CS 294-6, Quantum Computing (Umesh Vazirani) September 22, 2000
Fall 2000, University of California, Berkeley.
Lecture #4 (Fourier Transform) **DRAFT** Notes by Kunal Talwar

1 Introduction

In this lecture, we look at the concept of Fourier transforms over a finite abelian group. We start with the Fourier transform over $\mathbb{Z}_N$. In particular, we will look at the hidden subgroup problem. Except for some details, factoring and discrete log are instances of this problem. This problem will give us the intuition for them.

2 Discrete Fourier Transform

The discrete Fourier transform (FT) (in this discussion it will be over $\mathbb{Z}_N$), can be looked at from various viewpoints. The most pedestrian viewpoint is that of a matrix, multiplication by which gives us the Fourier transform. Let $\omega = e^{\frac{2\pi}{N}i}$ be an N^{th} root of unity. Then

$$\mathrm{FT}_N(\sum_k \alpha_k |k\rangle) = F_{N\times N} A_{N\times 1}$$

where $F_{l,m} = \frac{1}{\sqrt{N}}\omega^{lm}$, and A is the column vector with entries α_k. Thus

$$\sum_k \alpha_k |k\rangle \quad \xrightarrow{FT_N} \quad \sum_k \hat{\alpha_k} |k\rangle$$
$$|k\rangle \quad \xrightarrow{FT_N} \quad \frac{1}{\sqrt{N}} \sum_j \omega^{jk} |j\rangle$$

and for a superposition, we use linearity, i.e.

$$\sum_k \alpha_k |k\rangle \quad \xrightarrow{FT_N} \quad \sum_j \sum_k \alpha_k \omega^{jk} |j\rangle$$

2.1 Convolution property

Suppose we have two different superpositions $\sum_k \alpha_k|k\rangle$ and $\sum_l \beta_l|l\rangle$. Their convolution is defined as

$$\sum_k \alpha_k|k\rangle * \sum_l \beta_l|l\rangle = \sum_{k,l} \alpha_k\beta_l|k+l\rangle$$

where $+$ is the group operation. What is the Fourier transform of the convolution? Convolution can be viewed as a product over the algebra of the group $\mathbb{Z}_N$, and $\sum_k \alpha_k|k\rangle$ can be viewed as an element of that group. Now

$$\begin{aligned}
FT(\sum_k \alpha_k|k\rangle * \sum_l \beta_l|l\rangle) &= FT(\sum_{k,l} \alpha_k\beta_l|k+l\rangle) \\
&= \sum_{k,l} \frac{1}{\sqrt{N}} \sum_j \alpha_k\beta_l\omega^{(k+l)j}|j\rangle \\
&= \frac{1}{\sqrt{N}} \sum_j \sum_k (\alpha_k\omega^{kj} \sum_l \beta_l\omega^{lj})|j\rangle \\
&= \frac{1}{\sqrt{N}} \sum_j (\sum_k \alpha_k\omega^{kj})(\sum_l \beta_l\omega^{lj})|j\rangle \\
&= \sqrt{N} \sum_j \hat{\alpha}_j\hat{\beta}_j|j\rangle
\end{aligned}$$

2.2 Fast Fourier Transform

Let $N = 2^n$. The Fourier transform can be represented by multiplication with an $N \times N$ matrix F. Thus naively, we would imagine that it requires an $O(N^2)$ sized circuit to compute the Fourier transform (this is generally how long it takes to compute a matrix-vector multiplication with dimensions $N \times N$ and N, respectively). However, with the Fast Fourier Transform (FFT) we can do it with only an $O(N \log N)$ sized circuit.

The rows of the column vector x (and correspondingly the matrix F) in the matrix multiplication Fx can be reordered as in figure 1. The reordering consists of putting the even indices of x first, then the odd ones. Notice that the left parts of the matrix after this reordering are just Fourier transform matrices of size $N/2$, and the right parts are the same matrices but with each row j multiplied by ω^j. Thus if we proceed recursively, separating the inputs into even and odd, we get the circuit of figure 2. If the size of the fast Fourier

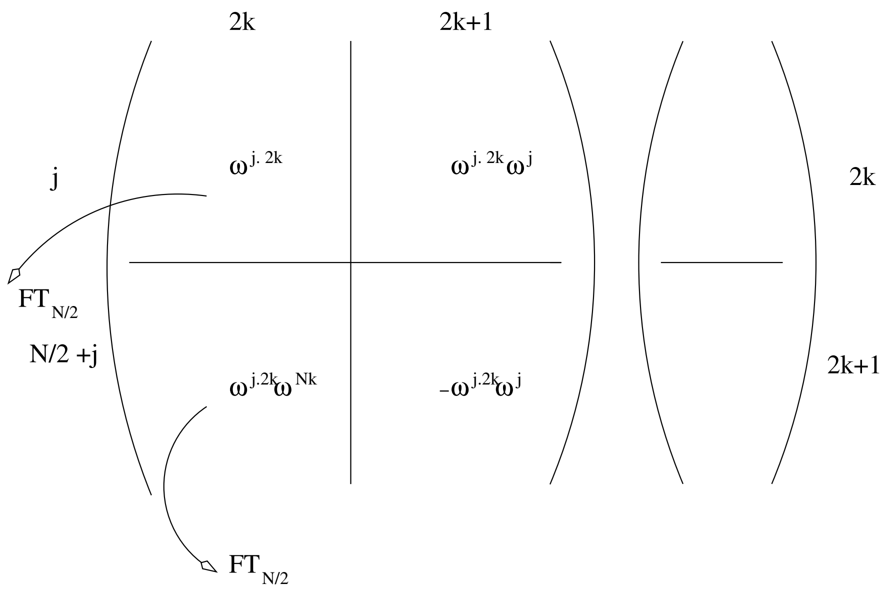

Figure 1: Splitting the Fourier Transform matrix

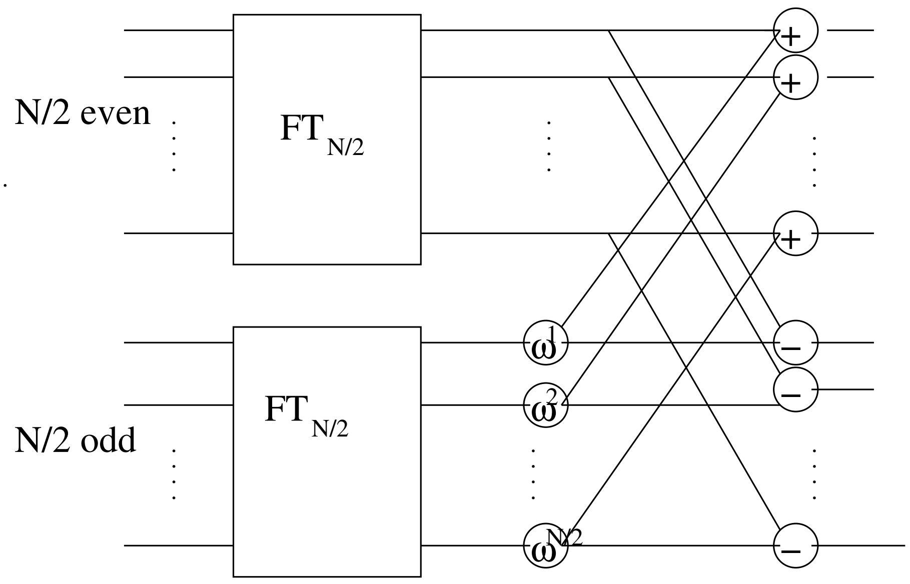

Figure 2: Fast Fourier transform circuit

transform circuit is denoted by $S(N)$, then

$$S(N) \;=\; 2S(N/2) + O(N)$$

which gives $S(N) = O(N \log N)$.

2.3 Quantum Fourier transform circuit

Now suppose that the N entries are in superposition, and there are only $n = \log N$ input wires. We want a unitary transformation such that given input $\phi = \sum_k \alpha_k |k\rangle$, the output should be $FT(\phi) = \sum_j \hat{\alpha}_j |j\rangle$.

In analogy with the classical FFT circuit, we first want to separate the even numbered and odd numbered states, and then perform a FT on each of them. This can be done simply by performing an FFT on the most significant $n-1$ qubits of the input (figure 3(a)). Next on the FT of the odd numbered states, we want to multiply by ω^j's. For this we should make use of the least significant bit. Note that we want to apply a phase shift of ω^j to the j^{th} state. This state is now represented in binary in the $n-1$ most significant qubits. If the binary representation of j is $j_{n-2} \ldots j_1 j_0$, then $\omega^j = \omega^{j_0} \omega^{2j_1} \omega^{4j_2} \ldots \omega^{2^{n-2} j_{n-2}}$ Now, conditioned on the least significant bit, we want to apply a phase shift (figure 3(b)), then add and subtract, as in figure 2. For this, note that applying a Hadamard transform on the least significant qubit does exactly what we want. The final quantum Fourier transform circuit is shown in figure 3(c).

Note that if $S(n)$ denotes the size of the quantum circuit to perform a Fourier transform over $\mathbb{Z}2^n$, then $S(n) = S(n-1) + O(n)$. Hence, $S(n) = O(n^2)$.

To reduce the size of the circuit, note that the phase shifts of the first few bits are very small. Thus neglecting the phase shifts in the first few bits amounts to a small error in the final output. (see lecture 2 for an analysis of "acceptable error"). Leaving out all but the most significant shifts can reduce the size of the circuit to $O(n\text{polylog}(n))$.

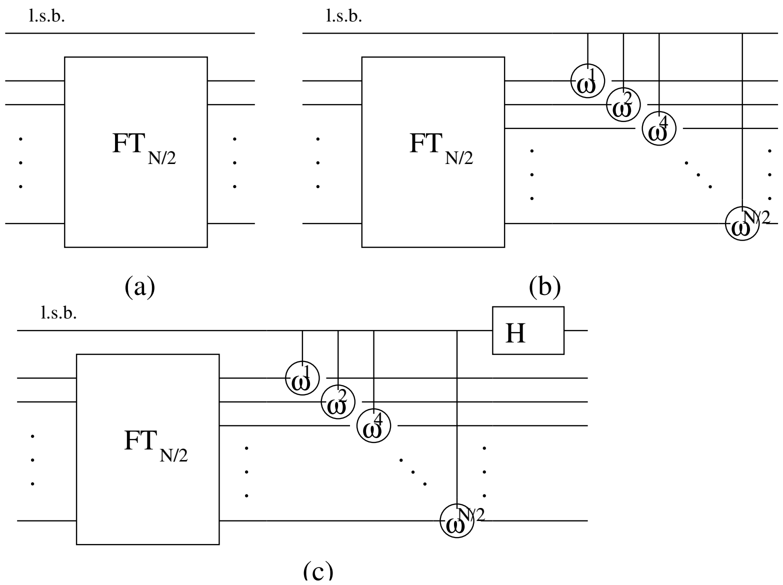

Figure 3: Quantum Fourier transform circuit

3 Another look at the Fourier transform matrix

Consider the Fourier transform matrix F, with $F_{j,k} = \frac{1}{\sqrt{N}}\omega^{jk}$. We claim that F is unitary. To show that, consider the inner product of the j^{th} and the l^{th} columns.

$$\begin{aligned}\langle F_j|F_l\rangle &= \frac{1}{N}\sum_k \omega^{jk}\overline{\omega^{lk}} \\ &= \frac{1}{N}\sum_k \omega^{(j-l)k}\end{aligned}$$

For $j \neq l$, this is just the sum of powers of some N^{th} root of unity. Since the powers turn out to be placed symmetrically about the origin, they cancel out, and hence the columns are orthogonal. Finally, for $j = l$, the inner product is 1, so the matrix is unitary.

Let $\chi_j : \mathbb{Z}_N \to \mathbb{C}$ be the function defined by $\chi_j(1) = \omega^j$ and $\chi_j(k) = \omega^{jk}$. Then χ_j is a homomorphism from $\mathbb{Z}_N$ to $\mathbb{C}$ with respect to the $+$ operation in the domain and the $\cdot$ operation in the range (in other words, $\chi_j(x+y) = \chi_j(x) \cdot \chi_j(y)$). Note also that χ_1 is an isomorphism. The set of all χ_j's form a group, called the dual group of $\mathbb{Z}_n$, denoted $\hat{\mathbb{Z}}_n$.

The Fourier transform can be written in the above notation as

$$|k\rangle \mapsto \frac{1}{\sqrt{N}} \sum_j \chi_j(k)|j\rangle$$

Now a new question arises: how can the Fourier transform be defined over an arbitrary abelian group? In the following discussion, call the abelian group G. By the structure theorem of finite abelian groups, $G \cong \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_l}$, so that any $g \in G$ can be written equivalently as $(a_1, a_2, \ldots, a_l)$, where $a_i \in \mathbb{Z}_{N_i}$. Here the group operation corresponds to componentwise group operations. Now let's ask: what are the homomorphisms from G to $\mathbb{C}$? Under mappings similar to the χ_j ones above,

$$\begin{aligned}
(1, 0, \ldots, 0) &\mapsto \omega_{N_1}^{k_1} \\
(0, 1, \ldots, 0) &\mapsto \omega_{N_2}^{k_2} \\
&\vdots \\
(0, 0, \ldots, 1) &\mapsto \omega_{N_l}^{k_l}
\end{aligned}$$

Then the full mapping will be

$$(a_1, a_2, \ldots, a_l) \mapsto \omega_{N_1}^{k_1 a_1} \cdot \omega_{N_2}^{k_2 a_2} \cdot \cdots \cdot \omega_{N_l}^{k_l a_l}$$

Finally, the Fourier transform of $(a_1, \ldots, a_l)$ can be defined as

$$(a_1, \ldots, a_l) \mapsto \frac{1}{\sqrt{|G|}} \sum_{(k_1, \ldots, k_l)} \omega_{N_1}^{k_1 a_1} \cdot \cdots \cdot \omega_{N_l}^{k_l a_l} |k_1 \cdots k_l\rangle$$

(Note: we could actually use $N' = \mathrm{lcm}(N_1, \ldots, N_l)$, let $\omega_{N'}$ be the N'th root of unity, then write $\omega_{N_1}^{k_1 a_1} \cdot \cdots \cdot \omega_{N_l}^{k_l a_l}$ as

$$\omega^{k_1 a_1 q_1 + \cdots + k_l a_l q_l}$$

where $q_i = N'/N_i$.

Exercise: Suppose you are given quantum circuits for the Fourier transform over any two pairs of $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_k}$, where p_i is prime for each i. Give a quantum circuit for $\mathbb{Z}_{p_1 \cdots p_k}$.

4 More on convolutions

The Fourier transform treats subgroups $H \subseteq G$ in a very special way. Define $H^\perp = \{k \in \hat{G} \mid k(h) = 1 \; \forall h \in H\}$, where $\hat{G}$ is the dual group of G. Also, writing a character function $k(a)$ on a general abelian group element can be written as

$$\vec{k}(\vec{a}) = \omega^{k_1 a_1 q_1 + \cdots + k_l a_l q_l}$$

which is 1 if the amplitude (exponent) of ω is 0. This can be viewed as k and a having a "dot product" of 0. Now the Fourier transform acts like this:

$$\frac{1}{\sqrt{|H|}}\sum|h\rangle \overset{FT_G}{\mapsto} \sqrt{\frac{|H|}{|G|}}\sum_{k\in H^\perp}|k\rangle \tag{1}$$

Proof: The proof will be in two parts: that (a), everything in $H^\perp$ has equal amplitude, and (b) that everything outside $H^\perp$ has zero amplitude. For part (a), first note that for any h,

$$|h\rangle \overset{FT_G}{\mapsto} \frac{1}{\sqrt{|G|}}\sum_k k(h)|k\rangle$$

Notice from this that for all $k \in H^\perp$, $k(h) = 1$, so each element on the left hand side of equation 1 contributes a magnitude of $1/\sqrt{|G|}$ to each element $|k\rangle$ on the right hand side. Summing over all h, we get that the coefficient of $k \in H^\perp$ is

$$\frac{1}{\sqrt{|G|}}\sum_{h\in H}\frac{1}{\sqrt{|H|}} = \frac{\sqrt{|H|}}{\sqrt{|G|}}$$

To show (b), start off with $(\sum_{k\in H}|h\rangle)\odot(|h'\rangle)$. Now $Hh' = H$ since H is a subgroup. Then (FT = Fourier transform)

$$\begin{aligned}
FT(\frac{1}{\sqrt{|H|}}\sum_{k\in H}|h\rangle) &= FT((\frac{1}{\sqrt{|H|}}\sum_{k\in H}|h\rangle)\odot(|h'\rangle)) \\
&= FT(\frac{1}{\sqrt{|H|}}\sum_{k\in H}|h\rangle)\cdot_{\text{ptwise}} FT(|h'\rangle) \\
&= FT(\frac{1}{\sqrt{|H|}}\sum_{h\in H}|h\rangle)\cdot_{\text{ptwise}} (\sum_k k(h')|k\rangle)
\end{aligned}$$

This can be true if and only if $k(h') = 1$ whenever the term of $FT(\frac{1}{\sqrt{|H|}}\sum_{k\in H}|h\rangle)$ involving h' is not zero. The contrapositive of this is that $k(h') \neq 1$ implies that the h' term of $FT(\frac{1}{\sqrt{|H|}}\sum_{k\in H}|h\rangle)$ is zero, which is what we wanted to prove for part (b). It also follows that $|H^\perp| = |G|/|H|$. ∎

What if we start out with a coset of H? Recall that a coset $Hg = \{hg \mid h \in H\}$. Then

$$\frac{1}{\sqrt{|H|}}\sum_{h\in H}|hg\rangle \overset{FT_G}{\mapsto} \sqrt{\frac{|H|}{|G|}}\sum_{k\in H^\perp}\omega^{\delta(g,k)}|k\rangle$$

Exercise: prove this (hint: not that a superposition over a coset is the same as a superposition over "$H \odot |g\rangle$").

The Fourier transform treats subgroups and cosets "well," but the amplitudes get messed up. However, if we do a measurement, the phase is irrelevant. This means that, starting with an even superposition over H, after a Fourier transform followed by a measurement we end up with a random element of $H^{\perp}$, independent of with what coset we originally started.

Now let's go back and think about the 2^n-slit experiment (from lecture 3). The thought was to somehow create an interesting slit pattern between the two Fourier transforms. The subgroup mechanism is the key to figuring out the slit pattern.

5 The hidden subgroup pattern

Let G again be a finite abelian group, and $f : G \to S$. Let $H \subseteq G$ be a subgroup of G which is unknown to us. Suppose f comes with the promise that it is constant on cosets of H and distinct on distinct cosets. The challenge is to find H.

A quantum algorithm to solve this is: start with $|0\rangle|0\rangle$. Now

$$
\begin{aligned}
|0\rangle|0\rangle \quad & \xrightarrow{FT_G \otimes I} \quad \frac{1}{\sqrt{|G|}} \sum_{a \in G} |a\rangle|0\rangle \\
& \xrightarrow{f} \quad \frac{1}{\sqrt{|G|}} \sum_{a \in G} |a\rangle|f(a)\rangle \\
& \xrightarrow{\text{measure 2nd reg}} \quad \frac{1}{\sqrt{|H|}} \sum_{h \in H} |hg\rangle
\end{aligned}
$$

If we were to measure $|hg\rangle$ we would just get a random element of the group, which is not very helpful. Instead we can do a Fourier transform again, then measure, so that we would get a random sample of $H^{\perp}$ (note that we can invoke the principle of safe storage and skip the measurement). Then each time this process is repeated, we get a random $k : k(h) = 0 \; \forall h \in H$. Using this, we can try to zero in on H.

6 Factoring and discrete log

The factoring problem is: given a natural number N, factor it into $N = N_1 N_2 \dots N_k$. For the sake of disposition, assume that $N = N_1 N_2$ and that both N_1 and N_2 are prime (this is considered the hardest version of the problem in any case).

To factor N it is sufficient to find the order of an element $x \mod N$, i.e. find a natural number r such that $x^r \equiv 1 \mod N$. It turns out that factoring has a randomized polynomial time reduction to this "order finding" problem. Let $\mathrm{ord}(x)$ denote the order of x. We know that

$$\mathrm{ord}(x) \mid |\mathbb{Z}_N^*|$$

where $\mathbb{Z}_N^*$ is the multiplicative group modulo N, and $|Z_N^*| = \phi(N)$, the number of positive natural numbers less than N which are relatively prime to it. It is well known that if $N = p_1^{e_1} \cdots p_k^{e_k}$ then $\phi(N) = (p_1 - 1)p_1^{e_1-1} \cdots (p_k - 1)p_k^{e_k-1}$.

Now let $f : \mathbb{Z}_{\phi(N)} \to \mathbb{Z}_N^*$ be defined as $f(a) = x^a \mod N$. Fix x, and let $r = \mathrm{ord}(x)$. Then $r \mid \phi(N)$, $\langle r \rangle = \{0, r, 2r, \dots\}$ is the subgroup generated by r, and f is constant on this subgroup, since $x^r \equiv 1 \mod N$, so that $x^{rk} \equiv (x^r)^k \equiv 1^k \equiv 1 \mod N$.

A coset looks like $\langle r \rangle + j$, and hence f is constant on cosets of $\langle r \rangle$ for essentially the same reason.

We first use f to generate a superposition over some coset, then do a Fourier transform to get a random element of $\langle r \rangle^\perp$ with non-negligible probability. Notice that the random element will have the form

$$l = s \cdot \frac{\phi(N)}{r}$$

If s is picked randomly from $\{0, \dots, r-1\}$, $\gcd(s, r) = 1$ will probably be true, in which case $\gcd(l, \phi(N)) = \phi(N)/r$.

However, this is only a high-level intuitive picture, since $\phi(N)$ is not known. (In fact, if $\phi(N)$ were known, we could factor classically in polynomial time.)