Lecture 8: Theory of Fourier analysis on finite abelian groups, BLR linearity test

Combinatorial Methods (Winter 2023)
University of Toronto
Swastik Kopparty
Scribes: Félix Gélinas and Alexey Zamozhskiy

1 Fourrier 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

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

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

1.1 Fourrier basis

A function $\chi : G \to \mathbb{C}$ is called a character if χ 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* $\mathbb{Z}_p$

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

Where ω *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).

- $G = \mathbb{Z}_2^n = \{(x_1, \ldots, x_n) |$ *each* $x_n \in \mathbb{Z} - 2\}$. *The homomorphism gives us that for any* χ *we should have the following:*

$$\chi(1, 0, 0, \ldots, 0) \in \{\pm 1\}$$
$$\chi(0, 1, 0, \ldots, 0) \in \{\pm 1\}$$
$$\chi(1, 1, 0, \ldots, 0) \in \{\pm 1\}$$
$$\vdots$$

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

We need to check that $\chi_S(x+y) = \chi_S(x) + \chi_S(y)$. *For a general collection of characters, pick* $(a_1, \ldots, a_n) \in \mathbb{Z}_2^p$ *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.* χ, χ' *be characters of* G. *Then:*

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

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

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

Proof.

$$\begin{aligned} \mathop{\mathbb{E}}_{x \in G}[\psi(x)] &= \frac{1}{|G|} \sum_{x \in G} \psi(x) \\ &= \frac{1}{|G|} \sum_{x \in G} \psi(x \cdot y) \\ &= \frac{1}{|G|} \psi(y) (\sum_{x \in G} \psi(x)) \end{aligned}$$

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

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

$$\{\chi_a | a \in \mathbb{Z}_2^p\}$$

$$\{\chi_a | a \in \mathbb{Z}^p\}$$

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

$$f = \sum_{a \in \mathbb{Z}_2^n} \hat{f}(a)\chi_a$$

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 Fourrier transform.

1.2 Perseval's Identity

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

Proof.

$$\begin{aligned}
\sum_{a \in \mathbb{Z}_2^n}[|\hat{f}(a)|^2] =& \sum_a |\mathop{\mathbb{E}}_x[f(x)\bar{\chi_a}(x)]|^2 \\
=& \sum_a (\mathop{\mathbb{E}}_x[f(x)\bar{\chi_a}(x)])(\mathop{\mathbb{E}}_{x'}[\bar{f}(x')\chi_a(x')]) \\
=& \sum_a (\mathop{\mathbb{E}}_{x,x'}[f(x)\bar{f}(x')\bar{\chi_a}(x)\chi_a(x')]) \\
=& \mathop{\mathbb{E}}_{x,x'}[\sum_a (f(x)\bar{f}(x')\bar{\chi_a}(x)\chi_a(x'))] \\
=& \mathop{\mathbb{E}}_{x,x'}[f(x)\bar{f}(x')\sum_a (\bar{\chi_a}(x)\chi_a(x'))]
\end{aligned}$$

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

$$\begin{aligned}
\|f\|_2^2 =& \mathop{\mathbb{E}}_{x,x'}[f(x)\bar{f}(x')\sum_a (\bar{\chi_a}(x)\chi_a(x'))] \\
=& \frac{1}{|G|^2}\sum |f(x)|^2(|G|) \\
=& \mathop{\mathbb{E}}_{x \in G}[|f(x)|^2]
\end{aligned}$$

Hence we have that $\mathbb{E}_{x \in G}[|f(x)|^2] = \sum_{a \in \mathbb{Z}_2^n}[|\hat{f}(a)|^2]$ 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 $f * h : G \to \mathbb{C}$ by given by the following:

$$f * h(x) = \frac{1}{|G|} \sum_{\substack{y,z \ s.t. \\ y+z=x}} f(y)h(z)$$

We also have the following:

$$\begin{aligned}
\widehat{f * h}(a) &= \mathop{\mathbb{E}}_{x \in G}[(f*h)(x)\bar{\chi_a}(x)] \\
&= \mathop{\mathbb{E}}_{x \in G}[\sum_{\substack{y,z \ s.t. \\ y+z=x}} f(y)h(z)\bar{\chi_a}(x)] \\
&= \frac{1}{|G|} \sum_x \frac{1}{|G|} \sum_{\substack{y,z \ s.t. \\ y+z=x}} f(y)h(z)\bar{\chi_a}(y+z)] \\
&= \frac{1}{|G|^2} \sum_x \sum_{\substack{y \ s.t. \\ z=x-y}} f(y)h(z)\bar{\chi_a}(y+z)] \\
&= \frac{1}{|G|^2} \sum_y \sum_x f(y)h(x-y)\bar{\chi_a}(y)\bar{\chi_a}(x-y)] \\
&= \frac{1}{|G|^2} \sum_y \sum_z f(y)h(x-y)\bar{\chi_a}(y)\bar{\chi_a}(z)] \\
&= \frac{1}{|G|^2} (\sum_y f(y)\bar{\chi_a}(y))(\sum_z h(z)\bar{\chi_a}(z))] \\
&= \hat{f}(a) \cdot \hat{h}(a)
\end{aligned}$$

This shows that it is indeed a homomorphism.

For $A \subseteq G$ we have the following:

$$\begin{aligned}
1_A * 1_A(x) &= \frac{1}{|G|} \sum_{\substack{y,z \ s.t. \\ y+z=x}} 1_A(y)1_A(z) \\
&= \frac{1}{|G|} \cdot \# \ ways \ of \ writting \ x \ as \begin{matrix} y+z \\ y \in A \\ z \in A \end{matrix} \\
&= \begin{cases} > 0 & if \ x \in A + A \\ = 0 & if \ x \notin A + A \end{cases}
\end{aligned}$$

Where $\text{support}(1_A * 1_A) = A + A$.

2 Linearity testing

Let f be a function:

$$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$$

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* ϵ*;*

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

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

$$\begin{aligned}
1 - \gamma &\leq \mathop{\mathbb{E}}_{x,y}(\mathbf{1}_{f(x+y)=f(x)+f(y)}) \\
&= \mathop{\mathbb{E}}_{x,y}(\frac{1 + F(x+y)F(x)F(y)}{2}) \\
&= \frac{1}{2} + \frac{1}{2}\mathop{\mathbb{E}}_{x,y}(F(x+y)F(x)F(y))
\end{aligned}$$

Write $F = \sum_a F\hat{(}a)\chi_a$

$$
\begin{aligned}
\mathop{\mathbb{E}}_{x,y}(F(x+y)F(x)F(y)) &= \mathop{\mathbb{E}}_{x,y}(\sum_a \hat{F}(a)\chi_a(x+y)\sum_b \hat{F}(b)\chi_b(x)\sum_c \hat{F}(c)\chi_c(y)) \\
&= \mathop{\mathbb{E}}_{x,y}(\sum_{a,b,c} \hat{F}(a)\hat{F}(b)\hat{F}(c)\chi_a(x+y)\chi_b(x)\chi_c(y)) \\
&= \sum_{a,b,c}(\hat{F}(a)\hat{F}(b)\hat{F}(c))\,\mathbb{E}(\chi_a(x)\chi_a(y)\chi_b(x)\chi_c(y)) \\
&= \sum_{a,b,c}(\hat{F}(a)\hat{F}(b)\hat{F}(c))\,\mathbb{E}(\chi_a(x)\chi_b(x))\,\mathbb{E}(\chi_a(y)\chi_c(y)) \\
&= \sum_{a,b,c}(\hat{F}(a)\hat{F}(b)\hat{F}(c))\delta_{ab}\delta_{ac} \\
&= \sum_a \hat{F}(a)^3
\end{aligned}
$$

So, we obtained that

$$1-\gamma \le \frac{1}{2}+\frac{1}{2}\sum_a \hat{F}(a)^3$$

$$1-2\gamma \le \sum_a \hat{F}(a)^3$$

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

$$1 = \mathop{\mathbb{E}}_x(|F(x)|^2) = \sum_a |\hat{F}(a)|^2$$

Therefore,

$$1-2\gamma \le \sum_a \hat{F}(a)^3 \le \max_a \hat{F}(a)(\sum_a |\hat{F}(a)|^2) = \max_a \hat{F}(a)$$

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

Proof.

$$\hat{F}(a) = \mathop{\mathbb{E}}_x(F(x)\chi_a(x))$$

$$= \frac{1}{2^n}(\#\{x : f(x) =< a, x >\} - \#\{x : f(x) \ne< a, x >\})$$

$$= \frac{1}{2^n}((1-\delta)2^n - \delta 2^n) = 1-2\delta$$

□

So $\max_a \hat{F}(a) \geq 1 - 2\gamma$, for that a the set:

$$|\{x : f(x) =< a, x >\}| \geq (1 - \gamma)2^n$$

$\square$