1. *Universality of reversible logic gates.*

The CCCNOT (triple-controlled NOT) gate is a four-bit reversible gate that flips its fourth bit if and only if the first three bits are all in the state 1.

(a) [2 points] Show how to compute CCCNOT using AND, OR, NOT and FANOUT gates.

**Solution:**

\[
\begin{align*}
\text{CCCNOT gate:} & \quad x_1 \land x_2 \land x_3 \oplus x_4 \\
\text{Solution:} & \quad x_1 \quad x_2 \quad x_3 \quad \text{and} \quad (x_1 \land x_2 \land x_3) \oplus x_4
\end{align*}
\]

(b) [3 points] Show how to implement a CCCNOT gate using Toffoli gates. You may use additional workspace as needed. You may assume that bits in the workspace start with a particular value, either 0 or 1, provided you return them to that value. For a bonus point, give a circuit that works regardless of the values of any bits of workspace.

**Solution:** The following circuit shows a simple construction using one bit of workspace in the 0 state:

\[
\begin{align*}
\text{Toffoli gate inputs:} & \quad x_1, x_2, x_3 \\
\text{Toffoli gate output:} & \quad (x_1 \land x_2 \land x_3) \oplus x_4 \\
\text{Solution:} & \quad \text{The first gate computes the AND of the first two bits in the fifth (workspace) bit. The second gate computes the AND of the third and fifth bits (i.e., the AND of the first three bits) in the fourth (target) bit. The final gate uncomputes the value in the workspace.}
\end{align*}
\]

This circuit can be modified to work for a workspace bit with any value as follows:

(c) [4 points] Show that a Toffoli gate cannot be implemented using any number of CNOT gates, with any amount of workspace. Hence the CNOT gate alone is not universal. (Hint: It may be helpful to think of the gates as performing arithmetic operations on integers mod 2.)

**Solution:** The CNOT gate acts as

\[
\text{CNOT gate inputs:} \quad x_1, x_2 \\
\text{CNOT gate output:} \quad \text{Uncomputed} x_1, \text{CNOT of} x_2
\]
(where \( \oplus \) denotes addition modulo 2), so composing any number of CNOT gates gives output bits that can be expressed as a sum modulo 2 of a subset of input bits. However, the Toffoli gate acts as

\[
\begin{array}{ccc}
  & x & \\
\downarrow & & \oplus \\
\downarrow & & \downarrow \\
y & & y \\
\downarrow & & \oplus \ \\
z & & xy \\
\end{array}
\]

and the product \( xy \) (representing logical AND) cannot be expressed as a sum modulo 2 of terms involving \( x \) and \( y \) (and the constants 0 and 1 if we allow work bits with known initial states), the only possibilities being \( 0, x, y, x \oplus y \) (and their negations if we allow work bits known to be in the 1 state).

2. **Product and entangled states.** Determine which of the following states are entangled. If the state is not entangled, show how to write it as a tensor product; if it is entangled, prove this.

(a) [2 points] \( \frac{2}{3}|00\rangle + \frac{1}{3}|01\rangle - \frac{2}{3}|11\rangle \)

**Solution:** This state is entangled. A product state has the form

\[
(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle
\]

for some \( \alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{C} \). If this were a product state, it would have \( \alpha_1\beta_0 = 0 \), so either \( \alpha_1 = 0 \) or \( \beta_0 = 0 \); but this contradicts \( \alpha_1\beta_0 = \frac{2}{3} \) and \( \alpha_1\beta_1 = -\frac{2}{3} \).

(b) [2 points] \( \frac{1}{2}(|00\rangle - i|01\rangle + i|10\rangle + |11\rangle) \)

**Solution:** This is a product state, with the decomposition

\[
\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle).
\]

(c) [2 points] \( \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle) \)

**Solution:** This state is entangled. Using the form of a product state from part (a), if this were a product state it would have \( \alpha_0\beta_0 = \alpha_1\beta_1 = 1 \), so \( \alpha_0\beta_0\alpha_1\beta_1 = 1 \); but this contradicts \( \alpha_1\beta_0 = 1 \) and \( \alpha_0\beta_1 = -1 \), which would imply \( \alpha_0\beta_0\alpha_1\beta_1 = -1 \).

3. **Unitary operations and measurements.** Consider the state

\[
|\psi\rangle = \frac{2}{3}|00\rangle + \frac{1}{3}|01\rangle - \frac{2}{3}|11\rangle.
\]

(a) [2 points] Let \( |\phi\rangle = (I \otimes H)|\psi\rangle \), where \( H \) denotes the Hadamard gate. Write \( |\phi\rangle \) in the computational basis.

**Solution:**

\[
|\phi\rangle = \frac{1}{\sqrt{2}} \left[ \frac{2}{3}(|00\rangle + |01\rangle) + \frac{1}{3}(|00\rangle - |01\rangle) - \frac{2}{3}(|10\rangle - |11\rangle) \right] \\
= \frac{1}{\sqrt{2}} \left( |00\rangle + \frac{1}{3}|01\rangle - \frac{2}{3}|10\rangle + \frac{2}{3}|11\rangle \right)
\]
(b) [3 points] Suppose the first qubit of $|\phi\rangle$ is measured in the computational basis. What is the probability of obtaining 0, and in the event that this outcome occurs, what is the resulting state of the second qubit?

**Solution:** Writing

$$|\phi\rangle = \frac{\sqrt{5}}{3} |0\rangle \otimes \left( \frac{3}{\sqrt{10}} |0\rangle + \frac{1}{\sqrt{10}} |1\rangle \right) - \frac{2}{3} |1\rangle \otimes \left( \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right)$$

(chosen so that the states in parentheses are normalized), we see that the probability of obtaining 0 when measuring the first qubit is \((\sqrt{5}/3)^2 = 5/9\), and the resulting post-measurement state of the second qubit is \(\frac{3}{\sqrt{10}} |0\rangle + \frac{1}{\sqrt{10}} |1\rangle\).

(c) [3 points] Suppose the second qubit of $|\phi\rangle$ is measured in the computational basis. What is the probability of obtaining 0, and in the event that this outcome occurs, what is the resulting state of the first qubit?

**Solution:** Writing

$$|\phi\rangle = \frac{\sqrt{13}}{3\sqrt{2}} \left( \frac{3}{\sqrt{13}} |0\rangle - \frac{2}{\sqrt{13}} |1\rangle \right) \otimes |0\rangle + \frac{\sqrt{5}}{3\sqrt{2}} \left( \frac{1}{\sqrt{5}} |0\rangle + \frac{2}{\sqrt{5}} |1\rangle \right) \otimes |1\rangle,$$

we see that the probability of obtaining 0 when measuring the second qubit is \((\sqrt{13}/3\sqrt{2})^2 = 13/18\), and the resulting post-measurement state of the first qubit is \(\frac{3}{\sqrt{13}} |0\rangle - \frac{2}{\sqrt{13}} |1\rangle\).

(d) [2 points] Suppose $|\phi\rangle$ is measured in the computational basis. What are the probabilities of the four possible outcomes? Show that they are consistent with the marginal probabilities you computed in the previous two parts.

**Solution:** Looking at the expression for $|\phi\rangle$ from part (a), we have $Pr(00) = 1/2$, $Pr(01) = 1/18$, and $Pr(10) = Pr(11) = 2/9$. The probability of measuring 0 for the first qubit is $Pr(00) + Pr(01) = 1/2 + 1/18 = 5/9$, agreeing with part (b), and the probability of measuring 0 for the second qubit is $Pr(00) + Pr(10) = 1/2 + 2/9 = 13/18$, agreeing with part (c).

4. **Distinguishing quantum states.** [6 points] Let $\theta$ be a fixed, known angle. Suppose someone flips a fair coin and, depending on the outcome, either gives you the state $|0\rangle$ or $\cos \theta |0\rangle + \sin \theta |1\rangle$ (but does not tell you which). Describe a measurement (consisting of an orthonormal qubit basis) for guessing which state you were given, succeeding with as high a probability as possible. Also indicate the success probability of your procedure. (You do not need to prove that your procedure is optimal, but your grade will depend on how close your procedure is to optimal.)

**Solution:** Suppose we perform the measurement \(\{ |\psi_1\rangle, |\psi_2\rangle \}\), where

$$|\psi_1\rangle = \cos(\phi) |0\rangle - e^{i\chi} \sin(\phi) |1\rangle,$$

$$|\psi_2\rangle = \sin(\phi) |0\rangle + e^{i\chi} \cos(\phi) |1\rangle.$$  

Then if we guess the first state when we get outcome 1 and the second state when we get outcome 2, the probability we guess correctly in the first case is $\cos^2 \phi$, and the probability we guess correctly in the second case is between $\sin^2(\theta + \phi)$ and $\sin^2(\theta - \phi)$, depending on the value...
of χ. Therefore, we can set χ = 0, and simply vary φ without loss of generality. On average, the success probability is

\[
\frac{1}{2}[\cos^2 \phi + \sin^2 (\theta + \phi)] = \frac{1}{4}[1 + \cos(2\phi) + 1 - \cos(2(\theta + \phi))] = \frac{1}{2}[1 + \sin(\theta + 2\phi) \sin \theta]
\]

(using some more trigonometric identities). This is clearly optimized by choosing

\[
\theta + 2\phi = \begin{cases} 
\pi/2 & 0 \leq \theta < \pi \\
3\pi/2 & \pi \leq \theta < 2\pi
\end{cases}
\]
i.e., \[
\phi = \begin{cases} 
\frac{\pi}{4} - \frac{\theta}{2} & 0 \leq \theta < \pi \\
\frac{3\pi}{4} - \frac{\theta}{2} & \pi \leq \theta < 2\pi
\end{cases}
\]

so that the success probability is \(\frac{1}{2}(1 + |\sin \theta|)\).

Geometrically, on the Bloch sphere, the optimal measurement is perpendicular to the state that lies in between the two states to be differentiated:

Note that angles are doubled in this picture since orthogonal states correspond to opposite directions. We have depicted a case where \(0 < \theta < \pi/2\).

5. Teleporting through a Hadamard gate.

(a) [1 point] Write the state \((I \otimes H)|\beta_{00}\rangle\) in the computational basis.

Solution:

\[
\frac{1}{\sqrt{2}}(I \otimes H)(|00\rangle + |11\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)
\]

(b) [3 points] Suppose Alice has a qubit in the state \(|\psi\rangle\) and also, Alice and Bob share a copy of the state \((I \otimes H)|\beta_{00}\rangle\). If Alice measures her two qubits in the Bell basis, what are the probabilities of the four possible outcomes, and in each case, what is the post-measurement state for Bob?

Solution: We could perform an explicit calculation, but we can avoid that by comparing to the case of standard teleportation. Recall that if teleportation were performed using the entangled state \(|\beta_{00}\rangle\), Alice would find each of the four outcomes of the Bell measurement with equal probability (1/4), and the postmeasurement state for Bob if Alice obtained the outcome \(|\beta_{xz}\rangle\) (where \(x, z \in \{0, 1\}\)) would be \(X^x Z^z |\psi\rangle\).
Since an operation on Bob’s qubit commutes with Alice’s actions, the distribution of her outcomes is the same if the initial entangled state is \((I \otimes H)|\beta_{00}\rangle\); to find Bob’s post-measurement state we simply apply a Hadamard gate to his system. Thus the possible outcomes are as follows:

<table>
<thead>
<tr>
<th>A’s outcome</th>
<th>Probability</th>
<th>B’s state</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>\beta_{00}\rangle)</td>
<td>1/4</td>
</tr>
<tr>
<td>(</td>
<td>\beta_{01}\rangle)</td>
<td>1/4</td>
</tr>
<tr>
<td>(</td>
<td>\beta_{10}\rangle)</td>
<td>1/4</td>
</tr>
<tr>
<td>(</td>
<td>\beta_{11}\rangle)</td>
<td>1/4</td>
</tr>
</tbody>
</table>

(c) [2 points] Suppose Alice sends her measurement result to Bob. In each possible case, what operation should Bob perform in order to have the state \(H|\psi\rangle\)?

**Solution:** According to the solution of the previous part, the desired recovery operations are as follows:

<table>
<thead>
<tr>
<th>A’s outcome</th>
<th>B’s recovery operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>\beta_{00}\rangle)</td>
</tr>
<tr>
<td>(</td>
<td>\beta_{01}\rangle)</td>
</tr>
<tr>
<td>(</td>
<td>\beta_{10}\rangle)</td>
</tr>
<tr>
<td>(</td>
<td>\beta_{11}\rangle)</td>
</tr>
</tbody>
</table>

Notice that in each case, we still only have to apply Pauli gates, even though the teleportation protocol effects a nontrivial operation on the input state.

**Total points:** 37