Exercise set #4

Exercise 1 (Hw2):

Suppose we have two qubits in the following states:

$$|\Psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$$

$$|\Psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

e) A convenient way to write down the probabilities of obtaining measurement outcomes when measuring the control qubit in the computational basis is by computing

$$p_0 = \langle\Phi| |0\rangle \langle 0| \otimes I \otimes I |\Phi\rangle$$

$$p_1 = \langle\Phi| |1\rangle \langle 1| \otimes I \otimes I |\Phi\rangle$$

$$|\phi\rangle = \frac{1}{2} |0\rangle \otimes \left(|\psi_2\rangle|\psi_1\rangle + |\psi_1\rangle|\psi_2\rangle \right) + \frac{1}{2}\left(|\psi_2\rangle|\psi_1\rangle - |\psi_1\rangle|\psi_2\rangle \right)$$

$$P_n = \langle \phi | \, |0\rangle\langle 0| \otimes I \otimes I \cdot \frac{1}{2}\Big(|0\rangle|\psi_2\rangle|\psi_1\rangle + |0\rangle|\psi_1\rangle|\psi_2\rangle + |1\rangle|\psi_2\rangle|\psi_1\rangle - |1\rangle|\psi_1\rangle|\psi_2\rangle \Big)$$

$$= \langle \phi | \; \frac{1}{2}\Big(|0\rangle\langle 0|0\rangle \otimes I|\psi_2\rangle \otimes I|\psi_1\rangle + |0\rangle\langle 0|0\rangle|\psi_1\rangle|\psi_2\rangle +$$

$$|0\rangle\langle 0|\cancelto{0}{1\rangle}\,|\psi_2\rangle|\psi_1\rangle - |0\rangle\langle 0|\cancelto{0}{1\rangle}\,|\psi_1\rangle|\psi_2\rangle \Big)$$

$$= \langle \phi | \; \frac{1}{2} \; |0\rangle|\psi_2\rangle|\psi_1\rangle + |0\rangle|\psi_1\rangle|\psi_2\rangle \Big)$$

$$= \frac{1}{4}\Big(\overbrace{\langle 0|0\rangle\langle \psi_2|\psi_2\rangle\langle \psi_1|\psi_1\rangle}^{1} + \langle 0|0\rangle\langle \psi_2|\psi_1\rangle\langle \psi_1|\psi_2\rangle + \langle 0|0\rangle\langle \psi_1|\psi_2\rangle\langle \psi_2|\psi_1\rangle +$$

$$\underbrace{\langle 0|0\rangle\langle \psi_1|\psi_1\rangle\langle \psi_2|\psi_2\rangle}_{1} \Big)$$

$$= \frac{1}{4}\Big(2 + \langle \psi_1|\psi_2\rangle^{*}\langle \psi_1|\psi_2\rangle + \langle \psi_1|\psi_2\rangle\langle \psi_1|\psi_2\rangle^{*} \Big)$$

$$= \frac{1}{2}\Big(1 + |\langle \psi_1|\psi_2\rangle|^2 \Big)$$

Apply this rule to show that

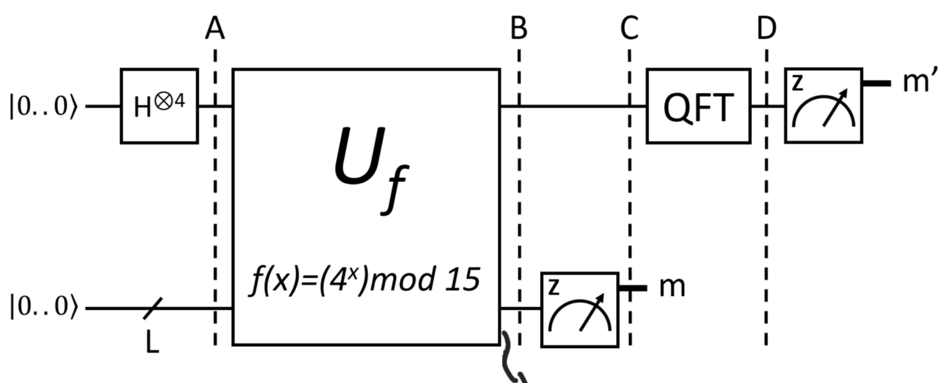
$$p_0 = \frac{1}{2} + \frac{|\langle\Psi_1|\Psi_2\rangle|^2}{2}$$
$$p_1 = \frac{1}{2} - \frac{|\langle\Psi_1|\Psi_2\rangle|^2}{2}$$

$p_0 = 1$
$p_1 = 0$

f) How can you use this circuit for testing whether $|\Psi_1\rangle = |\Psi_2\rangle$? Explain when your procedure works well, and when you will only gain some confidence. Many measurement should be done to get "0" measurement all the time.

Exercise 2:

We will go through the steps of Shor's algorithm to find the period r and factorize $N = 15$ for $a = 4$.



$|L \oplus f(x)\rangle$

a) For simplicity, we will only use 4 qubits for the top register. How many qubits L do we need for the bottom register? $L = \log_2 N = 4$

b) What is the state $|\Psi_A\rangle$ of all the qubits at point A?

b) $[H^{\otimes 4}|0\rangle]\,|0\rangle^{\otimes 4} = \frac{1}{4}\left[|0\rangle_4 + |1\rangle_4 + \cdots + |15\rangle_4\right]|0\rangle^{\otimes 4}$

$|\Psi_A\rangle = H^{\otimes 4} \otimes I^{\otimes 4}\, |0\rangle|0\rangle$

$$
\begin{array}{ccccccc}
 & 0 & 1 & 2 & 3 & 4 & \cdots \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
4^x \bmod 15 & 1 & 4 & 1 & 4 & 1 & \cdots
\end{array}
\qquad r = 2 \ (\text{period})
$$

c) What is the state $|\Psi_B\rangle$ of all the qubits at point B?

d) What is the state $|\Psi_C\rangle$ of all the qubits at point C if we measured $|1\rangle$ in the bottom register?

e) What is the state $|\Psi_D\rangle$ of the top register at point D?

f) What are the possible measurement outcomes for the top register? What is the value of r in each case?

g) Use the r from e) to determine the prime factors of N.

c)

$$\Psi_B = \frac{1}{4}\left[|0\rangle_4 |0 \oplus \underbrace{4^0 (\bmod 15)}_{1}\rangle_4 + |1\rangle_4 |0 \oplus \underbrace{4^1 (\bmod 15)}_{4}\rangle \cdots \right]$$

$$= \frac{1}{4}\Big[\underbrace{|0\rangle_4}_{\text{top}} \underbrace{|1\rangle_4}_{\text{(bottom)}} + |1\rangle_4 |4\rangle_4 + |2\rangle |1\rangle + |3\rangle|4\rangle +$$
$$+ |4\rangle |1\rangle + |5\rangle |4\rangle + |6\rangle |1\rangle + |7\rangle |4\rangle +$$
$$+ |8\rangle |1\rangle + |9\rangle |4\rangle + |10\rangle |1\rangle + |11\rangle |4\rangle +$$
$$+ |12\rangle |1\rangle + |13\rangle |4\rangle + |14\rangle |1\rangle + |15\rangle |4\rangle \Big]$$

d) $$\Psi_C = \frac{1}{2\sqrt{2}} \left[|0\rangle + |2\rangle + |4\rangle + |6\rangle + |8\rangle + |10\rangle + |12\rangle + |14\rangle \right] \otimes |1\rangle_4$$

$$QFT = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i}{N} xy} |y\rangle$$

$$QFT \quad |j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i\, jk}{N}} |k\rangle$$

e)

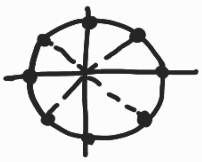
$$|\Psi_D\rangle = \frac{1}{\sqrt{2^7}}\left(\sum_{k=0}^{15}|k\rangle + \sum_{k=0}^{15} e^{\frac{2\pi i\, 2k}{16}}|k\rangle + \dots + \sum_{k=0}^{15} e^{\frac{2\pi i\, 14k}{16}}|k\rangle\right)$$

$$= \frac{1}{\sqrt{2^7}}\left(\sum_{k=0}^{7}|0\rangle + \sum_{k=0}^{7} e^{\frac{2\pi i\,\overset{2k}{(2k)}}{16}}|1\rangle + \sum_{k=0}^{7} e^{\frac{2\pi i\,\overset{4k}{(2k.2)}}{16}}|2\rangle + \quad 6k\right.$$

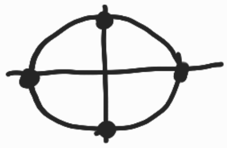
$$\left. \dots\dots + \sum_{k=0}^{7} e^{\frac{2\pi i\,(30k)}{16}}|15\rangle\right)$$

$$|\Psi_D\rangle = \frac{1}{\sqrt{2^7}}\left(\sum_{k=0}^{7}|0\rangle + 0 + \text{-------}\right)$$

→ Use Matlab



$|1\rangle$



$|2\rangle$

$$|\Psi_D\rangle = \frac{1}{\sqrt{2^7}}\left(\sum_{k=0}^{7}|0\rangle + \sum_{k=0}^{7} e^{\frac{2\pi i\,(16k)}{16}}|8\rangle\right)$$

f, g) $\frac{M}{16} = \frac{s}{r} \rightarrow \frac{8}{16} = \frac{1}{2} \rightarrow \boxed{r=2}$

↓

0, 8

↓ measurement

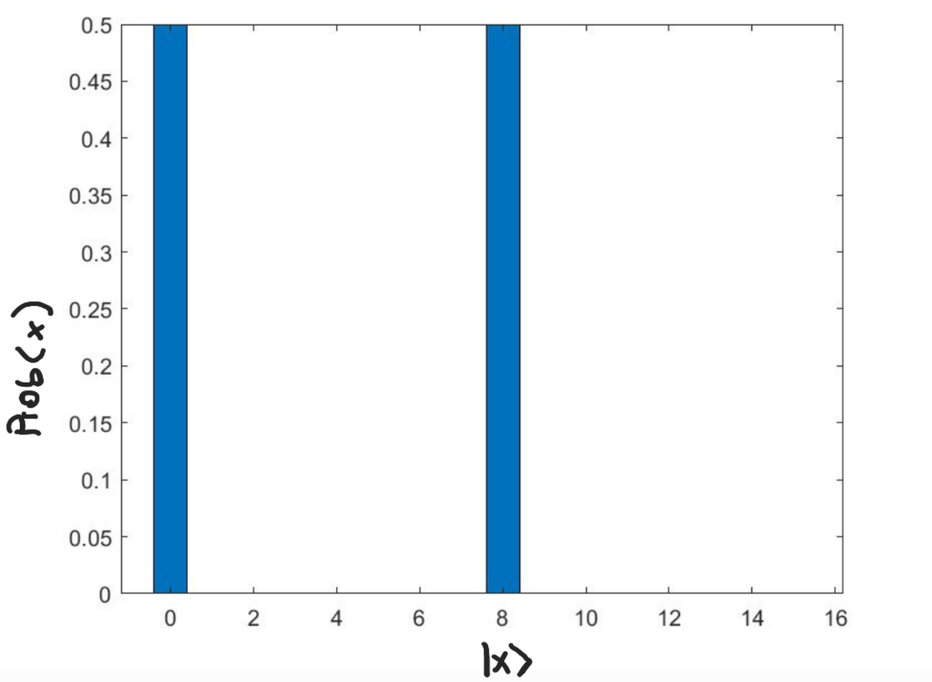
$a^{r/2} + 1 = 4 + 1 = 5$

$a^{r/2} - 1 = 4 - 1 = 3$

$p = \gcd(5, \overset{15}{N}) = 5$

$q = \gcd(3, N) = 3$

↳ does not give any information.




```
%for exercise 4 MICRO-435

klength=2^3;
ilength=2^4;

elmk=zeros(klength,1);
sumk=zeros(klength,1);
total_sum_i=zeros(ilength,1);
amplitude=zeros(ilength,1);

for i=0:1:ilength-1
    for k=0:1:klength-1
        elmk(k+1,1)=exp(2*pi*1j/(2^4)*2*i*k);
        sumk(1,1)=elmk(1,1);

        if(k ~= 0)
            sumk(k+1,1)=elmk(k+1,1)+sumk(k,1);
        end
    end

    total_sum_i(i+1,1)=sumk(klength,1)*(1/sqrt(2^7));

    amplitude(i+1,1)=abs(total_sum_i(i+1,1))^2;
end

bar(0:1:15,amplitude);
```