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^{h} 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 1.1. 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 an exercise).

Example 1.2. 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 1.3. 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 $||\hat{f}||_2^2 = \sum_t |\hat{f}(t)|^2$.

TODO: all the definitions/examples/lemmas follow the same numbering

Lemma 1.1. The following hold for all $f, g : \mathbb{F}_{p^n} \to \mathbb{C}$:

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

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

Proof. Exercise. □

Definition 1.2. 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 1.4. By Example 1.1, if $f = 1_V$ with $V \leq \mathbb{F}_{p^n}$, then $\forall \rho > 0$, $\mathrm{Spec}_\rho(f) = V^\perp$.

Lemma 1.2. For all $\rho > 0$, $|\mathrm{Spec}_\rho(f)| \leq \rho^{-2} \frac{||f||_2^2}{||f||_1^2}$.

Proof. By Parseval,

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

□