Part III – Introduction to Additive Combinatorics (Incomplete)

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

Lent 2024

Contents

1 Example Sheet 1

Problem 1.1. Construct $R \subseteq \mathbb{F}_p^n$ by selecting each element $x \in \mathbb{F}_p^n$ to lie in R independently at random with probability $\frac{1}{2}$. Show that, with high probability,

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

Proof. We use that if the X_i are independent with probability 1 then

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

Here we assume $t \neq 0$ and pick $X_x = \omega^{x \cdot t}(1_R(x) - \frac{1}{2})$. By assumption, the X_x are independent with mean 0. Hence our inequality applies. We see that $\|X_x\|_\infty = \frac{1}{2}$, $\sqrt{\sum_x \|X_x\|_\infty^2} = \frac{p^{\frac{n}{2}}}{2}$,

$$\sum_x X_x = \sum_x \omega^{x \cdot t} 1_R(x) = p^n \widehat{[1_R]}(t)$$

Hence the inequality becomes

$$\mathbb{P}(\left| \widehat{1_R}(t) \right| \geq \theta p^{-\frac{n}{2}}) \leq 4\exp(-\theta^2)$$

The union bound gives

$$\mathbb{P}\left(\sup_{t \neq 0} \left| \widehat{1_R}(t) \geq \theta p^{-\frac{n}{2}} \right| \right) \leq 4\exp(-\theta^2) = \frac{4}{p^n} \to 0$$

if we take $\theta = \sqrt{2\log(p^n)}$, as wanted. □

Problem 1.2. Let $p > 2$.

1. Let M be an $n \times n$ symmetric matrix with entries in $\mathbb{F}_p$, and let $b \in \mathbb{F}_p^n$. By squaring the expression on the left, show that

$$\left| \mathbb{E}_{x \in \mathbb{F}_p^n} \omega^{x^T M x + c^T x} \right| \leq p^{-\frac{\operatorname{rank} M}{2}}$$

2. Let $Q = \{x \in \mathbb{F}_p^n \mid x^T x = 0\}$. By expressing the indicator function of Q as a suitable exponential sum, show that

$$\frac{|Q|}{p^n} = \frac{1}{p} + O(p^{-\frac{n}{2}}) \text{ and } \sup_{t \neq 0} \left| \widehat{1_Q}(t) \right| = O(p^{-\frac{n}{2}})$$

Proof.

1.

$$\begin{aligned}
\left| \mathbb{E}_{x \in \mathbb{F}_p^n} \omega^{x^T M x + c^T x} \right|^2 &= \mathbb{E}_{x,y} \omega^{x^T M x + c^T x - (y^T M y + c^T y)} \\
&= \mathbb{E}_{x,y} \omega^{(x+y)^T M (x-y) + c^T (x-y)} \\
&= \mathbb{E}_{a,b} \omega^{a^T M b + c^T b} \\
&= \mathbb{E}_b 1_{b \in \ker M} \omega^{c^T b} \\
&\leq \mathbb{E}_b 1_{b \in \ker M} \\
&= p^{-\operatorname{rank} M}
\end{aligned}$$

2. $1_Q(x) = \mathbb{E}_a \omega^{x^T(aI)x}$, so

$$\begin{aligned}\widehat{1_Q}(t) &= \mathbb{E}_{a,x}\omega^{x^T(aI)x+x\cdot t}\\ &= \underbrace{\frac{1}{p}\mathbb{E}_x\omega^{x\cdot t}}_{1_{t=0}} + \underbrace{\frac{1}{p}\sum_{a\neq 0}\mathbb{E}_x\omega^{x^T(aI)x+x\cdot t}}_{\Delta}\end{aligned}$$

By the previous part, $|\Delta| \leq \frac{1}{p}\sum_{a\neq 0} p^{-\frac{\operatorname{rank}(aI)}{2}} = O(p^{-\frac{n}{2}})$. Hence

$$\widehat{1_Q}(t) = \frac{1}{p}1_{t=0} + O(p^{-\frac{n}{2}})$$

as wanted.

□

Problem 1.3. Given $f : \mathbb{F}_p^n \to \mathbb{C}$, define

$$\|f\|_{U^2}^4 = \mathbb{E}_{x+y=z+w} f(x)f(y)\overline{f(z)f(w)}$$

where the expectation is taken over $\{(x,y,z,w) \in (\mathbb{F}_p^n)^4 \mid x+y=z+w\}$.

1. Show that $\|f\|_{U^2} = \left\|\hat{f}\right\|_{\ell^4}$.
2. Let $f_1, f_2, f_3 : \mathbb{F}_p^n \to \mathbb{C}$. Without appealing to the Fourier transform, show that

$$|T_3(f_1,f_2,f_3)| \leq \|f_1\|_{U^2}\|f_2\|_\infty\|f_3\|_\infty, \|f_1\|_\infty\|f_2\|_{U^2}\|f_3\|_\infty, \|f_1\|_\infty\|f_2\|_\infty\|f_3\|_{U^2}$$

Proof.

1.

$$\begin{aligned}\left\|\hat{f}\right\|_4^4 = \left\|\hat{f}^2\right\|_2^2 = \left\|\widehat{f*f}\right\|_2^2 &= \|f*f\|_2^2 \text{ by Parseval}\\ &= \mathbb{E}_a(f*f)(a)\overline{(f*f)(a)}\\ &= \mathbb{E}_{a,x,y,z,w} f(x)f(y)1_{x+y=a}\overline{f(z)f(w)1_{z+w=a}}\\ &= \mathbb{E}_{x+y=z+w} f(x)f(y)\overline{f(z)f(w)}\end{aligned}$$

where in the last equality we check that the number of factors of $|G|$ is the same on both sides.

2. The trick to make $\|f_i\|_{U^2}$ appear here is to use Cauchy-Schwarz twice to each time duplicate the number of appearances of f_i in the expression. For this to work, we need one variable to not appear as an argument of f_i. A neat way to do this is to write 3APs in the form $2a-b, a-c, b-2c$, with reason $a-b+c$. For simplicity, assume $\|f_1\|_\infty = 1$. We get

$$\begin{aligned}
|T_3(f_1,f_2,f_3)|^2 &= |\mathbb{E}_{a,b,c} f_1(2a-b) f_2(a-c) f_3(b-2c)|^2 \\
&= |\mathbb{E}_{a,b} f_1(2a-b) \mathbb{E}_c f_2(a-c) f_3(b-2c)|^2 \\
&\le \underbrace{\left(\mathbb{E}_{a,b} |f_1(2a-b)|^2\right)}_{\le \|f_1\|_\infty^2} \mathbb{E}_{a,b} |\mathbb{E}_c f_2(a-c) f_3(b-2c)|^2 \\
&\le \mathbb{E}_{a,b} |\mathbb{E}_c f_2(a-c) f_3(b-2c)|^2 \\
&= \mathbb{E}_{c,c'} \left(\mathbb{E}_a f_2(a-c)\overline{f_2(a-c')}\right) \mathbb{E}_b f_3(b-2c)\overline{f_3(b-2c')}
\end{aligned}$$

Hence

$$\begin{aligned}
|T_3(f_1,f_2,f_3)|^4 &\le \left(\mathbb{E}_{c,c'} \left|\mathbb{E}_a f_2(a-c)\overline{f_2(a-c')}\right|^2\right) \\
&\quad \left(\mathbb{E}_{c,c'} \left|\mathbb{E}_b f_3(b-2c)\overline{f_3(b-2c')}\right|^2\right) \\
&= \left(\mathbb{E}_{a,a',c,c'} f_2(a-c)\overline{f_2(a-c') f_2(a'-c)} f_2(a'-c')\right) \\
&\quad \left(\mathbb{E}_{b,b',c,c'} f_3(b-2c)\overline{f_3(b-2c') f_3(b'-2c)} f_3(b'-2c')\right) \\
&= \|f_2\|_{U^2}^4 \|f_3\|_{U^2}^4
\end{aligned}$$

So we've proved $|T_3(f_1,f_2,f_3)| \le \|f_1\|_\infty \|f_2\|_{U^2} \|f_3\|_{U^2}$. Since $T_3(f_1,f_2,f_3) = T_3(f_3,f_2,f_1)$, we also get $|T_3(f_1,f_2,f_3)| \le \|f_1\|_{U^2} \|f_2\|_{U^2} \|f_3\|_\infty$ (and the third inequality $|T_3(f_1,f_2,f_3)| \le \|f_1\|_{U^2} \|f_2\|_\infty \|f_3\|_{U^2}$ can be obtained by an argument similar to the one above). Those inequalities are stronger than the ones we were after as $\|f\|_{U^2} \le \|f\|_\infty$ in general (by the triangle inequality).

□

Problem 1.4. Let $A = \{x \in \mathbb{F}_2^n \mid |x| \ge \frac{n}{2} + \frac{\sqrt{n}}{2}$ where $|x|$ denotes the number of 1s in x and n is to be thought of as large n.

1. Show that A has size at least $\frac{2^n}{8}$.
2. Let V be any subspace of $\mathbb{F}_2^n$ of codimension $< \sqrt{n}$. Show that $A+A$ does not contain any coset of V.

Proof.

1. $|A| \ge \frac{2^n}{8}$ is the same as saying that $\mathbb{P}(\sum_i X_i \ge \frac{n}{2} + \frac{\sqrt{n}}{2}) \ge \frac{1}{4}$ where the X_i are iid Bernoulli random variables with probability $\frac{1}{2}$. But $\operatorname{Var} X_i = \frac{1}{4}$, so the Central Limit Theorem tells us that

$$\sqrt{n}\left(\mathbb{E}_{i=1}^n - \frac{1}{2}\right) \xrightarrow{d} N\left(0, \frac{1}{4}\right)$$

In particular,

$$\mathbb{P}\left(\sum_i X_i \ge \frac{n}{2} + \frac{\sqrt{n}}{2}\right) \to \Phi\left(\frac{1}{2}\right) = 0.15 > \frac{1}{8}$$

2. Note that if $x, y \in A$ then

$$|x+y| = |x \cup y| - |x \cap y| \in \left[\frac{n}{2} + \frac{\sqrt{n}}{2}, n\right] - \left[\sqrt{n}, \frac{n}{2} + \frac{\sqrt{n}}{2}\right] = [0, n - \sqrt{n}]$$

Hence $A + A \subseteq \{x \in \mathbb{F}_2^n \mid |x| \leq n - \sqrt{n}\}$. But now we claim that if B is a coset of a subspace V of dimension k, then $|x| \geq k$ for some $x \in B$. Let's prove it by induction on k:

- For $k = 0$, it's clear.
- For $k+1$, pick $v \in V$ such that $v \neq 0$, say $v_i \neq 0$. Then $B_i^+ = \{x \in B \mid x_i = 1\}$ and $v + B_i^+ = \{x \in B \mid x_i = 0\}$ partition B. Hence $\left|B_i^+\right| = \frac{|B|}{2}$ and $B_i^- = e_i + B_i^+$ (where e_i is the i-th basis vector) is a coset of a subspace of V of codimension 1. Find by induction hypothesis $x \in B_i^-$ such that $|x| \geq k$. Then $x + e_i \in B_i^+$ and $|x + e_i| \geq k + 1$, as wanted.

□

Problem 1.5. Let $A \subseteq \mathbb{F}_p^n$ be of size $|A| \leq n$. Show that there exists $t \neq 0$ such that $\left|\widehat{1_A}(t)\right| = \frac{|A|}{p^n}$. Formulate an analogous result for the group $\mathbb{F}_p$ with p a prime.

Proof. Consider the map

$$\begin{aligned} \phi : \widehat{\mathbb{F}_p^n} &\to A \to \mathbb{F}_p \\ t &\mapsto x \mapsto x \cdot t \end{aligned}$$

and write $\Delta = \{(x, \dots, x) : A \to \mathbb{F}_p^n \mid x \in A\}$ the diagonal. ϕ is linear. Consider the subspace $\phi^{-1}\Delta$. If it is trivial, then ϕ is injective and

$$n = \dim \widehat{\mathbb{F}_p^n} = \operatorname{rank} \phi \leq \operatorname{codim} \Delta < |A|$$

Hence there is some $t \neq 0$ such that $\phi(t) \in \Delta$, namely $x \cdot t = c$ for all $x \in A$ and some $c \in \mathbb{F}_p$. Then

$$\left|\widehat{1_A}(t)\right| = \frac{1}{p^n}\left|\sum_{x \in A} \omega^{x \cdot t}\right| = \frac{1}{p^n}\left|\sum_{x \in A} \omega^c\right| = \frac{|A|}{p^n}$$

An analogous statement for $\mathbb{F}_p$ is that if $A \subseteq \mathbb{F}_p$ is of density α and $|A| < \frac{\log p}{\log 2\pi + \frac{1}{2}\log \varepsilon^{-1}}$ then there exists $t \neq 0$ such that $\left|\widehat{1_A}(t)\right| \geq (1 - \varepsilon)\alpha$.

Proof. First note that if $z \in \mathbb{C}$ is such that $|z - 1| \leq \sqrt{\varepsilon}$ then $\operatorname{Re} z \geq 1 - \varepsilon$ (draw a picture in the complex plane). Second, observe that

$$\left|B(A, \sqrt{\varepsilon})\right| \geq p \left(\frac{\sqrt{\varepsilon}}{2\pi}\right)^{|A|} > 1$$

by a theorem in the lectures and by assumption. Hence $B(A, \sqrt{\varepsilon})$ contains some $t \neq 0$. For that t and all $x \in A$, we have $|\omega^{xt} - 1| \leq \sqrt{\varepsilon}$. Therefore

$$\left|\widehat{1_A}(t)\right| = \frac{1}{p}\left|\sum_{x \in A} \omega^{xt}\right| \geq \frac{1}{p}\sum_{x \in A} \operatorname{Re} \omega^{xt} \geq (1 - \varepsilon)\alpha$$

□

$\square$

Problem 1.6. Let $A \subseteq \mathbb{F}_p$ with p a prime. Show that the number of 3-term arithmetic progressions in A plus the number of 3-term arithmetic progressions in A^c depends only on the cardinality of A. Is the same true for 4-term arithmetic progressions?

Proof. This works in a general group G whose elements all have odd order. First observe a few things: $(2 \cdot A)^c = 2 \cdot A^c, \widehat{1_A} + \widehat{1_{A^c}} = \hat{1} = 1_0, \widehat{1_{2 \cdot A}} + \widehat{1_{2 \cdot A^c}} = \hat{1} = 1_0$. Hence we calculate that

$$\begin{aligned}
\frac{\#\{\text{3APs in } A\} + \#\{\text{3APs in } A^c\}}{|G|^2} =& T_3(1_A, 1_A, 1_A) + T_3(1_{A^c}, 1_{A^c}, 1_{A^c}) \\
=& \langle 1_{2\cdot A}, 1_A * 1_A \rangle + \langle 1_{2\cdot A^c}, 1_{A^c} * 1_{A^c} \rangle \\
=& \left\langle \widehat{1_{2\cdot A}}, \widehat{1_A}^2 \right\rangle + \left\langle \widehat{1_{2\cdot A^c}}, \widehat{1_{A^c}}^2 \right\rangle \\
=& \sum_t \widehat{1_{2\cdot A}}(t) \widehat{1_A}(t)^2 + \widehat{1_{2\cdot A^c}}(t) \widehat{1_{A^c}}(t) \\
=& \alpha^3 + (1-\alpha)^3 \\
& + \sum_{t \neq 0} \widehat{1_{2\cdot A}}(t) \widehat{1_A}^2(t) + (-\widehat{1_{2\cdot A}}(t))(-\widehat{1_A}(t))^2 \\
=& 1 - 3\alpha + 3\alpha^2
\end{aligned}$$

Namely,

$$\#\{\text{3APs in } A\} + \#\{\text{3APs in } A^c\} = |G|^2 - 3|A||G| + 3|A|^2$$

The same is not true of 4APs since $\{0, 1, 2, 3\}, \{0, 1, 3, 4\} \subseteq \mathbb{F}_7$ have the same size but not the same number of 4APs in them and their complement. $\square$

Problem 1.7. Let p be a prime and let $L \leq \frac{p}{2} - 1$ be even. Given $x \in \mathbb{F}_p$, denote by $|x|$ the minimum distance of 0 from a member of the residue class of x module p.

1. Let $J = [-\frac{L}{2}, \frac{L}{2}] \subseteq \mathbb{F}_p$. By summing a geometric series, show that, for all $t \in \widehat{\mathbb{F}_p}$,

$$\left| \widehat{1_J}(t) \right| \leq \min\left(\frac{L+1}{p}, \frac{1}{2|t|} \right)$$

2. Let $A \subseteq \mathbb{F}_p$ be a set of density $\alpha > 0$ such that $A \cap [-L, L] = \varnothing$. Show that there exists $t \neq 0$ with $|t| \leq \sqrt{\frac{p}{2}} \frac{p}{L+1}$ such that $\left| \widehat{1_A}(t) \right| \geq \alpha \frac{L+1}{2p}$.

Proof.

1. If $t = 0$, then $\widehat{1_J}(t) = \frac{|J|}{p} = \frac{L+1}{p}$. If $t \neq 0$, then

$$\widehat{1_J}(t) = \mathbb{E}_x 1_J(x) \omega^{xt} = \mathbb{E}_{x=-\frac{L}{2}}^{\frac{L}{2}} \omega^{xt} = \frac{\omega^{(L+1)\frac{t}{2}} - \omega^{-(L+1)\frac{t}{2}}}{p(\omega^{\frac{t}{2}} - \omega^{-\frac{t}{2}})}$$

Noting that, for all $x \in [-\pi, \pi]$, we have $\left| e^{ix} - 1 \right| \geq \frac{2|x|}{\pi}$,

$$\left| \widehat{1_J}(t) \right| \leq \frac{2}{p} \left| \omega^t - 1 \right|^{-1} \leq \frac{2}{p} \left(\frac{2}{\pi} \frac{2\pi t}{p} \right)^{-1} = \frac{1}{2|t|}$$

2. We can turn the $A \cap [-L, L] = \varnothing$ condition into $\langle 1_A, 1_J * 1_J \rangle = 0$. Hence

$$0 = \langle 1_A, 1_J * 1_J \rangle = \langle \widehat{1_A}, \widehat{1_J}^2 \rangle = \alpha \left(\frac{L+1}{p} \right)^2 + \underbrace{\sum_{t \neq 0} \widehat{1_A}(t) \widehat{1_J}(t)^2}_{\Delta}$$

We calculate

$$\begin{aligned} |\Delta| &\leq \sum_{t \neq 0, |t| \leq C} \left| \widehat{1_A}(t) \right| \left| \widehat{1_J}(t) \right|^2 + \sum_{|t| > C} \left| \widehat{1_A}(t) \right| \left| \widehat{1_J}(t) \right|^2 \\ &\leq \sup_{t \neq 0, |t| \leq C} \left| \widehat{1_A}(t) \right| \left\| \widehat{1_J} \right\|_2^2 + \frac{1}{4C^2} \sum_{|t| > C} \left| \widehat{1_A}(t) \right| \\ &\leq \frac{L+1}{p} \sup_{t \neq 0, |t| \leq C} \left| \widehat{1_A}(t) \right| + \frac{p\alpha}{4C^2} \\ &= \frac{L+1}{p} \left(\sup_{t \neq 0, |t| \leq C} \left| \widehat{1_A}(t) \right| + \alpha \frac{L+1}{2p} \right) \end{aligned}$$

Hence

$$\sup_{t \neq 0, |t| \leq C} \left| \widehat{1_A}(t) \right| \geq \alpha \frac{L+1}{2p}$$

as wanted.

□

Problem 1.8. Combine Lemmas 1.21 and 1.23 from lectures to give a proof of (Roth's) Theorem 1.20. That is, show that any subset $A \subseteq [N]$ containing no non-trivial 3-term arithmetic progressions has size $O(N/\log\log N)$.

Proof. TODO □

Problem 1.9. In this exercise you will construct (Behrend's) Example 1.24.

1. Consider the d-dimensional integer grid $[m]^d$. Show that there exists at least one value of $r \in [dm^2]$ such that $S_r = \{x \in [m]^d \mid x_1^2 + \cdots + x_d^2 = r\}$ has size at least m^{d-2}/d.
2. Construct a map $\phi : [m]^d \to [N]$ for some suitable N such that if $S \subseteq [m]^d$ contains no non-trivial 3-term arithmetic progressions, then neither does $\phi(S)$.
3. Deduce that there exists a set $A \subseteq [N]$ of size at least $\exp(-c\sqrt{\log N})N$, for some constant $c > 0$, containing no non-trivial 3-term arithmetic progressions.

Proof.

1. Every $x \in [m]^d$ lies in S_r for some $r \in [dm^2]$ (namely $r = x_1^2 + \cdots + x_d^2$). Hence by pigeonhole there's some r such that $|S_r| \geq m^d/(dm^2)$.
2. The map

$$\begin{aligned} \phi : [m]^d &\to [(2m-1)^d] \\ x &\mapsto \sum_{i=0}^{d-1} (2m-1)^i x_i \end{aligned}$$

is such that if $\phi(a)+\phi(b)=2\phi(c)$ then $a+b=2c$ since the addition of $2m-1$-ary numbers whose digits are all $\leq m-1$ does not have carries.

3. The density of $\phi(S_r)$ is

$$\frac{m^{d-2}/d}{(2m-1)^d} \geq \frac{m^{d-2}/d}{(2m)^d} = \frac{1}{m^2 2^d d} = \frac{1}{N^{\frac{1}{d}} 2^{d-1} d}$$

Taking logs, we find

$$d-1+\log d - \frac{\log N}{d} \approx 2\sqrt{\log N}$$

if we pick $d=\sqrt{\log N}$. Hence we have found a set of density $\approx \exp(-2\sqrt{\log N})$

$\square$

Problem 1.10. Show that for all $\alpha > 0$, there exists a constant $c = c(\alpha)$ such that for every N and every subset $A \subseteq [N]$ of density at least α, the number of arithmetic progressions in A is at least $c(\alpha)N^2$.

Proof. TODO $\square$