CS 880: Quantum Information Processing 9/23/2010

Lecture 9: Phase Estimation

Instructor: Dieter van Melkebeek Scribe: Hesam Dashti

Last lecture we reviewed the classical setting of the Fourier Transform over the reals. In this class we discuss the Fourier Transform over finite Abelian groups, and show how to compute it efficiently in the Quantum setting. At the end of this lecture, we start introducing Phase Estimation as an application of the Quantum Fourier Transform.

1 Fourier Transform over Finite Abelian Groups

For a general group G, the Fourier Transform is an orthonormal basis transformation from the standard basis of delta functions δ_g, $g \in G$, for the space of functions $f : G \to \mathbb{C}$ such that convolutions are transformed into pointwise products. Such a transformation exists for any finite group, but the construction is significantly simpler when the group is Abelian. In that case the new orthonormal basis is formed by the normalized characters of the group. A character of G is a homomorphism from G to the group of complex numbers under multiplication, i.e., a function $\chi : G \to \mathbb{C}$ such that for all $a, b \in G$, $\chi(ab) = \chi(a).\chi(b)$.

Let us recall the two facts about the characters from the previous lecture:
Facts: For any two distinct characters χ, χ' and any $g \in G$, the following holds:

1. $|\chi(g)| = 1$; this means that range of the χ function lies on the unit circle in the complex plane.

2. χ and χ' are perpendicular to each other with respect to the inner product

$$(\chi, \chi') = \sum_{g \in G} \overline{\chi(g)} \chi'(g),$$

   i.e., $(\chi, \chi') = 0$.

Recall that orthogonality of nonzero vectors implies linear independence, and that the dimension of the space of functions from G to $\mathbb{C}$ is $|G|$. Thus, if we can find $|G|$ distinct characters, then they form a basis for that space. By Fact 2, the basis is orthogonal. By Fact 1, $(\chi, \chi) = |G|$, so in order to have an orthnormal basis we need to normalize the characters and use the functions $\frac{1}{\sqrt{G}}\chi$. If we then index the characters as χ_y where y ranges over G, every function $f : G \to \mathbb{C}$ can be written as a linear combination of the normalized characters $\frac{1}{\sqrt{G}}\chi_y$, or equivalently, of the normalized characters $\frac{1}{\sqrt{G}}\overline{\chi_y}$:

$$f(x) = \frac{1}{\sqrt{G}} \sum_{y \in G} \hat{f}(x) \overline{\chi_y(x)}.$$

By taking the inner product with $\bar{\chi}_{y*}$ on both side and using orthonormality, we find the following expression for $\hat{f}$:

$$\hat{f}(y*) = \frac{1}{\sqrt{|G|}} \sum_{x \in G} f(x) \chi_{y*}(x).$$

We wanted our new basis functions to have two properties: they should be orthonormal (as we showed) and the transformation should map convolutions to point-wise products. The new basis functions have this property and we leave the proof as an exercise.

Exercise 1. *For* $(f * g)(x) = \sum_{y \in G} f(y) g(x.y^{-1})$ *show that* $\widehat{f * g}(y) = \sqrt{|G|}\hat{f}(y).\hat{g}(y)$

Next, we show that for Abelian finite groups G, the number of distinct characteres is indeed equal to $|G|$, and we find all the characters.

First, let us start with a very simple group: the cyclic group over N elements $G = \mathbb{Z}_N, +$. In this case, $|G| = N$, so we need to find N characters. Since $\mathbb{Z}_N, +$ is generated by the element 1, each character of $\mathbb{Z}_N, +$ is fully determined by its value at 1: $\chi(x) = \chi(1)^x$. Moreover, the value $\chi(1)$ could be any $z \in \mathbb{C}$ that satisfies $z^N = 1$, i.e., any point on the regular N-gon inscribed in the unit circle and containing 1 (see Figure 1).

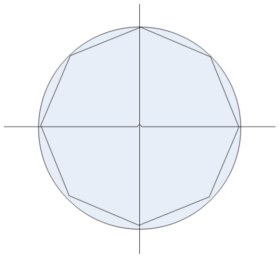


Figure 1: Choices for $\chi(1)$ for $G = \mathbb{Z}_8, +$.

Since these points are of the form $e^{2\pi i \frac{y}{N}}$ for $y \in \mathbb{Z}_N$, we set $\chi_y(1) = e^{2\pi i \frac{y}{N}}$. This generates the N distinct characters

$$\chi_y(x) = e^{\frac{2\pi i y x}{N}}.$$

which we need for the cyclic group $\mathbb{Z}_N, +$.

Now consider the case of a group G that is the direct product of a finite number of cyclic groups:

$$G = \oplus_{j=1}^{k} \mathbb{Z}_{m_j}, +.$$

Every element of $x \in G$ can be written as a k-tuple $x = (x_1, x_2, \ldots, x_k)$ where $x_j \in \mathbb{Z}_{m_j}$, and $|G| = \prod_{j=1}^{k} m_j$. In order to find characters of this group, we can pick a character from each of the constituent groups $\mathbb{Z}_{m_j}, +$ and multiply them to get a single character of G. For example, we can pick $(\chi_{y_1}(x_1), \chi_{y_1}(x_2), \ldots, \chi_{y_k}(x_k))$ and obtain

$$\prod_{j=1}^{k} \chi_{y_j}(x_j) = e^{2\pi i (\frac{x_1 \cdot y_1}{m_1} + \frac{x_2 \cdot y_2}{m_2} + \ldots + \frac{x_k \cdot y_k}{m_k})}.$$

For different choices of $(y_1, \ldots, y_k)$ the product gives us different characters of G. As the number of distinct choices equals $\prod_{j=1}^{k} m_j = |G|$, we obtained all characters of G this way.

Since every finite Abelian group is isomorphic to the direct product of cyclic groups, the latter case is the general one.

2 Quantum Fourier Transform

By viewing a base state $|x\rangle$ as the delta function δ_x for $x \in \{0,1\}^n$, we define the Quantum Fourier transform as mapping $|x\rangle$ onto the Fourier expansion of δ_x:

$$F : |x\rangle \to \sum_y \hat{\delta}_x(y) \, |y\rangle \, .$$

By linearity, if we apply F to a superposition $|\Psi\rangle = \sum \alpha(x) \, |x\rangle$ we get:

$$F \, |\Psi\rangle = \sum_y \hat{\alpha}(y) \, |y\rangle \, .$$

For the group $G = \mathbb{Z}_N, +$ this gives

$$F : |x\rangle \to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} \, |y\rangle \, .$$

2.1 Computing Fourier Transform over $\mathbb{Z}_N$ for $N = 2^n$

Now, we see how we can compute the Fourier Transform in the Quantum Setting for the special case of $\mathbb{Z}_N, +$ where $N = 2^n$ is a power of 2.

Let us start by considering the time complexity of computing the Fourier Transform in the Classical Setting and the Quantum Setting.

Classical Setting :
The trivial algorithm takes $O(N^2)$ operations. The Fast Fourier Transform takes $O(Nn)$ operations.

Quantum Setting :

1. A simple algorithm that we will develop, takes $O(n^2)$ operations.
2. A better algorithm takes $O(n(\log(n))^2 \log\log(n))$ operations.
3. An approximate algorithm with an error at most ϵ takes $O(n \log(\frac{n}{\epsilon}))$ operations.

The Simple Quantum Algorithm in time $O(n^2)$:
Recall that we can represent the Quantum Fourier Transform by

$$F \, |x\rangle = \frac{1}{\sqrt{N}} \sum e^{\frac{2\pi i x . y}{N}} \, |y\rangle \, . \tag{1}$$

Let us start by considering the binary representations $x = x_1 x_2 \ldots x_n$ and $y = y_1 y_2 \ldots y_n$, where $x_j, y_j \in \{0,1\}$. Note that we can write y as $y = \sum_{j=1}^n y_j 2^{n-j}$ and plug it into (1). We can rewrite the exponential function in the amplitude as a product

$$e^{\frac{2\pi i x y}{N}} = \prod_{j=1}^{n} e^{\frac{2\pi i x \cdot y_j \cdot 2^{n-j}}{2^n}} = \prod_{j=1}^{n} e^{2\pi i (\cdot x_{n-j+1} \ldots x_n) y_j} ,$$

where the latter step follows because $\frac{x 2^{n-j}}{2^n} = x_1 x_2 \ldots x_{n-j} \cdot x_{n-j+1} \ldots x_n$ and $e^{2\pi i . (Integer)} = 1$.

Using this equation we can write $F\left|x\right\rangle$ as the tensor product $F\left|x\right\rangle = \otimes_{j=1}^{n}\left|y_j\right\rangle$, where

$$\left|y_j\right\rangle = \frac{\left|0\right\rangle + e^{2\pi i(\cdot x_{n-j+1}\ldots x_n)}\left|1\right\rangle}{\sqrt{2}}.$$

Let us start to compute the first qubit of the output and see what is the value of $\left|y_1\right\rangle$:

$$\left|y_1\right\rangle = \frac{\left|0\right\rangle + e^{2\pi i x_n}\left|1\right\rangle}{\sqrt{2}}.$$

If x_n is zero we get $\frac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}}$ and in another case we get $\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}$. In fact, this is the Hadamard transform on $\left|x_n\right\rangle$, so

$$\left|y_1\right\rangle = H\left|x_n\right\rangle.$$

Now, let us consider the second qubit

$$\left|y_2\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + e^{2\pi i(\cdot x_{n-1}x_n)}\left|1\right\rangle),$$

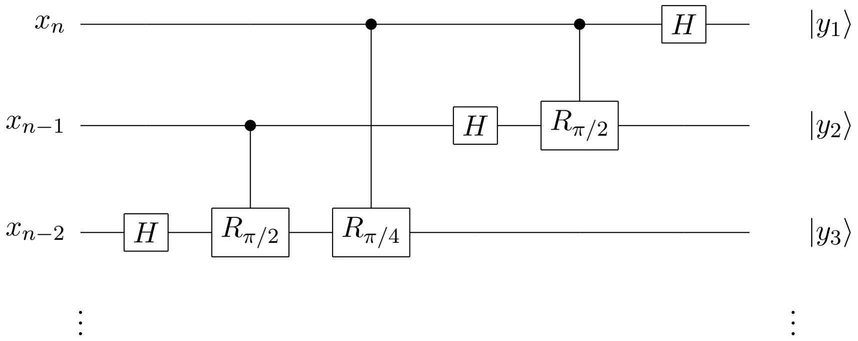
The Hadamard transform on $\left|x_{n-1}\right\rangle$ gives us

$$H\left|x_{n-1}\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + e^{2\pi i(\cdot x_{n-1})}\left|1\right\rangle).$$

When x_n is zero, $H\left|x_{n-1}\right\rangle$ is the output. But if x_n is 1 we need to apply the rotation operation $R_{2\pi/4}$ on $H\left|x_{n-1}\right\rangle$. Hence, we need to define a conditional rotation (CR_θ) based on the regular rotation (R_θ), as follows.

$$\text{When } R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \text{ then } CR_\theta = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix}.$$

For $\left|y_3\right\rangle$ we need two conditional rotations based on the values of x_n and x_{n-1}. We can keep going and construct our Quantum circuit as pictured following:



This gives us the correct output except that the y_j's are in the reverse order. We can easily swap them to get them in the right order. The number of gates to compute $\left|y_j\right\rangle$ is $O(j)$. In total, the circuit contains $O(n^2)$ gates.

We can construct a simpler circuit with a good approximation and lower complexity by ignoring the smaller rotation gates, which have a minor effect on the outputs.

Thus, we found the Fourier transform for the group $\mathbb{Z}_N$, where $N = 2^n$. In particular, when $n = 1$ the operation of the Fourier transform is the Hadamard transform. The Fourier Transform over $(\mathbb{Z}_2)^n$ is the tensor product of n Hadamard transforms: $F = H^{\bigotimes n}$. Each time we applied $H^{\bigotimes n}$ in the past, we were really applying the Fourier Transform over $(\mathbb{Z}_2)^n$.

3 Phase Estimation

Phase estimation is the following problem. **Problem:** For a given $|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \omega x} |x\rangle$, where $0 \leq \omega < 1$, the goal is estimate the value of ω.
To achieve this goal we consider two cases as follows:

Case 1: ω is of the form $\frac{z}{N}$, where $z \in \{0, \ldots, N-1\}$.
In this case, we can find ω exactly by performing inverse Fourier transform on the superposition $|\Psi\rangle$ and observe the z:

$$z := F^{-1} |\Psi\rangle = |z\rangle .$$

Case 2: In general, without the constraint on ω, we can find an approximation which is close to ω. We claim that the above procedure yields that with high probability, and now analyze its probability of success.

$$F^{-1} |\Psi\rangle = \sum_{z=0}^{N-1} \alpha_z |z\rangle ,$$

where

$$\alpha_z = \frac{1}{N} \sum_{j=0}^{N-1} e^{2\pi i \omega y} e^{-\frac{2\pi i z y}{N}} = \frac{1}{N} \sum_{y=0}^{N-1} (e^{2\pi i (\omega - \frac{z}{N})})^y = \frac{1}{N} . \frac{1 - e^{2\pi i (\omega - \frac{z}{N}) N}}{1 - e^{2\pi i (\omega - \frac{z}{N})}} .$$

The probability of observing z is $|\alpha_z|^2$. Using the above expression for α_z we will show in the next lecture that the probability of obtaining the closest approximation to ω of the form $\frac{z}{N}$ is high, and that the probability of obtaining one that is far from ω is small.

We will also discuss an important application of phase estimation, namely estimating the eigenvalues of unitary operations, which are all of the form $e^{2\pi i \omega}$ for some real $\omega \in [0, 1)$.