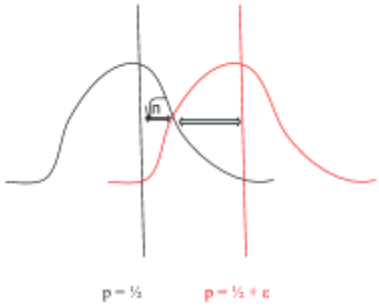
Lecture 5, Tues Jan 30: Coin Problem, Inner Products, Multi-Qubit States, Entanglement

Say you have a coin, and you want to figure out if it's fair ($p = \frac{1}{2}$) or if it's biased $p = \frac{1}{2} + \varepsilon$( ). How would you go about doing so?



The classical approach to solving this problem would be to flip the coin a lot (about $\frac{1}{\varepsilon^2}$ times), keeping track of heads and tails until you have a strong degree of certainty that randomness isn't affecting your results. Standard probability stuff.

This requires about $\log \frac{1}{\varepsilon}$ bits of memory to store the running totals. In fact, there's a theorem by Hellman and Cover from the 70's that says that any protocol to solve this problem requires that much storage.

What if instead we used quantum states?

We can start with a qubit in the $|0\rangle$ state, and consider the two rotations R_ε and $R_{-\varepsilon}$, which rotate by ε and $-\varepsilon$ radians respectively. We can repeatedly flip the coin, and if it lands tails apply R_ε (rotating clockwise) and if it lands heads apply $R_{-\varepsilon}$ (rotating counterclockwise). After many flips (order $\approx \frac{1}{\varepsilon^2}$) we can then measure the qubit and statistically infer that if it's in the $|0\rangle$ state, the coin was fair, while if it's in the $|1\rangle$ state, the coin is biased.

- Won't counting out the right number of steps again require a lot of storage?
  - No. We can give a protocol with a half-life (some independent probability of halting at each step) causing it to repeat approximately the number of times we want it to.
- What about if the qubit drifts by a multiple of π, won't that make a biased coin look fair?
  - That's possible, but we can make it so that a biased coin is more likely to land on $|1\rangle$ than a fair coin.

Quantum information protocols are like baking souffles.
Opening the oven too early will collapse the souffle.

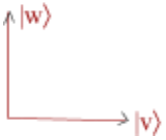
This is our first example of a quantum protocol getting a resource advantage:

the quantum solution takes **1 qubit of storage** as opposed to the classical solution's **bits**.

This result was shown by Professor Aaronson and his former student Andy Drucker.
It wasn't a particularly hard problem, but no one had asked the question before.
There's still "low hanging fruit," even in the mechanics of a single qubit!

Distinguishability of Quantum States

Given two orthogonal quantum states $|v\rangle$ and $|w\rangle$ there's a basis that distinguishes them.

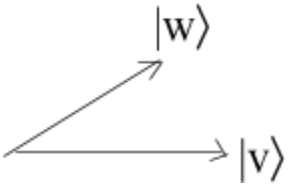


These on the other hand are indistinguishable.

$|\langle v|w\rangle|$ *gives a good measure of the distinguishability of arbitrary states.*

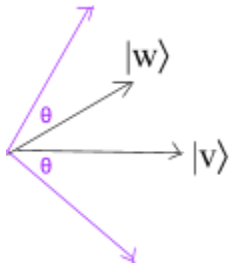
$|\langle v|w\rangle| = 1$ $|\langle v|w\rangle| = 0$

What about these?



More specifically: What measurement would minimize the chance of making a mistake in differentiating $|v\rangle$ from $|w\rangle$?

You may want to measure in $|v\rangle$ $|\text{something else}\rangle$the , basis, as it would eliminate one kind of error completely (not $|v\rangle$getting ensures $|w\rangle$the state was). But if you just want to maximize the probability of getting the right answer, $|v\rangle$and $|w\rangle$if and are equally likely, then there's a better way:



Take the bisector of $|v\rangle$ and $|w\rangle$, and get the angles $45°$ to either side, ensuring each original vector is the same distance to its closest basis vector.

A general state of **2 Qubits** is:

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

The probability of getting $|00\rangle = |\alpha|^2$ Note that $|00\rangle$ is the same as $|0\rangle|0\rangle$ or $|0, 0\rangle$ or $|0\rangle \otimes |0\rangle$

$|01\rangle = |\beta|^2$

$|10\rangle = |\gamma|^2$

$|11\rangle = |\delta|^2$

In principle there's no distance limitation between qubits. One qubit could be on Earth, and the other could be with your friend on the moon.

In such a case, though, you'd only be able to measure the first qubit:

The probability of getting $|0\rangle$ is $|\alpha|^2 + |\beta|^2$ because those are the amplitudes compatible with 0 in the first qubit.

The probability of getting $|1\rangle$ is $|\gamma|^2 + |\delta|^2$

Suppose I measure the first qubit and get the outcome $|0\rangle$. What can I say about the second qubit?

Well we've narrowed down the possibilities to $\alpha|00\rangle$ and $\beta|01\rangle$. The state of the system is thus now in the superposition: $|0\rangle \otimes \frac{\alpha|0\rangle+\beta|1\rangle}{\sqrt{|\alpha|^2+|\beta|^2}}$ ← Don't forget to normalize!

This is called the **Partial Measurement Rule**

Systems collapse however is needed to fit the measurement you made and the outcome you saw.

This is actually the last "basic rule" of quantum mechanics that we'll see in the course. Everything else is just logical consequences of rules we've already covered.

This $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ is the **Controlled NOT**.

Remember: it flips the 2nd bit iff the 1st bit is 1.

What if we wanted to always do NOT on the 2nd bit: $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

This is $\mathbf{I} \otimes \mathbf{NOT}$

/ |

(nothing on 1st bit) with (NOT on 2st bit)

It can be decomposed as: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ which makes it a tensor product unitary.

What if we want **NOT ⊗ I**?

$$\begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{array}{c} \\ \\ \\ \\ 00 \quad 01 \quad 10 \quad 11 \end{array}$$

Remember that rows and columns represent the transformation $f(\text{row}) = \text{col}$
so the amplitude on 00 in the input
is the amplitude on 10 in the output

Very often in quantum information we'll want to take a group of qubits and perform an operation on one of them: say, "Hadamard the third qubit."

What that really means is applying the unitary matrix $I \otimes I \otimes H \otimes \cdots \otimes I$:

The tensor product of the desired operation on the relevant qubit(s), with the identity operation on all the other qubits.

What's $H \otimes H$?

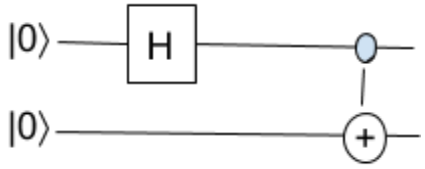
$$\frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Why should it look like this?

Let's look at the first row: $H|00\rangle = |{+}{+}\rangle$. Which means for each qubit there's an equal amplitude on $|0\rangle$ and $|1\rangle$.

All of these are examples of using tensor products to build bigger unitary matrices, except for the Controlled NOT, where the first qubit affects the second. We'll need operations like Controlled NOT in order to have one qubit affect another.

2 Qubits In Quantum Circuit Notation



Start with 2 qubits in $\|0\rangle$		Apply Hadamard to 1st qubit		Apply a Controlled NOT with the 1st qubit as the **control** and the 2nd as the **target**.	
$\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$	$\|00\rangle$	$\begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{bmatrix}$	$\frac{\|00\rangle + \|10\rangle}{\sqrt{2}}$ $= \|+\rangle \otimes \|0\rangle$	$\begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{bmatrix}$	$\frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$

The action of the Controlled NOT can also be written as $|x, y\rangle \rightarrow |x, y \otimes x\rangle$

The state that this circuit ends on, $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is called the **Singlet** or the **Bell Pair** or the **EPR Pair**

This state is particularly interesting because measuring the first qubit collapses the state of the second qubit. The state can't be factored into a tensor product of the first qubit's state and the second's. Such a state is called **entangled**, which for pure states simply means: not decomposable into a tensor product.

A state that's not entangled is called **unentangled** or **separable** or a **product state** (for pure states, which are the only kind being discussed at this point in the course, all three of these mean the same thing).

The basic rules of quantum mechanics, which we saw earlier, force entanglement to exist. It was noticed quite early in the history of the field. It turns out that *most* states are entangled.

As we mentioned earlier, entanglement was arguably what troubled Einstein most about quantum mechanics. He thought that it meant that quantum mechanics must entail "spooky action at a distance."

That's because particles need to be close to become entangled, but once they're entangled you can separate them to an arbitrary distance and they'll stay entangled. This has actually been demonstrated experimentally for distances of up to 150 miles (improved to a couple thousand miles by Chinese satellite experiments, while the course was being taught!).

Let's say that Alice and Bob entangle a pair of particles by setting their state to $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, then Alice brings her particle to the moon while Bob stays on Earth. If Alice measures her particle, she can *instantaneously* know whether Bob will observe a $|0\rangle$ or a $|1\rangle$ when he measures his.

This bothered Einstein, but others thought that it wasn't that big a deal. After all, Alice doesn't get to control the outcome of her measurement! She sees $|0\rangle$ and $|1\rangle$ with equal probability, which

means that in this case, the "spooky action" can be explained as just a correlation between two random variables, as we could already see in the classical world.

However, a famous 1935 paper of Einstein, Podolsky, and Rosen brought up a further problem: namely, there are other things Alice could do instead of measuring in the $|0\rangle$,$|1\rangle$ basis.

What happens if Alice measures in the $|+\rangle$,$|-\rangle$ basis?

She'll get either $|+\rangle$or $|-\rangle$, as you might expect.

Indeed, we can model the situation by Alice Hadamarding her qubit and then measuring in the $\{|0\rangle, |1\rangle\}$ basis.

That gives us the state:

$\frac{|00\rangle+|10\rangle+|01\rangle-|11\rangle}{2}$ Remember $H|0\rangle = |+\rangle$, etc.

So now, applying the *Partial Measurement Rule* what is Bob's state?

If Alice sees $|0\rangle$, then Bob's qubit collapses to the possibilities where Alice sees $|0\rangle$:

$\frac{|00\rangle+|01\rangle}{2} = |+\rangle$

Conversely, if Alice sees $|1\rangle$:

$\frac{|10\rangle-|11\rangle}{2} = |-\rangle$

The paper goes on to talk about how this is more troubling than before. If Alice measures in the $\{|0\rangle, |1\rangle\}$ basis, then Bob's state collapses to $|0\rangle$ or $|1\rangle$, but if she measures in the $\{|+\rangle, |-\rangle\}$ basis, then his state collapses to $|+\rangle$ or $|-\rangle$. And *that* looks a lot like faster-than-light communication!

How can we explain this?

One thing we can do is ask "what happens if Bob makes a measurement?"

- In the case where Alice measured her qubit in the $\{|0\rangle, |1\rangle\}$basis, Bob will see $|0\rangle$ or $|1\rangle$ with equal probability if he measures his qubit in the same basis.
- In the case where Alice measured her qubit in the $\{|+\rangle, |-\rangle\}$ basis…
    - Bob will still see $|0\rangle$ or $|1\rangle$ with equal probability (measuring in the $\{|0\rangle, |1\rangle\}$ basis)

So, at least in this case, the probability that Bob sees $|0\rangle$ or $|1\rangle$ is the same regardless of what Alice chooses to do. As an exercise, check that this remains the case even if Bob measures his qubit in the $\{|+\rangle, |-\rangle\}$ basis.

So, it looks like there might be something more general going on here! In particular, a different description should exist of Bob's part of the state that's unaffected by Alice's measurements. Which brings us to the next lecture…