Quantum Information and Computing Lecture- 24 :Period Finding and QFT

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

August 14, 2016

1 Introduction

In the last lecture we introduced the concept of Discrete Integral Transforms (DIT) and extended it to the case of discrete Fourier transform. We defined DIT of a function $f(x)$ of a discrete variable $x \in S_n = \{0, 1, \ldots, N-1\}$ by

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

where $K(y,x)$ is the Kernel associated with this transform, which, in general is a complex function of x and y. For the case where K is invertible (in our specific case, where K is unitary), we can define an inverse integral transform by

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

We generalized this to the case of a set of basis by recalling that a unitary operator U, acting on a basis state $\mid x\rangle$ gives a linear combination of basis states $U \mid x\rangle = \sum_y U(x,y) \mid y\rangle$, so that if the matrix elements $U(x,y)$ are identified as a kernel, we may consider the transformation to compute discrete integral transform of a basis in a similar way. The advantage of this is that DIT of all the members of the basis may be computed in a single operation because of parallelism. The Fourier transform was defined by choosing the kernel of the transform to be given by

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

where $\omega_n = e^{2\pi i/N}$ is the n-th root of unity.

In this lecture, we will discuss the quantum Fourier transform (QFT) a little more in detail and discuss its role in finding period of a function, the latter being useful in Shor's factorization algorithm.

2 Period Finding:

The period of a discrete function is defined analogously to that of a periodic continuous function such as a sine or a cosine function. Here the period P is defined as $f(x+P) = f(x)$, where x and P are both discrete, i.e the value of the function repeats after a discrete interval P, known as the period of the function. As with all quantum algorithms, we have with us an oracle which can compute this periodic function and output it to the target register, which is initialized to null.
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

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

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

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

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:

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

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

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

In a similar way, we can compute the state of the first register multiplying the state $\mid b \rangle$ in the second register and find that here too the non-vanishing terms are those for which the first register is in a state which is $\mid 0 \rangle$ or the state $\mid 4 \rangle$. The coefficient of the former has been shown in Eq. (1) to be 4. The coefficient associated with the state $\mid 4, b \rangle$ is seen to be

$$
\begin{aligned}
e^{-4 \cdot 1 \cdot 2 \cdot 2\pi i/8} &+ e^{-4 \cdot 3 \cdot 2\pi i/8} + e^{-4 \cdot 5 \cdot 2\pi i/8} + e^{-4 \cdot 7 \cdot 2\pi/8} \\
&= e^{-\pi i} + e^{-3\pi i} + e^{-5\pi i} + e^{-7\pi i} = -4
\end{aligned}
$$

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

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

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.