Part III – Introduction to Additive Combinatorics (Incomplete)

Based on lectures by Prof Julia Wolf
Notes taken by Yaël Dillies

Lent 2024

Contents

1 Fourier-analytic techniques

Lecture 1

Let $G = \mathbb{F}_p^n$ where p is a small fixed prime and n is large.

Notation. Given a finite set B and any function $f : B \to \mathbb{C}$, write

$$\mathbb{E}_{x\in B} f(x) = \frac{1}{|B|} \sum_{x\in B} f(x)$$

Write $\omega = E^{\frac{\tau i}{p}}$. Note $\sum_{a\in\mathbb{F}_p} \omega^a = 0$.

Definition 1.1. Given $f : \mathbb{F}_p^n \to \mathbb{C}$, define its **Fourier transform** $\hat{f} : \mathbb{F}_p^n \to \mathbb{C}$ by

$$\hat{f}(t) = \mathbb{E}_{x\in\mathbb{F}_p^n} f(x)\omega^{x\cdot t}$$

It is easy to verify the **inversion formula**

$$f(x) = \sum_{t\in\mathbb{F}_p^n} \hat{f}(t)\omega^{-x\cdot t}$$

Indeed,

$$\begin{aligned}\sum_{t\in\mathbb{F}_p^n} \hat{f}\omega^{-x\cdot t} &= \sum_{t\in\mathbb{F}_p^n} \left(\mathbb{E}_y f(y)\omega^{y\cdot t}\right)\omega^{-x\cdot t} \\ &= \mathbb{E}_y f(y) \sum_t \omega^{(y-x)\cdot t} \\ &= \mathbb{E}_y f(y) 1_{y=x} p^n \\ &= f(x)\end{aligned}$$

Notation. Given a set A of a finite group G, write

- 1_A the *characteristic function* of A, ie

$$1_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

- μ_A the *characteristic measure* of A, ie

$$\mu_A = \alpha^{-1} 1_A$$

  where $\alpha = \frac{|A|}{|G|}$.

- f_A for the *balanced function* of A, ie

$$f_A(x) = 1_A(x) - \alpha$$

Note $\mathbb{E}_x f_A(x) = 0, \mathbb{E}_x \mu_A(x) = 1, \widehat{1_A}(0) = \mathbb{E}_x 1_A(x) = \alpha$. Writing $-A = \{-a | a \in A\}$, we have

$$\begin{aligned}\widehat{1_{-A}}(t) &= \mathbb{E}_x 1_{-A}(x)\omega^{x\cdot t} \\ &= \mathbb{E}_x 1_A(-x)\omega^{x\cdot t} \\ &= \mathbb{E}_x 1_A(x)\omega^{-x\cdot t} \\ &= \overline{\widehat{1_A}(t)}\end{aligned}$$

Example 1.2. Let $V \leq \mathbb{F}_p^n$. Then

$$\widehat{1_V}(t) = \mathbb{E}_x 1_V(x)\omega^{x \cdot t} = \frac{|V|}{|G|} 1_{V^\perp}(t)$$

So

$$\hat{\mu}_V(t) = 1_{V^\perp}(t)$$

Example 1.3. Let $R \subseteq \mathbb{F}_p^n$ be such that each x is included with probability $\frac{1}{2}$ independently. Then with high probability

$$\sup_{t \neq 0} \left| \widehat{1_R}(t) \right| = O\left(\sqrt{\frac{\log(p^n)}{p^n}} \right)$$

This is on Example Sheet 1 using a **Chernoff-type bound**: Given $\mathbb{C}$-valued independent random variables $X_1, \dots, X_n$ with mean 0 and $\theta \geq 0$, we have

$$\mathbb{P}\left(\left| \sum_i X_i \right| \geq \theta \sqrt{\sum_i \|X_i\|_{L^\infty}^2} \right) \leq 4 \exp\left(-\frac{\theta^2}{4} \right)$$

Example 1.4. Let $Q = \{x \in \mathbb{F}_p^n \mid x \cdot x = 0\}$. Then $|Q| = \left(\frac{1}{p} + O(p^{-n}) \right) p^n$ and $\sup_{t \neq 0} \left| \widehat{1_Q}(t) \right| = O(p^{-\frac{n}{2}})$. See Example Sheet 1.

Notation. Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$, write

$$\langle f, g \rangle = \mathbb{E}_x f(x) \overline{g(x)}$$
$$\left\langle \hat{f}, \hat{g} \right\rangle = \sum_t \hat{f}(t) \overline{\hat{g}(t)}$$

Consequently,

$$\|f\|_2^2 = \mathbb{E}_x |f(x)|^2$$
$$\left\| \hat{f} \right\|_2^2 = \sum_t \left| \hat{f}(t) \right|^2$$

Lemma 1.5. For all $f, g : \mathbb{F}_p^n \to \mathbb{C}$,

$$\langle f, g \rangle = \left\langle \hat{f}, \hat{g} \right\rangle \qquad \text{(Plancherel)}$$

$$\|f\|_2 = \left\| \hat{f} \right\|_2 \qquad \text{(Parseval)}$$

Proof. Exercise. □

Definition 1.6. Let $\rho > 0$ and $f : \mathbb{F}_p^n \to \mathbb{C}$. Define the ρ-large spectrum of f to be

$$\mathrm{Spec}_\rho(f) = \{t \mid |\hat{f}(t)| \geq \rho \|f\|_1\}$$

Example 1.7. By Example 1.2, if $V \leq \mathbb{F}_p^n$, then $\mathrm{Spec}_\rho(1_V) = V^\perp$ for all $\rho > 0$.

Lemma 1.8. For all $\rho > 0$, $\left| \mathrm{Spec}_\rho(f) \right| \leq \rho^{-2} \frac{\|f\|_2^2}{\|f\|_1^2}$.

Proof.
$$\|f\|_2^2 = \left\|\hat{f}\right\|_2^2 \geq \sum_{t \in \mathrm{Spec}_\rho(f)} \left|\hat{f}(t)\right|^2 \geq \left|\mathrm{Spec}_\rho(f)\right| (\rho \|f\|_1)^2$$
□

Lecture 2

Definition 1.9. Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$, define their **convolution** $f * g : \mathbb{F}_p^n \to \mathbb{C}$ by
$$(f * g)(x) = \mathbb{E}_y f(y) g(x - y)$$

Example 1.10. Given $A, B \subseteq \mathbb{F}_p^n$,
$$\begin{aligned} (1_A * 1_B)(x) &= \mathbb{E}_y 1_A(y) 1_B(x-y) \\ &= \frac{1}{p^n} |A \cap (x - B)| \\ &= \frac{\#\text{ ways to write } x = a + b, a \in A, b \in B}{p^n} \end{aligned}$$
In particular, the support of $1_A * 1_B$ is the **sum set**
$$A + B = \{a + b \mid a \in A, b \in B\}$$

Lemma 1.11. Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$,
$$\widehat{f * g}(t) = \hat{f}(t)\hat{g}(t)$$

Proof.
$$\begin{aligned} \widehat{f * g}(t) &= \mathbb{E}_x \left(\mathbb{E}_y f(y) g(x-y)\right) \omega^{x \cdot t} \\ &= \mathbb{E}_y f(y) \mathbb{E}_u g(u) \omega^{(u+y)\cdot t} \\ &= \hat{f}(t)\hat{g}(t) \end{aligned}$$
□

Example 1.12. $\left\|\hat{f}\right\|_4^4 = \mathbb{E}_{x+y=z+w} f(x) f(y) \overline{f(z) f(w)}$. See Example Sheet 1.

Lemma 1.13 (Bogolyubov)**.** If $A \subseteq \mathbb{F}_p^n$ is of density $\alpha > 0$, then there exists a subspace V of codimension at most $2\alpha^{-2}$ such that $V \subseteq (A + A) - (A + A)$.

Proof. Observe that $(A+A) - (A+A) = \mathrm{supp}(\underbrace{1_A * 1_A * 1_{-A} * 1_{-A}}_{g})$, so we wish to find V such that $g(x) > 0$ for all $x \in V$. Let $K = \mathrm{Spec}_\rho(1_A)$ for some $\rho > 0$ and define $V = \langle K \rangle^\perp$. By Lemma 1.8, $\operatorname{codim} V \leq |K| \leq \rho^{-2}\alpha^{-1}$. We calculate
$$\begin{aligned} g(x) &= \sum_{t \in \mathbb{F}_p^n} \widehat{1_A * 1_A * 1_{-A} * 1_{-A}}(t) \omega^{-x \cdot t} \\ &= \sum_{t \in \mathbb{F}_p^n} \left|\widehat{1_A}(t)\right|^4 \omega^{-x\cdot t} \\ &= \alpha^4 + \underbrace{\sum_{t \in K \setminus \{0\}} \left|\widehat{1_A}(t)\right|^4 \omega^{-x \cdot t}}_{(1)} + \underbrace{\sum_{t \notin K} \left|\widehat{1_A}(t)\right|^4 \omega^{-x\cdot t}}_{(2)} \end{aligned}$$

We now see that

$$(1) = \sum_{t \in K \setminus \{0\}} \left| \widehat{1_A}(t) \right|^4 \geq 0$$

and

$$|(2)| \leq \sum_{t \notin K} \left| \widehat{1_A}(t) \right|^4 \leq \sup_{t \notin K} \left| \widehat{1_A}(t) \right|^2 \sum_{t \notin K} \left| \widehat{1_A}(t) \right|^2 \leq (\rho\alpha)^2 \left\| 1_A \right\|_2^2 = \rho^2 \alpha^3$$

by Parseval. Picking $\rho = \sqrt{\frac{\alpha}{2}}$, we thus get $\rho^2\alpha^3 \leq \frac{\alpha^4}{2}$ and $g(x) > 0$ whenever $x \in V$. $\square$

Example 1.14. The set $A = \{x \in \mathbb{F}_2^n \mid |x| \geq \frac{n}{2} + \frac{\sqrt{n}}{2}\}$ has density at least $\frac{1}{4}$ but there is no coset C of any subspace of codimension $\sqrt{n}$ such that $C \subseteq A + A$. See Example Sheet 1.

Lemma 1.15. Let $A \subseteq \mathbb{F}_p^n$ of density α be such that $\operatorname{Spec}_\rho(1_A)$ contains some $t \neq 0$. Then there exist $V \leq \mathbb{F}_p^n$ of codimension 1 and $x \in \mathbb{F}_p^n$ such that

$$|A \cap (x + V)| \geq \alpha \left(1 + \frac{\rho}{2}\right) |V|$$

Proof. Let $t \neq 0$ be such that $\left| \widehat{1_A}(t) \right| \geq \rho\alpha$ and let $V = \langle t \rangle^\perp$. For $j = 1, \dots, p$, write

$$v_j + V = \{x \in \mathbb{F}_p^n \mid x \cdot t = j\}$$

the cosets of V. Then

$$\begin{aligned}
\widehat{1_A}(t) &= \hat{f}_A(t) \\
&= \mathbb{E}_{x \in \mathbb{F}_p^n} (1_A(x)) - \alpha) \omega^{x \cdot t} \\
&= \mathbb{E}_j \omega^j \mathbb{E}_{x \in v_j + V} (1_A(x) - \alpha) \\
&= \mathbb{E}_j a_j \omega^j
\end{aligned}$$

where $a_j = \frac{|A \cap (v_j + V)|}{|V|} - \alpha$. Since $\sum_j a_j = 0$, we get

$$\rho\alpha \leq \left| \widehat{1_A}(t) \right| \leq \mathbb{E}_j |a_j| = \mathbb{E}_j (|a_j| + a_j)$$

So there is some j such that $|a_j| + a_j \geq \rho\alpha$. In particular, this a_j is positive, so

$$\frac{|A \cap (v_j + V)|}{|V|} \geq \alpha + \frac{\rho\alpha}{2}$$

as wanted. $\square$

Lecture 3

Lemma 1.16. Let $p \geq 3$ and $A \subseteq \mathbb{F}_p^n$ of density $\alpha > 0$ be such that $\sup_{t \neq 0} \left| \widehat{1_A}(t) \right| = o(1)$. Then A contains $(\alpha^3 + o(1)) |G|^2$ three terms arithmetic progressions (aka 3AP).

Notation. Given $f, g, h : \mathbb{F}_p^n \to \mathbb{C}$, write

$$T_3(f, g, h) = \mathbb{E}_x f(x) g(x + d) h(x + 2d)$$

Given $A \subseteq \mathbb{F}_p^n$, write $2 \cdot A = \{2a \mid a \in A\}$. This is distinct from $2A = \{a + b \mid a, b \in A\}$.

Proof. The number of 3AP (including the trivial ones of the form a, a, a) in A is $|G|^2$ times

$$\begin{aligned}
T_3(1_A, 1_A, 1_A) &= \mathbb{E}_{x,d} 1_A(x) 1_A(x+d) 1_A(x+2d) \\
&= \mathbb{E}_{x,y} 1_A(x) 1_A(y) 1_A(2y-x) \\
&= \mathbb{E}_y 1_A(y)(1_A * 1_A)(2y) \\
&= \langle 1_{2\cdot A}, 1_A * 1_A \rangle \\
&= \left\langle \widehat{1_{2\cdot A}}, \widehat{1_A}^2 \right\rangle \\
&= \alpha^3 + \sum_{t \neq 0} \widehat{1_A}(t) \overline{\widehat{1_{2\cdot A}}(t)} \text{ by Plancherel}
\end{aligned}$$

In absolute value, the error term is at most

$$\sup_{t \neq 0} \left| \widehat{1_{2\cdot A}}(t) \right| \sum_t \left| \widehat{1_A}(t) \right|^2 = \alpha \sup_{t \neq 0} \left| \widehat{1_A}(t) \right|$$

□

Theorem 1.17 (Meshulam)**.** Let $p \geq 3$ and $A \subseteq \mathbb{F}_p^n$ be a set containing only trivial 3AP. Then

$$|A| = O\left(\frac{p^n}{\log(p^n)}\right)$$

Proof. By assumption, $T_3(1_A, 1_A, 1_A) = \frac{\alpha}{p^n}$. But, as in Lemma 1.16,

$$\left| T_3(1_A, 1_A, 1_A) - \alpha^3 \right| \leq \alpha \sup_{t \neq 0} \left| \widehat{1_A}(t) \right|$$

Hence, provided that $2\alpha^{-2} \leq p^n$, Lemma 1.15 gives us a subspace $V \leq \mathbb{F}_p^n$ of codimension 1 and $x \in \mathbb{F}_p^n$ such that

$$|A \cap (x+V)| \geq \alpha \left(1 + \frac{\alpha^2}{4}\right) |V|$$

We iterate this observation. Let $A_0 = A, V_0 = \mathbb{F}_p^n$. At step i, we are given a set $A_i \subseteq V_i$ of density α_i with only trivial 3AP. Provided that $2\alpha_i^{-2} \leq p^{\dim V_i}$, find $V_{i+1} \leq V_i$ of codimension 1 and $x \in V_i$ such that $|A_i \cap (x + V_i)| \geq \left(\alpha_i + \frac{\alpha_i^2}{4}\right) |V_{i+1}|$ and set $A_{i+1} = (A_i - x) \cap V_i$. Note that $\alpha_{i+1} \geq \alpha_i + \frac{\alpha_i^2}{4}$ and A_{i+1} only contains trivial 3AP (because, very importantly, 3AP are **translation-invariant**).
Through this iteration, the density of A increases from α to 2α in at most $\lceil 4\alpha^{-1} \rceil$ steps, from 2α to 4α in at most $\lceil 2\alpha^{-1} \rceil$ steps, etc... Since density can't increase past 1, it takes at most

$$\underbrace{\lceil 4\alpha^{-1} \rceil + \lceil 2\alpha^{-1} \rceil + \dots}_{\lceil \log \alpha^{-1} \rceil \text{ terms}} \leq (4\alpha^{-1} + 1) + (2\alpha^{-1} + 1) + \dots \leq 8\alpha^{-1} + \log \alpha^{-1} \leq 9\alpha^{-1}$$

steps to reach a point where the condition $2\alpha_i^{-2} \leq p^{\dim V_i}$ is not respected anymore. Now either $\alpha \leq \sqrt{2} p^{-\frac{n}{4}}$ (in which case the inequality is obvious) or $\alpha \geq \sqrt{2} p^{-\frac{n}{4}}$ and

$$p^{n - 9\alpha^{-1}} \leq p^{\dim V_i} \leq 2\alpha_i^{-2} \leq 2\alpha^{-2} \leq p^{\frac{n}{2}}$$

namely $\alpha \leq \frac{18}{n}$, as wanted. □