# Quantum Computing Epiphany Assignment 3

**Q1** **1.1** We first want to set the 41 entry to 0. Applying the formulas in the lecture, or by inspection, a matrix that does the job is

$$U_{14} := \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix} .$$

We have $U_{14}^\dagger = U_{14}$ and

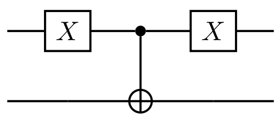
$$U_{14}U = U_{23} := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

Clearly $U_{23}^\dagger = U_{23} = U_{23}^{-1}$, so

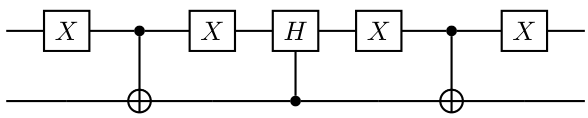
$$U = U_{23}U_{14} .$$

Note that in this case $U_{23}U_{14} = U_{14}U_{23}$, since the matrices act non-trivially on linearly independent subspaces.

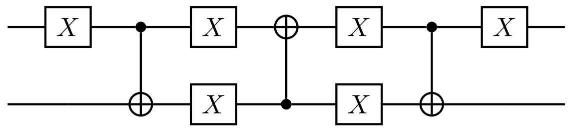
**1.2** $U_{14}$ acts on the $|00\rangle, |11\rangle$ subspace. To make it act on a single qubit subspace we use the Gray code $00 \to 01 \to 11$. The first step of the Gray code is implemented by a CNOT gate controlled on the top bit (when it's equal to 0). In circuit form:



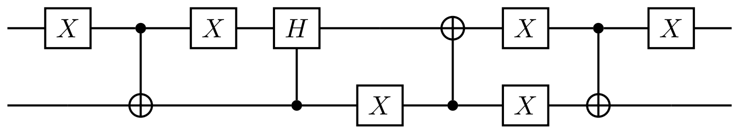

After this change of basis we have a standard controlled-Hadamard gate acting on the highest bit, so the full circuit for $U_{14}$ is



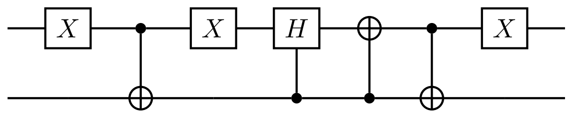

The $U_{23}$ gate also needs a change of basis, which we can implement via the Gray code $01 \to 00 \to 10$. The first step is just as above, and after the change of basis we have a CNOT gate acting on the top bit whenever the lowest bit is 0. So the full circuit is:



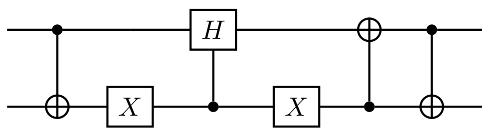
**1.3** Writing $U = U_{23}U_{14}$, we just need to concatenate the circuits above. There is a straightforward simplification coming from the fact that we are using the same Gray code in both cases, so when concatenating the two changes of basis cancel each other. We have



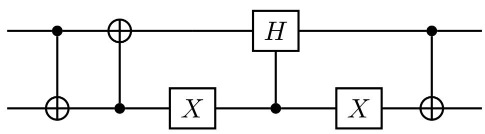
which after some minor simplifications becomes



or



or



with no obvious further simplification.

**Q2** After the first two steps, the state is $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\varphi}|1\rangle) \otimes |\psi\rangle$, and the further $H$ gives $\frac{1}{2}[(1+e^{2\pi i\varphi})|0\rangle + (1-e^{2\pi i\varphi})|1\rangle] \otimes |\psi\rangle$, so the probability of measuring 0 is as given (and the probability of measuring 1 is $\sin^2(\pi\varphi)$).

If we measure 0 the resulting state is already what we want (our original state $|0\rangle \otimes |\psi\rangle$), and if we measure 1 then the output is $|1\rangle \otimes |\psi\rangle$, which we can turn into back into our desired state by acting with $X_1$. So this is a classically controlled $X$ gate, where the control bit is the output of the measurement, and the target is the quantum state of the top qubit after measurement.

We could just measure $\cos^2(\pi\varphi)$ by repeatedly measuring, obtaining better estimates of $\cos^2(\pi\varphi)$. Note that whether we get the result 0 or 1, the state $|\psi\rangle$ is not changed so we can reuse it and repeat the process.

However, even if we determine $\cos^2(\pi\varphi)$ accurately there is a limitation regarding the value of $\varphi$. Due to periodicity we can take $\varphi \in (-1/2, 1/2]$ but we cannot distinguish between $\varphi$ and $-\varphi$ since all the probabilities are even functions of $\varphi$. So, up to this sign ambiguity, we determine $\varphi$ with the assumption that $\varphi \in [0, 1/2]$.

**Comment:** Actually, the accuracy of the estimate improves slowly if we just keep repeating the process as above. Instead we can speed up the estimation if use C-$U^k$ gates in the circuit (which is the same as replacing the single C-$U$ gate with $k$ C-$U$ gates) and vary the value of $k$. For any given $k$ the probability is $p(0) = \cos^2(\pi k\varphi)$.

Now, note that values for $\varphi \in [0, 1/2]$ can be written in binary as $\varphi = 0.0b_2b_3b_4\cdots = \sum_{j=2}^{\infty} b_j/2^j$. (The value 1/2 would normally be written in binary as 0.1 but this is also equal to $0.01111\cdots$.)

To determine the value of $b_2$ we just need to determine if $\varphi$ is less than 1/4 (so $b_2 = 0$) or not (so $b_2 = 1$). Hence, starting with $k = 1$, we only need to determine $p$ to sufficient accuracy to determine if $p < \cos^2(\pi/4) = 1/2$ or not.

Once we have done that we can set $k = 2$ and measure to estimate the probability $p = \cos^2(\pi 2\varphi)$ which is equivalent to the previous case of $k = 1$ but replacing $\varphi$ with $2\varphi$. If we had determined $b_2 = 0$ then we have exactly the same process to determine $b_3$. If instead we had found $b_2 = 1$ we would want to distinguish between $2\varphi \in [1/2, 3/4)$ giving $b_3 = 0$ for $p < 1/2$ and $2\varphi \in [3/4, 1]$ giving $b_3 = 1$ for $p \geq 1/2$.

We can then continue the process by taking $k = 2^2 = 4$ to determine $b_4$ with the details depending on the value of $b_3$, as for $b_3$ and $b_2$ above. Note that the value of $b_2$ is irrelevant here since $b_2$ will affect the integer part of $4\varphi$ and that does not matter due to periodicity. In general taking $k = 2^j$ will determine $b_{j+2}$ with the details depending on the value of $b_{j+1}$.