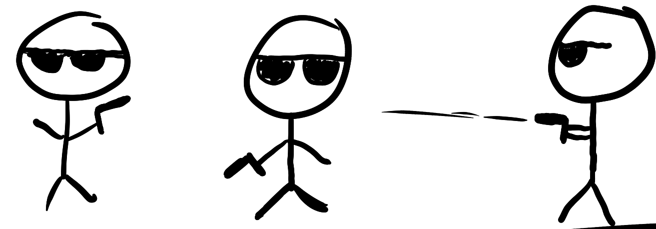
CMPT 476 Lecture 4

Operators



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

unit vector

States : $\sum_{i=0}^{d-1} a_i |i\rangle \in \mathbb{C}^d$, $\sum |a_i|^2 = 1$

measurement : $\sum_{i=0}^{d-1} a_i |i\rangle \xrightarrow{|a_i|^2} |i\rangle$

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.

(Unitary operators and state space evolution)

In the last class, we saw the hadamard basis $\{|+\rangle, |-\rangle\}$ of $\mathbb{C}^2$. We can write the change of basis matrix from $\{|0\rangle, |1\rangle\}$ to $\{|+\rangle, |-\rangle\}$ as

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

The matrix H is called the hadamard gate. Observe that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, 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.

"if and only if"

(Unitary)

A complex-valued matrix U is unitary iff

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

Where

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & \\ \vdots & & \ddots & \\ a_{n1} & & & a_{nn} \end{bmatrix}^\dagger = \begin{bmatrix} a_{11}^* & a_{21}^* & \cdots & a_{n1}^* \\ a_{12}^* & a_{22}^* & & \\ \vdots & & \ddots & \\ a_{1n}^* & & & a_{nn}^* \end{bmatrix}$$

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

Circuit notation

In circuit notation, a unitary is a labeled box

$$-\boxed{U}-$$

Ex.

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 (matrix) gate already, which maps

$$X: \left.\begin{array}{l} |0\rangle \longmapsto |1\rangle \\ |1\rangle \longmapsto |0\rangle \end{array}\right\} \text{bit flip}$$

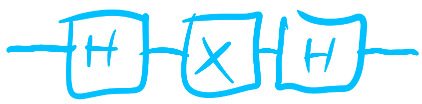
The Z gate is sometimes called a phase flip:

$$Z: \begin{array}{l} |0\rangle \longmapsto |0\rangle \\ |1\rangle \longmapsto \underbrace{(-1)}_{\text{phase}}|1\rangle \end{array}$$

The two are related by a basis change:

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

In circuit notation, HXH is written



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

$$Z|+\rangle = Z\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle$$

$$Z|-\rangle = Z\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = |+\rangle$$

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

$$X = HZH$$

(Unitaries are norm preserving)

A crucial property of unitary transformations is that they are inner product preserving:

$$\langle Uv, Uu\rangle = (\langle v|U^\dagger)(U|u\rangle) = \langle v|U^\dagger U|u\rangle = \langle v|u\rangle$$

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

$$\| U|u\rangle \| = \sqrt{\langle Uu, Uu\rangle} = \sqrt{\langle u,u\rangle} = \| |u\rangle \|$$

Ex.

Is the transformation $H_0 : \begin{matrix} |0\rangle \mapsto |+\rangle \\ |1\rangle \mapsto |+\rangle \end{matrix}$ unitary?

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

$$H_0|\psi\rangle = (a+b)|+\rangle = |\psi'\rangle$$

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

We could have also written

$$H_0 = \frac{1}{\sqrt{2}} \begin{array}{c} \begin{matrix} |0\rangle & |1\rangle \end{matrix} \\ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \end{array}$$

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

(Columns of unitaries)

The columns of an $n \times n$ unitary matrix U form an orthonormal basis $\{|e_i\rangle\}$ of $\mathbb{C}^n$, and U is the change of basis matrix $\{|i\rangle\} \underset{U^{-1}}{\overset{U}{\rightleftarrows}} \{|e_i\rangle\}$

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 $A : \mathcal{H} \longrightarrow \mathcal{H}$. Recall that linear means that for all $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$, $a, b \in \mathbb{C}$

$$A(a|\psi\rangle + b|\varphi\rangle) = aA|\psi\rangle + bA|\varphi\rangle$$

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 $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$ as

$$|\psi\rangle\langle\varphi|$$

This operator (linearly, by definition) maps

$$|\Phi\rangle \longmapsto \langle\varphi|\Phi\rangle\,|\psi\rangle$$

Using Dirac notation, this is simply

$$\begin{aligned}(|\psi\rangle\langle\varphi|)\,|\Phi\rangle &= |\psi\rangle\overbrace{(\langle\varphi|\Phi\rangle)}^{\text{scalar}} \\ &= \langle\varphi|\Phi\rangle\,|\psi\rangle\end{aligned}$$

Ex.

Let $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ i\end{bmatrix}$

1. What is the matrix of $|\psi\rangle\langle\psi|$?

$$|\psi\rangle\langle\psi| = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ i\end{bmatrix}\cdot\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -i\end{bmatrix}$$
$$= \frac{1}{2}\begin{bmatrix}1 & -i\\ i & 1\end{bmatrix}$$

2. What is the matrix of $|0\rangle\langle 0|$?

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

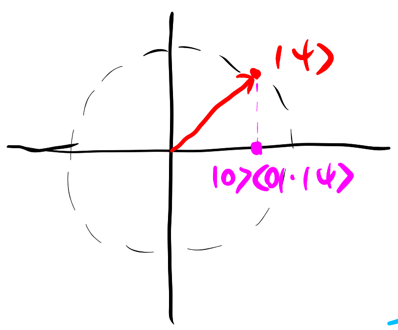
3. What is $(|0\rangle\langle 0|)|\psi\rangle$?

$$\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\cdot\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ i\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 0\end{bmatrix}$$

4. What is $(|1\rangle\langle 1|)|\psi\rangle$ in Dirac notation?

$$|1\rangle\langle 1|\cdot\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}|1\rangle\overbrace{\langle 1|\cdot|0\rangle}^{0} + \frac{i}{\sqrt{2}}|1\rangle\overbrace{\langle 1|\cdot|1\rangle}^{1}$$
$$= \frac{i}{\sqrt{2}}|1\rangle$$

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



Not norm preserving, hence not unitary!

(Projectors, formal definition)

An operator P on $\mathcal{H}$ is a projector iff

$$P^2 = P$$

I.e. projecting onto the same line (or subspace) again does nothing since we're already on the line.

(Resolution of the identity)

Let $\{|e_i\rangle\}$ be a basis of $\mathcal{H}$. Then

$$I = \sum_i |e_i\rangle\langle e_i|$$

Ex.

In $\mathbb{C}^2$, we have $|0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $|1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$$|0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \checkmark$$

With the basis $\{|+\rangle, |-\rangle\}$,

$$|+\rangle\langle +| = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$|-\rangle\langle -| = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

$$|+\rangle\langle +| + |-\rangle\langle -| = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \checkmark$$

(Theorem, matrix representations)

Let $\{|e_i\rangle\}$ be an orthonormal basis of $\mathcal{H}$. Then any linear operator T on $\mathcal{H}$ can be written as

$$T = \sum_{i,j} T_{i,j} |e_i\rangle\langle e_j|$$

where $T_{i,j} = \langle e_i | T | e_j \rangle$

Pf.

$$T = ITI = \left(\sum_i |e_i\rangle\langle e_i|\right) T \left(\sum_j |e_j\rangle\langle e_j|\right)$$
$$= \sum_{i,j} |e_i\rangle \left(\langle e_i | T | e_j\rangle\right) \langle e_j|$$
$$= \sum_{i,j} T_{i,j} |e_i\rangle\langle e_j| \qquad \square$$

The expression $\sum_{ij} T_{ij} |e_i\rangle\langle e_j|$ is the matrix of T over the basis $\{|e_i\rangle\}$. In particular, observe:

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

So $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|$

Aside

Formally, the space of linear operators on $\mathcal{H}$, denoted $\mathcal{L}(\mathcal{H})$ is a vector space. The above Thm states that $\{|e_i\rangle\langle e_j|\}$ is a basis of $\mathcal{L}(\mathcal{H})$.

(Back to quantum)

All of this (aside from introducing the language of operators which we will frequently come back to) is to say that the dagger of $T = \sum_{ij} T_{ij} |e_i\rangle\langle e_j|$ can be written concisely as

conjugated   swapped

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

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

(Reversibility (preview))

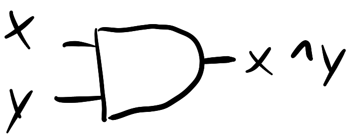
We close with the observation that unitary evolution implies the reversibility of time (not actually, just state evolution). In particular, if a computation sends

$$|\psi\rangle \xmapsto{U} |\varphi\rangle$$

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

$$|\varphi\rangle \xmapsto{U^{-1}} |\psi\rangle$$

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



If $x \wedge y = 0$, can we retrieve the values of x and y?

NO! $(0 \wedge 0 = 0 = 0 \wedge 1 = 1 \wedge 0)$

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