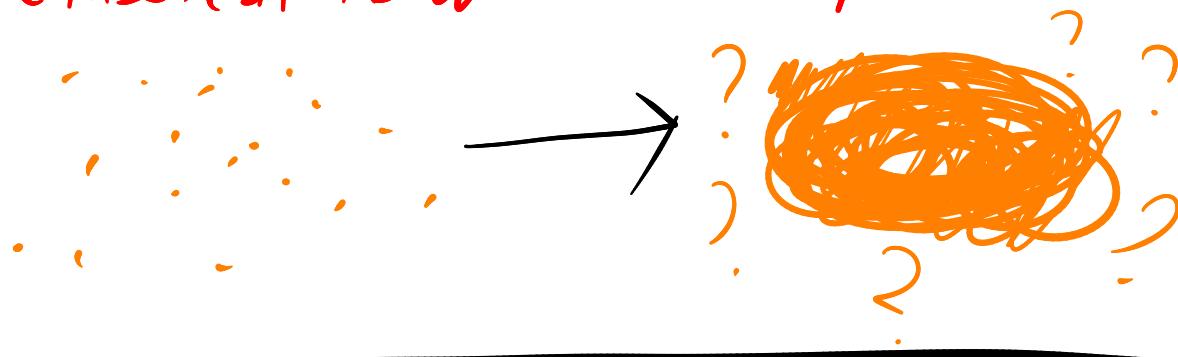


# CMPT 476 Lecture 3

From classical to quantum computation



Last class we saw two models of comp.

Classical  $\rightarrow$  States:  $\{0,1\}^n$

gates:  $\{0,1\}^n \rightarrow \{0,1\}^m$

probabilistic  $\rightarrow$  States: prob. vectors  $p \in \mathbb{R}^n$   
gates: Stoch. matrices  $A \in \mathbb{R}^{n \times n}$

Like these models, quantum computing is built on a notion of **states** and **gates**, with one additional ingredient of **measurements**. As a preview,

Quantum  $\rightarrow$  States: unit vectors  $v \in \mathbb{C}^n$   
gates: unitary matrices  $U \in \mathbb{C}^{n \times n}$   
measurement: ???

Today we begin to build a model of **quantum computation**, learning about Dirac notation and reviewing linear algebra along the way.

## (State of a physical system)

The state of an isolated physical system is a unit vector in a Hilbert space  $H$ . described by

In the finite-dimensional case (all we care about) we can take  $H$  as  $\mathbb{C}^d$  (complex vector space of dimension  $d$ ).

Let's unpack this postulate!

## (Dirac notation)

Let  $V$  be a vector space (VS). We write

$|v\rangle$  (Ket)

to denote a vector in  $V$ . The  $v$  here is a label and can be anything, e.g.  $|4\rangle$ ,  $|0\rangle$ ,  $|z\rangle$

## (Norm)

Let  $|v\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in \mathbb{C}^n$ . The (Euclidean) norm of  $|v\rangle$  is

$$\| |v\rangle \| = \sqrt{\sum_{i=1}^n |a_i|^2}$$

Recall that for  $a = a_1 + i a_2 \in \mathbb{C}$ ,  $a^* = a_1 - i a_2$

$$|a|^2 = a a^* = a_1^2 + a_2^2$$

Complex conjugate

## (Unit vector)

A unit vector  $|v\rangle$  has norm 1 (i.e.  $\| |v\rangle \| = 1$ )

Ex.

The following are unit vectors:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{3}} \begin{bmatrix} \sqrt{3} \\ 1 \end{bmatrix}, \frac{1}{2} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

The following are not

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \end{bmatrix}, \begin{bmatrix} 1-i \\ 0 \end{bmatrix}, \frac{1}{3} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

(Inner products)

Recall that the inner product of

$$v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}, u = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \in \mathbb{C}^n \text{ is defined as}$$

$$\langle v, u \rangle = \sum_{i=1}^n v_i^* u_i = [v_1^* \dots v_n^*] \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}$$

The row-vector  $[v_1^* \dots v_n^*]$  is the conjugate-transpose or Hermitian conjugate of  $v$ , denoted  $v^*$   
( $v$ -dagger)

We have special notation for  $v^*$  in Dirac notation:

$$(|v\rangle)^+ = \langle v | \quad (\text{Bra})$$

Then we write

$$\langle v, u \rangle = \langle v | \cdot | u \rangle = \langle v | u \rangle \quad (\text{Bra-Ket})$$

## (Properties of the inner product)

Let  $|v\rangle, |u\rangle, |w\rangle \in \mathbb{C}^n$  and  $\alpha, \beta \in \mathbb{C}$ . Then

1.  $\langle v|(\alpha|u\rangle + \beta|w\rangle) = \alpha\langle v|u\rangle + \beta\langle v|w\rangle$
2.  $\langle v|v\rangle = \| |v\rangle \|^2 \geq 0$
3.  $\langle v|u\rangle = \langle u|v\rangle^*$

useful for  
computation

## (Orthonormal basis)

Let  $H$  be a Hilbert space of dim.  $n$  (i.e.  $\mathbb{C}^n$ )

An **orthonormal basis** of  $H$  is a set

$$\{|e_i\rangle\} \subseteq H$$

of size  $n$  such that

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

Then every vector  $|v\rangle \in H$  can be written as

$$|v\rangle = \sum_{i=1}^n q_i |e_i\rangle, \quad q_i \in \mathbb{C}$$

(linear combination)

## (Aside: dual spaces)

The **Bra**  $\langle v|$  is really an element of the **Dual Space** of  $H$ ,  $H^*$ . The dual space is a VS of linear operators  $\langle v|: V \rightarrow \mathbb{C}$

$$|u\rangle \mapsto \langle v|u\rangle$$

If  $H$  has orthonormal basis  $\{|e_i\rangle\}$ , then

$H^*$  has orthonormal basis  $\{\langle e_i|\}$

## (Qubits (finally 😊))

The smallest non-trivial Hilbert space is  $\mathbb{C}^2$ . We say a qubit has state space  $\mathbb{C}^2$ . We define the computational basis of  $\mathbb{C}^2$  as

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

We say that a state

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

is in a **superposition** of  $|0\rangle$  and  $|1\rangle$ , with amplitudes  $a$  &  $b$ , respectively.

Ex.

Let  $|\psi\rangle = \sqrt{\frac{2}{3}}|0\rangle + \frac{i}{\sqrt{3}}|1\rangle$ ,  $|\varphi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ .

$$\begin{aligned} 1. \langle 0|\psi\rangle &= \langle 0| \left( \sqrt{\frac{2}{3}}|0\rangle + \frac{i}{\sqrt{3}}|1\rangle \right) \\ &= \sqrt{\frac{2}{3}} \underbrace{\langle 0|0\rangle}_0 + \frac{i}{\sqrt{3}} \underbrace{\langle 0|1\rangle}_0 \\ &= \sqrt{\frac{2}{3}} \end{aligned}$$

$$\begin{aligned} 2. \langle \psi|\varphi\rangle &= \left( \sqrt{\frac{2}{3}}\langle 0| - \frac{i}{\sqrt{3}}\langle 1| \right) \left( \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \\ &= \sqrt{\frac{2}{3 \cdot 2}} \langle 0|0\rangle + \underbrace{\sqrt{\frac{2}{3 \cdot 2}} \langle 0|1\rangle - \frac{i}{\sqrt{3 \cdot 2}} \langle 1|0\rangle - \frac{i}{\sqrt{3 \cdot 2}} \langle 1|1\rangle}_0 \\ &= \frac{1}{\sqrt{3}} - \frac{i}{\sqrt{3 \cdot 2}} \end{aligned}$$

Much easier than explicitly writing vectors when they get large...

## (More about qubits)

In principle, any physical system with 2 distinct states  $|0\rangle$  and  $|1\rangle$  is a qubit. However, to use it as a qubit, we need to maintain coherence of superpositions  $a|0\rangle + b|1\rangle$ . Examples of such systems include

- Photons in <sup>(tensor product)</sup> 2 different locations/paths
- Photons with horizontal or vertical polarization
- Spin- $\frac{1}{2}$  particles <sup>[g]</sup> <sub>= [ae]</sub> (no idea what these are)
- An electron in <sup>af</sup> its lowest energy orbital (its ground state) or <sup>ag</sup> a higher energy orbital
- And many more...

<sup>bg</sup>  
<sup>ce</sup>  
<sup>cf</sup>  
<sup>cg</sup>

## (Qudits)

If a system has 3 distinct states, we call it a quutrit and model its state in  $\mathbb{C}^3$  with basis

$$\{|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, |2\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}\}$$

More generally we can have systems with  $d$  states, called a qudit, which has state space  $\mathbb{C}^d$  and basis

$$\{|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \dots, |d-1\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}\}$$

When doing outer product, you are doing matrix multiplication

## (Aside:

A system of "n" qubits has  $2^n$  states, so we can describe its state space as  $\mathbb{C}^{2^n}$  and for  $0 \leq i \leq 2^n - 1$  associate  $|i\rangle$  with the state

$$|i_n\rangle|i_{n-1}\rangle\dots|i_1\rangle$$

Where  $i_n\dots i_0$  is the binary expansion of  $i$ )

## (Operations on States)

What can we do with a quantum state  $|ψ\rangle$ ?

We have two options:

1. Unitary (norm-preserving) linear operators
2. Measurement

We'll leave 1. for now and just talk about 2.

## (Measurement)

Don't know anything about the qubit until you measure it, limiting it to one possible state.

Given a qubit in the state  $α|0\rangle + β|1\rangle$ , measuring the state produces a result and a new state.

- With probability  $|\alpha|^2$ , result is 0

Difference between state and result:

result tells you what state it is in,  
the state is the vector representing that state

- With probability  $|\beta|^2$ , result is 1

new state is  $|1\rangle$

Intuition is measurement collapses the uncertainty state  $α|0\rangle + β|1\rangle$  to a particular state  $|0\rangle$  or  $|1\rangle$ .

The notation for measurement is



Ex.

Let  $|ψ\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{i}{2}|1\rangle$ . What are some examples of destructive measurements?

Measuring  $|ψ\rangle$  produces:

$$|0\rangle \text{ with probability } \left|\frac{\sqrt{3}}{2}\right|^2 = \frac{3}{4}$$

$$|1\rangle \text{ with probability } \left|\frac{i}{2}\right|^2 = \frac{i \cdot -i}{4} = \frac{1}{4}$$

We can verify that  $\frac{3}{4} + \frac{1}{4} = 1$  ☺

What would it mean to measure a qutrit?

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$$

Same thing!

- Get result 0 and state  $|0\rangle$  w/ prob.  $|\alpha|^2$
- Result 1 and state  $|1\rangle$  w/ prob.  $|\beta|^2$
- Result 2 and state  $|2\rangle$  w/ prob.  $|\gamma|^2$

In principle we can measure a state  $|\psi\rangle \in \mathcal{H}$  over **any orthonormal basis** of  $\mathcal{H}$ . We will see why we can do so in practice later on.

### (Measurement over a basis)

More generally, given a basis  $\{|e_i\rangle\}$  of  $\mathbb{C}^d$ , measuring the state  $\sum_i a_i |e_i\rangle$  produces the result  $i$  and state  $|e_i\rangle$  with probability  $|a_i|^2$

how much one vector projects onto one of the basis vectors,  
and factor out the component used

Observe that if  $|\psi\rangle = \sum_i a_i |e_i\rangle$ , then

$$a_i = \langle e_i | \psi \rangle$$

$$\text{and hence } |a_i|^2 = |\langle e_i | \psi \rangle|^2$$

never basis is mentioned, assume it is an orthonormal basis

### Notation

In circuit diagrams, we denote a qubit/qudit by a line/wire, and measurement in the computational basis by , e.g.



Ex.

Another common basis of  $\mathbb{C}^2$  is the **hadamard basis**

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{Also known as the x-basis}$$

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

Observe that

$$\langle +|+ \rangle = \frac{1}{2}(\langle 0|0 \rangle + \langle 0|1 \rangle + \langle 1|0 \rangle + \langle 1|1 \rangle) = 1$$

$$\langle -|- \rangle = \frac{1}{2}(\langle 0|0 \rangle - \langle 0|1 \rangle - \langle 1|0 \rangle + \langle 1|1 \rangle) = 1$$

$$\langle +|- \rangle = \frac{1}{2}(\langle 0|0 \rangle - \langle 0|1 \rangle + \langle 1|0 \rangle - \langle 1|1 \rangle) = 0$$

and hence  $\{|+\rangle, |- \rangle\}$  is orthonormal. Also note that

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

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

So measuring the state  $|0\rangle$  in the  $\{|+\rangle, |- \rangle\}$  basis produces

- $|+\rangle$  with prob.  $\frac{1}{2}$

- $|- \rangle$  with prob.  $\frac{1}{2}$

<sup>Text</sup> Geometrically, the  $|+\rangle, |- \rangle$  basis is a  $45^\circ$  rotation of  $|0\rangle, |1\rangle$

