Quantum Information Basics

COMS 4281 (Fall 2024)

Admin

1. Pset1 released Sept 18. Due October 6. Start thinking about forming problem set teams!
2. This week's practice sheet is available on course homepage. They will be discussed in office hours.
3. Weekly quiz is on gradescope tonight. Must complete it by Sunday night at 11:59pm.

Last Time: basics of a qubit

A qubit is a two-dimensional system, whose state is described by a **two-dimensional complex vector** $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.

If a qubit in the state $|\psi\rangle$ is measured, it **collapses** to the classical state $|0\rangle$ with probability $|\alpha|^2$ and the state $|1\rangle$ with probability $|\beta|^2$.

A qubit can also undergo **unitary evolution**, and its state gets updated $|\psi\rangle \mapsto U|\psi\rangle$ for some unitary matrix U.

Last Time: basics of a qubit

Examples of unitary matrices:

- Identity: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- Bit-flip: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- Phase-flip: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Last Time: basics of a qubit

The Hadamard gate turns a classical state into a quantum superposition:

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

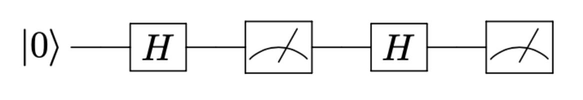
The measurement statistics of $|+\rangle , |-\rangle$ look the same, so can these states be distinguished?

Yes, by first applying a unitary, namely, the Hadamard matrix again!

$$|0\rangle = H\,|+\rangle \qquad |1\rangle = H\,|-\rangle \ .$$

Quantum vs classical bits, take 2

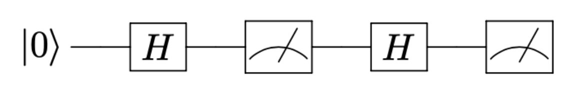
Consider **Experiment A**:



Circuit analysis: Do on board.

Quantum vs classical bits, take 2

Consider **Experiment A**:

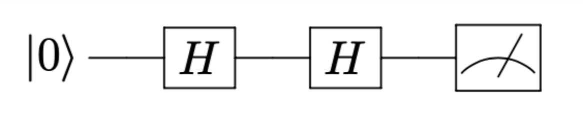


Final distribution of outcomes: $|0\rangle, |1\rangle$ with equal probability.

Based on this, one might conclude that the Hadamard gate simply creates a random classical bit!

Quantum vs classical bits, take 2

Consider **Experiment B**:

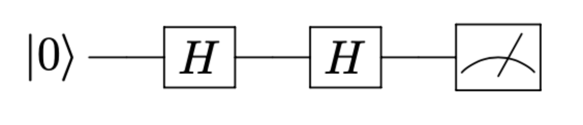


Measure only at the end.

Circuit analysis: Do on board.

Quantum vs classical bits, take 2

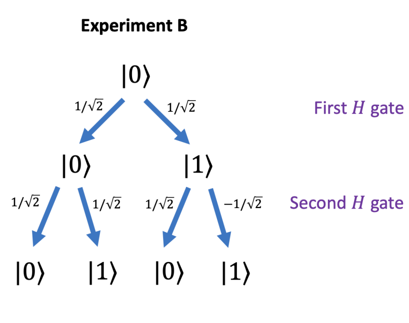
Consider **Experiment B**:



Final distribution of outcomes: $|0\rangle$ always.

Inserting or removing intermediate measurement can drastically change the behavior of a quantum system!.

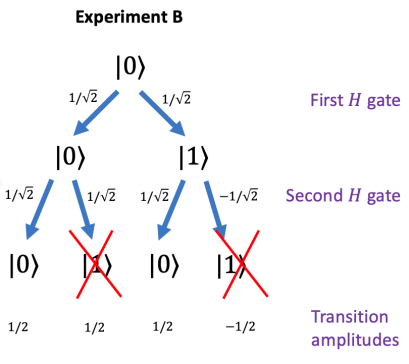
Quantum interference



Applying multiple unitary operations to a qubit gives rise to a tree of "paths" between states.

An edge between state $|a\rangle$ to $|b\rangle$ has a transition amplitude associated with, depending on the unitary.

Quantum interference

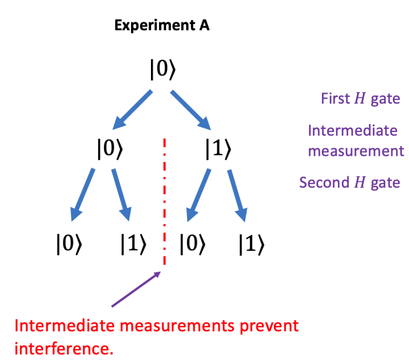


Each path has associated transition amplitude: product of amplitudes along the path.

Before measurement, amplitude of ending up in state $|b\rangle$ is the sum of transition amplitudes of all paths that end at $|b\rangle$.

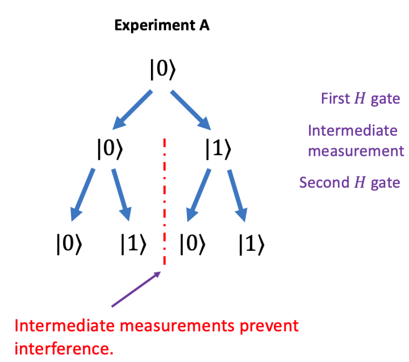
Since transition amplitudes can be negative or even complex, the paths can constructively or destructively interfere with each other!

Quantum interference



If there is an intermediate measurement, only paths consistent with the measurement outcome are added up.

Quantum interference



Takeway: Intermediate measurements destroy superpositions and prevent interference!

In classical physics, we only add up probabilities, which are positive. In quantum physics, we add up amplitudes, which can be negative. Interference is an example of "quantum weirdness".

Summary of one qubit

1. A qubit state $|\psi\rangle$ is a two-dimensional unit vector
2. Measuring qubits yields $|0\rangle, |1\rangle$ with probabilities determined by the Born rule.
3. State of qubit can also change via unitary matrices.
4. Positive and negative transition amplitudes lead to interference.
5. Measurements disrupt interference.

Dirac Notation

The $|\psi\rangle$ notation is called **Dirac notation**, after the quantum physicist Paul Dirac.

Mathematically, $|\psi\rangle$ ("ket vector") is a **column vector**.

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

The **dual/Hermitian conjugate** of column vectors (i.e., row vectors) are called "bra vectors":

$$\langle 0| = \begin{pmatrix} 1\,, & 0 \end{pmatrix} \qquad \langle 1| = \begin{pmatrix} 0\,, & 1 \end{pmatrix}$$

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \langle\psi| = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \end{pmatrix} = \overline{\alpha}\,\langle 0| + \overline{\beta}\,\langle 1|$$

$\overline{\alpha}, \overline{\beta} =$ **complex conjugates** of α, β.

Let $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|\theta\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$ be column vectors. Then we can take their inner product:

$$\langle\psi|\ |\theta\rangle = \langle\psi \mid \theta\rangle = \begin{pmatrix}\overline{\alpha}\,, & \overline{\beta}\end{pmatrix}\begin{pmatrix}\gamma \\ \delta\end{pmatrix} = \overline{\alpha}\gamma + \overline{\beta}\delta$$

Note the order of $|\psi\rangle$ and $|\theta\rangle$ matters!

$$\langle\theta \mid \psi\rangle = \overline{\gamma}\alpha + \overline{\delta}\beta = \overline{\langle\psi \mid \theta\rangle}$$

More generally, if

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{d-1} |d-1\rangle$$

$$|\theta\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle + \cdots + \beta_{d-1} |d-1\rangle$$

are d-dimensional column vectors, then their inner product is

$$\langle\psi \mid \theta\rangle = \overline{\alpha}_0\beta_0 + \cdots + \overline{\alpha}_{d-1}\beta_{d-1}$$

Dirac notation is very useful for quickly identifying scalars, row and column vectors, matrices in complicated expressions.

Naming: "bra" + "ket" = "bracket"

Composite quantum systems

If qubit 1 is in state $|\psi_1\rangle$, and qubit 2 is in state $|\psi_2\rangle$, then the joint state of both qubits is

$$|\psi_1\rangle \otimes |\psi_2\rangle$$

This is a **four-dimensional** unit vector in the tensor product space $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Hilbert spaces and tensor products

Quantum states live in a **Hilbert space** H. There's a precise mathematical definition, but for our purposes the important aspects of Hilbert spaces are:

- Finite-dimensional Hilbert spaces are isomorphic to $\mathbb{C}^d$ for some dimension d.
- There is an *inner product* operation between two vectors.
- You can take *tensor products* of Hilbert spaces.

Hilbert spaces and tensor products

A: Hilbert space with orthonormal basis $\{|a_1\rangle, \ldots, |a_m\rangle\}$

B: Hilbert space with orthonormal basis $\{|b_1\rangle, \ldots, |b_n\rangle\}$

$A \otimes B$ is $m \times n$ dimensional Hilbert space with basis

$$\left\{ |a_i\rangle \otimes |b_j\rangle \right\}_{1 \leq i \leq m, 1 \leq j \leq n}$$

In general, an element of the Hilbert space $A \otimes B$ is a vector of the form:

$$\sum_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \alpha_{ij} |a_i\rangle \otimes |b_j\rangle$$

where α_{ij} are complex numbers.

Hilbert spaces and tensor products

The Hilbert space for two qubits is $\mathbb{C}^2 \otimes \mathbb{C}^2$, with basis $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$.

We can abbreviate this to

$$|0,0\rangle \qquad |0,1\rangle \qquad |1,0\rangle \qquad |1,1\rangle$$

Hilbert spaces and tensor products

If $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi_2\rangle = \gamma|0\rangle + \delta|1\rangle$, then

$$|\psi_1\rangle \otimes |\psi_2\rangle = \alpha\gamma|0,0\rangle + \alpha\delta|0,1\rangle + \beta\gamma|1,0\rangle + \beta\delta|1,1\rangle .$$

In general, a two-qubit state is *some* linear combination of $|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle$.

$$|\psi\rangle = a|0,0\rangle + b|0,1\rangle + c|1,0\rangle + d|1,1\rangle = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

where a, b, c, d are complex numbers such that $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

Examples of two-qubit states

Example:

$$|0\rangle \otimes |1\rangle$$

Example:

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

Example:

$$\frac{1}{\sqrt{2}}\Big(|0,0\rangle + |1,1\rangle \Big) \; .$$

Example:

$$\frac{1}{\sqrt{6}}\,|0,1\rangle - \frac{1}{\sqrt{6}}\,|1,0\rangle + \sqrt{\frac{2}{3}}\,|1,1\rangle \; .$$

Hilbert spaces and tensor products

Inner product between $|\varphi\rangle = \sum_{ij} \alpha_{ij} |i,j\rangle$ and $|\theta\rangle = \sum_{ij} \beta_{ij} |i,j\rangle$:

$$\langle\varphi|\theta\rangle = \Big(\sum_{i,j} \overline{\alpha}_{ij} \langle i,j|\Big)\Big(\sum_{k,\ell} \beta_{k\ell} |k,\ell\rangle\Big) = \sum_{i,j} \overline{\alpha}_{ij}\beta_{ij}$$

The **cross-terms** $\langle i,j|k,\ell\rangle = 0$ if $i \neq k$ or $j \neq \ell$.

Quantum entanglement

Not all states in $\mathbb{C}^2 \otimes \mathbb{C}^2$ can be written as $|\psi_1\rangle \otimes |\psi_2\rangle$ (called **product states**).

An example of an **entangled state**, called **Einstein-Podolsky-Rosen (EPR)** pair or **Bell pair**.

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\Big(|0,0\rangle + |1,1\rangle \Big)$$

Entanglement is a **uniquely quantum phenomenon**: one qubit is intimately linked to another qubit in a way that classical physics cannot explain.

Measuring composite systems

$|\psi\rangle = \sum_{i,j} \alpha_{ij} |i,j\rangle$ two-qubit state. Measuring $|\psi\rangle$ yields

$$|i,j\rangle \qquad \text{with probability} \qquad |\alpha_{ij}|^2.$$

and state collapses to $|i,j\rangle$.

Unitary evolution of composite systems

If U, V are single-qubit unitaries acting on $\mathbb{C}^2$, then $U \otimes V$ is a *two-qubit* unitary acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$U \otimes V |\psi\rangle = \sum_{i,j} \alpha_{ij} (U \otimes V) |i,j\rangle = \sum_{i,j} \alpha_{ij} U |i\rangle \otimes V |j\rangle$$

Like with states, not all two-qubit unitaries W are **product unitaries**.

Example of an **entangling unitary**: $CNOT$ unitary.

Unitary evolution of composite systems

$CNOT$ gate can transform a product state to an entangled state:

$$CNOT \, |+\rangle \otimes |0\rangle = (\text{... do on board...})$$

No-Cloning Theorem

Classical bits are easily copied. Quantum information is different.

No-Cloning Theorem: Quantum Info cannot be copied.

Formal statement: there is no two-qubit unitary U such that for all single-qubit states $|\psi\rangle \in \mathbb{C}^2$,

$$U |\psi\rangle \otimes \underbrace{|0\rangle}_{\text{ancilla}} = |\psi\rangle \otimes |\psi\rangle$$

No-Cloning Theorem Proof

Suppose there was a Quantum Cloner U. Then on one hand:
$U\left|0\right\rangle \otimes \left|0\right\rangle = \left|0\right\rangle \otimes \left|0\right\rangle$.

and: $U\left|+\right\rangle \otimes \left|0\right\rangle = \left|+\right\rangle \otimes \left|+\right\rangle$.

but unitary operators have to preserve inner products!

No-Cloning Theorem Proof

So that means

$$\Big(\langle 0| \otimes \langle 0| \Big)\Big(|+\rangle \otimes |+\rangle \Big) = \Big(\langle 0| \otimes \langle 0| \Big)\Big(|+\rangle \otimes |0\rangle \Big)$$

But left-hand side is: $\langle 0|+\rangle \cdot \langle 0|+\rangle = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} = \frac{1}{2}$

and right-hand side is: $\text{RHS} : \langle 0|+\rangle \cdot \langle 0|0\rangle = \frac{1}{\sqrt{2}} \cdot 1 = \frac{1}{\sqrt{2}}$

Contradiction!

Exponentiality of Quantum Mechanics

The Hilbert space of n qubits is $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} = (\mathbb{C}^2)^{\otimes n}$.

This is a 2^n-dimensional Hilbert space. Each qubit doubles the dimensionality of the space.

A general state can be written as

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle .$$

Exponentiality of Quantum Mechanics

Applying a unitary U to a state $|\psi\rangle$ appears, mathematically, to be doing exponentially many computations in parallel:

$$U|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x U|x\rangle.$$

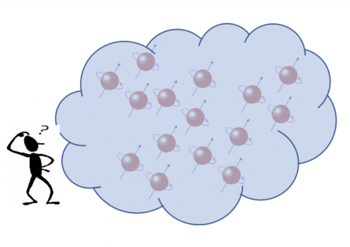
Nature is doing an incredible amount of work for us.

But we can only access the exponential information in $|\psi\rangle$ in a limited way.

Exponentiality of Quantum Mechanics

Quantum states are fragile, because of measurement. But measurement is the only way for us classical beings to access the information.

This leads to a **fundamental tension** in quantum computing.



Want to take advantage of Nature's extraordinary computation power, but it is hidden being a **veil of measurement**.