” nature, and specifically measurement.

We will see that they can also be viewed as change of basis matrices for the same reason.
In the last class, we saw the Hadamard basis \{1+, 1-\} of \( \mathbb{C}^2 \). We can write the change of basis matrix from \{10, 11\} to \{1+, 1-\} as

\[
H = \frac{1}{\sqrt{2}} \begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
\]

The matrix \( H \) is called the Hadamard gate. Observe that \( H10 = 1+ \) and \( H11 = 1- \), and in particular the columns of \( H \) are unit vectors, like we had with stochastic matrices. Quantum gates satisfy an even more restrictive property called unitarity which means that their Hermitian conjugate (i.e. dagger or conjugate transpose) is equal to their inverse.

\[
\text{A complex-valued matrix } U \text{ is unitary iff } \quad UU^* = U^*U = I
\]

where

\[
\begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{bmatrix}^* =
\begin{bmatrix}
a_{11}^* & a_{21}^* & \cdots & a_{n1}^* \\
a_{12}^* & a_{22}^* & \cdots & a_{n2}^* \\
\vdots & \vdots & \ddots & \vdots \\
a_{1n}^* & a_{2n}^* & \cdots & a_{nn}^*
\end{bmatrix}
\]

(i.e. take transpose and conjugate entry-wise)

In circuit notation, a unitary is a labeled box.
The following matrices are unitary:

\[
X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},
\]
\[
S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.
\]

We saw the $X$ or NOT gate already, which maps:

\[
\begin{cases}
|0\rangle \rightarrow |1\rangle \\
|1\rangle \rightarrow |0\rangle
\end{cases} \text{ bit flip}
\]

The $Z$ gate is sometimes called a phase flip:

\[
\begin{cases}
|0\rangle \rightarrow |0\rangle \\
|1\rangle \rightarrow (-1)|1\rangle \text{ phase}
\end{cases}
\]

The two are related by a basis change:

\[
HXH = \frac{1}{2} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -Z.
\]

Note also that $Z$ acts like $X$ in the $\{|1\rangle, |1\rangle\}$ basis:

\[
\begin{align*}
Z|1\rangle &= Z\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |1\rangle \\
Z|1\rangle &= Z\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |1\rangle
\end{align*}
\]

In particular, to flip a bit $|0\rangle \rightarrow |1\rangle$, we could either apply $X$, or apply a change of basis $H|0\rangle = |+\rangle$, phase flip $Z|+\rangle = |1\rangle$, then change back $H^+|1\rangle = H|1\rangle = |1\rangle$. As matrices:

\[
X = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} H Z H.
\]
A crucial property of unitary transformations is that they are inner product preserving:

$$\langle u v, u w \rangle = \langle (v l u^t) (u w) \rangle$$
$$= \langle v l u + u l u \rangle$$
$$= \langle v l u \rangle$$

This implies that unitaries take states to states, since in particular

$$|| v l u || = \sqrt{\langle u v, u v \rangle} = \sqrt{\langle u u \rangle} = || u ||$$

Ex.
Is the transformation $H_0: \{0\} \rightarrow \{+\}$ unitary?

Consider $\Psi = a|0\rangle + b|1\rangle$, $|a|^2 + |b|^2 = 1$. Then

$$H_0 \Psi = (a+b) \{+\} = \Psi'$$

But $\langle \Psi' | \Psi \rangle = |a|^2 + a^*b + ab^* + |b|^2 \neq 1$ in general.

We could have also written

$$H_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

and calculated $H_0 H_0^* = \frac{1}{2} \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

Columns of unitaries:
The columns of an $n \times n$ unitary matrix $U$ form an orthonormal basis $\{e_1; e_2; \ldots\}$ of $\mathbb{C}^n$, and $U$ is the change of basis matrix $\{e_1; e_2; \ldots\} \rightarrow \{u_1; u_2; \ldots\}$.
Recall how Dirac notation simplified our calculations involving vectors. Now we introduce some tools from operator theory that will allow us to do the same for matrix calculations.

(Operators)

An operator on a Hilbert space $\mathcal{H}$ is a linear transformation $A: \mathcal{H} \rightarrow \mathcal{H}$. Recall that linear means that for all $|\psi>, |\phi> \in \mathcal{H}, a, b \in \mathbb{C}$

$$A(a|\psi> + b|\phi>) = aA|\psi> + bA|\phi>$$

Ex.

An example of an operator in this more abstract sense is an outer product. In Dirac notation, we can write the outer product of two vectors $|\psi>, |\phi> \in \mathcal{H}$ as

$$|\psi><\phi|$$

This operator (linearly, by definition) maps

$$|\Phi> \rightarrow <\phi|\Phi><\psi>$$

Using Dirac notation, this is simply

$$<\psi|\Phi><\phi|=<\psi|\Phi><\phi>$$

$$= <\psi|\Phi><\psi>$$
Ex.

Let \( \langle \Psi | = \frac{1}{\sqrt{2}} \langle 1 | + \frac{i}{\sqrt{2}} \langle 1 | = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \\
\end{bmatrix} \)

1. What is the matrix of \( \langle \Psi | \Psi \rangle \)?
\[
\langle \Psi | \Psi \rangle = \frac{1}{2} \begin{bmatrix} 1 \\ i \\
\end{bmatrix} \cdot \frac{1}{2} \begin{bmatrix} 1 \\ -i \\
\end{bmatrix} = \frac{1}{4} \begin{bmatrix} 1 \\ -i \\
\end{bmatrix} \]

2. What is the matrix of \( \langle 0 | \Psi \rangle \)?
\[
\langle 0 | \Psi \rangle = \begin{bmatrix} 0 \\ 0 \\
\end{bmatrix} \begin{bmatrix} 1 \\ 1 \\
\end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\
\end{bmatrix}
\]

3. What is \( \langle 0 | \Psi \rangle \langle \Psi | 0 \rangle \)?
\[
\begin{bmatrix} 0 \\ 0 \\
\end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\
\end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\
\end{bmatrix}
\]

4. What is \( \langle 1 | 1 \rangle \langle 1 | \Psi \rangle \) in Dirac notation?
\[
\langle 1 | \Psi \rangle \langle 1 | 1 \rangle = \frac{1}{\sqrt{2}} \langle 1 | \Psi \rangle = \frac{1}{\sqrt{2}} \cdot \frac{i}{\sqrt{2}} = \frac{i}{2}
\]

The outer products \( \langle 0 | \Psi \rangle, \langle 1 | 1 \rangle, \langle \Psi | \Psi \rangle \) are special operators called projectors. Intuitively, \( \langle 0 | \Psi \rangle \) projects a state onto its \( \langle 0 | \) part. More generally, \( \langle \Psi | \Psi \rangle \) projects onto the line spanned by \( \langle \Psi | \).

Not norm preserving, hence not unitary!
(Projectors, formal definition)
An operator $P$ on $H$ is a projector if
\[ P^2 = P \]
I.e. projecting onto the same line (or subspace) again does nothing since we're already on the line.

(Resolution of the identity)
Let \( \{1e_i\} \) be a basis of $H$. Then
\[ I = \sum_{i} 1e_i \langle e_i | e_i \rangle \]

\[ \text{Ex.} \]
In $C^2$, we have $10\langle 0|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $11\langle 1|1\rangle = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$
\[ 10\langle 0|0\rangle + 11\langle 1|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \]

With the basis \( \{1+1, 1-1\} \),
\[ 1+\langle 1+1 \rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \]
\[ 1-\langle 1-1 \rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \]
\[ 1+\langle 1+1 \rangle + 1-\langle 1-1 \rangle = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \]
Let \( \{ |e_i\>\} \) be an orthonormal basis of \( \mathcal{H} \). Then any linear operator \( T \) on \( \mathcal{H} \) can be written as

\[
T = \sum_{i,j} T_{ij} |e_i><e_j|
\]

where \( T_{ij} = <e_i|T|e_j> \)

**Pf.**

\[
T = ITI = \sum (|e_i><e_i|) T (|e_j><e_j|)
\]

\[
= \sum T_{ij} |e_i><e_i| |e_j><e_j|
\]

\[
= \sum T_{ij} |e_i><e_j|
\]

The expression \( \sum_{i,j} T_{ij} |e_i><e_j| \) is the matrix of \( T \) over the basis \( \{ |e_i> \} \). In particular, observe:

\[
|10> = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |11> = \begin{bmatrix} 0 \\ 1 \end{bmatrix},
\]

\[
|10> = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |11> = \begin{bmatrix} 0 \\ 1 \end{bmatrix}
\]

So

\[
\begin{bmatrix} a & b \\ c & d \end{bmatrix} = q|10> + b|11> + c|10> + d|11>
\]

**Aside**

Formally, the space of linear operators on \( \mathcal{H} \), denoted \( \mathcal{L}(\mathcal{H}) \), is a vector space. The above Thm states that \( \{ |e_i> \} \) is a basis of \( \mathcal{L}(\mathcal{H}) \).
All of this (aside from introducing the language of operators which we will frequently come back to) is to say that the dagger of \( T = \sum_{ij} T_{ij} \langle e_i | e_j \rangle \) can be written concisely as

\[
T^\dagger = \sum_{ij} T_{ij}^* \langle e_j | e_i \rangle
\]

Note that \((AB)^\dagger = B^\dagger A^\dagger\) for any \(A, B \in \mathbb{C}(\mathcal{H})\), by properties of the transpose.

(Reversibility (preview))

We close with the observation that unitary evolution implies the reversibility of time (not actually, just state evolution). In particular, if a computation sends

\[
|\psi\rangle \quad \overset{U}{\longrightarrow} \quad |\phi\rangle
\]

then we could just invert \(U\) to get back the original state

\[
|\psi\rangle \quad \overset{U^{-1}}{\longrightarrow} \quad |\phi\rangle
\]

Can we do this with classical computation? In particular recall the AND gate

\[
\begin{array}{ccc}
\times \\
ym&\longrightarrow
\end{array}
\]

If \(x \land y = 0\), can we retrieve the values of \(x\) and \(y\)?

NO! \((0 \land 0 = 0 \land 1 = 1 \land 0)\)

If we expect quantum computation to be more powerful than classical, we'll have to reconcile this issue somehow in upcoming classes!