Quantum Computing 4/7/2022

Lecture 19: Fourier Transform

Instructor: Dieter van Melkebeek Scribe: Yang Gao

Last time we talked about Fourier Sampling that is based on the Fourier Transform, and we've seen Fourier Transform over $\mathbb{Z}_2^n$. In this lecture we discuss in more general about Fourier Transforms and solve the exercise on Fourier Sampling from last lecture. There is not a lot of quantum in this lecture, and the focus is on Fourier Transforms over finite Abelian group.

1 Fourier Sampling Exercise

We begin with the solution to the exercise from the last lecture, which posed the following question:

Exercise 1. *Given: Black-box access to one-to-one functions $f, g : \{0,1\}^n \to \{0,1\}^n$ where $g(x) = f(x \oplus s)$ for some $s \in \{0,1\}^n$. Find s, with certainty, using $O(n)$ queries.*

Solution

One natural thing to try is to have two registers. However this way two computations will evolve independently, but f and g need to interact somehow.

We use the Fourier sampling technique we discussed in the solution to Simon's problem. We begin with the initial superposition

$$\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle |0^n\rangle$$

where $N = 2^n$ as usual.

In order to allow interference between the output of f and g, we introduce an additional control qubit which we use to select whether to apply U_f or U_g. To implement this, consider the function $h : \{0,1\}^{n+1} \to \{0,1\}^n$ where $h(x,0) = f(x)$ and $h(x,1) = g(x)$ for $x \in \{0,1\}^n$. The controlled application of U_f and U_g is achieved by U_h.

We now have state

$$\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle |0^n\rangle$$

and, after applying H to the control qubit, we have

$$\frac{1}{\sqrt{2N}} \sum_{x \in \{0,1\}^n} |x\rangle (|0\rangle + |1\rangle) |0^n\rangle .$$

We now perform the controlled application of U_f and U_g; we get

$$\begin{aligned} &\frac{1}{\sqrt{2N}} \sum_{x \in \{0,1\}^n} |x\rangle (|0\rangle |f(x)\rangle + |1\rangle |g(x)\rangle) \\ = &\frac{1}{\sqrt{2N}} \sum_{x \in \{0,1\}^n} |x\rangle (|0\rangle |f(x)\rangle + |1\rangle |f(x \oplus s)\rangle). \end{aligned}$$

This is similar to last lecture about finding a hidden XOR shift in that there are two ways the tag can have a given value. We follow the same strategy as last time, applying the Hadamard gate $H^{\otimes n}$ to the first register. Recall that

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{N}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle .$$

Our state is now

$$\frac{1}{\sqrt{2}N} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle (|0\rangle |f(x)\rangle + |1\rangle |f(x \oplus s)\rangle).$$

Reparametrizing x in the components where the control qubit is 1 yields

$$\begin{aligned} &\frac{1}{2N} \sum_{x,y \in \{0,1\}^n} |y\rangle ((-1)^{x \cdot y} |0\rangle + (-1)^{(x \oplus s) \cdot y} |1\rangle) |f(x)\rangle \\ = &\frac{1}{2N} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle (|0\rangle + (-1)^{s \cdot y} |1\rangle) |f(x)\rangle \end{aligned}$$

Applying H to the control bit yields the following state:

$$\begin{aligned} &\frac{1}{2N} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} (1 + (-1)^{s \cdot y}) |y\rangle |0\rangle |f(x)\rangle \\ + &\frac{1}{2N} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} (1 - (-1)^{s \cdot y}) |y\rangle |1\rangle |f(x)\rangle \end{aligned}$$

If $s \neq 0^n$, due to the inference, observing the first register and control bit yields:

- With probability 1/2: $|y\rangle |0\rangle$ for uniform $y \in s^{\perp}$
- With probability 1/2: $|y\rangle |1\rangle$ for uniform $y \notin s^{\perp}$

Note that $|s^{\perp}| = |\{0,1\}^n - s^{\perp}|$, so we observe $|y\rangle |y \cdot s \bmod 2\rangle$ for y chosen uniformly at random from $\{0,1\}^n$.

If $s = 0^n$, we measure $|y\rangle |0\rangle$ for y chosen uniformly at random from $\{0,1\}^n$.

Hence in all cases where y is distributed uniformly over $\{0,1\}^n$, we observe $|y\rangle |y \cdot s \mod 2\rangle$.

We repeat the process until we have obtained n linearly independent such y. By using amplitude amplification with error elimination in the same way as discussed in Simon's problem, we can ensure that each time we repeat the process, we obtain a y that is linearly independent from the previously obtained y's using 3 applications of U_h. Once we have obtained n such y, which we can do with certainty in n iterations and $3n$ applications of U_h, we may solve the resulting system for s.

2 Standard Fourier Transform

Definition 1. *Let $f : \mathbb{R} \to \mathbb{C}$ such that $\int_x |f(x)|^2\,dx < \infty$. Then its Fourier transform $\hat{f}$ is a function from $\mathbb{R}$ to $\mathbb{C}$ such that $\hat{f}(\omega) = \int_x f(x)e^{2\pi i\omega x}\,dx$ for all $\omega \in \mathbb{R}$. The inverse Fourier transform of $\hat{f}$ is $f(x) = \int_\omega \hat{f}(\omega)e^{-2\pi i\omega x}\,d\omega$.*

Where ω denotes the frequency, and $e^{2\pi i\omega x} = \cos(2\pi\omega x) + i\sin(2\pi\omega x)$

Properties of the Fourier Transform

Note that the Fourier transform is a linear transformation: $\widehat{af + bg} = a\hat{f} + b\hat{g}$. The Fourier tranform is also unitary; we can see this property using several equivalent definitions of the unitary property. A unitary transformation can be viewed as one that preserves the 2-norm or one that transforms an orthonormal basis of its domain into an orthonormal basis. Another important definition, which we have used heavily in this class, is that a transform is unitary when its inverse is equal to its adjoint.

First, consider the a unitary transformation as one which preserves inner products. If we consider the inner product space of functions from $\mathbb{R}$ to $\mathbb{C}$ with inner product $(f, g) = \int_x f(x)\overline{g(x)}\,dx$, then the Fourier transform preserves inner products, i.e., $(\hat{f}, \hat{g}) = (f, g)$, and is hence a unitary transformation.

Now, recall that the inverse Fourier transform is

$$f(x) = \int_\omega \hat{f}(\omega)e^{-2\pi i\omega x}\,d\omega.$$

As $e^{-2\pi i\omega x}$ is the conjugate of $e^{2\pi i\omega x}$, we can see that the inverse Fourier transform is the conjugate transpose, or the adjoint, of the standard Fourier transform, which is thus unitary.

Another way to see that the Fourier transform is unitary as it tranforms the standard orthonormal basis (consisting of the Dirac delta functions) into an orthonormal basis, which is referred to as the Fourier basis consisting of the harmonics,

$$e^{2\pi i\omega x} = \cos(2\pi\omega x) + i\sin(2\pi\omega x).$$

Functions in the standard basis are referred to as being in the time domain, and functions in the Fourier basis are referred to as being in the frequency domain.

Definition 2. *The convolution of $f : \mathbb{R} \to \mathbb{C}$ with $g : \mathbb{R} \to \mathbb{C}$ is $f * g : \mathbb{R} \to \mathbb{C}$ where*

$$(f * g)(x) = \int_y f(x)g(x - y)\,dy.$$

One particularly important property of the Fourier transform is that convolution in the time domain is equivalent to point-wise product in the frequency domain, i.e., that $\widehat{f * g}(\omega) = \hat{f}(\omega)\hat{g}(\omega)$ for all $\omega \in \mathbb{R}$.

Next we discuss the more general form of the Fourier transform including over finite Abelian groups of size N, which is of particular interest in developing quantum algorithms. This form is also the one most commonly used in the practical applications which rely on the $O(N \log N)$ complexity of the fast Fourier tranform, an efficient algorithm to compute the discrete Fourier transform on

the group $\mathbb{Z}_N$. Due to the convolution property of the Fourier transform, the fast Fourier transform makes it possible to perform convolutions in time $O(N \log N)$ which would take $O(N^2)$ if done in the time domain instead. For this reason, the Fourier transform is heavily used in fields such as digital signal processing, computer vision, and statistics.

3 General Fourier Transform

In order to apply the Fourier Transform to quantum algorithms, we need to generalize it to a transformation of functions whose domain is a more general group; a Fourier transform exists for many important groups (for example, $\mathbb{R}$ under addition as above), though not for all groups. We show in this lecture that it is guaranteed to exist for an important class of groups, finite Abelian groups; the Fourier Transform is also unique (up to permutations of the basis elements) for this class of groups.

Definition 3. *Let G be a group. A Fourier Transform on G is a transformation on the space of functions $\{f : G \to \mathbb{C}\}$, mapping f to $\hat{f}$, that is:*

- *linear*
- *unitary*
- *turns convolutions into point-wise products: $\widehat{f * g}(x) = \hat{f}(x)\hat{g}(x)$ for $f, g : G \to \mathbb{C}$ and $x \in G$.*

The convolution of f and g on a finite group G is defined as $(f * g)(x) = \sum_y f(y)g(x-y)$. The group operation is used in the subtraction $x - y$; the other operations are in $\mathbb{C}$.

3.1 Characters of a Group

In constructing the Fourier Transform for finite Abelian G, *characters* take the place of harmonics.

Definition 4. *A character of a group G is a homomorphism from G to the multiplicative group $\mathbb{C}$, or equivalently, a mapping $\chi : G \to \mathbb{C}$ such that $\chi(x + y) = \chi(x) \cdot \chi(y)$.*

The properties of characters χ, χ' of a finite group G include the following (proofs follow):

1. **Roots of Unity** All members of the range of a character of G are roots of unity and, in particular, $|G|$-th roots of unity, i.e., $\chi(x)^{|G|} = 1$ for all $x \in G$.
2. **Orthogonality** Distinct charaters of G are orthogonal to each other:

   if $\chi \neq \chi'$, then $(\chi, \chi') = 0$ where the inner product of $f, g : G \to \mathbb{C}$ is defined as

$$(f, g) = \sum_{x \in G} f(x)\overline{g(x)}.$$

Notation: if x is a member of a group with operation $+$ and n is a positive integer, we write $n \cdot x$ to represent $x + x + \cdots + x$ where x appears n times.

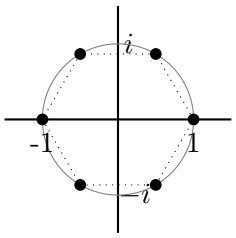

Figure 1: The sixth roots of unity

3.1.1 Roots of Unity Property

In the reals, the only roots of unity (i.e., of 1) are 1 and -1 (for integers k with even powers). However, given some positive integer n, there are n roots of unity in $\mathbb{C}$: specifically $e^{2k\pi i/n}$ for $0 \leq k < n$. Visualizing them in the complex plane, these values form the vertices of a regular n-gon inscribed in the unit circle, with the point 1 as one of the vertices : see Figure 1 for an example with $n = 6$.

We wish to show that $\chi(x)$ is a $|G|$-th root of unity for every character χ of a finite group G.

Proof. First, we show that $\chi(0) = 1$, which follows from the homomorphism property of χ. We have that $\chi(0) = \chi(0 + 0) = \chi(0)^2$. Since $\chi(0)$, an element of the multaplicative group $\mathbb{C}$, is invertible, we must have $\chi(0) = 1$.

Suppose that $x \in G$. We wish to show that $\chi(x)^{|G|} = 1$, i.e., that x is a $|G|$-th root of unity. Let $\langle x \rangle = \{x, x + x, x + x + x, \dots\} = \{1 \cdot x, 2 \cdot x, 3 \cdot x, \dots\}$ be the subgroup of G generated by x.

As $|G|$ is finite, $|\langle x \rangle| \leq |G|$ is finite as well, so we have some positive integer k such that $k \cdot x = 0$. Take the smallest such k, which we call the order of x (and which equals $|\langle x \rangle|$), and consider $\chi(x)^k$.

As χ is a homomorphism, $\chi(x)^k = \chi(k \cdot x) = \chi(0) = 1$. Now, from group theory we have that the order of a subgroup of a finite group divides the size of the group, so k divides $|G|$. Hence, $\chi(x)^{|G|} = 1$. □

3.1.2 Orthogonality Property

We now wish to show that distinct characters of a group G are orthogonal.

Proof. Suppose that $a \in G$. As a is invertible, we have that $x = y$ if and only if $a + x = a + y$. Now, as G is closed under addition, we have that

$$\begin{aligned}
\sum_{x \in G} \chi(x) &= \sum_{a+x \in G} \chi(a + x) \\
&= \sum_{x \in G} \chi(a + x) \\
&= \sum_{x \in G} \chi(a)\chi(x) \\
&= \chi(a) \sum_{x \in G} \chi(x)
\end{aligned}$$

as χ is a homomorphism.

Hence, we have either that $\sum_{x \in G} \chi(x) = 0$ or $\chi(a) = 1$ for all $a \in G$.

Noting that the conjugate of a root of unity is its inverse, we have, by the property shown above, that $\overline{\chi} = \chi^{-1}$ for all characters χ of G.

Suppose that χ_1, χ_2 are distinct characters of G. Now, let $\chi = \chi_1 \cdot \overline{\chi_2}$. As the conjugate of a character and the product of two characters both satisfy the homomorphism properties, they are also characters of G, and consequently, χ is a character of G. If χ is identically equal to 1, then we must have that $\overline{\chi_2} = \chi_1^{-1}$, and, by the above, that $\chi_1 = \chi_2$, a contradiction.

Thus, we must instead have

$$\begin{aligned} 0 &= \sum_{x \in G} \chi(x) \\ &= \sum_{x \in G} \chi_1(x)\overline{\chi_2(x)} \\ &= (\chi_1, \chi_2) \end{aligned}$$

and we are done. □

From the fact that $\chi(x)\overline{\chi(x)} = 1$ for all $x \in G$ and characters χ of G we immediately derive the following corollary.

Corollary 1. *The normalized characters* $\frac{1}{\sqrt{|G|}}\chi$ *are orthonormal.*

3.2 Properties of the General Fourier Transform

If $f : G \to \mathbb{C}$ can be written as

$$f = \frac{1}{\sqrt{|G|}} \sum_{\chi} \hat{f}(\chi)\overline{\chi} \tag{1}$$

for some $\hat{f}$, then $\hat{f}$ is our candidate Fourier Transform of f.

3.2.1 Unitary Property

The linearity property of the Fourier transform is clearly satisfied; consider the unitary property. We now show that the unitary property is satisfied. Suppose that f and g can be written in the form (1).

Then, by the orthogonality property of the characters χ, and the fact that $(\chi, \chi) = |G|$ for all

characters χ of G we must have that

$$\begin{aligned}
(f,g) &= \frac{1}{|G|}\sum_{x\in G}\sum_{\chi_1,\chi_2}\hat{f}(\chi_1)\chi_1(x)\overline{\hat{g}(\chi_2)\chi_2(x)} \\
&= \frac{1}{|G|}\sum_{\chi_1,\chi_2}\sum_{x\in G}\hat{f}(\chi_1)\overline{\hat{g}(\chi_2)}\chi_1(x)\overline{\chi_2(x)} \\
&= \frac{1}{|G|}\sum_{\chi_1,\chi_2}\hat{f}(\chi_1)\overline{\hat{g}(\chi_2)}\sum_{x\in G}\chi_1(x)\overline{\chi_2(x)} \\
&= \frac{1}{|G|}\sum_{\chi_1,\chi_2}\hat{f}(\chi_1)\overline{\hat{g}(\chi_2)}(\chi_1,\chi_2) \\
&= \sum_{\chi}\hat{f}(\chi)\overline{\hat{g}(\chi)} \\
&= (\hat{f},\hat{g})
\end{aligned}$$

and so our candidate Fourier Transform preserves inner products (and thus the 2-norm) and is unitary.

We can also show that our candidate Fourier Transform is unitary by showing that its inverse is equal to its adjoint. By the orthogonality of the characters χ, we must also have that our candidate Fourier Transform satisfies

$$\hat{f}(\chi) = (f,\overline{\chi}) = \frac{1}{\sqrt{|G|}}\sum_{x\in G} f(x)\chi(x) \tag{2}$$

Recall that the mapping $f \to \hat{f}$ is given by equation (1). From equation (2), we can see that the inverse mapping $\hat{f} \to f$ is the conjugate transpose, or adjoint, of the forward mapping, showing again that our candidate Fourier Transform is unitary.

3.2.2 Exercise: Convolutional Property

Exercise 2. *Show that our candidate Fourier Transform satisfies the convolution property of the Fourier Transform, i.e., that it transforms convolutions into point-wise products.*

1. *Show that if f and g can be written in the form (1), then so can $f * g : G \to \mathbb{C}$, defined by $(f*g)(x) = \sum_{y\in G} f(y)g(x-y)$.*
2. *Show that $\widehat{f*g}(\chi) = c(G)\cdot\hat{f}(\chi)\cdot\hat{g}(\chi)$.*
3. *Determine $c(G)$.*

We have now shown that our candidate Fourier Transform satisfies the basic properties of a Fourier Transform. It remains to be shown that all $f : G \to C$ can be written in form (1), i.e., that the characters of G form a basis for $\{f : G \to \mathbb{C}\}$.

We show that this holds for finite Abelian G, and thus that the Fourier Transform exists for those groups. This follows from the fact that the number of characters equals the size of the domain G.

3.2.3 Uniqueness of Fourier Basis

Theorem 2. *If the characters of a group G span the space of all functions $f : G \to \mathbb{C}$ then the normalized characters form the unique Fourier basis up to a permutation of the basis elements and global phase.*

Proof. We have already shown above that, if the characters span the space of all functions $f : G \to \mathbb{C}$ that they form a Fourier basis; it remains to show uniqueness.

Suppose that χ_1 and χ_2 are characters of G. From the convolution property,

$$\widehat{\chi_1 * \chi_2} = c(G) \cdot \hat{\chi}_1 \cdot \hat{\chi}_2.$$

By the definition of convolutions of $f : G \to \mathbb{C}$ and the homomorphism properties of χ_2

$$\begin{aligned}(\chi_1 * \chi_2)(x) &= \sum_{y \in G} \chi_1(y)\chi_2(x-y) \\ &= \sum_{y \in G} \chi_1(y)\chi_2(x)\overline{\chi_2(y)} \\ &= (\chi_1, \chi_2) \cdot \chi_2(x)\end{aligned}$$

as $\chi_2(-y) = \chi_2(y)^{-1} = \overline{\chi_2(y)}$.

Hence, if $\chi_1 \neq \chi_2$, then we have

$$c(G) \cdot \hat{\chi}_1 \cdot \hat{\chi}_2 = \widehat{\chi_1 * \chi_2} = (\chi_1, \chi_2) \cdot \hat{\chi}_2 = 0$$

and so $\operatorname{supp}(\hat{\chi}_1) \cap \operatorname{supp}(\hat{\chi}_2) = \emptyset$.

As the vector space of functions $f : G \to \mathbb{C}$ is $|G|$-dimensional, and as the characters span the set of all such functions, we must have at least $|G|$ characters. Furthermore, because the characters are orthogonal by the above, we can have no more than $|G|$ characters and thus there exist exactly $|G|$ distinct characters of G. Since $\hat{\chi}(\chi) = (\chi, \chi) = |G| \neq 0$ for all characters of G, we have $|\operatorname{sup}(\hat{\chi})| \geq 1$ for all χ and hence

$$|G| \leq \sum_{\chi} |\operatorname{sup}(\hat{\chi})|.$$

But as, by the above, the supports of distinct χ_1 and χ_2 are disjoint, we must also have that

$$\sum_{\chi} |\operatorname{sup} \hat{\chi}| \leq |G| = |\cup_{\chi} \operatorname{supp}(\hat{\chi})|.$$

Hence, $\sum_{\chi} |\operatorname{sup} \hat{\chi}| = |G|$ and we must have $|\operatorname{sup}(\hat{\chi})| = 1$ for all χ.

For any function $f : G\mathbb{C}$, $|\operatorname{supp}(\hat{f})|$ equals the number of the Fourier basis that are needed to express f as a linear combination of them. Thus, $|\operatorname{supp}(\hat{\chi})| = 1$ means that χ is itself an element of the Fourier basis, up to a scalar. As the Fourier basis is orthonormal, $\frac{\chi}{\sqrt{|G|}}$ must, in particular, be a member of the basis up to global phase. Consequently, the Fourier basis consisting of the normalized characters is unique up to a permutation of the basis elements and global phase. □

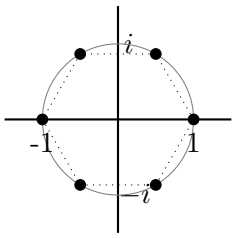

Figure 2: The sixth roots of unity

3.3 Characters of Finite Abelian Groups

We now use the following result from group theory:

Theorem 3 (Structure Theorem). *Every finite Abelian group is isomorphic to*

$$\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \mathbb{Z}_{N_3} \times \cdots \times \mathbb{Z}_{N_k}$$

under component-wise addition for some $N_1, N_2, \ldots, N_k \in \mathbb{N}$.

By our previous result it suffices to find $|G|$ distinct characters. We first find N characters for $\mathbb{Z}_N$ for $N \in \mathbb{N}$ and then find $|G_1| \cdot |G_2|$ characters of $G_1 \times G_2$ where G_1 and G_2 have $|G_1|$ and $|G_2|$ characters, respectively.

3.3.1 Characters of Modular Addition

We simply construct the following N distinct characters. Recall that the range of the characters of G is the set of N-th roots of unity (see Figure 2 for an example for $N = 6$). For each element $y \in \mathbb{Z}_N$, we construct a unique character that maps 1 to $\exp(2\pi iy/N)$.

Explicitly, for $y \in \mathbb{Z}_N$, let $\chi_y : \mathbb{Z}_{\mathbb{N}} \to \mathbb{C}$ such that $\chi_y(1) = (e^{2\pi i/N})^y = e^{2\pi iy/N}$ and $\chi_y(x) = \chi_y(1)^x = e^{2\pi ixy/N}$ for $x \in \mathbb{Z}_N$. As χ_y is a homomorphism and distinct for each $y \in \mathbb{Z}_N$, we are done.

For the special case of $N = 2$, the simple group with only two elements:
$\chi_y(x) = (-1)^{xy}$
$\chi_0(x) \equiv 1$ and $\chi_1(x) = (-1)^x$

3.3.2 Characters of Direct Product

We construct the following $|G_1| \cdot |G_2|$ characters. For $y_1 \in G_1$ and $y_2 \in G_2$ let

$$\chi_{y_1,y_2}(x_1, x_2) = \chi_{y_1}^{(G_1)}(x_1) \cdot \chi_{y_2}^{(G_2)}(x_2).$$

As we have given a distinct $\chi_{y_1}^{(G_1)}$ for each $y_1 \in G_1$ and similarly for G_2, we have $|G_1| \cdot |G_2| = |G_1 \times G_2|$ of these, which are distinct because the $\chi_{y_1}^{(G_1)}$ and $\chi_{y_2}^{(G_2)}$ are.

To show this, note that, where 0_1 and 0_2 are the identities of G_1 and G_2, respectively, we have that $\chi_{y_1,y_2}(0_1, x_2) = \chi_{y_2}^{(G_2)}(x_2)$ and $\chi_{y_1,y_2}(x_1, 0_2) = \chi_{y_1}^{(G_1)}(x_1)$ since homomorphisms map identities to identities (in this case, to 1). If $(y_1, y_2) \neq (y_1', y_2')$ it follows that χ_{y_1,y_2} and $\chi_{y_1',y_2'}$ will disagree on some point. It remains to show that they are characters, i.e., that they are homomorphisms.

Proof. By the definition of χ_{y_1,y_2} and as $\chi_{y_1}^{(G_1)}$ and $\chi_{y_2}^{(G_2)}$ are homomorphisms,

$$\begin{aligned}\chi_{y_1,y_2}(x_1+z_1,x_2+z_2) &= \chi_{y_1}^{(G_1)}(x_1+z_1)\cdot\chi_{y_2}^{(G_2)}(x_2+z_2)\\ &= (\chi_{y_1}^{(G_1)}(x_1)\chi_{y_1}^{(G_1)}(z_1))\cdot(\chi_{y_2}^{(G_2)}(x_2)\chi_{y_2}^{(G_2)}(z_2))\\ &= (\chi_{y_1}^{(G_1)}(x_1)\chi_{y_2}^{(G_2)}(x_2))\cdot(\chi_{y_1}^{(G_1)}(z_1)\chi_{y_2}^{(G_2)}(z_2))\\ &= \chi_{y_1,y_2}(x_1,x_2)\cdot\chi_{y_1,y_2}(z_1,z_2).\end{aligned}$$

□

As we have constructed N distinct characters for each $\mathbb{Z}_N$ for all $N \in \mathbb{N}$, the result which we have just shown that the direct product of groups G_1 and G_2 with $|G_1|$ and $|G_2|$ distinct characters has $|G_1|\cdot|G_2|$ characters allows us to show by induction that all groups of the form

$$\mathbb{Z}_{N_1}\times\mathbb{Z}_{N_2}\times\mathbb{Z}_{N_3}\times\cdots\times\mathbb{Z}_{N_k}$$

for $N_1, N_2, \ldots, N_k \in \mathbb{N}$ have

$$N_1\cdot N_2\cdot\cdots\cdot N_k = |\mathbb{Z}_{N_1}\times\mathbb{Z}_{N_2}\times\mathbb{Z}_{N_3}\times\cdots\times\mathbb{Z}_{N_k}|$$

distinct characters.

By the Structure Theorem, all finite Abelian groups are isomorphic to such a group, and hence have a unique Fourier transform, up to a permutation of the basis elements and global phase.

For the case of $G = (\mathbb{Z}_2)^n$, we know what the characters are for $\mathbb{Z}_2$. The n-fold product of this group is obtained by taking n independent copies:

$$\chi_y(x) = \Pi_j\chi_{y_j}(x_j)) = \Pi_j(-1)^{x_jy_j} = (-1)^{x\cdot y}$$

3.3.3 Putting Things Together

We reviewed the classical Fourier Transform, and extracted 3 important properties of it:

1. Linear transformation
2. Is unitary
3. Transforms convolutions into point wise products.

We defined Fourier Transform over general group as any transformation that has these three properties. We showed that in the case of finite Abelian groups, the Fourier Transform exists and is unique.