Introduction to Additive Combinatorics
Part III

Lectured by Julia Wolf

Artur Avameri

Contents

1 Fourier–analytic techniques

19 Jan 2024, Lecture 1

Let $G = \mathbb{F}_p^n$ for p a small fixed prime (usually $p = 2, 3, 5$) and n is large (often we consider $n \to \infty$).

Notation. Given a finite set B and any function $f : B \to \mathbb{C}$, we write $\mathbb{E}_{x \in B} f(x)$ to mean $\frac{1}{B} \sum_{x \in B} f(x)$. Also write $\omega = e^{2\pi i/p}$ for the p^{th} root of unity. Note that $\sum_{a \in \mathbb{F}_p} \omega^a = 0$.

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

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

where $x \cdot t$ is the standard scalar product.

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

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

Indeed,

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

Remark. We could use an unnormalized sum in our definition and a normalized sum in the inversion formula, or a minus sign in our definition and a plus sign in the inversion formula – this doesn't matter as long as we're consistent.

Given a subset A of a finite group G, write:

- 1_A for the **characteristic function** of A, i.e. $1_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$.

  This is also called the **indicator function**.
- f_A for the **balanced function** of A, i.e. $f_A(x) = 1_A(x) - \alpha$, where $\alpha = \frac{|A|}{|G|}$.
- μ_A for the **characteristic measure** of A, i.e. $\mu_A(x) = \alpha^{-1} 1_A(x)$.

Note $\mathbb{E}_{x \in G} f_A(x) = 0$ and $\mathbb{E}_{x \in G} \mu_A(x) = 1$. Given $A \subset \mathbb{F}_p^n$, we have

$$\hat{1}_A(t) = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) \omega^{x \cdot t}.$$

At $t = 0$, we get $\hat{1}_A(0) = \mathbb{E}_{x\in\mathbb{F}_p^n} 1_A(x) = \alpha$.

Writing $-A = \{-a \mid a \in A\}$, we have

$$\begin{aligned}\hat{1}_{-A}(t) &= \mathbb{E}_{x\in\mathbb{F}_p^n} 1_{-A}(x)\omega^{x\cdot t} = \mathbb{E}_{x\in\mathbb{F}_p^n} 1_A(-x)\omega^{x\cdot t} \\ &\overset{y=-x}{=} \mathbb{E}_{y\in\mathbb{F}_p^n} 1_A(y)\omega^{-y\cdot t} = \overline{\mathbb{E}_{y\in\mathbb{F}_p^n} 1_A(y)\omega^{y\cdot t}} = \overline{\hat{1}_A(t)}.\end{aligned}$$

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

$$\hat{1}_V(t) = \mathbb{E}_{x\in\mathbb{F}_p^n} 1_V(x)\omega^{x\cdot t} = \frac{|V|}{p^n} 1_{\{x\cdot t=0\ \forall x\in V\}} = \frac{|V|}{p^n} 1_{V^\perp}(t),$$

so $\hat{\mu}_V(t) = 1_{V^\perp}(t)$. (Here we use the fact that if $t \notin \{x \cdot t = 0\ \forall x \in V\}$, then $x \cdot t$ runs over the values uniformly and the sum is zero - details left as exercise).

Example 1.3. Let $R \subset \mathbb{F}_p^n$ be such that each $x \in \mathbb{F}_p^n$ lies in R independently with probability $\frac{1}{2}$. Then with high probability (i.e. $\mathbb{P} \to 1$ as $n \to \infty$),

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

Proving this is on Ex. Sheet 1. This is proved using a Chernoff–type bound: given complex–valued independent random variables $X_1, \ldots, X_n$ with mean 0, $\forall \theta \geq 0$,

$$\mathbb{P}\left(\left|\sum_{i=1}^n X_i\right| \geq \theta \sqrt{\sum_{i=1}^n ||X_i||^2_{L^\infty(\mathbb{P})}}\right) \leq 4\exp\left(-\theta^2/4\right).$$

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 $\sup_{t\neq 0} |\hat{1}_Q(t)| = O(p^{-n/2})$. This is again on Ex. Sheet 1.

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

$$\langle f, g\rangle = \mathbb{E}_{x\in\mathbb{F}_p^n} f(x)\overline{g(x)}$$

and

$$\langle \hat{f}, \hat{g}\rangle = \sum_{t\in\mathbb{F}_p^n} \hat{f}(t)\overline{\hat{g}(t)}.$$

Consequently, $||f||_2^2 = \mathbb{E}_x|f(x)|^2$ and $||\hat{f}||_2^2 = \sum_t |\hat{f}(t)|^2$.

Lemma 1.5. The following hold for all $f, g : \mathbb{F}_p^n \to \mathbb{C}$:

(i) $\langle f, g\rangle = \langle \hat{f}, \hat{g}\rangle$ (Plancherel's identity).

(ii) $||f||_2 = ||\hat{f}||_2$ (Parseval's identity).

Proof. (ii) follows from (i). For (i), compute

$$\begin{aligned}\langle \hat{f}, \hat{g}\rangle &= \sum_{t\in\mathbb{F}_p^n} \hat{f}(t)\overline{\hat{g}(t)} = \sum_{t\in\mathbb{F}_p^n} \frac{1}{p^{2n}} \sum_{x\in\mathbb{F}_p^n} f(x)\omega^{x\cdot t} \sum_{y\in\mathbb{F}_p^n} \overline{g(y)\omega^{y\cdot t}} \\ &= \frac{1}{p^{2n}} \sum_{x,y\in\mathbb{F}_p^n} f(x)\overline{g(y)} \sum_{t\in\mathbb{F}_p^n} \omega^{(x-y)t} = \frac{1}{p^{2n}} \sum_{x\in\mathbb{F}_p^n} p^n f(x)\overline{g(x)} = \langle f, g\rangle.\end{aligned}$$

□

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

$$\mathrm{Spec}_\rho(f) = \{t \in \mathbb{F}_p^n \mid |\hat{f}(t)| \geq \rho||f||_1\}.$$

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

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

Proof. By Parseval,

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

□

22 Jan 2024, 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

$$f * g(x) = \mathbb{E}_{y\in\mathbb{F}_p^n} f(y)g(x-y) \ \forall x \in \mathbb{F}_p^n.$$

Example 1.10. Given $A, B \subset \mathbb{F}_p^n$,

$$\begin{aligned}1_A * 1_B(x) &= \mathbb{E}_{y\in\mathbb{F}_p^n} 1_A(y)1_B(x-y) = \frac{1}{p^n}|A \cap (x-B)| \\ &= \frac{1}{p^n}\#\text{ways } x \text{ can be written as } x = a+b \text{ with } a \in A, b \in B.\end{aligned}$$

In particular, the support of $1_A * 1_B$ is the **sum set**

$$A + B = \{a + b \mid a \in A, b \in B\}$$

of A and B.

Lemma 1.11. Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$,

$$\widehat{f * g}(t) = \hat{f}(t)\hat{g}(t) \ \forall t \in \mathbb{F}_p^n.$$

Proof. Set $u = x - y$ to get

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

□

Example 1.12. $||\hat{f}||_4^4 = \mathbb{E}_{x+y=z+w} f(x) f(y) \overline{f(z) f(w)}$. This is on Ex. Sheet 1.

Lemma 1.13 (Bogolyubov's Lemma)**.** Given $A \subset \mathbb{F}_p^n$ of density $\alpha > 0$, there exists a subspace $V \leq \mathbb{F}_p^n$ of codimension at most $2\alpha^{-2}$ s.t. $A + A - A - A \supset V$.

Proof. Observe that

$$A + A - A - A = \mathrm{supp}(\underbrace{1_A * 1_A * 1_{-A} * 1_{-A}}_{:=g}).$$

Hence we wish to find $V \leq \mathbb{F}_p^n$ such that $g(x) > 0$ $\forall x \in V$. Let $K = \mathrm{Spec}_\rho(1_A)$ with ρ to be determined later and let $V = \langle K \rangle^\perp$. By Lemma 1.8, $|K| \leq \rho^{-2}\alpha^{-1}$ and hence $\mathrm{codim}(V) \leq |K| \leq \rho^{-2}\alpha^{-1}$. By the inversion formula,

$$\begin{aligned}g(x) &= \sum_{t \in \mathbb{F}_p^n} (1_A * 1_A \widehat{* 1_{-A}} * 1_{-A})(t) \omega^{-x \cdot t} \\ &= \sum_{t \in \mathbb{F}_p^n} |\hat{1}_A(t)|^4 \omega^{-x \cdot t} \\ &= \alpha^4 + \underbrace{\sum_{t \in K \setminus \{0\}} |\hat{1}_A(t)|^4 \omega^{-x \cdot t}}_{(1)} + \underbrace{\sum_{t \notin K} |\hat{1}_A(t)|^4 \omega^{-x \cdot t}}_{(2)}.\end{aligned}$$

For (1), we see it is ≥ 0 since $x \cdot t = 0$ $\forall t \in K, x \in V$. (Note we could give better lower bounds but we don't need them).

For (2), we have

$$\begin{aligned}|(2)| &\leq \sum_{t \notin K} |\hat{1}_A(t)|^4 \leq \sup_{t \notin K} |\hat{1}_A(t)|^2 \sum_{t \notin K} |\hat{1}_A(t)|^2 \leq \sup_{t \notin K} |\hat{1}_A(t)|^2 \sum_t |\hat{1}_A(t)|^2 \\ &\leq (\rho\alpha)^2 ||1_A||_2^2 = \rho^2 \alpha^3.\end{aligned}$$

Now pick ρ such that $\rho^2\alpha^3 \leq \frac{\alpha^4}{2}$, e.g. $\rho = \sqrt{\frac{\alpha}{2}}$. □

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 $\frac{1}{4}$, and there is no coset C of any subspace of codimension at most $\sqrt{n}$ such that $C \subset A + A$. This is on Ex. Sheet 1.

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

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

Proof. Let $t \neq 0$ be such that $|\hat{1}_A(t)| \geq \rho\alpha$ and let $V = \langle t \rangle^\perp$. Write $v_j + V$ for $j \in [p] := \{1, 2, \ldots, p\}$ for the cosets of V such that $v_j + V = \{x \in \mathbb{F}_p^n \mid x \cdot t = j\}$. Then

$$\begin{aligned} \hat{1}_A(t) &= \hat{f}_A(t) \\ &= \mathbb{E}_{x \in \mathbb{F}_p^n} (1_A(x) - \alpha)\omega^{x \cdot t} \\ &= \mathbb{E}_{j \in [p]} \underbrace{\mathbb{E}_{x \in v_j + V} (1_A(x) - \alpha)}_{=: a_j = \frac{|A \cap (v_i + V)|}{|V|} - \alpha} \omega^j. \end{aligned}$$

By the triangle inequality, $\mathbb{E}_{j \in [p]} |a_j| \geq \rho\alpha$. Since $\mathbb{E}_{j \in [p]} a_j = 0$, $\mathbb{E}_{j \in [p]}(a_j + |a_j|) \geq \rho\alpha$, so $\exists j \in [p]$ such that $a_j + |a_j| \geq \rho\alpha \implies a_j \geq \frac{\rho\alpha}{2}$. $\square$