Quantum Information and Computing
Lecture- 25 : Implementing QFT

Dipan Kumar Ghosh
Physics Department,
Indian Institute of Technology Powai, Mumbai 400076

August 14, 2016

1 Introduction

In the previous lecture we discussed the role of quantum Fourier transform (QFT) in determining the periodicity of a function. We found through an example that if we have an oracle to determine a periodic function which has as its input the linear combination of computational basis states in the first register and a null state in the second register, the oracle would compute the function for each of the basis states and output it into the second register. The two registers are therefore entangled. If after the oracle has output the function, we subject the first register through a Fourier transform. After this if we measure the first register, we would get a state in the second register which depends on the period of the function, i.e., the periodicity determines the non-vanishing states of the first register. We now ask the question as to whether a unitary operation exists which performs the aforesaid task.

2 Unitary Operator Determining Fourier Transform

How does one carry this out? In other words, is there a unitary operation, which acting on a given sate will create a new state whose expansion in terms of the basis has coefficients which are Fourier transforms of the coefficients in the expansion of the original state in the same basis?
Consider a state $\mid \psi\rangle = \sum_x \alpha_x \mid x\rangle$. we wish to find U such that

$$\mid \psi'\rangle = U \mid \psi\rangle = U \sum_x \alpha_x \mid x\rangle$$

$$= \sum_y \tilde{\alpha}_y \mid y\rangle$$

where

$$\tilde{\alpha}_y = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega^{xy} \alpha_y$$

The operator U clearly exists and is given by

$$U = \sum_{y,z=0}^{N-1} \frac{e^{2i\pi yz/N}}{\sqrt{N}} \mid y\rangle\langle z \mid$$

because,

$$\begin{aligned} U \mid \psi\rangle &= \sum_{y,z=0}^{N-1} \frac{e^{2i\pi yz/N}}{\sqrt{N}} \sum_{x=0}^{N} \alpha_{|} y\rangle\langle z \mid\mid x\rangle \\ &= \sum_{y,z=0}^{N-1} \frac{e^{2i\pi yz/N}}{\sqrt{N}} \alpha_z \mid y\rangle \\ &= \sum_{y=0}^{N-1} \tilde{\alpha}_y \mid y\rangle \end{aligned}$$

where

$$\tilde{\alpha}_y = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} e^{2i\pi yz/N} \alpha_z$$

Starting with the standard computational basis $\mid x\rangle$, we can now define a new basis

$$\mid \tilde{x}\rangle = U \mid x\rangle$$

which has the following property

$$\begin{aligned} \mid \langle \tilde{x} \mid y\rangle \mid^2 &= \langle y \mid \tilde{x}\rangle\langle \tilde{x} \mid y\rangle \\ &= \langle y \mid U \mid x\rangle\langle x \mid U^\dagger \mid y\rangle \\ &= \frac{\omega^{xy}}{\sqrt{N}} \cdot \frac{\omega^{-xy}}{\sqrt{N}} = \frac{1}{N} \end{aligned}$$

Thus, $\mid \tilde{x}\rangle$ is an equal superposition of all computational basis states as well. However, this is different from the state obtained by application of the Hadamard transform on a null vector as unlike in the case of Hadamard transformed state, the coefficients in this case all complex.

2.1 Implementation

Before constructing a circuit which implements QFT, it is instructive to consider simple case of $n = 1$ and $n = 2$.
Consider $n = 1$. Let $\mid x\rangle$ be a one qubit basis state. The Fourier transform is given by

$$\mid \tilde{x}\rangle = \frac{1}{\sqrt{2}} \sum_{y\in 0,1} e^{2i\pi xy/N} \mid y\rangle = \frac{1}{\sqrt{2}} \left(\mid 0\rangle + e^{2i\pi x/2} \mid 1\rangle \right)$$

Since $x/2$ can be written in a binary decimal formal as $0.x$, we have

$$\mid \tilde{x}\rangle = \frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2i\pi(0.x)} \mid 1\rangle\right)$$

Consider now QFT for $n = 2$. Let $\mid x\rangle = \mid x_1x_0\rangle$. We can write $x = 2x_1 + x_0 = x_1 \cdot 2^1 + x_0$. Further, in the binary fraction representation, we can write

$$0.x_1x_0 = x_1 \cdot 2^{-1} + x_0 2^{-2}$$

The QFT of $\mid x\rangle$ is a two qubit state

$$\mid \tilde{x}\rangle = \frac{1}{2}\sum_y e^{2\pi ixy/2^2} \mid y\rangle$$

Remember that xy is a normal product of two numbers x and y (and not bitwise product). Thus we have

$$\begin{aligned}
\mid \tilde{x}\rangle &= \frac{1}{2}\sum_{y_0,y_1} e^{2\pi ix(2y_1+y_0)/2^2} \mid y\rangle \\
&= \frac{1}{2}\sum_{y_1\in 0,1} e^{2\pi ixy_1/2} \mid y_1\rangle \otimes \sum_{y_0\in 0,1} e^{2\pi ixy_0/2^2} \mid y_0\rangle \\
&= \frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi ix/2} \mid 1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi ix/2^2} \mid 1\rangle\right)
\end{aligned}$$

Since $x = 2x_1 + x_0$, $\dfrac{x}{2} = x_1 + \dfrac{x_0}{2}$ $\dfrac{x}{2^2} = \dfrac{x_1}{2} + \dfrac{x_0}{2^2} = 0.x_1x_0$. This gives

$$\mid \tilde{x}\rangle = \frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi i(0.x_0)} \mid 1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi i(0.x_1x_0)} \mid 1\rangle\right)$$

where in the first term we have used $e^{2\pi ix_1=1}$.

One can easily generalize the above to $n-$ qubit case. Let $\mid j\rangle = \mid j_{n-1}j_{n-2}\ldots j_0\rangle$. We have $j = j_{n-1}2^{n-1} + \ldots + j_0 2^0$ and $0.j_{n-1} + \ldots + j_0 = j_{n-1}2^{-1} + j_{n-2}2^{-2} + \ldots + j_0 2^{-n}$. Using these, we can write,

$$\mid \tilde{j}\rangle = \frac{1}{2^{n/2}}\left(\mid 0\rangle + e^{2\pi i(0.j_0)} \mid 1\rangle\right)\left(\mid 0\rangle + e^{2\pi i(0.j_1j_0)} \mid 1\rangle\right)\ldots\otimes\left(\mid 0\rangle + e^{2\pi i(0.j_{n-1}j_{n-2})}\ldots j_0) \mid 1\rangle\right)$$

Note that each term in the above can be realized by a Hadamard transform followed by a rotation, the amount of rotation depends on the value of the other bits. Consider the $m+1$-th term on the rhs of the above product,

$$\mid 0\rangle + e^{2\pi i(0.j_mj_{m-1}\ldots j_0)} \mid 1\rangle$$

If the $m-$ th bit of j is zero, the term becomes

$$\mid 0\rangle + e^{2\pi i(0.0j_{m-1}\ldots j_0)} \mid 1\rangle = \mid 0\rangle + e^{2\pi i(j_{m-1}\ldots j_0)/2^{m+1}} \mid 1\rangle$$

On the other hand if the $m-$ th bit is 1, this becomes

$$\mid 0\rangle - e^{2\pi i(j_{m-1}\ldots j_0)/2^{m+1}} \mid 1\rangle$$

because $e^{2\pi i(0.j_m)} = e^{\pi i} = -1$. The amount of rotation is given by

$$2\pi(j_{m-1}\ldots j_0)/2^m$$

Thus the m-th term is given by

$$\mid 0\rangle + (-1)^{j_m} e^{2\pi i(j_{m-1}\ldots j_0)/2^{m+1}} \mid 1\rangle \tag{1}$$

Returning back to the case of $n = 2$, we had,

$$\mid \tilde{x}\rangle = \frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi i(0.x_1)} \mid 1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi i(0.x_1x_0)} \mid 1\rangle\right)$$

Since $0.x_1 = x_1/2$ and $0.x_1x_0 = \dfrac{x_1}{2} + \dfrac{x_0}{4}$, we get

$$\mid \tilde{x}\rangle = \frac{1}{\sqrt{2}}\left(\mid 0\rangle + (-1)^{x_0} \mid 1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(\mid 0\rangle + (-1)^{x_1} e^{\dfrac{2\pi i x_0}{4}} \mid 1\rangle\right)$$

The first term is the ordinary Hadamard transform since it gives $\mid 0\rangle \pm \mid 1\rangle$ depending on whether x_0 is 0 or 1. The second term is a little more complicated. This is a Hadamard transform followed by an amount $2\pi x_0/4$, i.e., only if $x_0 = 1$, there is a rotation of the state $\mid 1\rangle$ by $2\pi/4$. We define a **controlled** B_{jk} gate by

$$B_{jk} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^{k-j+1}} \end{pmatrix}$$

with $k > j$, which gives a rotation of the state $\mid 1\rangle$ only if the control bit is 1,

$$\begin{aligned} B_{jk} \mid x, y\rangle &= e^{i\theta_{jk}xy} \mid x, y\rangle \\ &= \exp[\frac{2\pi i}{2^{k-j+1}}xy] \mid x, y\rangle \end{aligned}$$

In the circuit, the first state will be used as a control bit while the second as the target bit. If $x = 0$, the action of the gate is identical to application of the identity. However, if $x = 1$, the phase acts on $\mid y\rangle$ giving

$$\exp(\frac{2\pi i}{2^{k-j+1}}xy) \mid x, y\rangle = \begin{cases} \mid y\rangle & \text{if } \ y = 0 \\ \exp[\dfrac{2\pi i}{2^{k-j+1}}] \mid y\rangle & \text{if } y = 1 \end{cases}$$

Returning to the case of $n = 2$,

$$\begin{aligned} \mid \tilde{x}\rangle &= \frac{1}{2}[\mid 0\rangle + (-1)^{x_0} \mid 1\rangle] \otimes [\mid 0\rangle + (-1)^{x_1} e^{2\pi i x_0/4} \\ &= \frac{1}{2}[\mid 0\rangle + (-1)^{x_0} \mid 1\rangle] \otimes B_{12}^0[\mid 0\rangle + (-1)^{x_1} \mid 1\rangle] \end{aligned}$$

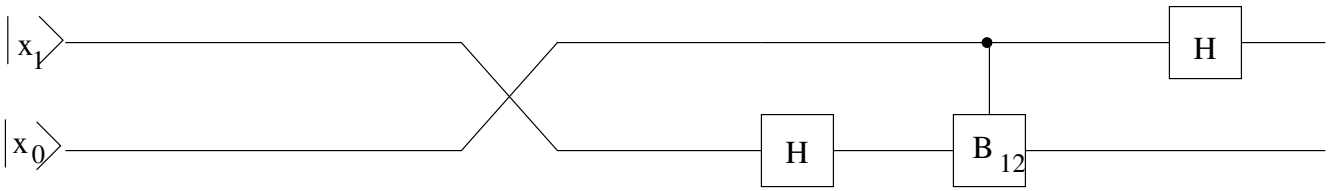

Figure 1: QFT for n=2

where B_{12}^0 means a rotation by $2\pi/(2^{2-1+1}) = 2\pi/4$ with x_0 as the control. The above state is entangled because the first term has $(-1)^{x_0}$ while the second has $(-1)^{x_1}$. Note that our input was $\mid x_1x_0\rangle$ while the order in which the result appears has a reverse order. We can write

$$\begin{aligned} \mid \tilde{x}\rangle &= \frac{1}{2}[U_H \mid x_0\rangle] \otimes B_{12}^0[U_H \mid x_1\rangle] \\ &= \frac{1}{2}(U_H \otimes I)B_{12}^0(I \otimes U_H) \mid x_0x_1\rangle \\ &= \frac{1}{2}(U_H \otimes I)B_{12}^0(I \otimes U_H)U_{SWAP} \mid x_1x_0\rangle \end{aligned}$$

Thus execution of Fourier transform requires swapping of the order of bits before application of the Hadamard and controlled B_{jk} gates.

Generalization of the above to $n-$ qubit gate is straightforward. In the next lecture we will first explain this with reference to three qubits and then suggest a generalization.