❖ Information 1: No Cloning and Quantum Money (1/29)

6.1 No Cloning Theorem

One operation we take for granted in classical information is the ability to copy information. We copy and paste text, functions make copies of parameters they are given, and we can buy a new phone and put in the same information stored in our old one. Can we do the same using quantum information? We will define the problem formally as follows.

Suppose we have a qubit in an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Is there a generic algorithm (think unitary) we can apply such that

$$|\psi\rangle|0\rangle \to |\psi\rangle|\psi\rangle? \tag{1}$$

Note that this is different from

$$|\psi\rangle|0\rangle = (\alpha|0\rangle + \beta|1\rangle)|0\rangle \to \alpha|00\rangle + \beta|11\rangle\,. \tag{2}$$

Question 2. Suppose we have the following two quantum states.

- $|\phi_1\rangle = \alpha|00\rangle + \beta|11\rangle$
- $|\phi_2\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$

Suppose we measure the first qubit for each of the above two states. What is the probability of measuring $|0\rangle$ in each case? What is the state after the measurement result?

Theorem 6.1 (No Cloning Theorem)**.** Let $|\psi\rangle$ be a state on n qubits. There is no unitary operator U such that

$$U(|\psi\rangle|0^n\rangle) = |\psi\rangle|\psi\rangle \tag{3}$$

for any state $|\psi\rangle$.

One way to prove this theorem is by showing that there exists no unitary U such that

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle\,, \tag{4}$$

but we will prove it in a different way.

Question 3. Consider two quantum states $|v\rangle$ and $|w\rangle$. Suppose we apply some unitary U to each of these states to get $U|v\rangle$ and $U|w\rangle$. What happens to the "overlap" or "angle" between the two states?

Inner product between separable states (multi qubit states which can be decomposed into a tensor product). If we have two states $|A\rangle = |a_1\rangle |a_2\rangle$ and $|B\rangle = |b_1\rangle |b_2\rangle$, the inner product of these states is

$$\langle A|B\rangle = (\langle a_1| \otimes \langle a_2|)(|b_1\rangle \otimes |b_2\rangle) = \langle a_1|b_1\rangle \langle a_2|b_2\rangle . \tag{5}$$

That is, the inner product is taken independently for each subsystem.

Question 4. Suppose there exists a unitary U which can clone any quantum state. Then, we can start with two systems $|v\rangle |0\rangle$ and $|w\rangle |0\rangle$ and apply U to clone them resulting in $|v\rangle |v\rangle$ and $|w\rangle |w\rangle$.

What is the overlap between the states before and after applying U? What does this say about U?

Question 5. Based on the results from the previous problem, when *can* we clone a quantum state (if any)?

The result of the above question means that for a set of states that span an orthonormal basis, there exists a unitary that can copy states in that basis, but this will not work for a generic state.

Question 6. Find a unitary U that "clones" single qubit standard basis states. That is, an operator U such that

$$U(|0\rangle |0\rangle) = |0\rangle |0\rangle \quad U(|1\rangle |0\rangle) = |1\rangle |1\rangle \tag{6}$$

Question 7. What does that unitary U from above do if the state we want to copy is in the state $|+\rangle$?

Question 8. Find a unitary V that clones a single qubit Hadamard basis state. That is, an operator V such that

$$V(|+\rangle |0\rangle) = |+\rangle |+\rangle \quad V(|-\rangle |0\rangle) = |-\rangle |-\rangle \tag{7}$$

Question 9. What does that unitary V from above do if the state we want to copy is in the state $|0\rangle$?

6.2 Weisner's Quantum Money Scheme

Not being able to copy information sounds like a severe limitation, and it is for many information processing tasks and algorithm design. However, people have also been working on ways to exploit the no-cloning property of quantum information, by creating money that can't be counterfeited.

When discussing money, there are two basic properties we want before anything else: Unclonability and verifiability. Here, we study an early iteration of quantum money.

Imagine a bank that prints bills using some quantum technology. To satisfy the basic requirements, we will give every bill the following:

- A classical serial number s with n bits.
- A quantum state $|\psi_{f(s)}\rangle$ on n qubits.

The function $f(s)$ is a mapping from an n bit serial number to a $2n$ bit description of the state being stored. Every pair of bits in $f(s)$ will be used to track which state is being stored.

- $|\psi_{00}\rangle = |0\rangle$
- $|\psi_{01}\rangle = |1\rangle$
- $|\psi_{10}\rangle = |+\rangle$
- $|\psi_{11}\rangle = |-\rangle$

The bank keeps track of the tuple $(s, f(s))$.

Example 6.2 (3 bit example)**.** Consider a bank that prints quantum money with 3 bit serial numbers. The following is an example of the information related to **one** of the bills:

- Serial number: 110
- Function mapping: $f(110) = 001011$
- Quantum state: $|0\rangle\,|+\rangle\,|-\rangle$

The client carries around the bill, but does not know what the function mapping is! The bank is able to verify that the client has the correct bill.

Question 10. A client comes in and brings in the bill from example 6.2. What should the bank do to verify that this is the correct bill? Remember, the bank stores the tuple $(s, f(s))$.

Now let's see what the strategy of a counterfeiter would look like. The goal of the counterfeiter is to create multiple copies of a bill that will be verified by the bank. Remember though, there is no unitary to generically clone states **if they do not form an orthonormal basis**. One strategy is the following

Example 6.3 (3 bit example continued)**.** Suppose a counterfeiter measures our bill in the standard basis and observes the result $|0\rangle\,|0\rangle\,|1\rangle$. They can now have two (or even many more) copies of quantum bills with the serial number 110 and state $|0\rangle\,|0\rangle\,|1\rangle$.

Question 11. What are the measurement outcomes and corresponding probabilities when the counterfeiter submits these two bills to the bank?

Question 12. Suppose we have a quantum bill with a single bit serial number. For simplicity, suppose there is an equal probability of being in any of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$. Let's say that we measured this state in the standard basis to clone it. What is the probability that both of the bills pass the verification procedure?

Question 13. What if instead of the standard basis, we measure and clone in the Hadamard basis. What is the probability that both of the bills pass the verification procedure?

Question 14. If we had a quantum bill with an n bit serial number, and we measured and cloned the bill in the standard basis, what is the probability of two bills passing the verification procedure?

6.3 The frontier of Quantum Money

We won't prove it here, but for Weisner's quantum money scheme, it can be shown that no counterfeiting strategies can do better than $\left(\frac{3}{4}\right)^n$. It can also be shown that the scheme can be broken if the same bill is used twice. There are ways to avoid this, for example, if the bank reissues a new quantum state every time a bill is verified. This scheme and many of its alternatives are referred to as "private key quantum money" schemes. As you may have noticed, they have a large downside, requiring users to verify their bills with the bank every time they want to make a transaction. Researchers are working on developing a "public key quantum money" scheme, where this verification procedure will not be necessary while maintaining the properties of money that we want.

In terms of implementation, this scheme will probably not be feasible to implement in the near future, as it requires us to have quantum hardware which can maintain their states for a long time. These **coherence times** (how long a quantum state can be preserved) are a bit engineering challenge for the next era of research.