ACCQ206

Lecturer: Alex B. Grilo
Lecture # 04 - Simon's algorithm, QFT and Shor's algorithm

Quantum Fourier transform

1. Show that QFT_N is unitary.

   Solution: We have that $QFT_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \dots & 1 & \dots & 1 \\ 1 & \omega & \dots & \omega^{j-1} & \dots & \omega^{N-1} \\ & & & \dots & & \\ 1 & \omega^{i-1} & \dots & \omega^{(i-1)(j-1)} & \dots & \omega^{i(N-1)} \\ & & & \dots & & \\ 1 & \omega^{N-1} & \dots & \omega^{(N-1)(j-1)} & \dots & \omega^{(N-1)^2} \end{pmatrix}$

   and

   $QFT_N^\dagger = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \dots & 1 & \dots & 1 \\ 1 & \omega^{-1} & \dots & \omega^{-j+1} & \dots & \omega^{-N+1} \\ & & & \dots & & \\ 1 & \omega^{-i+1} & \dots & \omega^{-(i-1)(j-1)} & \dots & \omega^{-i(N-1)} \\ & & & \dots & & \\ 1 & \omega^{-N-1} & \dots & \omega^{-(N-1)(j-1)} & \dots & \omega^{-(N-1)^2} \end{pmatrix}.$

   Let $A = QFT_N QFT_N^\dagger$.
   We have that

   $$A_{i,i} = \frac{1}{N} \sum_{j \in [N]} \omega^{(i-1)(j-1)} \omega^{-(j-1)(i-1)} = \frac{1}{N} \sum_{j \in [N]} \omega^0 = 1.$$

   Morefore, for $i \neq k$, we have that

   $$A_{i,k} = \frac{1}{N} \sum_{j \in [N]} \omega^{(i-1)(k-1)} \omega^{-(k-1)(j-1)} = \frac{1}{N} \sum_{j \in [N]} \omega^{(j-1)(i-k)} = \frac{1}{N} \sum_{j \in [N]} \omega^{(j-1)} = 0,$$

   where in the third equality we use the fact that for some fixed $i \neq k$, we are summing up all roots of unity, which is equal to 0.

2. In this exercise we will show how to compute QFT_N for $N = 2^n$ with a gateset composed of H, $SWAP$[1] and the controlled version of one-qubit gates of the form

   $$R_s = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^s} \end{pmatrix}.$$

   (a) Show that for every string $x \in \{0,1\}^n$, we have that $QFT_N|x\rangle$ is equal to

   $$\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i k/2}|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i k/2^2}|1\rangle\right)\right) \otimes \dots \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i k/2^n}|1\rangle\right)\right). \quad (1)$$

---

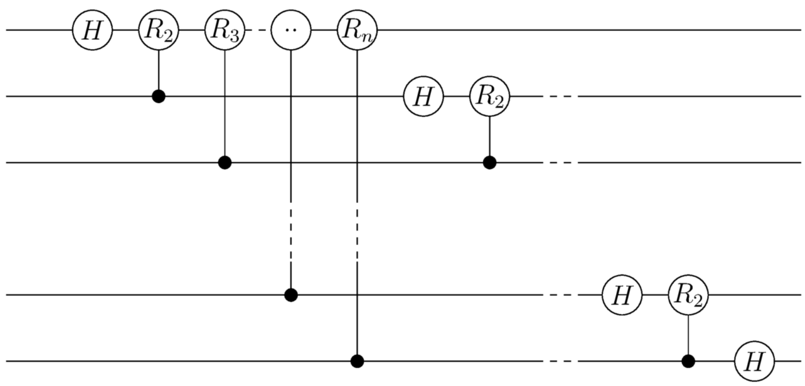
[1]Remember that $SWAP$ is the two-qubit gate such that $SWAP|a\rangle|b\rangle = |b\rangle|a\rangle$.

Solution:

$$\begin{aligned}
QFT_N|x\rangle &= \frac{1}{\sqrt{N}}\sum_{y\in N} e^{2\pi i xy/N}|y\rangle &(2)\\
&= \frac{1}{\sqrt{N}}\sum_{y\in N} e^{2\pi i(\sum_{k=1}^{n} y_k 2^{-k})x}|y\rangle &(3)\\
&= \frac{1}{\sqrt{N}}\sum_{y\in N}\prod_{k=1}^{n} e^{2\pi i y_k x/2^k}|y\rangle &(4)\\
&= Equation\ (1), &(5)
\end{aligned}$$

where in the second equality we denote y_k as the k-th bit of y, written in binary.

(b) What is the output of the following circuit on input $|x\rangle$. [2]



Solution: The first qubit of the output is

$$R_n^{x_n}...R_2^{x_2}H|x_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}e^{2\pi i x_2/4}...e^{2\pi i x_n/2^n}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i x/2^n}),$$

where we use the fact that $(-1)^{x_1} = e^{2\pi i x_1/2}$ and that $\sum_j x_j/2^j = x/2^n$.
Simiarly, we have that the j-th output qubit is

$$R_{n-j+1}^{x_{n-j+1}}...R_2^{x_2}H|x_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle+(-1)^{x_j}e^{2\pi i x_{j+1}/4}...e^{2\pi i x_n/2^{n-j+1}}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i x/2^{n-j+1}}|1\rangle),$$

where we use the fact that for $a = b \pmod c$, we have that $e^{2\pi i b/c} = e^{2\pi i a/c}$.

(c) What is the difference between the answer of Exercise 2b and Equation 1?
Solution: The qubits have an inverse order.

(d) Can you propose a quantum circuit to compute QFT_N?
Solution: We can apply the circuit of Exercise 2b and SWAP qubits i and $n-j+1$.

(e) **Pour aller plus loin...** Show that R_s can be approximated using H, R_1, R_2 and R_3.

[2] In this picture, the gates are described using circles instead of rectangles, but that is just a different notation.

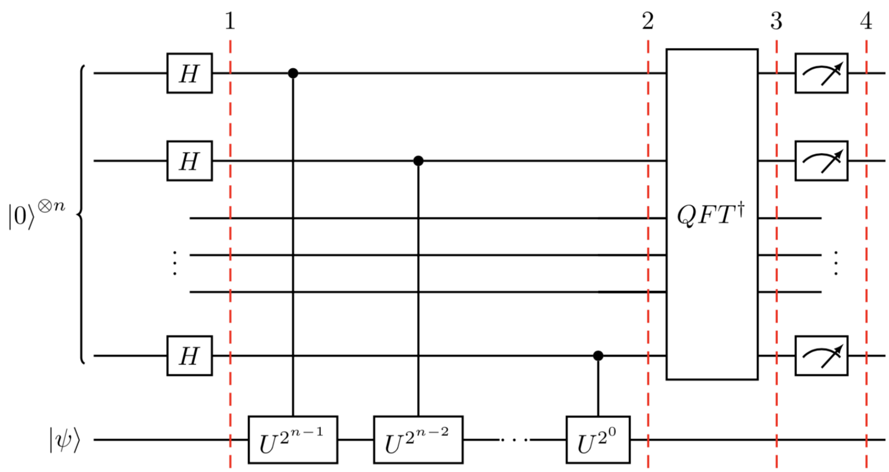
3. Let U be an m-qubit unitary and $|\psi\rangle$ is an m-qubit quantum state such that $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$ for some $\theta = [0, 1)$ (i.e. $|\psi\rangle$ is an eigenvector of U with eigenvalue $e^{2\pi i\theta}$). In this exercise we show that using QFT, we can estimate the eigenvalue $e^{i\theta}$ (or equivalently, that we can compute θ). For simplicity, we assume that θ can be computed with n bits of precision (meaning that $2^n\theta$ is an integer number).

   (a) Show that $U^j|\psi\rangle = e^{2\pi i\theta j}|\psi\rangle$.
   Solution: We show by induction. The basis case $j = 0$ is trivial.
   Let us assume then that $U^{j-1}|\psi\rangle = e^{2\pi i\theta(j-1)}|\psi\rangle$, and we will show that $U^j|\psi\rangle = e^{2\pi i\theta j}|\psi\rangle$. For that notice that

   $$U^j|\psi\rangle = U(U^{j-1}|\psi\rangle) = U(e^{2\pi i\theta(j-1)}|\psi\rangle) = e^{2\pi i\theta(j-1)}U|\psi\rangle = e^{2\pi i\theta j}|\psi\rangle,$$

   where in the second equality we use our induction hypothesis.

   (b) Compute the state of the following computation at phases 1,2,3 and 4.



   Solution:

   Phase 1: $\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|\psi\rangle$.

   Phase 2: Notice that for a fixed $|x\rangle$, the controlled unitaries of phase 2 implement the operation $|x\rangle|\psi\rangle \to |x\rangle U^x|\psi\rangle = e^{2\pi i\theta x}|x\rangle|\psi\rangle$. By linearity, we have that the state at the end of phase 2 is then

   $$\frac{1}{\sqrt{2^n}}\sum_x e^{2\pi i\theta x}|x\rangle|\psi\rangle = \left(\frac{1}{\sqrt{2^n}}\sum_x e^{2\pi i\theta x}|x\rangle\right) \otimes |\psi\rangle.$$

   Phase 3: Notice that $\frac{1}{\sqrt{2^n}}\sum_x e^{2\pi i\theta x}|x\rangle = QFT_{2^n}|2^n\theta\rangle$. Therefore

   $$(QFT^\dagger \otimes I)\left(\frac{1}{\sqrt{2^n}}\sum_x e^{2\pi i\theta x}|x\rangle\right) = (QFT^\dagger QFT|2^n\theta\rangle) \otimes |\psi\rangle = |2^n\theta\rangle|\psi\rangle.$$

Phase 4: By measuring the first register of the state of phase 3 gives us the value of $2^n\theta$, which allows us to compute the eigenvalue $e^{2\pi i\theta}$ which is the eigenvalue of U associated with the eigenvector $|\psi\rangle$.

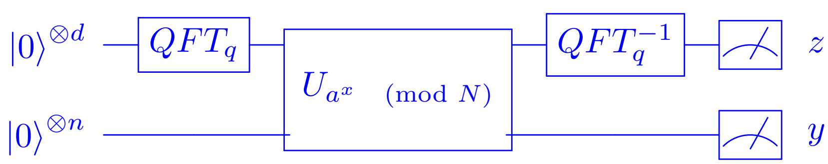
Shor's algorithm

4. Let us consider the function $f = 7^x \pmod{10}$.

   (a) What is the period of this function?
   Solution:
   - $7^1 \pmod{10} = 7$
   - $7^2 \pmod{10} = 9$
   - $7^3 \pmod{10} = 3$
   - $7^4 \pmod{10} = 1$
   - $7^5 \pmod{10} = 7$

   The period is 4.

   (b) Compute the state corresponding to each step of the period finding algorithm with $q = 128$. Give an example of measurement outcome ℓ that would allow you to compute the period (i.e. $\frac{\ell}{q} = \frac{k}{r}$ in its lowerst terms).
   Solution: Recall that the period finding algorithm is the following:



After the first step the state is

$$\frac{1}{8\sqrt{2}} \sum_{i=0}^{127} |i\rangle|0\rangle.$$

After the second step the state is

$$\begin{aligned}&\frac{1}{8\sqrt{2}} \sum_{i=0}^{127} |i\rangle|7^i \pmod{10}\rangle \\ &= \frac{1}{8\sqrt{2}} \left(\sum_{j=0}^{31} |4j\rangle|1\rangle + \sum_{j=0}^{31} |1+4j\rangle|7\rangle + \sum_{j=0}^{31} |2+4j\rangle|9\rangle + \sum_{j=0}^{31} |3+4j\rangle|3\rangle \right).\end{aligned}$$

After the third step the state is

$$\begin{aligned}&\frac{1}{4}\Big(\sum_{j=0}^{3} |32j\rangle|1\rangle + \sum_{j=0}^{3} e^{2\pi i(1+32j)/128}|1+32j\rangle|7\rangle \\ &+ \sum_{j=0}^{3} e^{2\pi i2(2+32j)/128}|2+32j\rangle|9\rangle + \sum_{j=0}^{3} e^{2\pi i3(3+32j)/128}|3+32j\rangle|3\rangle\Big).\end{aligned}$$

One example of measurement outcome that would allow us to compute the period is $\frac{32}{128}$ because it is equal to $\frac{1}{4}$ in its lowest terms.