1 Fourier Analysis on Groups

Let’s $G$ be a finite abelian group

**Example 1.** $\mathbb{Z}_2^n$, $\mathbb{Z}_p$, $\mathbb{Z}_p^n$

The crux of this section is to consider the set consisting of all the functions

$$f : G \rightarrow \mathbb{C}$$

For $\mathbb{C}$-vector space and dim $= |G|$.

1.1 Fourier basis

A function $\chi : G \rightarrow \mathbb{C}$ is called a character if $\chi$ is a homomorphism from $G$ to $\mathbb{C}^X$.

$$\chi(a + b) = \chi(a) + \chi(b), \forall a, b \in G$$

**Example 2.**

- $G = \mathbb{Z}_p = \{0, 1, \ldots, p - 1\}$ and $a$ is any element of $\mathbb{Z}_p$

  $$\chi_a(j) = e^{2\pi i aj/p} = \omega^{aj}$$

  Where $\omega$ is $p^{th}$ root of unity. This gives us all characters of $\mathbb{Z}_p$, $p$ of them. We can add a remark denoting that:

  $$\chi_a \chi_b(x) = \chi_{a+b}(x)$$

  Which is the group of character (Hom).
• \( G = \mathbb{Z}_2^n = \{(x_1, \ldots, x_n) | \text{each } x_n \in \mathbb{Z} - 2\} \). The homomorphism gives us that for any \( \chi \) we should have the following:

\[
\begin{align*}
\chi(1,0,0,\ldots,0) & \in \{\pm 1\} \\
\chi(0,1,0,\ldots,0) & \in \{\pm 1\} \\
\chi(1,1,0,\ldots,0) & \in \{\pm 1\} \\
\vdots \\
\end{align*}
\]

Hence, \( \chi_S(x_1, \ldots, x_n+ \) = \[
\begin{cases}
+1 & \text{if } \# \text{’s in } \chi \text{ is even} \\
-1 & \text{if } \# \text{’s in } \chi \text{ is odd}
\end{cases}
\]

We need to check that \( \chi_S(x + y) = \chi_S(x) + \chi_S(y) \). For a general collection of characters, pick \((a_1, \ldots, a_n) \in \mathbb{Z}_2^n\) and define \( \chi_a(x) = (-1)^{\sum_{i=1}^n a_i x_i} \). Therefore, we have the following:

\[
\chi_a(x + y) = (-1)^{\sum_{i=1}^n a_i (x_i + y_i)} = (-1)^{\sum_{i=1}^n a_i x_i} + (-1)^{\sum_{i=1}^n a_i y_i} = \chi_a(x) \cdot \chi_a(y)
\]

**Remark 3.** \( \mathbb{R}/\mathbb{Z} \) is the circle. \( \chi : \mathbb{R}/\mathbb{Z} \to \mathbb{C}^X \). For \( n \in \mathbb{Z} \) we have \( \chi_n(x) = e^{2\pi i n x} \)

**Lemma 4.** Let \( G \) be a finite abelian group. \( \chi, \chi' \) be characters of \( G \). Then:

\[
\mathbb{E}_{x \in G} [\chi(x) \overline{\chi'(x)}] = \begin{cases} 1 & \text{if } \chi = \chi' \\ 0 & \text{otherwise} \end{cases}
\]

Here, we consider \( \mathbb{E} \) to be the average on the cardinality of \( G \). Since \( \chi \chi' \) is also a character of \( G \) since if \( \omega \) is a root of unity then \( \bar{\omega} = \omega^{-1} \). Hence, if we can denote it by \( \chi \overline{\chi'} = \psi \), we have the following:

\[
\mathbb{E}_{x \in G} [\psi(x)] = \begin{cases} 1 & \text{if } \psi \equiv 1 \\ 0 & \text{otherwise} \end{cases}
\]

**Proof.**

\[
\mathbb{E}_{x \in G} [\psi(x)] = \frac{1}{|G|} \sum_{x \in G} \psi(x)
= \frac{1}{|G|} \sum_{x \in G} \psi(x \cdot y)
= \frac{1}{|G|} \psi(y) \left( \sum_{x \in G} \psi(x) \right)
\]

\( \implies \forall y, (\psi(y) - 1)(\sum \psi(x)) = 0 \). Therefore, if \( \psi \not\equiv 1 \), then \( \sum_{x \in G} \psi(x) = 0 \)

So for \( G \in \mathbb{Z}_2^n, G = \mathbb{Z}_p \)

\[
\{\chi_a | a \in \mathbb{Z}_2^n\}
\]
{\chi_a | a \in \mathbb{Z}^p}

Form orthonormal basis for function \( \{ f : G \to \mathbb{C} \} \). Thus, for any \( f : G \to \mathbb{C} \) we can write

\[
f = \sum_{a \in \mathbb{Z}^p} \hat{f}(a) \chi_a
\]

Where \( \hat{f}(a) = \langle f, x \rangle = \mathbb{E}_{x \in G} [f(x) \bar{\chi}_a(x)] \)
\( \hat{f} : \mathbb{Z}_p^n \to \mathbb{C} \) is called the Fourier transform.

### 1.2 Perseval’s Identity

\[
\| f \|_2^2 = \mathbb{E}_{x \in G} [\| f(x) \|_2^2] = \sum_{a \in \mathbb{Z}^p} [\| \hat{f}(a) \|_2^2] = \| \hat{f} \|_2^2
\]

**Proof.**

\[
\sum_{a \in \mathbb{Z}^p} [\| \hat{f}(a) \|_2^2] = \sum_{a} [\mathbb{E}_{x}[f(x) \bar{\chi}_a(x)]^2]
\]

\[
= \sum_{a} [\mathbb{E}_{x}[f(x) \bar{\chi}_a(x)](\mathbb{E}_{x'}[\bar{\chi}_a(x')]])
\]

\[
= \sum_{a} (\mathbb{E}_{x,x'}[f(x) \bar{\chi}_a(x) \bar{\chi}_a(x')])
\]

\[
= \mathbb{E}_{x,x'}[\sum_a (f(x) \bar{\chi}_a(x) \bar{\chi}_a(x'))]
\]

Denote that if \( x = x' \), then \( \sum_a (\bar{\chi}_a(x) \chi_a(x')) = |G| \), else it is 0. Hence, we have:

\[
\| f \|_2^2 = \mathbb{E}_{x,x'}[f(x) \bar{\chi}_a(x) \chi_a(x')]
\]

\[
= \frac{1}{|G|^2} \sum_{x} [f(x)]^2(\mathbb{E}[\| f \|_2^2])
\]

Hence we have that \( \mathbb{E}_{x \in G} [\| f(x) \|_2^2] = \sum_{a \in \mathbb{Z}^p} [\| \hat{f}(a) \|_2^2] \) which gives us that \( \| f \|_2^2 = \| \hat{f} \|_2^2 \)

### 1.3 Convolution

For functions \( f : G \to \mathbb{C} \) and \( h : G \to \mathbb{C} \) we define the convolution to be a function \( f \ast h : G \to \mathbb{C} \) by given by the following:
\[
f \ast h(x) = \frac{1}{|G|} \sum_{y,z \text{ s.t. } y + z = x} f(y)h(z)
\]

We also have the following:

\[
\hat{f} \ast \hat{h}(a) = \mathbb{E}_{x \in G} [(f \ast h)(x)\check{\chi}_a(x)]
= \mathbb{E}_{x \in G} \left[ \sum_{y,z \text{ s.t. } y + z = x} f(y)h(z)\check{\chi}_a(y + z) \right]
= \frac{1}{|G|} \sum_{x} \frac{1}{|G|} \sum_{y,z \text{ s.t. } y + z = x} f(y)h(z)\check{\chi}_a(y + z)
= \frac{1}{|G|^2} \sum_{x} \sum_{y \text{ s.t. } z = x - y} f(y)h(x - y)\check{\chi}_a(y)\check{\chi}_a(x - y)
= \frac{1}{|G|^2} \sum_{y} \sum_{z} f(y)h(x - y)\check{\chi}_a(y)\check{\chi}_a(z)
= \frac{1}{|G|^2} (\sum_{y} f(y)\check{\chi}_a(y))(\sum_{z} h(z)\check{\chi}_a(z))
= \hat{f}(a) \cdot \hat{h}(a)
\]

This shows that it is indeed a homomorphism.

For \(A \subseteq G\) we have the following:

\[
1_A \ast 1_A(x) = \frac{1}{|G|} \sum_{y,z \text{ s.t. } y + z = x} 1_A(y)1_A(z)
= \frac{1}{|G|} \cdot \# \text{ ways of writing } x \text{ as } y + z \quad \text{ with } y \in A, \quad z \in A
= \begin{cases} > 0 & \text{if } x \in A + A \\ 0 & \text{if } x \notin A + A \end{cases}
\]

Where \(\text{support}(1_A \ast 1_A) = A + A\).
2 Linearity testing

Let f be a function:

\[ f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2 \]

Example 5.

1. \( f(x) \equiv 0 \)
2. \( f(x) = x_7 \)
3. \( f(x) = \sum_{i=1}^n x_i \)
4. \( f(x) = < a, x > \)

We want to check if f is a linear function by evaluating f at some points.

Remark 6. Need \( 2^n \) queries into f for the deterministic checks, and \( \Omega(2^n) \) queries into f for random checks with success probability 0.99.

2.1 BLR linearity test

Pick \( x, y \in \mathbb{Z}_2^n \) uniformly at random, and check if \( f(x) + f(y) = f(x + y) \)

Theorem 7.

1. If \( f(x) \) is linear, then the test accepts with probability 1;
2. If f differs in \( \epsilon 2^n \) evaluations from every linear function, then the test rejects with probability at least \( \epsilon \)

Proof. Take f such that it passes the test with probability at least \( 1 - \gamma \). Let \( F : \mathbb{Z}_2^n \rightarrow \mathbb{C} \) be a function defined by \( F(x) = (-1)^{f(x)} \)

Plan: express what we know in terms of \( \hat{F} \).

\[
1 - \gamma \leq \mathbb{E}_{x,y} \left( 1_{f(x+y)=f(x)+f(y)} \right) \\
= \mathbb{E}_{x,y} \left( \frac{1 + F(x + y)F(x)F(y)}{2} \right) \\
= \frac{1}{2} + \frac{1}{2} \mathbb{E}_{x,y} (F(x + y)F(x)F(y))
\]

Write \( F = \sum_a F(a)\chi_a \)
\[
\mathbb{E} (F(x + y)F(x)F(y)) = \mathbb{E} \left( \sum_{a} \hat{F}(a) \chi_a(x + y) \sum_{b} \hat{F}(b) \chi_b(x) \sum_{c} \hat{F}(c) \chi_c(y) \right)
\]
\[
= \mathbb{E} \left( \sum_{a,b,c} \hat{F}(a) \hat{F}(b) \hat{F}(c) \chi_a(x + y) \chi_b(x) \chi_c(y) \right)
\]
\[
= \sum_{a,b,c} (\hat{F}(a) \hat{F}(b) \hat{F}(c)) \mathbb{E}(\chi_a(x) \chi_b(y) \chi_c(y))
\]
\[
= \sum_{a,b,c} (\hat{F}(a) \hat{F}(b) \hat{F}(c)) \mathbb{E}(\chi_a(x) \chi_b(x)) \mathbb{E}(\chi_a(y) \chi_c(y))
\]
\[
= \sum_{a,b,c} (\hat{F}(a) \hat{F}(b) \hat{F}(c)) \delta_{ab} \delta_{ac}
\]
\[
= \sum_{a} \hat{F}(a)^3
\]

So, we obtained that
\[
1 - \gamma \leq \frac{1}{2} + \frac{1}{2} \sum_{a} \hat{F}(a)^3
\]
\[
1 - 2\gamma \leq \sum_{a} \hat{F}(a)^3
\]

WTS: if \(\sum_{a} \hat{F}(a)^3\) is close to 1, then exists some \(a\) s.t. \(f\) agrees with \(< a, \cdot >\) on most inputs.

Using Parseval’s equality we get that
\[
1 = \mathbb{E}(|F(x)|^2) = \sum_{a} |\hat{F}(a)|^2
\]

Therefore,
\[
1 - 2\gamma \leq \sum_{a} \hat{F}(a)^3 \leq \max_{a} \hat{F}(a) \left( \sum_{a} |\hat{F}(a)|^2 \right) = \max_{a} \hat{F}(a)
\]

Lemma 8. If \(|\{x : f(x) = < a, x >\}| = (1 - \delta)2^n\) then \(\hat{F}(a) = 1 - 2\delta\)

Proof.
\[
\hat{F}(a) = \mathbb{E}_x(F(x)\chi_a(x))
\]
\[
= \frac{1}{2^n} (\#\{x : f(x) = < a, x >\} - \#\{x : f(x) \neq < a, x >\})
\]
\[
= \frac{1}{2^n} ((1 - \delta)2^n - \delta 2^n) = 1 - 2\delta
\]
So \( \max_a \hat{F}(a) \geq 1 - 2\gamma \), for that \( a \) the set:

\[
|\{x : f(x) = \langle a, x \rangle\}| \geq (1 - \gamma)2^n
\]