ASSIGNMENT 3: Solutions

1. **A qubit cannot send more than a bit.**

Suppose Alice wants to send a trit of classical information (i.e., an element $x \in \{0, 1, 2\}$) to Bob, and she is able to send him a qubit. Specifically, suppose that on input $x$ she sends him $|\psi_x\rangle = \alpha_x |0\rangle + \beta_x |1\rangle$. Clearly, Bob can only reliably distinguish two outcomes by measuring $|\psi_x\rangle$ in some basis. However, if he interacts the qubit he receives with $n - 1$ ancilla qubits for $n > 1$, he can perform a measurement with more than two outcomes on the resulting $n$-qubit state. In this problem you will show that even using such a protocol, Bob cannot reliably determine a trit encoded by Alice.

In Bob’s protocol, suppose he applies the unitary operation $U$ to the state $|\psi_x\rangle \otimes |0\rangle^{\otimes n - 1}$ and measures in the computational basis, obtaining an outcome $m \in \{0, 1\}^n$. He then applies some function $f: \{0, 1\}^n \rightarrow \{0, 1, 2\}$ to obtain a trit. He succeeds if $f(m) = x$.

(a) [4 points] For $x \in \{0, 1, 2\}$, let $V_x$ denote the span of the rows of the matrix $U$ that are indexed by some $m \in \{0, 1\}^n$ such that $f(m) = x$. In other words, if $U = \sum_{m \in \{0, 1\}^n} |m\rangle \langle \phi_m|$, we have $V_x = \text{span}\{|\phi_m\rangle : f(m) = x\}$. Show that the subspaces $V_0, V_1, V_2$ are pairwise orthogonal.

**Solution:** Since $U$ is unitary, we have

$$UU^\dagger = \sum_{m, m' \in \{0, 1\}^n} |m\rangle \langle \phi_m| \langle \phi_{m'}| m'\rangle$$

$$= \sum_{m, m' \in \{0, 1\}^n} \langle \phi_m| \phi_{m'}\rangle |m\rangle \langle m'|$$

$$= I = \sum_{m \in \{0, 1\}^n} |m\rangle \langle m|,$$

so we must have $\langle \phi_m| \phi_{m'}\rangle = \delta_{m,m'}$. In other words, the states $\{|\phi_m\rangle : m \in \{0, 1\}^n\}$ are orthonormal. If $|\alpha\rangle \in V_0$ and $|\beta\rangle \in V_1$, then we have

$$|\alpha\rangle = \sum_{m : f(m) = 0} \alpha_m |m\rangle \quad \text{and} \quad |\beta\rangle = \sum_{m : f(m) = 1} \beta_m |m\rangle$$

for some coefficients $\alpha_m$ and $\beta_m$. Then

$$\langle \alpha|\beta\rangle = \sum_{m : f(m) = 0} \sum_{m' : f(m') = 1} \alpha_m^* \beta_{m'} \langle \phi_m| \phi_{m'}\rangle = 0$$

since $\langle \phi_m| \phi_{m'}\rangle = 0$ whenever $f(m) \neq f(m')$. Thus the subspaces $V_0$ and $V_1$ are orthogonal. An analogous argument shows orthogonality of $V_0$ and $V_2$ and of $V_1$ and $V_2$.

(b) [3 points] Explain why, for Bob to succeed, we must have $|\psi_x\rangle |0\rangle^{\otimes n - 1} \in V_x$ for all $x \in \{0, 1, 2\}$.

**Solution:** Let $|\Psi_x\rangle = |\psi_x\rangle |0\rangle^{\otimes n - 1}$. Bob’s protocol prepares the state $U|\Psi_x\rangle$. To succeed, his measurement outcome $m$ must satisfy $f(m) = x$. His success probability is therefore

$$\sum_{m : f(m) = x} |\langle m|U|\Psi_x\rangle|^2 = \sum_{m : f(m) = x} |\langle \phi_m|\Psi_x\rangle|^2.$$
Now expand $|\Psi_x\rangle = \sum_{m \in \{0,1\}^n} c_m |\phi_m\rangle$ with $\sum_{m \in \{0,1\}^n} |c_m|^2 = 1$. If $|\Psi_x\rangle \notin V_x$, then there is some $m'$ with $f(m') \neq x$ such that $|c_{m'}| > 0$. But the success probability is

$$\sum_{m: f(m) = x} |c_m|^2 = \sum_{m: f(m) \neq x} |c_m|^2,$$

which is less than 1 if such an $m'$ exists.

(c) [3 points] Prove that it is impossible to have $|\psi_x\rangle |0\rangle \otimes |0\rangle \in V_x$ for all $x \in \{0,1,2\}$.

**Solution:** If $|\Psi_x\rangle \in V_x$ for all $x \in \{0,1,2\}$, then by part (a), the states $|\Psi_x\rangle$ are pairwise orthogonal. Since $\langle \Psi_x | \Psi_y \rangle = \langle \psi_x | \psi_y \rangle$, this means the states $|\psi_x\rangle$ are pairwise orthogonal. But these are states of a qubit, which can support at most two pairwise orthogonal states.

2. The Hadamard gate and qubit rotations.

(a) [4 points] Suppose that $(n_x, n_y, n_z) \in \mathbb{R}^3$ is a unit vector and $\theta \in \mathbb{R}$. Show that

$$e^{-i\frac{\theta}{2}(n_x X + n_y Y + n_z Z)} = \cos(\frac{\theta}{2}) I - i \sin(\frac{\theta}{2})(n_x X + n_y Y + n_z Z).$$

**Solution:** Let $A := n_x X + n_y Y + n_z Z$. Observe that

$$A^2 = (n_x^2 + n_y^2 + n_z^2) I + n_x n_y (XY + YX) + n_x n_z (XZ + ZX) + n_y n_z (YZ + ZY) = I,$$

using the facts that $(n_x, n_y, n_z)$ is a unit vector and that $XY = -YX, XZ = -ZX$, and $YZ = -ZY$ (as can be verified by straightforward calculation). Then we have

$$e^{-i\frac{\theta}{2}A} = \sum_{j=0}^{\infty} \frac{(-i\frac{\theta}{2}A)^j}{j!}$$

$$= \sum_{\substack{j=0 \text{ even} \atop j \geq 0}} \frac{(-i\frac{\theta}{2})^j}{j!} I + \sum_{\substack{j=0 \text{ odd} \atop j \geq 0}} \frac{(-i\frac{\theta}{2})^j}{j!} A$$

$$= \cos(\frac{\theta}{2}) I - i \sin(\frac{\theta}{2}) A$$

as claimed.

(b) [3 points] Find a unit vector $(n_x, n_y, n_z) \in \mathbb{R}^3$ and numbers $\phi, \theta \in \mathbb{R}$ so that

$$H = e^{i\phi} e^{-i\frac{\theta}{2}(n_x X + n_y Y + n_z Z)},$$

where $H$ denotes the Hadamard gate. What does this mean in terms of the Bloch sphere?

**Solution:** The simplest solution is $n_x = n_z = 1/\sqrt{2}, n_y = 0, \phi = \pi/2, \text{ and } \theta = \pi$. Using the previous part, we then find

$$e^{i\pi/2} e^{-i\frac{\pi}{2}(X + Z)/\sqrt{2}} = i[\cos(\frac{\pi}{2}) I - i \sin(\frac{\pi}{2})(X + Z)/\sqrt{2}] = \frac{X + Z}{\sqrt{2}} = H.$$

In other words, $H$ is a rotation of the Bloch sphere by an angle $\pi$ about an axis halfway between the $x$ and $z$ axes.

2
(c) [3 points] Write the Hadamard gate as a product of rotations about the $x$ and $y$ axes. In particular, find $\alpha, \beta, \gamma, \phi \in \mathbb{R}$ such that $H = e^{i\phi} R_y(\gamma) R_x(\beta) R_y(\alpha)$.

**Solution:** We can perform the Hadamard gate by rotating its axis of rotation to the $x$ axis, performing the desired rotation about that axis, and then rotating back. In other words, we claim that up to a phase, the Hadamard gate is given by $R_y(-\frac{\pi}{4}) R_x(\pi) R_y(\frac{\pi}{4})$. To check this (and determine the global phase), we have

$$R_x(\pi) = \cos(\frac{\pi}{2}) I - i \sin(\frac{\pi}{2}) X = -i X$$

and

$$R_y(\pm \frac{\pi}{4}) = \cos(\frac{\pi}{8}) I \mp i \sin(\frac{\pi}{8}) Y.$$  

Then, letting $c := \cos(\pi/8)$ and $s := \sin(\pi/8)$, we find

$$R_y(-\frac{\pi}{4}) R_x(\pi) R_y(\frac{\pi}{4}) = -i \begin{pmatrix} c & s \\ -s & c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c & -s \\ s & c \end{pmatrix}$$

$$= -i \begin{pmatrix} s & c \\ c & -s \end{pmatrix} \begin{pmatrix} c & -s \\ s & c \end{pmatrix}$$

$$= -i \begin{pmatrix} 2cs & c^2 - s^2 \\ c^2 - s^2 & -2cs \end{pmatrix}$$

$$= -i \begin{pmatrix} \sin(\frac{\pi}{4}) & \cos(\frac{\pi}{4}) \\ \cos(\frac{\pi}{4}) & -\sin(\frac{\pi}{4}) \end{pmatrix}$$

$$= -i \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

where we have used some basic trigonometric identities. To get the correct global phase, we need to multiply by $i = e^{i\pi/2}$. Therefore we can take $\alpha = \pi/4$, $\beta = \pi$, $\gamma = -\pi/4$, and $\phi = \pi/2$.

3. **Circuit identities.**

(a) [3 points] What does the following circuit do? Show that your answer is correct.

\[ 
\begin{array}{c}
\bullet \\
\bullet \\
\bullet \\
\bullet
\end{array}
\]

**Solution:** We consider the action of the circuit on the computational basis:

$$
|00\rangle \mapsto |00\rangle \mapsto |00\rangle \mapsto |00\rangle$$

$$|01\rangle \mapsto |01\rangle \mapsto |11\rangle \mapsto |10\rangle$$

$$|10\rangle \mapsto |11\rangle \mapsto |01\rangle \mapsto |01\rangle$$

$$|11\rangle \mapsto |10\rangle \mapsto |10\rangle \mapsto |11\rangle$$

Thus the circuit acts to interchange the two qubits if they are in computational basis states. Since it implements a linear transformation, it acts to interchange the two qubits in general.

(b) [1 point] Verify that $H X H = Z$, where $H$ is the Hadamard gate and $X, Z$ denote Pauli matrices.

**Solution:**

$$H X H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$$
(c) [3 points] Verify the following circuit identity:

\[ \begin{array}{ccc}
& H & \\
\downarrow & \circ & \downarrow \\
H & & H
\end{array} = \begin{array}{ccc}
& H & \\
\downarrow & \circ & \downarrow \\
H & & H
\end{array} \]

**Solution:** The controlled-not gate can be written in Dirac notation as \(|0\rangle\langle0| \otimes I + |1\rangle\langle1| \otimes X\). Thus we have

\[
(I \otimes H)(|0\rangle\langle0| \otimes I + |1\rangle\langle1| \otimes X)(I \otimes H) = |0\rangle\langle0| \otimes HHH + |1\rangle\langle1| \otimes HXH \\
= |0\rangle\langle0| \otimes I + |1\rangle\langle1| \otimes Z
\]

by the previous part. In other words, this gate acts as

\[
\begin{array}{c|c}
|00\rangle & \mapsto |00\rangle \\
|01\rangle & \mapsto |01\rangle \\
|10\rangle & \mapsto |10\rangle \\
|11\rangle & \mapsto -|11\rangle.
\end{array}
\]

This transformation is the same if we interchange the qubits, so we have the same operation when we apply the three gates to the qubits in the opposite direction.

(d) [3 points] Verify the following circuit identity:

\[ \begin{array}{ccc}
& H & \\
\downarrow & \circ & \downarrow \\
H & & H
\end{array} = \begin{array}{ccc}
& H & \\
\downarrow & \circ & \downarrow \\
H & & H
\end{array} \]

Give an interpretation of this identity.

**Solution:** By the previous identity, we have

\[ \begin{array}{ccc}
& H & \\
\downarrow & \circ & \downarrow \\
H & & H
\end{array} = \begin{array}{ccc}
& H & \\
\downarrow & \circ & \downarrow \\
H & & H
\end{array} \]

where the second step follows from the simple fact that \(H^2 = I\). This shows that the controlled-not gate acts in the opposite direction when considered in the eigenbasis of \(X\).

4. **Universality of gate sets.**

Prove that each of the following gate sets either is or is not universal. You may use the fact that the set \{\text{cnot}, H, T\} is universal.

(a) [2 points] \{\text{H, T}\}

**Solution:** This set is not universal because it does not contain an entangling gate.

(b) [2 points] \{\text{cnot}, T\}

**Solution:** This set is not universal because both gates map any computational basis state to another computational basis state times a phase.

(c) [2 points] \{\text{cnot}, H\}

**Solution:** This set is not universal because both of its gates have only real matrix elements; therefore it cannot approximate a gate with an entry that is far from real, such as \(T\) (or even \(T^2\)).
(d) [4 points] \{cZ, K, T\}, where cZ denotes a controlled-Z gate and \( K = \frac{1}{\sqrt{2}} \left( \begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right) \)

**Solution:** This set is universal. A simple calculation shows that \( H = T^6 K T^6 \), so we can implement \( H \). Furthermore, \((I \otimes H)cZ(I \otimes H) = \text{cnot}\) (by question 2c above). Since we can exactly implement the universal gate set \{\text{cnot}, H, T\}, the given set is universal.

5. **Swap test.**

(a) [4 points] Let \(|\psi\rangle\) and \(|\phi\rangle\) be arbitrary single-qubit states (not necessarily computational basis states), and let \(\text{swap}\) denote the 2-qubit gate that swaps its input qubits (i.e., \(\text{swap}|x\rangle|y\rangle = |y\rangle|x\rangle\) for any \(x, y \in \{0, 1\}\)). Compute the output of the following quantum circuit:

\[
\begin{array}{c}
|0\rangle \\
|\psi\rangle \\
|\phi\rangle
\end{array}
\quad
\begin{array}{c}
H \\
\text{SWAP} \\
H
\end{array}
\]

**Solution:** We have

\[
|0\rangle|\psi\rangle|\phi\rangle \xrightarrow{H \otimes I \otimes I} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle|\phi\rangle
\]

\[
\xrightarrow{\text{CSWAP}} \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\psi\rangle)
\]

\[
\xrightarrow{H \otimes I \otimes I} \frac{1}{2}(|0\rangle + |1\rangle)|\psi\rangle|\phi\rangle + (|0\rangle - |1\rangle)|\phi\rangle|\psi\rangle)
\]

\[
= \frac{1}{2}([|0\rangle(|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle) + |1\rangle(|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle)])
\]

(b) [3 points] Suppose the top qubit in the above circuit is measured in the computational basis. What is the probability that the measurement result is 0?

**Solution:** The probability is the square of the factor needed to normalize the term with \(|0\rangle\) for the first qubit, namely

\[
\left\| \frac{1}{2}(|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle) \right\|^2 = \frac{1}{4}(|\langle \psi \rangle|\phi\rangle + |\langle \phi \rangle|\psi\rangle| + |\langle \phi \rangle|\psi\rangle)
\]

\[
= \frac{1}{4}(|\langle \psi \rangle|\phi\rangle + |\langle \phi \rangle|\psi\rangle| + |\langle \phi \rangle|\psi\rangle) + |\langle \phi \rangle|\psi\rangle| + |\langle \phi \rangle|\psi\rangle|)
\]

\[
= \frac{1}{4}(2 + |\langle \psi \rangle|\phi\rangle)
\]

\[
= \frac{1 + |\langle \psi \rangle|\phi\rangle}{2}.
\]

(c) [2 points] If the result of measuring the top qubit in the computational basis is 0, what is the (normalized) post-measurement state of the remaining two qubits?

**Solution:** The state is obtained by normalizing \((|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle)|/2 \) with the square root of the factor determined above. In other words, the state is

\[
\sqrt{\frac{2}{1 + |\langle \psi \rangle|\phi\rangle}} \cdot \frac{|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle}{2} = \frac{|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle}{\sqrt{2(1 + |\langle \psi \rangle|\phi\rangle|^2)}}.
\]
(d) [1 point] 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?

**Solution:** All the calculations above are unchanged in that case.

**Total points:** 50