Reversible Computing and Quantum Information Basics

COMS 4281

Last Time: classical reversible computing

d-dimensional systems:

- State labels: $|0\rangle, \ldots, |d-1\rangle$.
- Transformations T: permutations on d labels

Composite systems using *tensor product*:

- If system A in state $|x\rangle$, system B in state $|y\rangle$, then joint state is $|x\rangle \otimes |y\rangle$.

Can implement universal classical computation.

Reversible computing, linear algebra style

As a sneak preview of quantum math, let's put reversible computing on a linear algebraic foundation: the math of vectors, matrices, tensors.

Reversible computing, linear algebra style

As a sneak preview of quantum math, let's put reversible computing on a linear algebraic foundation: the math of vectors, matrices, tensors.

States of a d-dimensional system S are represented by d-dimensional **column vectors**.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \qquad \cdots \qquad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Transformation matrices

Reversible transformations correspond to $d \times d$ **permutation matrices**.

$$R = \begin{pmatrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \end{pmatrix}$$

Matrix with exactly one 1 in each column and row.

Transformation matrices

Applying transformation R to $|x\rangle$ corresponds to matrix-vector multiplication.

$$|y\rangle = R\,|x\rangle = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Transformation matrices

The transformation corresponding to applying R first and then U corresponds to the matrix product UR. **Note:** order matters!

Transformation matrices

The transformation corresponding to applying R first and then U corresponds to the matrix product UR. **Note:** order matters!

The inverse transformation R^{-1} is simply the matrix inverse of R.

Since R is a permutation matrix, R^{-1} is also the **transpose** $R^\top$ of R, where the rows and columns of R are switched.

$$R = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \qquad R^\top = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Tensor products

Let S_1, S_2 be d-dimensional systems, and $|x\rangle, |y\rangle$ be d-dimensional states.

The tensor product state $|x\rangle \otimes |y\rangle$ is represented as a d^2-dimensional vector, where entries are indexed by some ordering of all states of $S_1 \otimes S_2$.

Tensor products

Let S_1, S_2 be d-dimensional systems, and $|x\rangle, |y\rangle$ be d-dimensional states.

The tensor product state $|x\rangle \otimes |y\rangle$ is represented as a d^2-dimensional vector, where entries are indexed by some ordering of all states of $S_1 \otimes S_2$.

The tensor product transformation $R_1 \otimes R_2$ is represented as a $d^2 \times d^2$ matrix, where rows and columns are indexed by the same ordering of states.

Vector/matrix representations of tensor products implicitly use some ordering that changes depending on the textbook/scientist/API/blog… **make sure you're aware of the convention!**

Tensor products, representations

Let

$$|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}, \qquad |w\rangle = \begin{pmatrix} w_1 \\ \vdots \\ w_d \end{pmatrix}.$$

Then

$$|v\rangle \otimes |w\rangle = \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_2 w_1 \\ \vdots \\ v_d w_d \end{pmatrix}.$$

Tensor products, representations

Let

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1d} \\ \vdots & \ddots & \vdots \\ A_{d1} & \cdots & A_{dd} \end{pmatrix}, \qquad B = \begin{pmatrix} B_{11} & \cdots & B_{1d} \\ \vdots & \ddots & \vdots \\ B_{d1} & \cdots & B_{dd} \end{pmatrix}.$$

Then

$$A \otimes B = \begin{pmatrix} A_{11}B & \cdots & A_{1d}B \\ \vdots & \ddots & \vdots \\ A_{d1}B & \cdots & A_{dd}B \end{pmatrix}$$

is a $d^2 \times d^2$ block matrix.

Tensor products, representations

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \otimes \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 2\begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \\ 3\begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 4\begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \end{pmatrix}$$

Tensor products, representations

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \otimes \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 2 \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \\ 3 \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 4 \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \end{pmatrix}$$

$$= \left(\begin{array}{cc|cc} 0 & 3 & 0 & 6 \\ 2 & 1 & 4 & 2 \\ \hline 0 & 9 & 0 & 12 \\ 6 & 3 & 8 & 4 \end{array} \right).$$

Tensor products, bits

S is a bit, i.e., $d = 2$. Vector representation of states:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad\qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Tensor products, bits

S is a bit, i.e., $d = 2$. Vector representation of states:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Transformations:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Tensor products, bits

Vector representation of two bits:

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Tensor products, bits

Matrix representation of transformations:

$$I \otimes X = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad X \otimes I = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Tensor products, bits

Matrix representation of transformations:

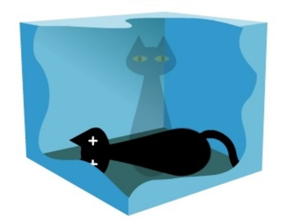
$$\mathrm{CNOT} = \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \end{pmatrix}.$$

First bit: control. Second bit: target.

Making the quantum leap

A **bit** is a classical system with *two* distinguishable states $|0\rangle, |1\rangle$, also called *Classical states*, or *standard basis states*.

A **qubit** (quantum bit) can be in a **superposition** of the classical states $|0\rangle, |1\rangle$.



Mathematically, states of a qubit are **complex linear combination** of $|0\rangle, |1\rangle$:

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\ &= \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \end{aligned}$$

where $\alpha, \beta \in \mathbb{C}$ are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$.

In other words, $|\psi\rangle$ is a two-dimensional unit vector in $\mathbb{C}^2$.

Example: a qubit can be in the state

$$\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle.$$

Another example:

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}.$$

Another example:

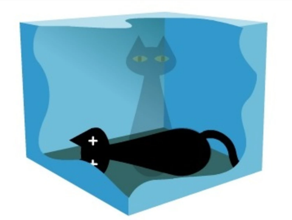
$$\frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}.$$

A non-valid qubit state:

$$i|0\rangle - \frac{1}{2}|1\rangle.$$

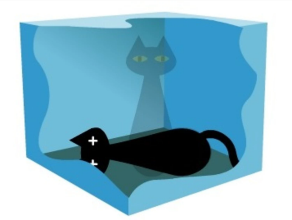
So what *is* a qubit

A qubit in the state $\alpha |0\rangle + \beta |1\rangle$ is commonly said to be $|0\rangle$ and $|1\rangle$ "at the same time". But what does that mean?



So what *is* a qubit

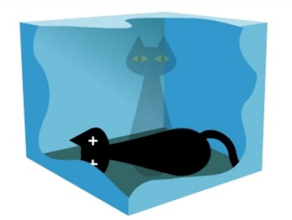
A qubit in the state $\alpha|0\rangle + \beta|1\rangle$ is commonly said to be $|0\rangle$ and $|1\rangle$ "at the same time". But what does that mean?



α, β are like probabilities, except they can be *negative* or even *complex* numbers!

So what *is* a qubit

A qubit in the state $\alpha |0\rangle + \beta |1\rangle$ is commonly said to be $|0\rangle$ and $|1\rangle$ "at the same time". But what does that mean?



α, β are like probabilities, except they can be *negative* or even *complex* numbers!

α, β are called the **amplitudes** of the states $|0\rangle$ and $|1\rangle$, respectively.

Observing qubits

The state of a qubit cannot be directly observed. It must be **measured**, yielding a classical state $|0\rangle$ or $|1\rangle$ with probabilities

$$\Pr[\text{ observing } |0\rangle\ ] = |\alpha|^2 \qquad \Pr[\text{ observing } |1\rangle\ ] = |\beta|^2.$$

Observing qubits

The state of a qubit cannot be directly observed. It must be **measured**, yielding a classical state $|0\rangle$ or $|1\rangle$ with probabilities

$$\Pr[\text{ observing } |0\rangle\ ] = |\alpha|^2 \qquad \Pr[\text{ observing } |1\rangle\ ] = |\beta|^2.$$

Because qubit states have unit length, these probabilities add up to 1.

This formula is called the **Born Rule**.

Observing qubits

After measurement, the system becomes **classical**.

The state of qubit **collapses** to either $|0\rangle$ or $|1\rangle$, and the previous state is lost.

In quantum mechanics, measurement generally disturbs the system.

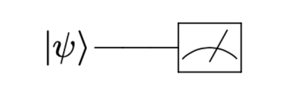
Observing qubits

After measurement, the system becomes **classical**.

The state of qubit **collapses** to either $|0\rangle$ or $|1\rangle$, and the previous state is lost.

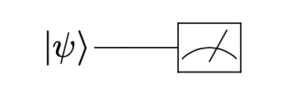
In quantum mechanics, measurement generally disturbs the system.

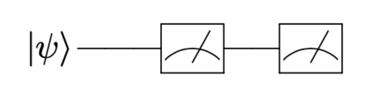
We represent qubit measurements using this diagram:



Observing qubits

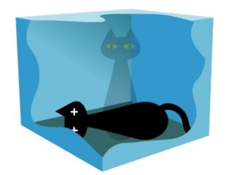
If the state collapses to the classical state $|0\rangle$ and we measure it again, it stays in state $|0\rangle$ **with probability** 1. Same with collapsing to $|1\rangle$.



same as


Measuring a system twice is the same as measuring once.

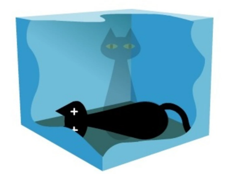
Example: Schrödinger's cat



A box with two classical states:

sleeping cat: $|0\rangle$ awake cat: $|1\rangle$

Example: Schrödinger's cat

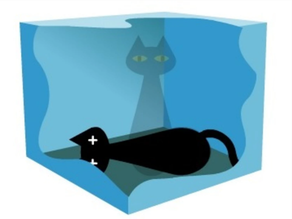


A box with two classical states:

sleeping cat: $|0\rangle$ awake cat: $|1\rangle$

In quantum mechanics, the box can be in a superposition of sleeping and awake cat, *as long as you don't open the box* (i.e. measure it).

Example: Schrödinger's cat

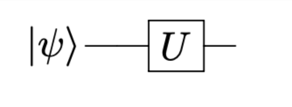


Suppose the box starts in the state $\frac{1}{\sqrt{3}}|0\rangle - i\frac{\sqrt{2}}{\sqrt{3}}|1\rangle$ and is measured.

1. With probability $\left|\frac{1}{\sqrt{3}}\right|^2 = \frac{1}{3}$, the state collapses to $|0\rangle$ (i.e., sleeping cat).
2. With probability $\left|-i\frac{\sqrt{2}}{\sqrt{3}}\right|^2 = \frac{2}{3}$, the state collapses to $|1\rangle$ (i.e., awake cat).

In addition to measurement, the state of a qubit can change via a **unitary transformation**. Just like transformations in classical reversible computing, unitary transformations can be represented as matrices.

We represent a unitary transform *U* acting on state $|\psi\rangle$ using the following circuit diagram:



Several equivalent definitions of unitary matrices

Definition 1. The inverse of U is its Hermitian conjugate $U^\dagger$, pronounced "U dagger", whose (i, j)'th entry is the *complex conjugate* of the (j, i)'th entry of U:

$$U^\dagger_{i,j} = \overline{U}_{j,i}$$

Several equivalent definitions of unitary matrices

Definition 1. The inverse of U is its Hermitian conjugate $U^\dagger$, pronounced "U dagger", whose (i,j)'th entry is the *complex conjugate* of the (j,i)'th entry of U:

$$U^\dagger_{i,j} = \overline{U}_{j,i}$$

Definition 2. U maps unit vectors to unit vectors (i.e. quantum states to quantum states)

Several equivalent definitions of unitary matrices

Definition 1. The inverse of U is its Hermitian conjugate $U^\dagger$, pronounced "U dagger", whose (i, j)'th entry is the *complex conjugate* of the (j, i)'th entry of U:

$$U^\dagger_{i,j} = \overline{U}_{j,i}$$

Definition 2. U maps unit vectors to unit vectors (i.e. quantum states to quantum states)

Definition 3. The rows of U form an orthonormal basis for $\mathbb{C}^d$, and the columns form an orthonormal basis for $\mathbb{C}^d$.

Several equivalent definitions of unitary matrices

Definition 1. The inverse of U is its Hermitian conjugate $U^\dagger$, pronounced "U dagger", whose (i, j)'th entry is the *complex conjugate* of the (j, i)'th entry of U:

$$U^\dagger_{i,j} = \overline{U}_{j,i}$$

Definition 2. U maps unit vectors to unit vectors (i.e. quantum states to quantum states)

Definition 3. The rows of U form an orthonormal basis for $\mathbb{C}^d$, and the columns form an orthonormal basis for $\mathbb{C}^d$.

Definition 4. U preserves the inner products between vectors: inner product between $|\psi\rangle$ and $|\theta\rangle$ is the same as the inner product between $U|\psi\rangle$ and $U|\theta\rangle$.

Examples of qubit unitary matrices

Identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

For all qubit states $|\psi\rangle$, $I\,|\psi\rangle = |\psi\rangle$.

Examples of qubit unitary matrices

Bit flip matrix $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Examples of qubit unitary matrices

Bit flip matrix $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle$$

Examples of qubit unitary matrices

Bit flip matrix $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle$$

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle\ .$$

So far, have only seen classical transformations.

Examples of qubit unitary matrices

Phase flip matrix $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Examples of qubit unitary matrices

Phase flip matrix $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$$Z\,|0\rangle = |0\rangle \qquad Z\,|1\rangle = -\,|1\rangle$$

Examples of qubit unitary matrices

Phase flip matrix $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle$$

$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle \ .$$

Examples of qubit unitary matrices

Hadamard matrix $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$H\left|0\right\rangle = \cdots \text{(do on board)} \cdots$$

$$H\left|1\right\rangle = \cdots \text{(do on board)} \cdots$$

Examples of qubit unitary matrices

Hadamard matrix $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$H |0\rangle = \cdots \text{(do on board)} \cdots$$

$$H |1\rangle = \cdots \text{(do on board)} \cdots$$

H maps classical basis states $|0\rangle, |1\rangle$ into **quantum** superpositions.