# Problem Set #3 Solutions

Introduction to Quantum Information Science

Ryan Zhou (rz3974)

## 1. Local Evolution of Entangled States.

Let $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $U^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Then

$$\begin{aligned}
(U \otimes I) |\psi\rangle &= \frac{1}{\sqrt{2}} \left[ \begin{pmatrix} a \\ c \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} b \\ d \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \\
&= \frac{1}{\sqrt{2}} \left[ \begin{pmatrix} a \\ 0 \\ c \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ b \\ 0 \\ d \end{pmatrix} \right] \\
&= \frac{1}{\sqrt{2}} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \frac{1}{\sqrt{2}} \left[ \begin{pmatrix} a \\ b \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ c \\ d \end{pmatrix} \right] \\
&= \frac{1}{\sqrt{2}} \left[ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} \right] \\
&= (I \otimes U^T) |\psi\rangle .
\end{aligned}$$

## 2. Multi-qubit quantum circuits

**a)** Writing the circuit in terms of matrix multiplication, we have

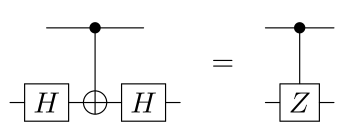
$$
\begin{aligned}
(H\otimes H)\mathrm{cX}(H\otimes H) &= \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \\
&= \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \\
&= \frac{1}{4}\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 4 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.
\end{aligned}
$$

Note that this final array is a reverse cX gate with the 2nd q-bit is used as the control.

**b)** Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The answers to the questions are below:

1. What is the state of the first qubit before the CNOT? $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ e^{i\pi/4} \end{pmatrix}$.
2. What is the state of the two qubits before the measurement? $\frac{1}{\sqrt{2}}\begin{pmatrix} \beta \\ \alpha e^{i\pi/4} i \\ \beta e^{i\pi/4} \\ \alpha i \end{pmatrix}$.
3. What are the probabilities of measuring $|0\rangle$ or $|1\rangle$? $P[|0\rangle] = \frac{1}{2}(\beta^2+\alpha^2) = \frac{1}{2}$, $P[|1\rangle] = \frac{1}{2}(\alpha^2+\beta^2) = \frac{1}{2}$.
4. 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 $|1\rangle$? If the first qubit is $|0\rangle$, $|\psi_{\text{out}}\rangle = \beta|0\rangle + \alpha e^{i\pi/4} i|1\rangle$. If the first qubit is $|1\rangle$, $|\psi_{\text{out}}\rangle = \beta e^{i\pi/4}|0\rangle + \alpha i|1\rangle$.

**c)** The circuit is below:



**3. Quantum Money Attacks.** If we expand all the tensor products, we get the giant vector

$$\begin{pmatrix} \frac{\sqrt{3}}{2} \\ 0 \\ 0 \\ \frac{1}{\sqrt{12}} \\ 0 \\ \frac{1}{\sqrt{12}} \\ \frac{1}{\sqrt{12}} \\ 0 \end{pmatrix}.$$

Then the probability of success for any given qubit state is $P(\text{success}) = (\frac{5}{6})(\frac{9}{10}) + (\frac{1}{6})(0) = \frac{3}{4}$. Note that each case is symmetric, thus the overall probability is $4(\frac{1}{4})(\frac{3}{4}) = \frac{3}{4} > \frac{5}{8}$.

**4. SARG04 Quantum Key Distribution**

**a)** $a = 011001$, $b = 101011$, $|\psi\rangle = |+\rangle |1\rangle |-\rangle |0\rangle |+\rangle |-\rangle$.

**b)** $b' = 100111$, $|\psi'\rangle = |+\rangle |1\rangle |0\rangle |-\rangle |+\rangle |-\rangle$, $a' = 010101$.

**c)** Alice and Bob will discard indices 2 and 3, so $a = a' = 0101$.

**d)** Assign $\{|0\rangle, |+\rangle\} = 00$, $\{|0\rangle, |-\rangle\} = 01$, $\{|1\rangle, |+\rangle\} = 10$ or $\{|1\rangle, |-\rangle\} = 11$. Then we can encode $|psi\rangle$ with the classical string 101111001001.

**e)** Using $a'$ from part b, we get a $b' = 1?1111$.

**f)** Alice and Bob will discard indices 1 and 2, so $a = 0001$ and $a' = 0101$. I'm not sure if $a, a'$ are supposed to match in this scheme. It seems like they should, but I didn't really understand the instructions we were given for SARG04.