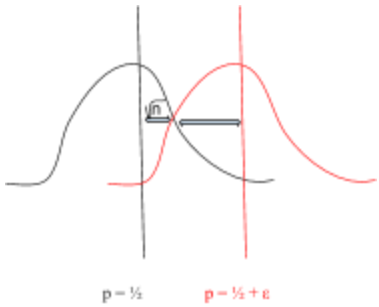
Tues Jan 30

Say you have a coin, and you want to figure out if it's fair ($p = ½$) or if it's biased ($p = ½ + \varepsilon$). How would you go about doing so?

The classical approach to solving this problem would be to flip the coin a lot (about $1/\varepsilon^2$ 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 $\log 1/\varepsilon^2$ 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 computing?

We can start with a qubit in the $|0\rangle$ state, and consider two rotations R_ε and $R_{-\varepsilon}$. We can repeated 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 (about $1/100\varepsilon^2$) we can measure the qubit and know with a reasonable degree of certainty that if it's in the $|0\rangle$ state, the coin is fair, if it's in the $|1\rangle$ state, the coin is biased.

- Won't counting that high require plenty of storage?
  - No. We can write a protocol with a half-life (some probability that it'll halt 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 bias coin will very likely land on $|1\rangle$.

Quantum information protocols are like baking souffles.
Opening the oven will *literally* collapse the souffle.

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

the quantum version takes **1 qubit of storage** as opposed to the classical solution's **$\log 1/\varepsilon^2$ bits**.

This result was shown by Professor Aaronson and a student of his. 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

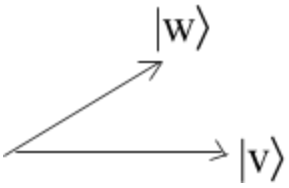
Given two orthogonal quantum states $|v\rangle$ and $|w\rangle$ there's a basis that distinguishes them.

These on the other hand are indistinguishable.

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

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

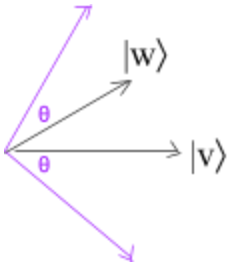
What about these?



More specifically: What measurement would minimize the chance of making a mistake in differentiating |v⟩ and |w⟩?

You may want to measure in the |v⟩,|something else⟩ basis, as it would eliminate one kind of error completely (not getting |v⟩ ensures the state was |w⟩), but there's a better way:

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



The 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. You could have one on Earth, and the other could be with your friend on the moon.

You'd only be able to measure the first bit:

The probability of getting $|0\rangle = |\alpha|^2 + |\beta|^2$ because those are the amplitudes compatible with 0 in the 1st bit.

$|1\rangle = |\gamma|^2 + |\delta|^2$

Suppose I measure the first qubit to $|0\rangle$. 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 minimally to fit your measurements.

This is actually the last rule of quantum mechanics that we'll cover in the course. Everything else is just a consequence of rules we've already covered.

This (1 0 0 0) is the **Controlled NOT**.

(0 1 0 0) Remember: it flips the 2nd bit if the 1st bit is 1.

(0 0 0 1)

(0 0 1 0)

What if we wanted to always do NOT on the 2nd bit: (0 1 0 0)
(1 0 0 0)
This is **I ⊗ NOT** (0 0 0 1)
/ | (0 0 1 0)
(nothing on 1st bit) with (NOT on 2st bit)

It can be decomposed as: (1 0) ⊗ (0 1) which makes it a tensor product unitary.
(0 1) (1 0)

What if we want **NOT ⊗ I**?
^{00}(0 0 1 0)
^{01}(0 0 0 1)
^{10}(1 0 0 0)
^{11}(0 1 0 0)
00 01 10 11

Remember that rows and cols represent the transformation
f(row) = col so the prob the input is 00
is the prob that the output is 10

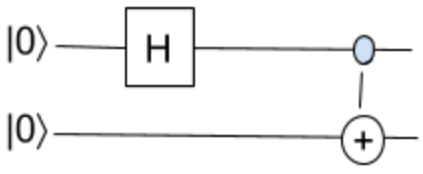
Very often in quantum information we'll want to take a group of qubits and perform an operation to one of them, say Hadamard the 3rd qubit.
What that means in terms of the matrices is applying I ⊗ I ⊗ H ⊗ … ⊗ I

What's H ⊗ H?
(1 1 1 1)
(1 -1 1 -1)
½ (1 1 -1 -1)
(1 -1 -1 1)

Why should it look like this?
Let's look at the first row: H|00⟩ = |++⟩. Which means for each qubit there's an equal prob it's output lands on |0⟩ or |1⟩.

All of these are examples of using tensor products to build bigger unitary matrices, except for the Controlled NOT, where the 1st bit affects the 2nd. We'll need operations like that in order to have one qubit affect another.

2 Qubits In Quantum Circuit Notation



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

The Controlled NOT can also be shown 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 EPR Pair**

This state is particularly interesting because measuring the 1st qubit collapses the 2nd qubit. It can't be factored into a tensor product of the 1st qubit's state and the 2nd's.

An **Entangled** state cannot be decomposed into a tensor product, while an **Unentangled** state can.

The basic rules of quantum mechanics force these properties to exist. They were noticed fairly early in the history of of the field. It turns out that most states are entangled.

As we mentioned earlier, entanglement was what troubled Einstein about quantum mechanics. He thought that it meant that quantum mechanics must ential faster than light communication.

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.

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 *faster-than-the-speed-of-light* know what position Bob's particle is in.

This bothered Einstein, but others thought that it wasn't that big a deal since Alice sees $|0\rangle$ and $|1\rangle$ in equal probability, which means it can be explained as a correlation between two random variables. However, a famous 1935 paper brought up a further problem: there's 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 $|+\rangle$ as you might expect.

But what if before that, Alice takes this state and Hadamards the 1st bit?

Well it maps $|00\rangle$ to $|00\rangle + |10\rangle$ and $|11\rangle$ to $|01\rangle - |11\rangle$ (ignoring normalization).

That gives us: $\frac{|00\rangle + |10\rangle + |01\rangle - |11\rangle}{2}$ 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. Alice's choice to measure in the $|+\rangle,|-\rangle$ basis is affecting Bob's qubit when he measures in the $|+\rangle,|-\rangle$ basis. And *that* looks a lot like faster than light communication.

How can we explain this?

One thing we can do is as “what happens if Bob makes a measurement?”

- In the case where Alice measured in $|0\rangle$,$|1\rangle$, Bob will see $|0\rangle$ or $|1\rangle$ with equal probability.
- In the case where Alice Hadamards her bit, then measures in $|+\rangle$,$|-\rangle$…
    - Bob will still see $|0\rangle$ or $|1\rangle$ with equal probability (measuring in the $|0\rangle$,$|1\rangle$ basis)

So the probability that Bob sees $|0\rangle$ or $|1\rangle$ is the same regardless of what Alice does.

People decided that it looked like there was something more general going on here, though. And so a different description should exist of Bob’s part of the state that’s unaffected by Alice’s measurements. Which brings us to…

Mixed States

We’ve only talked about **Pure States** so far (isolated quantum systems), but you can have quantum uncertainties layered together with regular, old uncertainty. This becomes important when we talk about states where we’re only measuring one part. If we look at the whole Alice-and-Bob-system together, it’ll look like a pure state.