COMP760, LECTURES 2,3: FOURIER ANALYSIS OF FINITE ABELIAN GROUPS

HAMED HATAMI

In this lecture we develop the basic Fourier analysis of finite Abelian groups. Recall that the cyclic group $\mathbb{Z}_N$ is the Abelian group with elements $\{0, 1, \ldots, N-1\}$, where the group product is defined as $a + b := a + b \pmod N$. Finite Abelian groups can be characterized as the products of cyclic groups:

Theorem 0.1. *Every finite Abelian group G is isomorphic to the group $\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$ for some positive integers $N_1, \ldots, N_k$.*

In this course, we will be mostly interested in the group $\mathbb{Z}_2^n$ as it can be identified with the set $\{0,1\}^n$. Hence boolean functions $f : \{0,1\}^n \to \{0,1\}$ can be identified with functions $f : \mathbb{Z}_2^n \to \{0,1\}$, and this shall allow us to use Fourier analysis of $\mathbb{Z}_2^n$ to study boolean functions.

1. Basic Fourier Theory

Let G be a finite Abelian group. A function $\chi : G \to \mathbb{C} \setminus \{0\}$ mapping the group to the non-zero complex numbers is called a *character* of G if it is a group homomorphism. That is, $\chi(a + b) = \chi(a)\chi(b)$ for all $a, b \in G$, and $\chi(0) = 1$, where 0 is the identity of G. The constant function 1 is called the *principal character* of G.

Let χ be a character of G, and consider an element $a \in G$. Since G is a finite group, a is of some finite order n (that is $na = 0$). Hence $1 = \chi(0) = \chi(na) = \chi(a)^n$ which shows that $\chi(a)$ is an n-th root of unity. In particular, every character $\chi \in \widehat{G}$ satisfies

$$\chi : G \to \mathbb{T}, \tag{1}$$

where $\mathbb{T}$ is the unit complex circle.

Theorem 1.1. *If G is a finite Abelian group, then the characters of G together with the usual pointwise product of complex valued functions form a group $\widehat{G}$.*

Proof. The principal character 1 is the identity of $\widehat{G}$. Note that if χ and ξ are characters of G, then $\chi\xi$ is also a character. Indeed $\chi(ab)\xi(ab) = \chi(a)\xi(a)\chi(b)\xi(b)$, and $\chi(0)\xi(0) = 1 \times 1 = 1$. To check the existence of the inverse element, note that if χ is a character, then $\chi^{-1} = \frac{1}{\chi} = \overline{\chi}$ is also a character. □

The group $\widehat{G}$ is called the *Pontryagin dual* of G. Fourier analysis is based on expressing functions $f : G \to \mathbb{C}$ as linear combinations of characters. It will be convenient to treat the set of these functions as a Hilbert space: Let $L_2(G)$ denote the set of functions $f : G \to \mathbb{C}$, where here G is endowed with the uniform probability measure. Recall (see Lecture 1, Section 3.1) that $L_2(G)$ is a Hilbert space with the inner product

$$\langle f, g \rangle = \mathbb{E}_{x \in G} f(x)\overline{g(x)} = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}.$$

In the sequel we will usually consider G as a probability space, and $\mathbb{E}_{x\in G}$ shall always mean that x is a random variable that takes values in G uniformly at random. To simplify the notation we usually abbreviate $\mathbb{E}_{x\in G}$ to simply $\mathbb{E}$. Hence for a function $f : G \to \mathbb{C}$, the notation $\mathbb{E}[f]$ means $\mathbb{E}_{x\in G}[f(x)]$ (which is equal to $\frac{1}{|G|}\sum_{x\in G} f(x)$).

Our next goal will be to prove that the characters form an orthonormal basis for this space. First let us prove a simple lemma.

Lemma 1.2. *Let G be a finite Abelian group, and χ be a non-principal character of G. Then $\sum_{x\in G}\chi(x) = 0$.*

Proof. Suppose to the contrary that $\sum_{x\in G}\chi(x) \neq 0$. Consider an arbitrary $y \in G$. Then We have

$$\chi(y)\sum_{x\in G}\chi(x) = \sum_{x\in G}\chi(y+x) = \sum_{x\in G}\chi(x)$$

which shows that $\chi(y) = 1$. Since y was arbitrary, we conclude that χ must be the principal character which is a contradiction. □

Now we can prove the orthogonality properties of the characters.

Lemma 1.3. *The characters of a finite Abelian group G are orthonormal functions in $L_2(G)$.*

Proof. It follows from (1) that every $\chi \in \widehat{G}$ satisfies

$$\|\chi\|_2^2 = \mathbb{E}\left[|\chi(x)|^2\right] = \mathbb{E}[1] = 1.$$

So characters are unit vectors in $L_2(G)$. It remains to verify the orthogonality. Let $\chi \neq \xi$ be two different characters. Then $\chi\overline{\xi} = \chi\xi^{-1}$ is a non-principal character of G. Hence by Lemma 1.2, we have

$$\langle \chi, \xi\rangle = \mathbb{E}\left[\chi(x)\overline{\xi}(x)\right] = \mathbb{E}\left[\chi\overline{\xi}(x)\right] = 0.$$

□

So far we have discussed the Pontryagin dual of G in an abstract manner. Since finite Abelian groups have simple structures (Theorem 0.1), it is quite easy to describe the characters of G. We start with the basic case of $G = \mathbb{Z}_N$. For every $a \in \mathbb{Z}_N$, define $\chi_a \in L_2(G)$ as

$$\chi_a : x \mapsto e^{\frac{2\pi i}{N}ax}.$$

Let us verify that χ_a is actually a character. Indeed $\chi_a(0) = e^{\frac{2\pi i}{N}0} = e^0 = 1$, and since $e^{2\pi i} = 1$, we have

$$\chi_a(x)\chi_a(y) = e^{\frac{2\pi i}{N}ax}e^{\frac{2\pi i}{N}ay} = e^{\frac{2\pi i}{N}a(x+y \pmod N)} = \chi_a(x+y).$$

Note that $L_2(G)$ is $|G|$-dimensional, and hence by Lemma 1.3, G has at most $|G|$ characters. It follows that $\{\chi_a : a \in G\}$ are all the characters of G. The principal character is $\chi_0 = 1$. Also $\chi_a\chi_b = \chi_{a+b}$ which shows that the dual group $\widehat{G}$ is isomorphic to G. As we shall see below this is in general true for all finite Abelian groups.

Now let us consider the general case of $G = \mathbb{Z}_{N_1} \times \ldots \mathbb{Z}_{N_k}$ for some positive integers $N_1, \ldots, N_k$. For every $a = (a_1, \ldots, a_k) \in G$, define $\chi_a \in L_2(G)$ as

$$\chi_a : x \mapsto \prod_{i=1}^{k} e^{\frac{2\pi i}{N_i}a_i x_i}.$$

As in the case of $\mathbb{Z}_N$, it is straightforward to verify that χ_a is a character by showing that $\chi_a(0) = 1$, and $\chi_a(x+y) = \chi_a(x)\chi_a(y)$. Again Lemma 1.3 shows that $\{\chi_a : a \in G\}$ are all the characters of G. We also have the identify $\chi_a\chi_b = \chi_{a+b}$ which proves Theorem 1.4.

Theorem 1.4. *If G is a finite Abelian group, then the characters of G form an orthonormal basis for $L_2(G)$. Furthermore we have $\widehat{G} \cong G$.*

Before continuing further, let us look at the characters of our favorite group $\mathbb{Z}_2^n$. Consider an element $a \in \mathbb{Z}_2^n$. Then

$$\chi_a(x) = e^{\frac{2\pi i}{2}\sum_{i=1}^n a_i x_i} = (-1)^{\sum_{i=1}^n a_i x_i}.$$

Note that in this case the characters are actually real valued (they only take values 1 and -1). Since the coordinates of a are 0 or 1, we will sometimes identify a with the set $S = \{j \in \{1, \ldots, n\} : a_j = 1\}$, and denote the characters as χ_S for $S \subseteq \{1, \ldots, n\}$. This notation is sometimes more intuitive as

$$\chi_a(x) = e^{\frac{2\pi i}{2}\sum_{i=1}^n a_i x_i} = (-1)^{\sum_{i=1}^n a_i x_i} = (-1)^{\sum_{i \in S} x_i}.$$

Later when we take a probabilistic approach to decomposing functions, this notation becomes more natural as it extends to general product spaces (where there is no group structure).

Definition 1.5. *The Fourier transform of a function $f : G \to \mathbb{C}$ is the unique function $\widehat{f} : \widehat{G} \to \mathbb{C}$ defined as*

$$\widehat{f}(\chi) = \langle f, \chi \rangle = \mathbb{E} f(x)\overline{\chi(x)}.$$

Theorem 1.4 shows that G is isomorphic to its dual $\widehat{G}$, and so it shall be convenient to identify the two groups in the sequel. Let us restate Definition 1.5 in this new notation.

Definition 1.6 (Definition 1.5 Restated)**.** *The Fourier transform of a function $f : G \to \mathbb{C}$ is the unique function $\widehat{f} : G \to \mathbb{C}$ defined as*

$$\widehat{f}(a) = \langle f, \chi_a \rangle = \mathbb{E} f(x)\overline{\chi_a(x)}.$$

Let us state a simple example of the Fourier transform of a function on $\mathbb{Z}_2^n$.

Example 1.7. Let $f : \mathbb{Z}_2^n \to \mathbb{C}$ be the parity function $f : x \mapsto \sum_{i=1}^n x_i (\text{mod } 2)$. Then

$$\widehat{f}(0) = \mathbb{E} f(x)\chi_0 = \mathbb{E} f(x) = \frac{1}{2}.$$

We also have

$$\widehat{f}(1, \ldots, 1) = \mathbb{E} f(x)(-1)^{\sum_{j=1}^n x_j} = -\frac{1}{2},$$

as $f(x) = 1$ if and only if $\sum_{j=1}^n x_j = 1(\text{mod } 2)$. Next consider $a \in \mathbb{Z}_2^n$ with $a \neq (1, \ldots, 1)$ and $a \neq 0$. Let j_0, j_1 be such that $a_{j_0} = 0$ and $a_{j_1} = 1$. We have (why?)

$$\widehat{f}(a) = \mathbb{E} f(x)\chi_a(x) = \frac{1}{2}\mathbb{E}\left[f(x)\chi_a(x) + f(x + e_{j_0} + e_{j_1})\chi_a(x + e_{j_0} + e_{j_1})\right],$$

where e_j denotes the vector in $\mathbb{Z}_2^n$ which has 1 at its jth coordinate and 0 everywhere else. Note that $f(x) = f(x + e_{j_0} + e_{j_1})$ and furthermore $\chi_a(x) = -\chi_a(x + e_{j_0} + e_{j_1})$. We conclude that $\widehat{f}(a) = 0$ for every $a \in \mathbb{Z}_2^n$ satisfying $a \neq (1, \ldots, 1)$ and $a \neq 0$. ■

Lecture 3

The Fourier transform is a linear operator: $\widehat{\lambda f + g} = \lambda \widehat{f} + \widehat{g}$, and we have the following easy observation.

Lemma 1.8. *The Fourier transform considered as an operator from $L_1(G)$ to $L_\infty(\widehat{G})$ is norm decreasing:*

$$\|\widehat{f}\|_\infty \leq \|f\|_1.$$

Proof. By (1) for every $a \in G$, we have

$$|\widehat{f}(a)| = \left|\mathbb{E} f(x)\overline{\chi_a(x)}\right| \leq \mathbb{E}|f(x)||\overline{\chi_a(x)}| = \mathbb{E}|f(x)| = \|f\|_1.$$

□

The Fourier coefficient $\widehat{f}(0)$ is of particular importance as

$$\widehat{f}(0) = \mathbb{E}[f(x)].$$

So if 1_S is the indicator function of a subset $1_S \subseteq G$, then $\widehat{1_S}(0) = \frac{|S|}{|G|}$ corresponds to the density of S.

It follows from the fact that the characters from an orthonormal basis for $L_2(G)$ that

$$f = \sum_{a \in G} \widehat{f}(a)\chi_a,$$

and that this expansion of f as a linear combination of characters is unique. This formula is called the *Fourier inversion formula* as it shows how the functions f can be reconstructed from its Fourier transform.

If $S \subseteq G$, then the orthogonal complement of S is defined as

$$S^\perp = \{a \in G : \chi_a(x) = 1 \ \forall x \in S\}.$$

It follows from the identities $\chi_0 = 1$ and $\chi_a \chi_b = \chi_{a+b}$ that $S^\perp$ is a subgroup of G. The Fourier transform of the indicator function of a subgroup of G has a simple form:

Lemma 1.9. *If H is a subgroup of G, then for every $a \in G$, we have*

$$\widehat{1_H}(a) = \begin{cases} |H|/|G| & a \in H^\perp \\ 0 & a \notin H^\perp \end{cases}$$

Proof. If $a \in H^\perp$, then

$$\widehat{1_H}(a) = \langle 1_H, \chi_a \rangle = \mathbb{E} 1_H(x)\overline{\chi_a(x)} = \mathbb{E} 1_H(x) = |H|/|G|.$$

On the other hand if $a \notin H^\perp$, then there exists $y \in H$ such that $\chi_a(y) \neq 1$. Then

$$\sum_{z \in H} \overline{\chi_a(z)} = \chi_a(y) \sum_{z \in H} \overline{\chi_a(z-y)} = \chi_a(y) \sum_{z \in H} \overline{\chi_a(z)},$$

which shows that $\sum_{z \in H} \overline{\chi_a(z)} = 0$. Hence

$$\widehat{1_H}(a) = \mathbb{E} 1_H(x)\overline{\chi_a(x)} = \frac{1}{|G|} \sum_{z \in H} \mathbb{E} 1_H(z) = 0.$$

□

Remark 1.10. It follows from Lemma 1.9 that if $S = y + H$ is a coset of H in G (i.e. H is a subgroup of G and $y \in G$), then for every $a \in G$,

$$\begin{aligned}\widehat{1_S}(a) &= \mathbb{E}1_S(x)\overline{\chi_a(x)} = \mathbb{E}1_H(x-y)\overline{\chi_a(x)} = \mathbb{E}1_H(x)\overline{\chi_a(x+y)} = \overline{\chi(y)}\widehat{1_H}(a) \\ &= \begin{cases} \overline{\chi(y)}|H|/|G| & a \in H^\perp \\ 0 & a \notin H^\perp \end{cases}\end{aligned}$$

■

Example 1.11. Let us revisit Example 1.7 in light of Remark 1.10. Note that $H = \{x \in \mathbb{Z}_2^n : \sum_{i=1}^n x_i = 0 \pmod 2\}$ is a subgroup of $\mathbb{Z}_2^n$. Now the function f defined in Example 1.7 is the indicator function of $S = e_1 + H$. Note that

$$H^\perp = \{a : (-1)^{\sum_{i=1}^n x_i a_i} = 1 \ \forall x \in H\} = \{(0,\ldots,0),(1,\ldots,1)\}.$$

Hence

$$\widehat{f}(a) = \widehat{1_S}(a) = \begin{cases} \overline{\chi_a(e_1)}|H|/|G| & a \in H^\perp \\ 0 & a \notin H^\perp \end{cases}$$

We conclude that $\widehat{f}(0) = 1/2$ and $\widehat{f}(1,\ldots,1) = -1/2$, and $\widehat{f}(a) = 0$ for every $a \in \mathbb{Z}_2^n$ satisfying $a \neq (1,\ldots,1)$ and $a \neq 0$. ■

Theorem 1.12 (Parseval)**.** *For every $f \in L_2(G)$,*

$$\|f\|_2^2 = \sum_{a \in G} |\widehat{f}(a)|^2.$$

Proof. We have

$$\|f\|_2^2 = \langle f, f\rangle = \left\langle \sum_{a\in G} \widehat{f}(a)\chi_a, \sum_{b \in G}\widehat{f}(b)\chi_b \right\rangle = \sum_{a,b\in G} \widehat{f}(a)\overline{\widehat{f}(b)}\langle \chi_a, \chi_b\rangle.$$

The identify now follows from orthonormality of characters:

$$\langle \chi_a, \chi_b \rangle = \begin{cases} 0 & a \neq b; \\ 1 & a = b. \end{cases}$$

□

The proof of the Parseval identity, when applied to two different functions $f, g \in L_2(G)$, implies the *Plancherel theorem*:

$$\langle f, g\rangle = \sum_{a\in G} \widehat{f}(a)\overline{\widehat{g}(a)}.$$

As the first example of an application of the Parseval identity, let us show that for every subgroup H of G, we have

$$|H||H^\perp| = |G|. \tag{2}$$

Indeed by Lemma 1.9, we have

$$\frac{|H|}{|G|} = \mathbb{E}1_H = \mathbb{E}1_H^2 = \langle 1_H, 1_H\rangle = \|1_H\|_2^2 = \sum_{a\in G}|\widehat{1_H}(a)|^2 = \sum_{a \in H^\perp}(|H|/|G|)^2 = \frac{|H|^2|H^\perp|}{|G|^2}$$

which simplifies to (2).

Next we introduce the important notion of *convolution*.

Definition 1.13. *Let G be a finite Abelian group. For two functions $f, g : G \to \mathbb{C}$, we define their convolution $f * g : G \to \mathbb{C}$ as*

$$f * g(x) = \mathbb{E}_{y \in G}[f(x-y)g(y)].$$

Note that $f * g(x)$ is the average of $f(a)f(b)$ over all pairs a, b with $a + b = x$. This gives a combinatorial nature to convolution which makes it very useful in dealing with certain discrete problems. Consider a set $S \subseteq G$. Then $f * 1_S(x)$ is the average of f over the set $x - S := \{x - y : y \in S\}$. For example if S is the Hamming ball[1] of radius r around 0 in $\mathbb{Z}_2^n$, then $f * 1_S(x)$ is the average of f over the Hamming ball of radius r around x. These types of averaging operators usually "smooth" f, and makes it more similar to a constant functions. This smoothing property of the convolution is one of the main tools in harmonic analysis and this course.

Next let us list some basic facts about the convolution. We define the *support* of $f : G \to \mathbb{C}$, denoted by $\mathrm{Supp}(f)$, to be the set of the points $x \in G$ with $f(x) \neq 0$.

Lemma 1.14. *Consider three functions $f, g, h : G \to \mathbb{C}$.*

(a) *We have*

$$f * g = g * f.$$

(b) *We have*

$$(f * g) * h = f * (g * h).$$

(c) *We have*

$$f * (\lambda h + g) = \lambda f * h + f * g.$$

(d) *We have*

$$\mathrm{Supp}(f + g) \subseteq \mathrm{Supp}(f) + \mathrm{Supp}(g).$$

(e) *We have*

$$\|f * g\|_\infty \leq \|f\|_1 \|g\|_\infty.$$

(f) *More generally, if p and q are conjugate exponents, then*

$$\|f * g\|_\infty \leq \|f\|_p \|g\|_q.$$

(g) *We have*

$$\|f * g\|_1 \leq \|f\|_1 \|g\|_1.$$

Proof. **(a)** For every $x \in G$, we have

$$f * g(x) = \mathbb{E}_y[f(x-y)g(y)] = \mathbb{E}_y[f(x-y)g(x-(x-y))] = \mathbb{E}_z[f(z)g(x-z)] = g * f(x).$$

(b) By Part **(a)**,

$$\begin{aligned} (f * g) * h(x) &= (g * f) * h(x) = \mathbb{E}_z \mathbb{E}_y [g(x-z-y)f(y)]h(z) = \\ &= \mathbb{E}_{y,z} g(x-z-y)f(y)h(z) = (h * g) * f(x) = f * (g * h)(x). \end{aligned}$$

(c) is trivial.

(d) follows from the fact that $f(x)$ is the average of $f(a)g(b)$ over all pairs of points $a, b \in G$ with $a + b = x$.

(e) is a special case of **(f)**.

(f) Note that for every $x \in G$, by Hölder's inequality we have

$$|f * g(x)| \leq \mathbb{E}_{y \in G}|f(x-y)||g(y)| \leq \left(\mathbb{E}|f(x-y)|^p\right)^{1/p} \left(\mathbb{E}|g(y)|^q\right)^{1/q} = \left(\mathbb{E}|f(y)|^p\right)^{1/p} \|g\|_q = \|f\|_p \|g\|_q.$$

(g) We have

$$\|f * g\|_1 = \mathbb{E}_x |f * g(x)| \leq \mathbb{E}_{x,y}|f(x-y)||g(y)| = \mathbb{E}_{z,y}|f(z)||g(y)| = \mathbb{E}_z|f(z)|\mathbb{E}_y|g(y)| = \|f\|_1 \|g\|_1.$$

[1] The Hamming ball of radius r around 0 is defined as $\{x \in \mathbb{Z}_2^n : \sum_{i=1}^n x_i \leq r\} \subseteq \mathbb{Z}_2^n$.

□

The relevance of the Fourier transform to convolution lies in the following lemma.

Lemma 1.15. *If $f, g : G \to \mathbb{C}$, then*
$$\widehat{f * g} = \widehat{f} \cdot \widehat{g}.$$

Proof. We have
$$\begin{aligned}
\widehat{f * g}(a) &= \mathbb{E}_x f * g(x)\overline{\chi_a(x)} = \mathbb{E}_x \left(\mathbb{E}_y f(x-y)g(y)\right)\overline{\chi_a(x)} = \mathbb{E}_{x,y} f(x-y)g(y)\overline{\chi_a(x-y)\chi_a(y)} \\
&= \mathbb{E}_{z,y} f(z)g(y)\overline{\chi_a(z)\chi_a(y)} = \mathbb{E}_z f(z)\overline{\chi_a(z)}\mathbb{E}_y g(y)\overline{\chi_a(y)} = \widehat{f}(a)\cdot\widehat{g}(a).
\end{aligned}$$

□

Note that Lemma 1.15 in particular shows that
$$\mathbb{E}f(x)\mathbb{E}g(x) = \widehat{f}(0)\widehat{g}(0) = \widehat{f * g}(0) = \mathbb{E}f * g(x).$$
We also have the dual version of Lemma 1.15,
$$\widehat{f \cdot g}(x) = \sum_{y \in G} \widehat{f}(x-y)\widehat{g}(y), \tag{3}$$
which converts pointwise product back to convolution.

Exercise 1.16. Prove the Identity (3). ■

For a function $h : G \to \mathbb{C}$, define $\tilde{h} : G \to \mathbb{C}$ as $h : x \mapsto \overline{h(-x)}$. Note that $\tilde{h} = \sum_{a \in G} \overline{\widehat{h}(a)}\chi_a$. Hence it follows from the Parseval identity and Lemma 1.15 that for $f, g, h : G \to \mathbb{C}$, we have
$$\langle f * h, g\rangle = \langle f, g * \tilde{h}\rangle = \sum_{a \in G} \widehat{f}(a)\widehat{h}(a)\overline{\widehat{g}(a)}.$$

School of Computer Science, McGill University, Montréal, Canada
E-mail address: hatami@cs.mcgill.ca