No Cloning Theorem and Teleportation

1 No cloning theorem

A quantum operation which copied states would be very useful. For example, we considered the following problem in Homework 2: Given an unknown quantum state, either $|\phi\rangle$ or $|\psi\rangle$, use a measurement to guess which one. If $|\phi\rangle$ and $|\psi\rangle$ are not orthogonal, then no measurement perfectly distinguishes them, and we always have some constant probability of error. However, if we could make many copies of the unknown state, then we could repeat the optimal measurement many times, and make the probability of error arbitrarily small. The no cloning theorem says that this isn't physically possible. Only sets of mutually orthogonal states can be copied by a single unitary operator.

Assume we have a unitary operator U and two quantum states $|\phi\rangle$ and $|\psi\rangle$ which U copies, i.e.,

$$\begin{aligned} |\phi\rangle \otimes |0\rangle &\xrightarrow{U} |\phi\rangle \otimes |\phi\rangle \\ |\psi\rangle \otimes |0\rangle &\xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \ . \end{aligned}$$

Then $\langle\phi|\psi\rangle$ is 0 or 1.

Proof: $\langle\phi|\psi\rangle = (\langle\phi| \otimes \langle 0|)(|\psi\rangle \otimes |0\rangle) = (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) = \langle\phi|\psi\rangle^2$. In the second equality we used the fact that U, being unitary, preserves inner products.□

2 Superdense Coding

Suppose Alice and Bob have a *quantum* communications channel, over which Alice can send qubits to Bob. However, Alice just wants to send a regular classical letter (sequence of bits). One way to send her message is to encode a 0 as $|0\rangle$ and a 1 as $|1\rangle$. But can she do better than sending as many qubits as bits in her message?

Intuitively, since quantum systems are more complex than classical systems, they can hold information – so maybe Alice can do better. But quantum information is hard to access; when you measure a quantum state, it looks classical – so maybe she can't.

In fact, if Alice and Bob share a Bell state, then she can send two classical bits of information using only one qubit.

Say Alice and Bob share $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Depending on the message Alice wants to send, she applies a gate to her qubit, then sends it to Bob. If Alice wants to send 00, then she does nothing to her qubit, just sends it to Bob. If Alice wants to send 01, she applies the phase flip Z to her qubit, changing the quantum state to $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle$. To send 10, she applies the NOT gate, giving $\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\Psi^+\rangle$. To send 11, she applies both NOT and Z, giving $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\Psi^-\rangle$.

After receiving the qubit from Alice, Bob has one of the four mutually orthogonal Bell states. He can therefore apply a measurement to distinguish between them with certainty, and determine Alice's message. In practice, the way he'll make this measurement is by running the circuit we saw in Lecture 2 backwards (i.e., applying $(H \otimes I) \circ CNOT$), then measuring in the standard basis.

Note that Alice really did use two qubits total to send the two classical bits. After all, Alice and Bob somehow had to start with a shared Bell state. However, the first qubit – Bob's half of the Bell state – could have been sent well before Alice had decided what message she wanted to send. Perhaps only much later did she decide on her message and send over the second qubit.

One can show that it is not possible to do any better. Two qubits are necessary to send two classical bits. Superdense coding allows half the qubits to be sent before the message has been chosen.

2.1 Another Example: Quantum Teleportation

The *No Cloning Theorem* states that no quantum system can copy a qubit; that is, there is no transform sending $|\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$. However, if we are willing to destroy the original, we can transmit a qubit, even to a remote location.

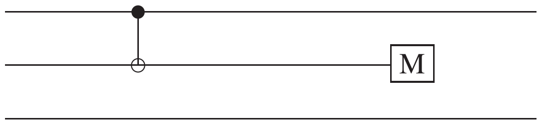
Suppose A has access to a quantum state $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$, which she wants to transmit to a remote party B. She can accomplish this by transmitting only classical bits of information, provided A and B share the entangled two-qubit state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

The technique is known as *quantum teleportation.*

The basic idea is this. A controls $|\psi\rangle$ and the first qubit of $|\phi\rangle$. A's strategy, roughly speaking, is to forcibly entangle $|\psi\rangle$ with the first qubit $|\phi\rangle$. A then measures the first qubit of $|\phi\rangle$, resolving it completely, and hopes this will cause $|\psi\rangle$ to become entangled with the *second* qubit of $|\phi\rangle$. Presumably, B could then transfer $|\psi\rangle$ to the second qubit of $|\phi\rangle$.

As a first try, consider the following diagram. The top line represents $|\psi\rangle$; the bottom two represent the two qubits of $|\phi\rangle$.



That is, A passes $|\psi\rangle$ and the first qubit of $|\phi\rangle$ through a CNOT gate, and then measures the first qubit of $|\phi\rangle$. Now the input into the system as a whole is

$$|\phi\rangle \otimes |\psi\rangle = \sum_{i=0,1} a_i|i\rangle \otimes \sum_{j=0,1} \frac{1}{\sqrt{2}}|j,j\rangle.$$

After passing through the CNOT gate this becomes

$$\sum_{i,j} a_i \big| i, i\oplus j, j\big\rangle.$$

Now A measures the middle qubit. Suppose it is measured as l; then $l = i \oplus j$. The state is now

$$\sum_{j} a_{j\oplus l} \big| j\oplus l, j\big\rangle.$$

Next, A transmits l to B. If $l = 0$, B takes no action, while if $l = 1$, then B performs a bit flip on his qubit (the bottom qubit in the diagram.) A bit flip is just the transformation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus we have

$$\sum_{j} a_{j\oplus l} \big| j, j\big\rangle.$$

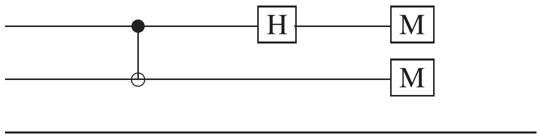
Finally, B does a phase flip on his qubit, yielding

$$\sum_j a_j \big| j, j \big\rangle.$$

This is almost exactly what we want. The only problem is that now, the qubit corresponding to $|\psi\rangle$ is entangled with B's qubit. The entanglement that was necessary to get the whole process started is now a liability. One way to disentangle them would be for A to measure her remaining qubit. But this would destroy B's qubit as well.

The ideal solution would be to send the entangle qubits through a CNOT gate—but A controls the first qubit and B controls the second. This would require quantum communication between A and B, which is prohibited.

The correct solution is to go back and modify the original diagram, inserting a Hadamard gate and an additional measurement:



Now the algorithm proceeds exactly as before. However A's application of the Hadamard gate now induces the transformation

$$\sum_j a_j \big| j, j \big\rangle \longrightarrow \sum_{ij} a_j (-1)^{ij} \big| i, j \big\rangle.$$

Finally A measures i and sends the measurement to B. The state is now:

$$\sum_j a_j (-1)^{ij} | j \rangle.$$

If $i = 0$ then we are done; if $i = 1$ then B applies a phase flip. In either case the state is now $a_0|0\rangle + a_1|1\rangle$.

So A has transported the quantum state to B simply by sending two classical bits.