18.435/2.111 Homework 5 Solutions

1: We can imagine 2 places where Simon's algorithm might fail: First, it would fail if we ever measured a $|z\rangle$ in the first register such that $z \cdot c \neq 0$. Second, it would fail if it took exponentially long to build up a set of n linearly independent $|z\rangle$. It turns out that we always get $z \cdot c = 0$, but that we are very likely (exponentially close to probability 1) that we observe $z = 0$, so that it takes exponentially many trials to get n linearly independent z's.

Let's prove that $z \cdot c = 0$ for every case. We can partition the input strings $\mathcal{X}$ into two sets $\mathcal{X}_1$ and $\mathcal{X}_2$, where for $x \in \mathcal{X}_1$, we have that $x \oplus c \in \mathcal{X}_2$. (Note that if $x = 0 \in \mathcal{X}_1$, then $y = 0 \oplus c \in \mathcal{X}_2$.) When we apply Simon's algorithm, we get the following state, prior to measurement:

$$\frac{1}{2^n} \sum_{z=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{z \cdot x} |z\rangle |f(x)\rangle =$$

$$\frac{1}{2^n} \sum_{z=0}^{2^n-1} \sum_{x \in \mathcal{X}_1} (-1)^{z \cdot x} (1 + (-1)^{z \cdot c}) |z\rangle |f(x)\rangle .$$

From the $(1 + (-1)^{z \cdot c})$ term, we can see that we will never get a z such that $z \cdot c \neq 0$. Note that here we have used only the periodicity of f, and said nothing about the values it takes.

Let's now look at the state that comes out of the oracle. For convenience, let's define the set $\mathcal{Y} = \{0, y\}$ and its complement $\mathcal{Y}^c$. We now have the state

$$\begin{aligned} \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x \in \mathcal{Y}^c} |x\rangle |0\rangle + \frac{1}{\sqrt{2^n}} (|0\rangle + |y\rangle) |1\rangle \\ &\equiv A_1 |\mathcal{Y}^c\rangle |0\rangle + A_2 |\mathcal{Y}\rangle |1\rangle , \end{aligned} \tag{1}$$

where we have defined the kets $|\mathcal{Y}^c\rangle = \frac{1}{\sqrt{2^n - 2}} \sum_{x \in \mathcal{Y}^c} |x\rangle$ and $|\mathcal{Y}\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |y\rangle)$. The normalization constants are $A_1 = \sqrt{2^n - 2}/\sqrt{2^n}$ and $A_2 = 1/\sqrt{2^{n-1}}$.

What happens when we measure a $|1\rangle$ on register 2? First of all, this will happen with probability $|A_2|^2 = 2^{-(n-1)}$. When we apply the Hadamard gate to $|\mathcal{Y}\rangle$, we get

$$H^{\otimes n} |\mathcal{Y}\rangle = \sum_{z=0}^{2^n-1} (1 + (-1)^{z \cdot c}) |z\rangle . \tag{2}$$

This is the desired interference pattern. When we measure register 1, we get a z such that $z \cdot c = 0$ with each such z equally likely.

What happens when we measure a $|0\rangle$ on register 2? This will happen with probability $|A_1|^2 = 1 - 2^{-(n-1)}$. To see what happens in this case, it is easier to express $|\mathcal{Y}^c\rangle$ in terms of $|\mathcal{Y}\rangle$ and $|s\rangle = 2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle$, the superposition of all states. This is given by $|\mathcal{Y}^c\rangle = A_1^{-1}|s\rangle - A_2/A_1|\mathcal{Y}\rangle$. Written this way, the effect of the Hadamard is clearer:

$$\begin{aligned} H^{\otimes n}|\mathcal{Y}^c\rangle &= \frac{1}{A_1}H^{\otimes n}|s\rangle - \frac{A_2}{A_1}H^{\otimes n}|\mathcal{Y}\rangle \\ &= \frac{1}{A_1}|0\rangle - \frac{A_2}{2^{n/2}A_1}\sum_{z=0}^{2^n-1}(1+(-1)^{z\cdot c})|z\rangle\,. \end{aligned}$$

From here, we can see that the probability of measuring any $z \neq 0$ is $|A_2/2^{n/2}A_1|^2$, which is exponentially small. Thus, with probability exponentially close to 1, we will measure $z = 0$.

What does this mean? In order to determine c, we need n linearly independent z, but each time we run through an iteration of Simon's algorithm, we are exponentially unlikely to get any z other than 0.

1b: We saw in the first part that Simon's algorithm would work, but would take an exponentially long time to find n linearly independent z to determine c completely. We can do the same for other non-two-to-one functions $h(x) = h(x+c)$. The first analysis, that $z \cdot c = 0$, will still hold true. We could repeat the second analysis, and partition the input strings into the sets $\mathcal{X}_i$ for which the elements all give the same $h(x)$. This is the generalization of our sets $\mathcal{Y}$ and $\mathcal{Y}^c$ above. Based on the size of each of these sets, we can determine how likely the given z outputs are, and hence how long it will take to build up n linearly independent z's.

Consider some two-to-one function $f(x)$. Now let's take out a set $\mathcal{X}_0 = \{x_i, x_i \oplus c\}$ and define h such that

$$\left\{ \begin{array}{cc} h(x) = f(x), & x \in \mathcal{X}_0^c \\ h(x) = 0, & x \in \mathcal{X}_0 \end{array} \right\}. \tag{3}$$

Here, we will get a $|0\rangle$ on the second register with probability 2^{-n}(# of elements in $\mathcal{Y}$). The rest of the time, we will get a value $z \cdot c = 0$, and when we get n linearly independent z's, we're done.

2: First, we need to find the qutrit equivalent to the Hadamard gate. We saw some of this in the second problem set. Let's define this as

$$H_3 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, \tag{4}$$

where $\omega = e^{2\pi i/3}$. The circuit looks just the same as in the qubit case, substituting H_3 for H. When we measure the second register and get a result $|f(x_0)\rangle$, we have the first register in the state $3^{-1/2}(|x_0\rangle + |x_0 + c\rangle + |x_0 + 2c\rangle)$. When we apply $H_3^{\otimes n}$ again to the first register, we get

$$\frac{1}{3^{(n+1)/2}} \sum_{z=0}^{3^n-1} \omega^{x_0 \cdot z}(1 + \omega^{c \cdot z} + \omega^{2c \cdot z}) \, |z\rangle \, . \tag{5}$$

(Remember that the dot product is now defined mod 3). We again get the result that the amplitude is 0 unless $c \cdot z = 0$. We still need only n linearly independent z to obtain the value c.

3: There are two main things to see. The first is the number of gates in the QFT. From the circuit given in class (also Nielsen and Chuang figure 5.1), we can quickly see that the number of gates for an n-qubit QFT is $\sum_{k=1}^{n} k = n(n+1)/2$ which is $O(n^2)$. (If we're counting only the controlled-R_k gates, as the problem seems to imply, this is $n(n-1)/2$, which is still $O(n^2)$.) As stated in the problem, the precision of each one of these gates is $\Delta = 1/p(n)$. As we learned when we talked about universality with a discrete set of gates, we know that errors grow linearly in the number of gates. This is laid out in Nielsen and Chuang 4.5.3. More specifically, we can use Eq. (4.63) to conclude that the error in the QFT is bounded by $n(n+1)/2p(n)$ which scales as $n^2/p(n)$, the desired result.