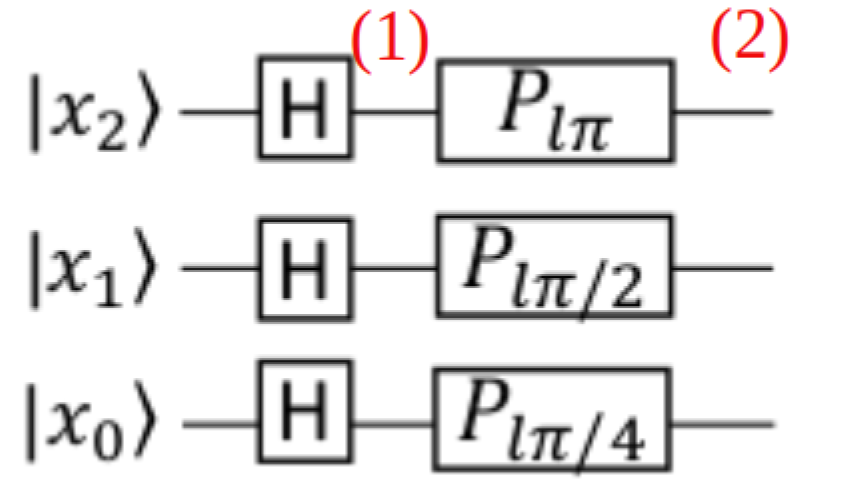

Figure 1: First Circuit

Ali Al Kadhim
Quantum Computing
Problem set 7

Problem 1

0.1 Part a

We have the following circuit shown in Figure 1

We start with states $|0\rangle|0\rangle|0\rangle$. When acting on state $|0\rangle|0\rangle|0\rangle$the circuit shown first acts with H on each of the $|0\rangle$ states. Therefore at position (1) indicated by Figure 1 and reading the qubits from top to bottom, this gives

$$H^2 \otimes H^1 \otimes H^0|0\rangle|0\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{1}$$

Where here my notation is H^n means H being applied to the nth qubit. Now we are at position (2), applying the phase gates we get

$$\left(P_{l\pi}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(P_{l\pi/2}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(P_{l\pi/4}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \tag{2}$$

The controlled two-qubit Z_k gate is defined as $Z_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2^k} \end{pmatrix}$, or equivalently

$$Z_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^k} \end{pmatrix}$$

acting on the two-qubit standard basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ (it only applied $e^{i\pi/2^k}$ to the target state if the control state is 1.)

Similar to Z_k, P_ϕ is defined as $P_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$, it does nothing to the first ($|0\rangle$) state and applies $e^{i\phi}$ to the second. Therefore (2) becomes

$$\left(\frac{1}{\sqrt{2}}(|0\rangle + e^{il\pi}|1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + e^{il\pi/2}|1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + e^{il\pi/4}|1\rangle)\right) \tag{3}$$

Now consider $|\psi_l\rangle$; we use the definition

$$|\psi_l\rangle = \frac{1}{2^{3/2}} \sum_{x=0}^{7} e^{2\pi ixl/8} \, |x_2 x_1 x_0\rangle \tag{4}$$

Now using

$$x = x_{number} = x_0^{bin} + 2x_1^{bin} + 4x_2^{bin} \tag{5}$$

Where x_{bin} a binary number (0 or 1), therefore (4) becomes

$$|\psi_l\rangle = \frac{1}{2^{3/2}} \sum_{x=0}^{7} e^{2\pi i(x_0+2x_1+4x_2)l/8} |x_2 x_1 x_0\rangle \tag{6}$$

We can break this up as a sum on each individual qubit, i.e.

$$\begin{aligned} |\psi_l\rangle &= \left(\frac{1}{\sqrt{2}} \sum_{x_0=0}^{1} e^{2\pi ix_0 l/8} |x_0\rangle\right) \otimes \left(\frac{1}{\sqrt{2}} \sum_{x_1=0}^{1} e^{2\pi i(2x_1)l/8} |x_1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}} \sum_{x_2=0}^{1} e^{2\pi i(4x_2)l/8} |x_2\rangle\right) \\ &= \left(\frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi l/4}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi l/2}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi l}|1\rangle\right) \end{aligned} \tag{7}$$

This is precicely what we got in equation (3)!!! Hence we have verified the requested relation!

0.2 Part b

Starting with the definition of $|\psi_l\rangle$ in (4), we have

$$|\psi_{-l}\rangle = \frac{1}{2^{3/2}} \sum_{x=0}^{7} e^{-2\pi ixl/8} \, |x_2 x_1 x_0\rangle \tag{8}$$

With the definition of the quantum Fourier transform,

$$U_{FT}|x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi ixy/2^n} \, |y\rangle_n \tag{9}$$

Then

$$\begin{aligned}
U_{FT}|\psi_{-l}\rangle_3 &= U_{FT}\frac{1}{2^{3/2}}\sum_{x=0}^{7} e^{-2\pi ixl/8}\,|x\rangle_3 \\
&= \frac{1}{2^{3/2}}\sum_{x=0}^{7} e^{-2\pi ixl/8} U_{FT}\,|x\rangle_3 \\
&= \frac{1}{8}\sum_{x=0}^{7} e^{-2\pi ixl/8}\sum_{y=0}^{7} e^{2i\pi xy/8}|y\rangle_3 \\
&= \frac{1}{8}\sum_{x=0}^{7}\sum_{y=0}^{7} e^{2i\pi x(y-l)/8}|y\rangle_3
\end{aligned} \tag{10}$$

Aside (not completely required): Now let's review a bit on Fourier transforms to complete the calculation above. Recall that if $f(x)$ is periodic such that $f(x+L) = f(x)$, then the Fourier expansion of it is

$$f(x) = \sum_{n=-\infty}^{\infty} c_n e^{2i\pi nx/L} \tag{11}$$

If we define $I(l) = \int_{-L/1}^{L/2} e^{2\pi lx/L}$ then $I(l) = \frac{L}{2i\pi l}(e^{2i\pi l} - e^{-2i\pi l})$ if $l \neq 0$.
If on the other hand $l = 0$, then $e^{2i\pi l} = e^{-2i\pi l}(= 1)$ [a] and $I(l) = 0$. If $l = 0$ then $I(0) = \int_{-L/2}^{L/2} 1dx = L$, therefore it follows that

$$\int_{-L/2}^{L/2} e^{2i\pi(n-m)x/L}dx = L\delta_{nm} \tag{12}$$

Then the coefficients of (11) can be found by multiplying (11) by $e^{-2i\pi mx}/L$ and integrating from $-L/2$ to $L/2$.

[a] Because $e^{i\pi} = -1$, therefore $e^{i\pi l} = (e^{i\pi})^l = (-1)^l$. Therefore, $e^{2i\pi l} = (-1)^{2l} = 1$ for all any integer l.

Now that this Fourier transform aside is complete, we can continue computing (10) by treating it just as a math problem without having to worry about the bits into their binary representations. Doing the x sum first,

$$U_{FT}|\psi_{-l}\rangle_3 = \sum_{y=0}^{7}\left(\frac{1}{8}\sum_{x=0}^{7} e^{2i\pi x(y-l)/8}\right)|y\rangle_3 \tag{13}$$

It's clear to see that if $y = l$ the sum in (13) is a sum of 1's (8 1's times 1/8) which gives 1. Further, this is a unitary transformation so we know that all the other amplitudes (for $y \neq l$) give zero. Hence clearly this sum is $(something) \times \delta_{yl}$.

In fact, (13) can just be written as

$$U_{FT}|\psi_{-l}\rangle_3 = \sum_{y=0}^{7}\widetilde{h}(y)|y\rangle_3 \tag{14}$$

Where $\widetilde{h}(y)$ are the phases in the expansion above ($\widetilde{h}(y) = \frac{1}{8}\sum_{x=0}^{7} e^{2i\pi x(y-l)/8} = 1\text{if } y = l$). The amplitude square of these factors give the corresponding probability that is required. For example the probability that the state is found in $y = l$ is

$$\text{Prob}(y = l) = |\widetilde{h}(y)|^2 = 1 \tag{15}$$

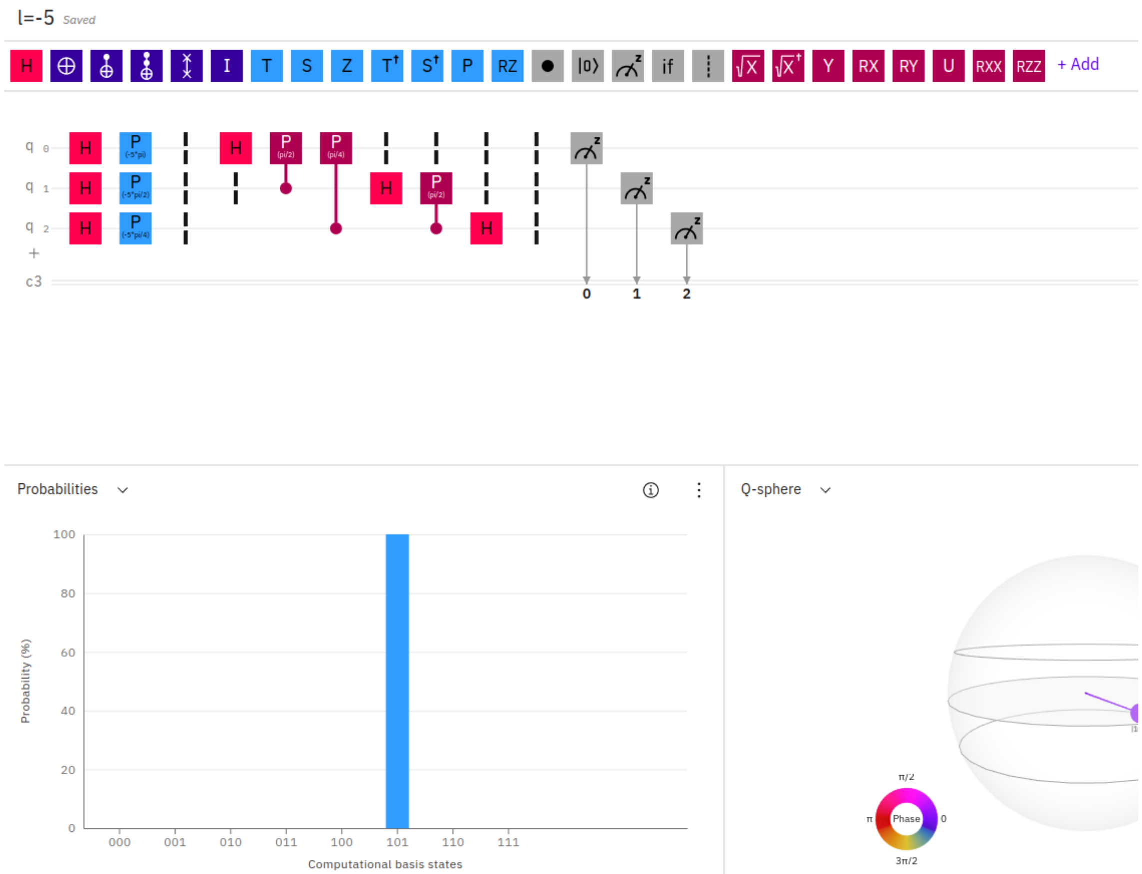

Figure 2: Circuit for $U_{FT}|\psi_{-l}\rangle$ where $l = -5$. The resulting state is $|l\rangle$ so that $l = 5$ in binary (=101) as expected. Note that technically $5_{10} = 0101_2$ but we're using only 3 qubits and hence we have $5 = 101$ in binary

Where the product 1 is calculated and discussed above. This tells us that the state above in which $y = l$ is by definition the state $|l\rangle$, i.e.

$$\begin{aligned} \text{Prob}(y = l) = 1 &\implies \sum_{y=0}^{7} \widetilde{h}(y)|y\rangle_3 = |l\rangle \\ &\implies U_{FT}|\psi_{-l}\rangle_3 = |l\rangle \end{aligned} \tag{16}$$

0.3 Part c

Figure 2 shows the circuit for $U_{FT}|\psi_{-l}\rangle$ where $-l = -5$. The resulting state is $|l\rangle$ so that $l = 5$ in binary (=101) as expected.

Figure 3 shows the circuit for $U_{FT}|\psi_{-l}\rangle$ where $-l = -3$. The resulting state is $|l\rangle$ so that $l = 3$ in binary (=011) as expected.

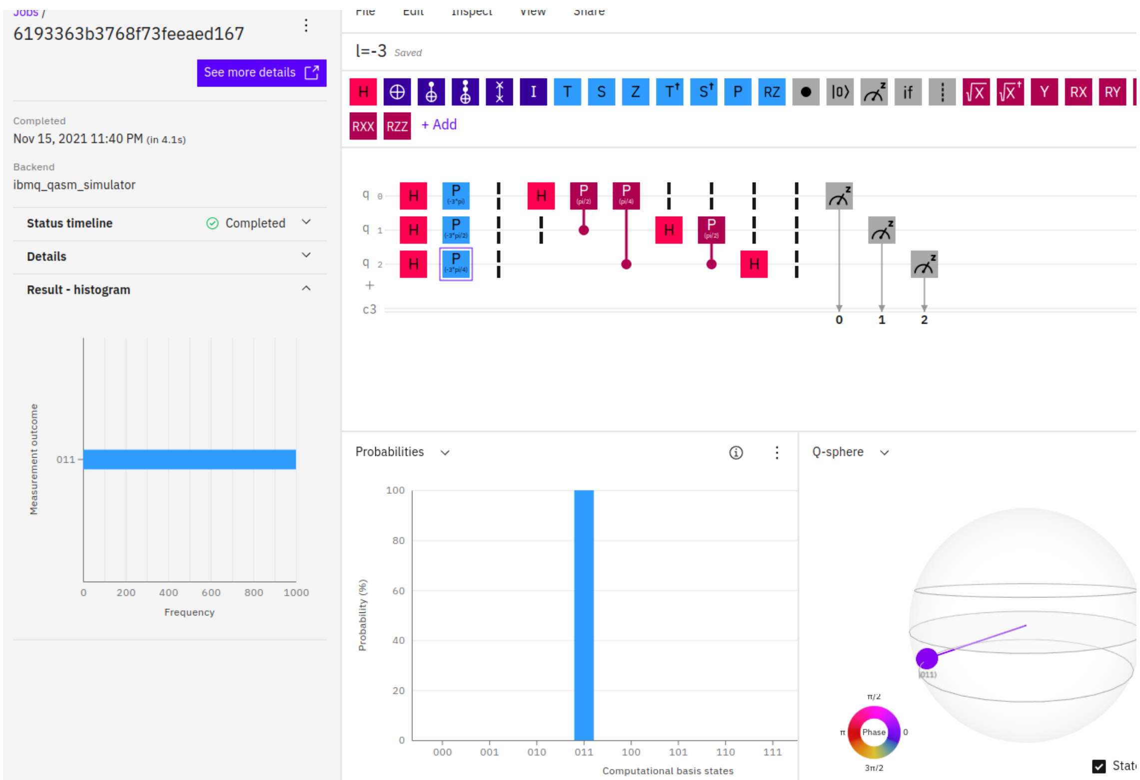

Figure 3: Circuit for $U_{FT}|\psi_{-l}\rangle$ where $-l = -3$. The resulting state is $|l\rangle$ so that $l = 3$ in binary (=011) as expected.

1 Problem 2

All of my code for this problem is provided in an external PDF document that was submitted with this write-up.

1.1 Part a

Bob chooses p and q

$$p = 3,\ 1 = 11 \tag{17}$$

Such that

$$N = pq = 3 \times 11 = 33 \tag{18}$$

We now must choose an integer $c < N \rightarrow c < 33$ that share no common divisors with

$$(p-1)(q-1) = 2 \times 10 = 20 \tag{19}$$

One choice that suffices the above conditions is

$$c = 17 \tag{20}$$

1.2 Part b

We determine integer $d < N$ which satisfies

$$cd(\mathrm{mod}(p-1)(q-1)) = 1 \tag{21}$$

This can be done quickly with the python code And we attain $d = 13$.

1.3 Part c

Picking $a < N$ we compute b via

$$b = a^c(\mathrm{mod} N) \tag{22}$$

$$\text{Choosing} a = 5 \text{ gives} b = 14. \tag{23}$$

1.4 Part d

Now computing

$$b^d(modN) \tag{24}$$

with our choice of b from (23) gives 5, i.e. what the value we chose for a.

1.5 Part e

Now we wish to find the period of

$$f(x) = b^x(modN) \tag{25}$$

Since $N = 33$ is so small, we can find the period by doing a direct check of $f(x)$, computationally this means calculating the array of $f(x)$ where $x = 1, 2, ...33$ and checking the minimum index in this array in which the output of the function starts repeating. My code attached does this. In this case we get

$$r = 10 \tag{26}$$

1.6 Part f

we calculate d' by

$$cd'(\text{mod}r) = 1 \tag{27}$$

and attain

$$d' = 3 \tag{28}$$

1.7 Part h

The value of r is even (from above), and

$$b^{r/2}(mod)N \neq N - 1 \tag{29}$$

therefore, the answer to both of the questions is yes, and we proceed to part (i).

1.8 Part i

$$\text{GCD}(b^{r/2} + 1, N) = 3 \tag{30}$$

$$\text{GCD}(b^{r/2} - 1, N) = 11 \tag{31}$$