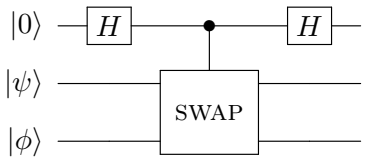
CS333 - Problem Set 11 (review)

Doing all of the problems on this pset might be a bit much, so I encourage you to focus on those problems where you feel you need the most practice. I've put skills/concepts in parenthesis at the beginning of each question to help you choose.

1. (Circuit analysis, partial measurements, also a really frequently used algorithmic tool)

   (a) Consider the following circuit on 3 qubits. Let $|\psi\rangle$ and $|\phi\rangle$ be any single-qubit states (not necessarily standard basis states or orthogonal states), and let SWAP denote the 2-qubit gate that swaps its input qubits (i.e., $\text{SWAP}|\eta\rangle|\mu\rangle = |\mu\rangle|\eta\rangle$ for any states $|\mu\rangle$ and $|\eta\rangle$). What is the final state of the following circuit (in terms of $|\psi\rangle$ and $|\phi\rangle$)?

   (1)

   (b) Suppose the first (top) qubit in the above circuit is measured in the standard basis. What is the probability that the measurement outcome is $|0\rangle$? Your answer should depend on the inner product of $|\psi\rangle$ and $|\phi\rangle$.

   (c) How do the results of the previous parts change if $|\psi\rangle$ and $|\phi\rangle$ are n-qubit states, and SWAP denotes the $2n$-qubit gate that swaps the first n qubits with the last n qubits?

   (d) What is the purpose of this circuit?

2. (Analyzing cryptography protocols, analyzing measurement of 2-qubit system where each qubit is measured independently) We didn't have time to get into this topic this semester, but it is impossible to make copies of quantum states. Because of this, people have been working to develop secure quantum money that can't be counterfeited. Eve knows it is impossible to clone quantum states, but she thinks she has found a pretty good cloner that will help her break the BB84 cryptography scheme. For each round of the cryptography protocol, she prepares a qubit in the state $|0\rangle_E$. When the photon that Alice is sending to Bob comes to her, she applies the unitary:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{2}$$

   to the combined state of $|\psi\rangle|0\rangle_{AE}$ where $|\psi\rangle_A$ is the state of Alice's photon that she has intercepted. (Her goal is to clone some of the information from A into her E system.) Then after acting with the unitary, she sends qubit A to Bob, and keeps system E but doesn't measure it yet. When Alice and Bob announce their measurement bases, if Alice and Bob's measurement bases were the same, Eve measures her system in that basis.

(a) In what way does $CNOT$ act like a cloner? In what situations does $CNOT$ act like a cloner and when does it not? Please explain.

(b) Is this a good strategy? Compare to Eve's strategy where she always chooses to measure each incoming photon in the basis $\{|0\rangle, |1\rangle\}$.

3. (Complex phases, unitaries represented using summation notation)Quantum Fourier Transform and Period Finding. For a standard basis states $|x\rangle \in \mathbb{C}^t$,

$$QFT_t|x\rangle = \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{2\pi i xy/t}|y\rangle; \qquad QFT_t^{-1}|x\rangle = \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{-2\pi i xy/t}|y\rangle \tag{3}$$

Show that QFT_t^{-1} is the inverse of QFT. In other words, show:

$$QFT_t^{-1} QFT_t = I. \tag{4}$$

4. (Error correction) This problem is a bit computational heavy, but good practice.

In this problem, we consider the same bit flip code as before: $a|0\rangle + b|1\rangle$ is encoded as $a|000\rangle + b|111\rangle$, which we have seen is protected against X-type rotations on a single qubit. We have so far only considered the case where exactly one qubit has been affected by a unitary error. A more realistic error model is that small rotations affect all of the qubits at any time step. Consider an error model where the error is the unitary X_θ acting in parallel on all 3 qubits in the code:

$$X_\theta^{\otimes 3}, \tag{5}$$

where

$$X_\theta = \begin{pmatrix} \cos(\theta) & i\sin(\theta) \\ i\sin(\theta) & \cos(\theta) \end{pmatrix}. \tag{6}$$

In this problem, you should imagine that θ is very small.

(a) If the logical qubit is initially in the state $a|000\rangle + b|111\rangle$ for $a, b \in \mathbb{R}$, (i.e. a, b are not complex - this just makes the calculations simpler), what is the state of the logical qubit after this error has occurred? (That is, calculate $X_\theta^{\otimes 3}(a|000\rangle + b|111\rangle)$. You can keep your answer undistributed if that is easier.)

(b) Consider the projective measurement:

$$\begin{aligned} M = \{&P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|, P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|, \\ &P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|, P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|\}. \end{aligned} \tag{7}$$

Use the projective measurement formalism to analyze the probability that P_0 and P_1 each occur, and how the state collapses in each case. (By symmetry, the case of P_2 and P_3 will be similar to P_1, so you do not need to go through them.)

(c) If outcome P_0 occurs, we do nothing , and if outcome P_1 occurs, we apply X to the first qubit. What does the state become in this case?

(d) Even though error correction (in either the P_0 outcome or the P_1 outcome) doesn't return us to our original state $a|000\rangle + b|111\rangle$, the states that we do recover are extremely close to $a|000\rangle + b|111\rangle$ when θ is not too large. To see this, we can calculate the absolute value squared of the inner product between the resultant state after error correction and $a|000\rangle + b|111\rangle$. Given two states $|\psi\rangle$ and $|\phi\rangle$, the absolute value squared of their inner product tells you about how difficult it is to distinguish between them: a value close to 1 means they are almost indistinguishable, and inner product close to 0 means they are close to orthogonal and hence can be distinguished by a measurement.

Plot the absolute value of the inner product between $a|000\rangle + b|111\rangle$ and the resulting states after error correction, averaged over the probability of the 4 different outcomes P_0, P_1, P_2, and P_3 as a function of θ in the two cases that $a = b = 1/\sqrt{2}$ and $a = 1$, $b = 0$ (which are the two extremal cases). So if p_i is the probability of getting outcome P_i and $|\psi_i\rangle$ is the state that results after error correction when outcome P_i is measured, you should calculate

$$\sum_{i=0}^{3} p_i |\langle \psi_i | (a|000\rangle + b|111\rangle)|^2. \tag{8}$$

(You should assume the probability of getting outcomes P_2 and P_3 are the same as for P_1, and that the inner product is also the same as for P_1).

On the same plots, compare to $|\langle \psi_{error} | (a|000\rangle + b|111\rangle)|^2$, where $|\psi_{error}\rangle$ is the state after the error occurs if no error correction is applied. Comment on the efficacy of this error correction protocol.