# CS166 WI24: Homework 3 (Due Tuesday Feb 6 11:59pm)

## ❖ Problem 1

We've discussed the Bell pair in class, but more accurately, the Bell states are a collection of four two qubit states, which form an orthonormal basis over $\mathbb{C}^4$. The four states are

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1}$$

$$|\Phi^-\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{2}$$

$$|\Psi^+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{3}$$

$$|\Psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{4}$$

1. Design a circuit that starts in the state $|00\rangle$, and ends with $|\Psi^-\rangle$.

2. For the remaining parts for this problem, we will use the following notation.

$$|\theta\rangle := \cos(\theta)\,|0\rangle + \sin(\theta)\,|1\rangle\,. \tag{5}$$

   Consider the basis $\{|\pi/6\rangle\,, |4\pi/6\rangle\}$. Write down $|0\rangle$ and $|1\rangle$ as a weighted sum of $|\pi/6\rangle$ and $|4\pi/6\rangle$ in the above basis. Recall that

$$\cos(\pi/6) = \sqrt{3}/2 \quad \sin(\pi/6) = 1/2 \tag{6}$$

$$\cos(4\pi/6) = -1/2 \quad \sin(4\pi/6) = \sqrt{3}/2 \tag{7}$$

$$\tag{8}$$

3. Suppose Alice has the first qubit and Bob has the second qubit of a $|\Psi^-\rangle$ state. If Alice measures her qubit in the $\{|\pi/6\rangle\,, |4\pi/6\rangle\}$ basis, what are the probabilities of each outcome, and the state of the two qubits after the measurement?

## ❖ Problem 2

### 2.1 $|i\rangle$ basis

Recall the basis $\{|i\rangle\,, |-i\rangle\}$, which were defined as

$$|i\rangle := \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \tag{9}$$

$$|-i\rangle := \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle). \tag{10}$$

Design a quantum circuit that clones a state in this basis. That is, a quantum circuit $U$ such that

$$U(|i\rangle\,|0\rangle) = |i\rangle\,|i\rangle \tag{11}$$
$$U(|-i\rangle\,|0\rangle) = |-i\rangle\,|-i\rangle \tag{12}$$

### 2.2 Challenge: Bell basis

Design a four qubit circuit that takes as input a Bell basis state in the first two qubits, and $|00\rangle$ in the second two qubits, and clones the Bell state to the second pair of qubits. That is, the circuit $U$ should have the action of

$$U(|\Phi^+\rangle\,|00\rangle) = |\Phi^+\rangle\,|\Phi^+\rangle \tag{13}$$
$$U(|\Phi^-\rangle\,|00\rangle) = |\Phi^-\rangle\,|\Phi^-\rangle \tag{14}$$
$$U(|\Psi^+\rangle\,|00\rangle) = |\Psi^+\rangle\,|\Psi^+\rangle \tag{15}$$
$$U(|\Psi^-\rangle\,|00\rangle) = |\Psi^-\rangle\,|\Psi^-\rangle \tag{16}$$

## ❖ Problem 3

We consider the Weisner quantum money scheme. Suppose that after every verification process, the bank returns the bill to you, regardless of whether it passed the verification or not. They also allow you to submit your bill multiple times. Let's design a scheme to counterfeit this money scheme to make a fake bill that passes the verification.

Recall, that a quantum bill in this scheme can be written as a tensor product of $n$ qubits,

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle\,, \tag{17}$$

where each $|\psi_i\rangle$ is in one of the four states $\{|0\rangle\,, |1\rangle\,, |+\rangle\,, |-\rangle\}$.

1. Suppose we replace $|\psi_1\rangle$ with a qubit in the state $|0\rangle$. Assuming that the "correct" state is any of the four possible states, what is the probability that the verification was successful?

2. If the verification was successful, what is the state of $|\psi\rangle$?

3. If the verification was unsuccessful, what is the state of $|\psi\rangle$? You can use the shorthand $|\psi_i^\perp\rangle$ to represent a state orthogonal to $|\psi_i\rangle$.

4. Design a counterfeiting strategy to create a copy of $|\psi\rangle$.

# ❖ Problem 4

## 4.1 Teleportation

Design a quantum teleportation protocol where Alice and Bob share the $|\Psi^+\rangle$ state, instead of the $|\Phi^+\rangle$ state. You should follow the analysis we did in class to verify that this works successfully. The analysis should include:

- A diagram of the circuit for the protocol
- A description of the state of Bob's qubit after Alice's measurements
- The sequence of gates to apply to Bob's state depending on the measurement observed.

## 4.2 Code implementation

Write a circuit that implements the quantum teleportation protocol you just designed, where Alice and Bob share a $|\Psi^+\rangle$ state. Test your protocol on a random input. One way to generate a random input is to create the $|\theta\rangle$ state from Problem 1, by sampling a random $\theta$ and applying a $R_\theta$ gate to your first qubit.

Experimentally verify that the teleportation was successful. One way to do this is to take samples of Alice's original state, and then take samples from Bob's state after the teleportation is applied.

# ❖ Bonus Reading

- Scott Aaronson on Quantum Money: If you are interested in the state of the art around quantum money theory, this article does a great job of describing the results and progress around the subject, as well as ideas researchers are interested in. https://dl.acm.org/doi/pdf/10.1145/2240236.2240258
- Why Quantum Money Could Replace Blockchain-Based Cryptocurrencies: Recent article discussing how quantum money may serve as a more sustainable alternative to cryptocurrencies. https://www.discovermagazine.com/technology/why-quantum-money-could-replace-blockchain-based-cryptocurrencies

## ❖ Open Questions

- **Public key quantum money** The big open question from this week is if there exists a public key quantum money protocol. The best option for this that is known right now is based on the theory of knots. https://arxiv.org/pdf/1004.5127.pdf

  Here is a quick video on the topic that is pretty neat!

  https://www.youtube.com/watch?v=81do_7Axe9I