

# Lecture 7: Tues Feb 7

The No Communication Theorem says that if Alice and Bob share an entangled state

$|\Psi\rangle = \sum_{i,j=1}^N \alpha_{ij} |i\rangle_{\text{Alice}} |j\rangle_{\text{Bob}}$  there's nothing that Alice can do to her subsystem that can affect Bob's density matrix.

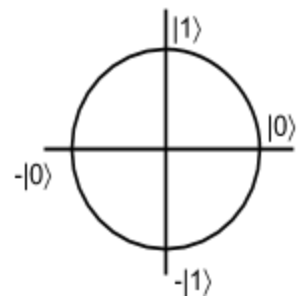
We have the tools to prove this: just apply a tensor product to Alice's side, then see if Bob's density matrix changes. Or have Alice measure her qubit, then see if Bob's density matrix changes, etc.

Note that if we condition on the outcome of Alice's measure (i.e. say that if Alice sees  $i$  then Bob will see  $j$ ), we may need to update Bob's density matrix, but that's also true in the classical world.

## Bloch Sphere

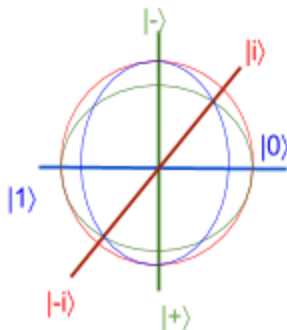
is a geometric representation of all possible states of a qubit.

We've often drawn the state of qubits as a circle, which is already a little awkward: half of the circle is going to waste since  $|0\rangle = -|0\rangle$  (both represent the same density matrix).



Instead, what if vectors that pointed in opposite directions were orthogonal?

We get the Bloch Sphere...



We can see that  $|+\rangle$  and  $|-\rangle$  should be between  $|0\rangle$  and  $|1\rangle$ . Then we can add  $|i\rangle$  and  $|-i\rangle$  as a new dimension.

In this representation, points on the surface of the sphere are pure states, such that

if they're  $180^\circ$  apart, they're orthogonal,  
and if they're  $90^\circ$  apart, they're conjugate.

What about mixed states?

Well we know that the maximally mixed state,  $I/2$ , can be defined as  $\frac{|0\rangle + |1\rangle}{2}$ ,  $\frac{|+\rangle + |-\rangle}{2}$ , or  $\frac{|i\rangle + |-i\rangle}{2}$ .

The sum of any two of these vectors on the sphere is the origin.

We can in this way represent any mixed state as any point inside of the sphere.

The mixture of any states  $|v\rangle$  and  $|w\rangle$  represented as points in or on the sphere can be said to be a point between the two.

We can show geometrically that every mixed state can be written as a mixture of only two pure states because you can always draw a line that connects any pure state you want to some point in the sphere representing a mixed state, and then see which other pure state that the line intersects on the way out. By some vector math, the point can be described as some linear combination of the vectors representing pure states.

Experimentalists love the Bloch sphere, because it works almost identically to how spin works with electrons.

With these things called **Spin- $\frac{1}{2}$  Particles** you can measure the electron spin relative to any axis of the sphere. You see if the electron is spinning clockwise or counterclockwise relative to the axis. And that behaves just like a qubit, in that the measurement collapses a more complex behavior into a binary result.

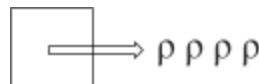
The weird part about Spin- $\frac{1}{2}$  Particles is that you *could have* asked the direction of the spin relative to any other axis. So what's really going on: What's the real spin direction? It turns out that it's some point on the Bloch Sphere. So if the state of the electron is that it's spinning in the (1,0,0) direction, we can say that it's in the  $|0\rangle$  state, and if it's spinning in the (0,1,0) direction, we can say that it's in the  $|+\rangle$  direction, and so forth.

### The No Cloning Theorem

We've seen how entanglement seems to lead to non-local effects, like for the state  $\frac{|00\rangle + |11\rangle}{2}$  if Alice measures her qubit's state, she can figure out Bob's. The reason that Alice isn't communicating faster than light boils down to Bob not being able to tell if his qubit's state is in the  $|0\rangle, |1\rangle$  basis or on the  $|+\rangle, |-\rangle$  basis.

But what if Bob could make unlimited copies of his qubit? He could figure it out through repeated measurements, and so he'd be able to tell what basis Alice measured in. FTL communication!

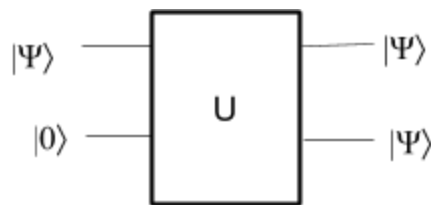
This is called **Quantum State Tomography**,  
we'll see it later.



It turns out that we can prove that a procedure to reliably copy an unknown quantum state cannot exist. It's fairly easy to prove, but it's a fundamental fact about quantum mechanics.

Let's try to clone a single quantum bit,  $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

In our quantum circuit we want to apply some unitary transformation that takes  $|\Psi\rangle$  and outputs  $|\Psi\rangle$ , and takes an ancilla from  $|0\rangle$  to  $|\Psi\rangle$ .



Algebraically, a cloner would need to do:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \rightarrow (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

The cloner would need to look like:

$$\begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{pmatrix} = \begin{pmatrix} & & & \\ & U & & \\ & & & \\ & & & \end{pmatrix} \begin{pmatrix} \alpha \\ \alpha \\ \alpha \\ \alpha \end{pmatrix}$$

The problem: this transformation **isn't linear** so it can't be unitary!

To clarify, a procedure that outputs some  $|\Psi\rangle$  can be rerun to get  $|\Psi\rangle$  repeatedly. What the No Cloning Theorem says is that if the  $|\Psi\rangle$  is unknown, then you can't make a copy.



cNOT seems like a copying gate [as it maps  $|00\rangle \rightarrow |00\rangle$ ,  $|10\rangle \rightarrow |11\rangle$ ]  
why isn't it in violation of the No Cloning Theorem?

Because it only works for  $|0\rangle$  and  $|1\rangle$ . Classical information CAN be copied. Just ask Stallman!

In general, for any orthonormal basis you can clone basis vectors.

Doing cNOT on  $|+\rangle$  and  $|0\rangle$  produces the Bell Pair:  $\frac{|00\rangle + |11\rangle}{2}$ . Which sort of copies the first

qubit in an entangled way, but that's different making a copy of  $|+\rangle$ .  
Having two qubits be  $1/2, 1/2$  is not the same as  $|+\rangle, |+\rangle$ .

Since the No Cloning Theorem is so important, we'll present another proof of it:

A unitary transformation can be defined as a linear transformation that preserves inner product. Which is to say that the angle between  $U|v\rangle$  and  $U|w\rangle$  is the same as the one between  $|v\rangle$  and  $|w\rangle$ .



$$\text{Thus } \langle w|U^T U|v\rangle = \langle w|v\rangle.$$

What would a cloning map do to this inner product?

$$\begin{aligned} |\langle v|w\rangle|^2 &= C \\ |(\langle v|\otimes\langle v|)(|w\rangle\otimes|w\rangle)|^2 &= C^2 \end{aligned}$$

$C$  only ever equals  $C^2$  if the inner product is 0 or 1: so the transformation is only linear if the  $v$  and  $w$  are in the same orthonormal basis.

There's a problem in classical probability that's a nice analog to the No Cloning Theorem.

If we have a coin of some probability heads, can we produce another coin with the same probability distribution? [Assuming the coin was made to have a certain probability distribution through some process unknown to us]

You'd need  $\begin{pmatrix} p^2 \\ p(1-p) \end{pmatrix} = \begin{pmatrix} S \\ 1-S \end{pmatrix} \begin{pmatrix} p \\ 1-p \end{pmatrix}$  to be true for some stochastic matrix.

$$\begin{aligned} \begin{pmatrix} p(1-p) \\ (1-p)^2 \end{pmatrix} &= \begin{pmatrix} S \\ 1-S \end{pmatrix} \begin{pmatrix} p \\ 1-p \end{pmatrix} \end{aligned}$$

But this transformation isn't stochastic (the result matrix doesn't sum to 1).

The No Cloning Theorem has all sorts of applications to science fiction, because you can't make arbitrary copies of a physical system (say for teleporting yourself) if any of the relative information (say, in your brain) is encoded in quantum states.

## Quantum Money

is an application of the No Cloning Theorem. In some sense it was the first idea in quantum information, and was involved in the birth of the field. The original quantum money scheme was proposed by Wiesner in 1969, though it was only published in the 80s.

Wiesner had left research by then. He eventually became a sheep herder.

Wiesner realized that uncloneability is useful for money to prevent counterfeiting. In practice, mints use special ink, watermarks, etc., but that's essentially just an arms race with the counterfeiters. So Wiesner proposed using qubits to make physical uncounterfeitable money.

The immediate problem is that money systems need *cloneability* and verifiability.


## Wiesner's Scheme

Have quantum bills (WLOG all are the same denomination). Each has:

- A classical serial number  $S = \{0,1\}^n$
- A quantum state  $|\Psi_{f(S)}\rangle$  (of  $n$  qubits)
  - The qubits in this state are unentangled and will always be in one of four states:
    - $|\Psi_{00}\rangle = |0\rangle$   $|\Psi_{01}\rangle = |1\rangle$   $|\Psi_{10}\rangle = |+\rangle$   $|\Psi_{11}\rangle = |-\rangle$

In order to decide the state of a given bill, the bank maintains a giant database that stores for all bills in circulation:

The classical serial number, and a function that takes the serial number as input and decides which basis to measure each qubit in (and which basis vector it should be).

$S_1, f(S_1)$			
$S_2, f(S_2)$			\
$S_3, f(S_3)$			/

Wiesner's scheme has an important engineering problem though: you need to ensure that qubits don't lose their state (coherence). With current technology, qubits in a lab decohere in like an hour, tops.

There's two basic things needed for a scheme like this: verifiability and uncloneability.

To verify a bill: bring it back to the bank. Bank verifies the bill by looking at the serial number, looking at how each qubit in the bill was supposed to be prepared. If the qubit was supposed to be prepared in  $|0\rangle, |1\rangle$  measure in that basis.

Consider a counterfeiter that doesn't know what basis each qubit is supposed to be in, and they encode each qubit in a random allowable state. They only have a  $\frac{1}{2}^n$  chance of guessing all the right bases.

The security of this scheme wasn't considered when it was proposed. Professor Aaronson asked about it on Stack Exchange a few years ago which prompted someone to write a paper on it.