Quantum Information and Computing
Topic- 12: Quantum Fourier Transform

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

March 19, 2017

1 Introduction

It is well known that prime factorization, i.e., factorisation of a large composite number to its prime factors is computationally a hard problem requiring exponential time and memory. Shor's factorisation uses built in parallelism of a quantum computer to speed up this process so that the task can be achieved to a high degree of probability in a polynomial time. The execution of the algorithm requires implementation of a fast Fourier transform to determine period of a function using a quantum computer. We begin our discussion with an introduction to a few mathematical tools required for implementing Shor's factorisation algorithm. First, we introduce the concept of an integral transform of a function of a discrete variable. We are familiar with integral transforms, such as, Fourier transform and Laplace transforms of functions of continuous variables. The primary use of such transforms is to convert a complicated problem into a relatively simpler one. For instance, we could, using such technique, convert a differential equation for an unknown function f into an algebraic equation for the transform $\tilde{f}$ of the function f. Once we have solved for $\tilde{f}$, we can apply an inverse transform to get a solution for f itself.

2 Discrete Integral Transforms

In quantum information theory we deal with discrete quantities rather than continuous ones. Accordingly, we define discrete integral transforms (DIT). They are defined analogously to that of transforms of functions of continuous variables. If n belongs to the set of natural numbers $\mathbb{N}$ and S_n is a set of $N = 2^n$ integer $\{0, 1, 2, \ldots, N-1\}$, we define the kernel $K(x, y)$ to be a bivariate function (in general, complex) of discrete variables x and y ($x, y \in S_n$). The discrete integral transform of a function f of a discrete variable is

defined by

$$\tilde{f}(y) = \sum_{y=0}^{N-1} K(x,y) f(y) \tag{1}$$

Since x and y are discrete, one can think of this as a matrix equation with f (and $\tilde{f}$) being an $N \times 1$ column vector and $K(x,y)$ an $N \times N$ matrix.
If K is unitary, i.e. if $K^\dagger = K^{-1}$, an inverse transform also exists

$$f(x) = \sum_{y=0}^{N-1} K^\dagger(x,y) \tilde{f}(y) \tag{2}$$

Proof of (2) is obvious, as using (1), we can write the rhs of the above as follows:

$$\begin{aligned}
\sum_{y=0}^{N-1} K^\dagger(x,y)\tilde{f}(y) &= \sum_{y=0}^{N-1} K^\dagger(x,y) \sum_{z=0}^{N-1} K(y,z) f(z) \\
&= \sum_{z=0}^{N-1} \left(\sum_{y=0}^{N-1} K^\dagger(x,y) K(y,z) \right) f(z) \\
&= \sum_{z=0}^{N-1} \delta_{x,z} f(z) = f(x)
\end{aligned}$$

Till now we have restricted ourselves to a set of numbers. We can extend the formalism to define a unitary operator in the $n-$ qubit space $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$.
Let $\mid x\rangle = \mid x_{n-1}, \ldots, x_1, x_0\rangle$ be a basis vector in the $n-$ qubit space where $x_i \in 0, 1$. Using completeness, we have

$$\begin{aligned}
U \mid x\rangle &= \sum_{y=0}^{N-1} \mid y\rangle\langle y \mid U \mid x\rangle \\
&= \sum_{y=0}^{N-1} U(y,x) \mid y\rangle
\end{aligned} \tag{3}$$

The matrix element $U(y,x)$ is given by

$$U(y,x) = \langle y \mid U \mid x\rangle$$

Comparing (3) with (1) we see that if U is a unitary matrix such that

$$U \mid x\rangle = \sum_{y=0}^{N-1} K(x,y) \mid y\rangle$$

then we can say that U computes the discrete integral transform. Moreover, as the process is quantum in nature U can compute the DIT of functions of all the basis variables

parallel. This is because, if we define a state $\sum_{x=0}^{N-1} f(x) \mid x\rangle$, then the action of U on this superposition is as follows:

$$\begin{aligned} U\sum_{x=0}^{N-1} f(x) \mid x\rangle &= \sum_{x=0}^{N-1} f(x)U \mid x\rangle \\ &= \sum_{x=0}^{N-1} f(x) \sum_{y=0}^{N-1} K(y,x) \mid y\rangle \\ &= \sum_{y=0}^{N-1} [\sum_{x=0}^{N-1} K(y,x)f(x)] \mid y\rangle \\ &= \sum_{y=0}^{N-1} \tilde{f}(y) \mid y\rangle \\ &= \sum_{x=0}^{N-1} \tilde{f}(x) \mid x\rangle \end{aligned}$$

where $\tilde{f}(x)$ is the DIT of $f(x)$. This shows that U computes the Integral transform of all the 2^n basis states by a single computation. Thus what the unitary operator U does is to find the transform of the amplitudes of various components of a vector in a standard basis.

3 Quantum Fourier Transform

We will now consider a particularly important integral transform, viz., the quantum Fourier transform (QFT) in which the kernel $K(x,y)$ is defined to be

$$K(x,y) = \frac{1}{\sqrt{N}} e^{2i\pi xy/N} \equiv \frac{1}{\sqrt{N}} \omega_n^{xy} \tag{4}$$

where

$$\omega_n = e^{2i\pi/N}$$

is the $N-$th root of unity. Note that in the definition (4), x and y are usual numbers of the decimal system and is not to be confused with a bitwise product. Example of the kernel for $n = 1$ and $n = 2$ are as follows:

$$n = 1, \quad \text{i.e. } N = 2 \quad (x, y \in 0, 1), \quad \omega_1 = -1 \quad K = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Note that this is just the Hadamard transform defined in earlier lectures. Thus QFT in $\mathbb{C}^2$ implements Hadamard transform

$$n = 2, \quad \text{i.e. } N = 4 \quad (x, y \in 0, 1, 2, 3), \quad \omega_1 = e^{\pi i/2} = i$$

$$K = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^8 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Thus we have

$$\tilde{f}(x) = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2i\pi xy/N} f(y) \tag{5}$$

$$f(y) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2i\pi xy/N} \tilde{f}(x) \tag{6}$$

The process of finding QFT is to find the transform of the components of a vector in a basis. note that K is unitary because

$$\begin{aligned} \langle x \mid KK^\dagger \mid y\rangle &= \sum_{z=0}^{N-1} \langle x \mid K \mid z\rangle\langle z \mid K^\dagger \mid y\rangle \\ &= \sum_{z=0}^{N-1} K(x,z)K^\dagger(z,y) \\ &= \frac{1}{N}\sum_{z=0}^{N-1} e^{2i\pi xz/N} e^{-2i\pi zy/N} \\ &= \frac{1}{N}\sum_{z=0}^{N-1} e^{2\pi iz(x-y)/N} \end{aligned}$$

If $x \neq y$, the above is a finite geometric series of N terms having a sum

$$\frac{1}{N}\frac{e^{2\pi iz(x-y)} - 1}{e^{2\pi iz(x-y)/N} - 1}$$

whose numerator is zero as $e^{2\pi i} = 1$. If $x = y$, however, each term of the series is 1 and there are N terms in the series. so that we have $\langle x \mid KK^\dagger \mid y\rangle = \delta_{x,y}$.

Example : Find the QFT of $\mid \psi\rangle = \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} \cos\left(\frac{2\pi x}{N}\right) \mid x\rangle$, where $N = 2^n$.

Solution:

The QFT is given by

$$\begin{aligned} QFT \mid \psi\rangle &= \sqrt{\frac{2}{N}}\frac{1}{\sqrt{N}}\frac{1}{\sum_y}\sum_x e^{-2\pi ixy/N}\cos(2\pi x/N) \mid y\rangle \\ &= \frac{1}{\sqrt{2}N}\sum_x\sum_y \left[e^{-2\pi i(y+1)x/N} + e^{-2\pi i(y-1)x/N}\right] \mid y\rangle \end{aligned}$$

We perform the sum over x by the formula for the finite geometric series,

$$\sum_x \left[e^{-2\pi i(y+1)x/N} + e^{-2\pi i(y-1)x/N}\right] = \frac{e^{-2\pi i(y+1)} - 1}{e^{-2\pi i(y+1)/N} - 1} + \frac{e^{-2\pi i(y+1)} - 1}{e^{-2\pi i(y+1)/N} - 1}$$
$$= N(\delta_{x,1} + \delta_{x,N-1})$$

where we have used the fact that the numerators of both the terms are zero but the denominator is not, except when the exponential in the denominator becomes 1, i.e. when $\frac{y+1}{N} = 1$, i.e. $y = N-1$ in the first term and $\frac{y-1}{N} = 1$, i.e. $y = N+1 \equiv 1$ in the second term. When this happens, going back to the original sum, we find each term is 1 and the sum becomes N. Hence

$$QFT \mid \psi\rangle = \frac{1}{\sqrt{2}}\left[\mid 1\rangle + \mid N-1\rangle\right]$$

4 Period Finding:

We will illustrate the process of period finding for a three qubit input. In the Register 1, we have a linear combination of the standard basis, obtained by putting a three qubit initial state 000. Thus

$$\mid Reg_1\rangle = \frac{1}{\sqrt{8}}(\mid 000\rangle + \mid 001\rangle + \ldots + \mid 111\rangle) = \frac{1}{\sqrt{8}}(\mid 1\rangle + \mid 2\rangle + \ldots \mid 7\rangle)$$

The second register contains the state $\mid 000\rangle$. We pass the two registers through oracle which calculate the function $f(x)$ corresponding to the input x in the first register and get a state $\mid \psi\rangle$ as the output

$$\mid \psi\rangle = U_f \frac{1}{\sqrt{8}} \sum_x \mid x\rangle \mid 0\rangle = \frac{1}{\sqrt{8}} \sum_x \mid x, f(x)\rangle$$
$$= \frac{1}{\sqrt{8}}\left[\mid 0, f(0)\rangle + \mid 1, f(1)\rangle + \ldots + \mid 7, f(7)\rangle\right]$$

Thus the coefficient of each vector $\mid x\rangle \mid f(x)\rangle$ is $1/\sqrt{8}$ but it is zero for $\mid y\rangle \mid f(x)\rangle$ with $y \neq x$. We now apply QFT on the first register, leaving the second register as it is

$$\mid \psi'\rangle = U_{QFT} \mid \psi\rangle = \frac{1}{8} \sum_{x,y} e^{-2\pi i xy/8} \mid y, f(x)\rangle$$
$$= \frac{1}{8}\left[\mid 0\rangle \left(\mid f(0)\rangle + \mid f(1)\rangle + \ldots + \mid f(7)\rangle\right)\right]$$
$$+ \frac{1}{8}\left[\mid 1\rangle \left(\mid f(0)\rangle + e^{-2\pi i/8} \mid f(1)\rangle + \ldots + e^{-2\pi i 7/8} \mid f(7)\rangle\right)\right]$$
$$+ \ldots$$
$$+ \frac{1}{8}\left[\mid 1\rangle \left(\mid f(0)\rangle + e^{-14\pi i/8} \mid f(1)\rangle + \ldots + e^{-14\cdot\pi i 7/8} \mid f(7)\rangle\right)\right]$$

There are 64 terms in the above expression. Suppose $f(x)$ is periodic with $f(x+P) = f(x)$. In particular, suppose $P = 2$, i.e., let

$$f(0) = f(2) = f(4) = f(6) = a$$

and

$$f(1) = f(3) = f(5) = f(7) = b$$

with $a \neq b$. We can then rearrange the above expression as follows:

$$\begin{aligned}
\mid \psi' \rangle = U_{QFT} \mid \psi \rangle &= \frac{1}{8} \sum_{x,y} e^{-2\pi i x y/8} \mid y, f(x) \rangle \\
&= \frac{1}{8} \left[\mid 0 \rangle (4 \mid a \rangle + \mid b \rangle) \right] \\
&+ \frac{1}{8} \left[\mid 1 \rangle \left(\mid a \rangle \left(1 + e^{-2\cdot 2\pi i/8} + e^{-4\cdot 2\pi i/8} + e^{-6\cdot 2\pi i/8} \right) + \mid b \rangle \left(e^{-1\cdot 2\pi i/8} + e^{-3\cdot 2\pi i/8} + e^{-5\cdot 2\pi i/8} + e^{-7\cdot 2\pi i/8} \right) \right) \right] \\
&+ \ldots \\
&+ \frac{1}{8} \left[\mid 7 \rangle \left(\mid a \rangle \left(1 + e^{-14\cdot 2\pi i/8} + e^{-28\cdot 2\pi i/8} + e^{-42\cdot 2\pi i/8} \right) + \mid b \rangle \left(e^{-7\cdot 2\pi i/8} + e^{-21\cdot 2\pi i/8} + e^{-35\cdot 2\pi i/8} + e^{-49\cdot 2\pi i/8} \right.\right.\right.
\end{aligned}$$

Consider the coefficients of, say, state $\mid 1 \rangle$. We have for the term proportional to $\mid a \rangle$

$$\begin{aligned}
1 + e^{-1\cdot 2\cdot 2\pi i/8} + e^{-1\cdot 4\cdot 2\pi i/8} + e^{-1\cdot 6\cdot 2\pi i/8} \\
= 1 + e^{-\pi i/2} + e^{-\pi i} + e^{-3\pi i/2} \\
= 1 + (-i) + (-1) + (+i) = 0
\end{aligned}$$

In a similar way, one can show that the only other non-zero term (apart from the coefficient of is the $\mid 0 \rangle$ term is the term with the state $\mid 4 \rangle$, for which, the term proportional to $\mid a \rangle$ is

$$\begin{aligned}
1 + e^{-4\cdot 2\cdot 2\cdot 2\pi i/8} + e^{-4\cdot 4\cdot 2\pi i/8} + e^{-4\cdot 6\cdot 2\pi i/8} \\
= 1 + e^{-2\pi i} + e^{-4\pi i} + e^{-6\pi i} = 4
\end{aligned}$$

The state $\mid \psi' \rangle$ works out to

$$\mid \psi' \rangle = \frac{1}{2} \left[\mid 0, a \rangle + \mid 0, b \rangle + \mid 4, a \rangle + \mid 4, b \rangle \right]$$

Thus when we measure the register 1, we would get either 0 or 4 if the periodicity is 2. Periodicity determines the possible result of measurement of the first register.

5 Unitary Operator for QFT

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

$$\begin{aligned} \mid \psi'\rangle = U \mid \psi\rangle &= U \sum_x \alpha_x \mid x\rangle \\ &= \sum_y \tilde{\alpha}_y \mid y\rangle \end{aligned}$$

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,

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

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.

5.1 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 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

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

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

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

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

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

where in the first term we have used $e^{2\pi i x_1 = 1}$.

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,

$$\mid \tilde{j}\rangle = \frac{1}{2^{n/2}}\left(\mid 0\rangle + e^{2\pi i(0.j_0)} \mid 1\rangle\right)\left(\mid 0\rangle + e^{2\pi i(0.j_1 j_0)} \mid 1\rangle\right)\ldots\otimes\left(\mid 0\rangle + e^{2\pi i(0.j_{n-1}j_{n-2})}\ldots j_0)\mid 1\rangle\right)$$

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-th term on the rhs of the above product,

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

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

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

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

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

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

$$\mid 0\rangle + (-1)^{j_m} e^{2\pi i(j_{m-1}\ldots j_0)/2^m} \mid 1\rangle \tag{7}$$

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

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

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

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

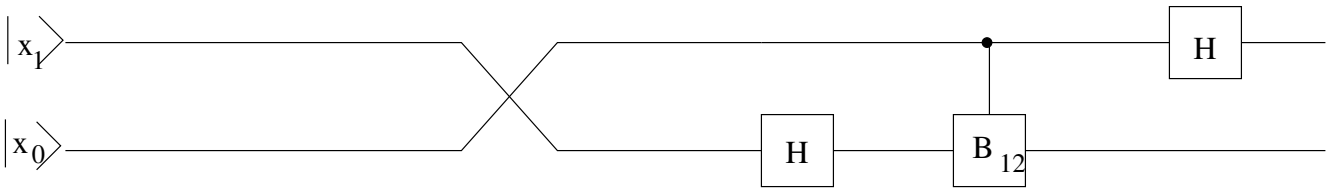

Figure 1: QFT for n=2

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

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

Returning to the case of $n = 2$,

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

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 $\mid x_1 x_0\rangle$ while the order in which the result appears has a reverse order. We can write

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

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

6 QFT for $n = 3$ qubits

We could directly discuss generalization to n qubits which though straightforward is clumsy. Instead, we will take the case of three qubits first which will suggest the way to

generalize the procedure to n qubits by observing a pattern which emerges from discussion of two and three qubits.
Recalling what we did in the last lecture, the QFT for n=2 case is given by the expression

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

We can see that the expression is obtained by applying a Hadamard transform on the second qubit followed by a Hadamard transform on the first qubit along with a controlled phase rotation. The phase rotation is controlled because a rotation is there only if $x_0 = 1$. The point to note in this process is the following. We cannot change the value of the second qubit before we use its value for the purpose of controlling the operations on the first qubit. This is achieved by interchanging x_1 and x_0 and then applying the Hadamard gate. Thus execution of Fourier transform requires swapping of the order of bits before application of the Hadamard and controlled B_{jk} gates.

The QFT for $\mid x\rangle = \mid x_2 x_1 x_0\rangle$ is given by

$$\begin{aligned}
\mid \tilde{x}\rangle &= \frac{1}{\sqrt{8}} \sum_{y_2,y_1,y_0=0}^{1} e^{2\pi i x(4y_2+2y_1+y_0)/8} \mid y_2 y_1 y_0\rangle \\
&= \frac{1}{\sqrt{2}} \sum_{y_2=0}^{1} e^{2\pi i x(4y_2/8)} \mid y_2\rangle \otimes \frac{1}{\sqrt{2}} \sum_{y_1=0}^{1} e^{2\pi i x(2y_1/8)} \mid y_1\rangle \otimes \frac{1}{\sqrt{2}} \sum_{y_0=0}^{1} e^{2\pi i x(y_0/8)} \mid y_0\rangle
\end{aligned}$$

Consider the first term in the product and perform the sum over the two values that y_2 takes

$$\begin{aligned}
\frac{1}{\sqrt{2}} \sum_{y_2=0}^{1} e^{2\pi i x(4y_2/8)} \mid y_2\rangle &= \frac{1}{\sqrt{2}}\left[\mid 0\rangle + e^{2\pi i x/2} \mid 1\rangle\right] \\
&= \frac{1}{\sqrt{2}}\left[\mid 0\rangle + e^{\pi i(4x_2+2x_1+x_0)} \mid 1\rangle\right]
\end{aligned}$$

In the last line we have expanded x as $4x_2 + 2x_1 + x_0$. It may be observed that since x_2, x_1 and x_0 take values 0 and 1, the factor in front of the state $\mid 1\rangle$ due tp x_2 and x_1 is 1 irrespective of the value that these take. However, the multiplying factor is $+1$ for $x_0 = 0$ and -1 for $x_0 = 1$, i.e. the factor multiplying $\mid 1\rangle$ is $(-1)^{x_0}$. This term is simply implemented by a Hadamard transform of the first qubit. We may similarly simplify the second and the third terms in the product as follows. The second term is

$$\begin{aligned}
\frac{1}{\sqrt{2}} \sum_{y_1=0}^{1} e^{2\pi i x(2y_1/8)} \mid y_2\rangle &= \frac{1}{\sqrt{2}}\left[\mid 0\rangle + e^{2\pi i x/4} \mid 1\rangle\right] \\
&= \frac{1}{\sqrt{2}}\left[\mid 0\rangle + e^{\pi i(2x_2+x_1+x_0/2)} \mid 1\rangle\right]
\end{aligned}$$

Once again, the factor multiplying $\mid 1\rangle$ depends on the value of x_1 and x_0 because the factor contributed by x_2 is 1 irrespective of the value taken by x_2. The second term is thus given by

$$\frac{1}{\sqrt{2}}\left[\mid 0\rangle + (-1)^{x_1} e^{2\pi i x_0/4} \mid 1\rangle\right]$$

Looking at the above, clearly, the way to implement is to have a Hadamard transform along with a selective phase rotation by an amount $2\pi x_0/4$. The rotation is selective in the sense that the rotation is conditional upon tx_0 being equal to 1. This is implemented by a controlled B_{jk} gate with x_0 as the control. The phase of this gate is given by $2\pi/(2^{k-j+1})$. Thus the required gate for this qubit is $B_{01}^{x_0}$.
Coming to the third term in the product, one can do a similar expansion and show this term to be given by

$$\frac{1}{\sqrt{2}}\left[\mid 0\rangle + e^{2\pi i(4x_2+2x_1+x_0)/8} \mid 1\rangle\right] = \frac{1}{\sqrt{2}}\left[\mid 0\rangle + (-1)^{x_2} e^{2\pi i x_1/4} e^{2\pi i x_0/8} \mid 1\rangle\right]$$

What we require here is a Hadamard, a controlled phase rotation using x_1 as control and a phase rotation of $2\pi x_1.4$, i.e. a $B_{12}^{x_1}$ gate, followed by another controlled phase rotation $B_{12}^{x_0}$.
Putting the three terms together, the result is

$$\frac{1}{\sqrt{2}}\left[\mid 0\rangle + (-1)^{x_2} \mid 1\rangle\right] \frac{1}{\sqrt{2}}\left[B_{01}^{x_0}(\mid 0\rangle + (-1)^{x_1} \mid 1\rangle)\right] \otimes \frac{1}{\sqrt{2}}\left[B_{01}^{x_0} B_{12}^{x_1}(\mid 0\rangle + (-1)^{x_2} \mid 1\rangle\right]$$

The sequence of operation may be seen to be as follows : (i) A Hadamard gate on the *third* qubit. This is important to note as if we apply the Hadamard now, it will alter the third qubit which then cannot be used with its original value as the control. (ii) A Hadamard on the second qubit and a controlled $B_{01}^{x_0}$ and (ii) a Hadamard on the first qubit along with two controlled gates $B_{02}^{x_0} B_{12}^{x_1}$.
What it tells us is that we need to apply the gates in such a manner that the control bits for the B_{jk} gates are not changed before such gates are applied. In 3 qubit case it is achieved by interchanging the first and the third qubits.

Generalization of the above to $n-$ qubit gate is straightforward 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,

$$\mid \tilde{j}\rangle = \frac{1}{2^{n/2}}\left(\mid 0\rangle + e^{2\pi i(0.j_0)} \mid 1\rangle\right)\left(\mid 0\rangle + e^{2\pi i(0.j_1 j_0)} \mid 1\rangle\right) \ldots \otimes \left(\mid 0\rangle + e^{2\pi i(0.j_{n-1} j_{n-2})} \ldots j_0) \mid 1\rangle\right)$$

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-th term on the rhs of the above product,

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

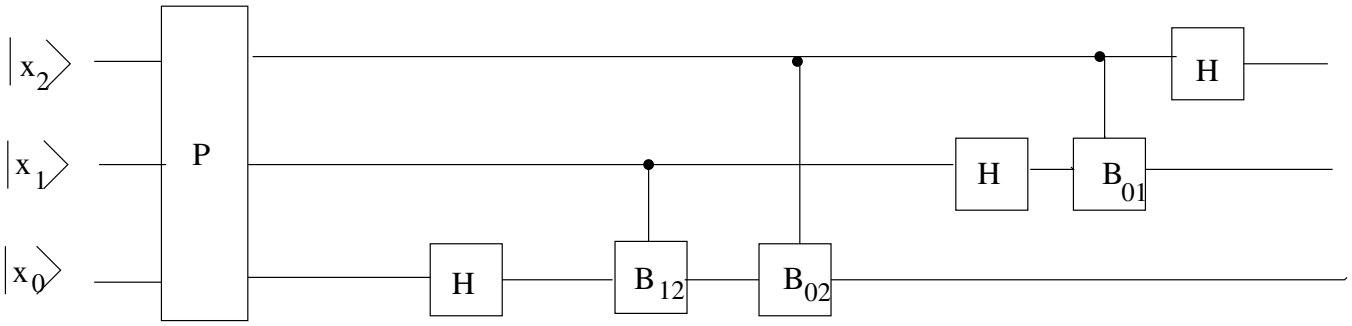

Figure 2: QFT for n=3. Here P represents a permutation which reverses the order of the lines

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

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

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

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

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

$$\mid 0\rangle + (-1)^{j_m} e^{2\pi i(j_{m-1}\ldots j_0)/2^m} \mid 1\rangle \tag{8}$$

that we had shown that in the m-th term (8) in the general expression was given by

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

The phase term can be written as

$$\exp(2\pi i j_{m-1} 2^{m-1}/2^m) \exp(2\pi i j_{m-2} 2^{m-2}/2^m) \ldots \exp(2\pi i j_0 2^0/2^m)$$

Thus a sequence of phase gates act on the state $\mid 1\rangle$ depending on the value of $j_0, j_1, \ldots j_{m-1}$. The phase due to the k-th bit is $\theta = 2\pi/(2^{m-k+1})$. Thus the circuit for $n = 3$ would look as in Figure 2.