Homework 4

Introduction to Quantum Information Science
Due Sunday, February 19 at 11:59 PM

1. Bloch Sphere.

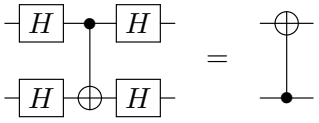
Give three different representations of the 1-qubit mixed state

$$\rho = \begin{pmatrix} \frac{2}{3} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$$

as a mixture of two pure states. What do these decompositions correspond to on the Bloch sphere?

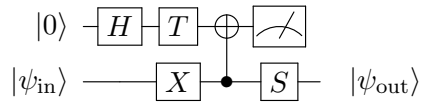
2. Multi-qubit quantum circuits

a) Prove the following identity.



In other words: show that a CNOT by which qubit A controls qubit B, when viewed in a different basis, is actually a CNOT by which qubit B controls qubit A! This illustrates how, with quantum information, unlike with classical information, there's no way for one system to affect another one without the possibility of being affected itself.

b) Consider the following circuit. Write $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.



Where: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$, $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

What is the state of the first qubit before the CNOT?
What is the state of the two qubits before the measurement?
What are the probabilities of measuring $|0\rangle$ or $|1\rangle$?
What is the second qubit state $|\psi_{\text{out}}\rangle$ when the first qubit is measured as $|0\rangle$. How about when it's measured as $|1\rangle$?

c) The 2-qubit CSIGN gate (also known as a controlled-Z gate) operates by applying a relative phase shift of -1 to the $|1\rangle$ component of the second qubit if the first qubit is equal to 1 and otherwise does nothing. As a matrix it is given explicitly by the diagonal matrix diag(1,1,1,-1). Show how to simulate a CSIGN gate using only CNOT and Hadamard gates by writing down the appropriate circuit.

3. SARG04 Quantum Key Distribution

In class we discussed the BB84 QKD scheme. There is a similar protocol, called SARG04, which we study in this problem.

a) Alice randomly samples two bitstrings $a = 011001$ and $b = 101011$. She prepares a six qubit state $|\psi\rangle$ that encodes the string a in a basis given by b. For the i'th qubit, if $b_i = 0$ then she uses the $|0\rangle, |1\rangle$ basis and if $b_i = 1$ then she uses $|+\rangle, |-\rangle$. Write down $|\psi\rangle$.

b) Alice sends $|\psi\rangle$ to Bob on a public quantum channel. Eve could intercept it, but say for now she leaves $|\psi\rangle$ untouched. Bob samples a bitstring $b' = 100111$, and measures $|\psi\rangle$ in the basis specified by b'. What is a state that could Bob measure? What bitstring a' does it correspond to?

c) In BB84 Alice now publicly announces b and Bob publicly announces where it differs from b'. They then discard the parts of a and a' where b and b' differ. What are they left with in each case?

d) In SARG04 Alice for each qubit in $|\psi\rangle$ sends a classical description of one of the pairs $\{|0\rangle, |+\rangle\}$, $\{|0\rangle, |-\rangle\}$, $\{|1\rangle, |+\rangle\}$ or $\{|1\rangle, |-\rangle\}$, so that her qubit in $|\psi\rangle$ is part of that pair. What is a string of pairs she could send?

e) Bob now analyses each pair, and sees if the a' he measured can be used to determine the correct basis. For your a', for which pairs is the basis unambiguous, and what basis is it?

f) When the basis was not ambiguous, Bob announces the positions where b' had the correct basis. Alice and Bob keep the respective parts of b and b'. What are they left with?

4. Quantum Money Attacks. Suppose you're a quantum money counterfeiter, trying to forge a banknote in Wiesner's scheme. You're given a qubit that's $|0\rangle$,$|1\rangle$, $|+\rangle$ or $|-\rangle$, each with equal probability 1/4. You can apply any quantum circuit you like to the qubit to produce a two-qubit state. Then, both of your output qubits will separately be given back to the bank for verification. (I.e., if the original qubit was $|0\rangle$ or $|1\rangle$ then the bank will measure both output qubits in the $\{|0\rangle, |1\rangle\}$ basis and accept if and only if both outcomes match the original qubit, and likewise if the original qubit was $|+\rangle$ or $|-\rangle$ the bank will measure and check in the $\{|+\rangle, |-\rangle\}$ basis.) Your goal is to maximize the probability that the bank accepts.

a) Give a procedure that succeeds with probability at least $\frac{5}{8}$. Your procedure should not involve creating any entangled states.

b) Now consider the following procedure. Among 3 qubits, initialize the first two qubits to $|0\rangle$ and let the third qubit be the qubit from the original banknote to be counterfeited. Then apply a 3 qubit unitary transformation whose effect is the following mapping:

$$|000\rangle \mapsto \frac{\sqrt{3}}{2}|000\rangle + \frac{|110\rangle + |101\rangle + |011\rangle}{\sqrt{12}}$$
$$|001\rangle \mapsto \frac{\sqrt{3}}{2}|111\rangle + \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{12}}$$

Finally, discard (perform partial trace over) the first qubit and output the state given by the second two qubits.

Show that the probability of success for this procedure is higher than what was achieved in part a. *Note: This procedure actually turns out to be the optimal one.*