Quantum Information and Computing
Lecture- 23 :Quantum Fourier Transform

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

August 14, 2016

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 $\langle x \mid KK^\dagger \mid y\rangle = \delta_{x,y}$.