

Additive Combinatorics Notes

Leart Ajvazaj

January 2024

Notes from my Additive Combinatorics class at Cambridge with Julia Wolf. Any mistake is with very high certainty mine.

Chapter 1: Fourier-Analytic Techniques

Lecture 1

Let $G = \mathbb{F}_p^n$ where p is a small fixed prime ($p = 2, 3, 5$) and n is large ($n \rightarrow \infty$). Notation: Given a finite set B and any function $f : B \rightarrow \mathbb{C}$, write $\mathbb{E}_{x \in B} f(x) := \frac{1}{|B|} \sum_{x \in B} f(x)$. Write $\omega = e^{2\pi i/p}$ for a p -th root of unity. Note $\sum_{a \in \mathbb{F}_p} \omega^a = 0$.

Definition 1.1 Given $f : \mathbb{F}_p^n \rightarrow \mathbb{C}$, define its **Fourier transform** $\widehat{f} : \mathbb{F}_p^n \rightarrow \mathbb{C}$ by $\widehat{f}(t) = \mathbb{E}_{x \in \mathbb{F}_p^n} f(x) \omega^{x \cdot t}$ for all $t \in \mathbb{F}_p^n$.

It's easy to verify the **inversion formula**: $f(x) = \sum_{t \in \mathbb{F}_p^n} \widehat{f}(t) \omega^{-x \cdot t}$. Indeed,

$$\sum_{t \in \mathbb{F}_p^n} \widehat{f}(t) \omega^{-x \cdot t} = \sum_{t \in \mathbb{F}_p^n} (\mathbb{E}_y f(y) \omega^{-y \cdot t}) \omega^{-x \cdot t} = \mathbb{E}_y f(y) \underbrace{\sum_{t \in \mathbb{F}_p^n} \omega^{(y-x) \cdot t}}_{p^n 1_{\{y=x\}}} = f(x).$$

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

- 1_A for the **characteristic function** of A (or 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 $\mathbb{E}_{x \in G} \mu_A(x) = 1$. Note that given $A \subset \mathbb{F}_p^n$, we have $\widehat{1_A}(f) = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) \omega^{x \cdot t}$. So $\widehat{1_A}(0) = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) = \alpha$. Writing $-A = \{-a : a \in A\}$, we have

$$\widehat{1_{-A}}(t) = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_{-A}(x) \omega^{x \cdot t} = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(-x) \omega^{x \cdot t} = \mathbb{E}_{y \in \mathbb{F}_p^n} 1_A(y) \omega^{-y \cdot t} = \overline{\mathbb{E}_{y \in \mathbb{F}_p^n} 1_A(y) \omega^{y \cdot t}} = \overline{\widehat{1_A}(t)}.$$

Example 1.2 Let $V \leq \mathbb{F}_p^n$. Then $\widehat{1_V}(t) = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_V(x) \omega^{x \cdot t} = \frac{|V|}{p^n} 1_{\{x \cdot t = 0 \forall x \in V\}}(t) = \frac{|V|}{p^n} 1_{V^\perp}(t)$. So $\widehat{\mu_V}(t) = 1_{V^\perp}(t)$.

Let's look at the opposite. Instead of having a lot of structure in the subvectorspace, we'll go to the other extreme with R a random set.

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 $1/2$. Then with high probability $\sup_{t \neq 0} |\widehat{1}_R(t)| = O\left(\sqrt{\frac{\log(p^n)}{p^n}}\right)$.

We'll show this in the first example sheet using a **Chernoff-type bound**: Given \mathbb{C} -valued independent random variables X_1, \dots, X_n with mean 0, for all $\theta \geq 0$ we have $\mathbb{P}[|\sum x_i| \geq \theta \sqrt{\sum \|x_i\|_{L^\infty(\mathbb{P})}^2}] \leq 4 \exp(-\theta^2/4)$.

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

Notation: Given $f, g : \mathbb{F}_p^n \rightarrow \mathbb{C}$, write $\langle f, g \rangle := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x) \overline{g(x)}$ and $\langle \widehat{f}, \widehat{g} \rangle := \sum_{t \in \mathbb{F}_p^n} \widehat{f}(t) \overline{\widehat{g}(t)}$. Consequently, $\|f\|_2^2 = \mathbb{E}_x |f(x)|^2$ while $\|\widehat{f}\|_2^2 = \sum_{t \in \mathbb{F}_p^n} |\widehat{f}(t)|^2$.

Lemma : 1.5

The following hold for all $f, g : \mathbb{F}_p^n \rightarrow \mathbb{C}$:

- (i) $\langle f, g \rangle = \langle \widehat{f}, \widehat{g} \rangle$ (**Plancharel's identity**)
- (ii) $\|f\|_2 = \|\widehat{f}\|_2$ (**Parseval's identity** or energy conservation)

Proof. Exercise. □

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

$$\text{Spec}_\rho(f) = \{t \in \mathbb{F}_p^n : |\widehat{f}(t)| \geq \rho \|f\|_1\}.$$

Lemma : 1.8

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

Proof. $\|f\|_2^2 = \|\widehat{f}\|_2^2 \geq \sum_{t \in \text{Spec}_\rho(f)} |\widehat{f}(t)|^2 \geq |\text{Spec}_\rho(f)|(\rho \|f\|_1)^2$. □

Lecture 2

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

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

$$1_A * 1_B(x) = \mathbb{E}_{y \in \mathbb{F}_p^n} 1_A(y)1_B(x - y) = \frac{1}{p^n} |A \cap (x - B)|$$

So

$$1_A * 1_B(x) = \frac{1}{p^n} \# \text{ways } x \text{ can be written as } x = a + b \text{ with } a \in A, b \in B.$$

In particular, the support of $1_A * 1_B$ is the **sum set** $A + B = \{a + b : a \in A, b \in B\}$.

Lemma : 1.11

Given $f, g : \mathbb{F}_p^n \rightarrow \mathbb{C}$: $\widehat{f * g}(t) = \widehat{f}(t)\widehat{g}(t)$ for $t \in \mathbb{F}_p^n$.

Proof.

□

Example 1.12. $\|\widehat{f}\|_4^4 = \mathbb{E}_{x+y=w+z} f(x)f(y)\overline{f(w)f(z)}$.

We'll prove this in the first example sheet.

Lemma : 1.13 (Bogolyubov)

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 $2\alpha^{-2}$ such that $A + A - A - A \supset V$.

Proof. Observe that $A + A - A - A = \underbrace{\text{supp}(1_A * 1_A * 1_{-A} * 1_{-A})}_{g(x)}$. We wish to find $V \leq \mathbb{F}_p^n$

such that $g(x) > 0$ for all $x \in V$. Let $K = \text{Spec}_\rho(1_A)$ with ρ to be determined. Let $V = \langle K \rangle^\perp$. By lemma 1.8 we have $|K| \leq \rho^{-2}\alpha^{-1}$ and therefore $\text{codim}(V) \leq |K| \leq \rho^{-2}\alpha^{-1}$.

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

Clearly (1) ≥ 0 since $x \cdot t = 0$ for all $t \in K$ and $x \in V$.

On the other hand,

$$|(2)| \leq \sum_{t \notin K} |\widehat{1}_A(t)|^4 \leq \sup_{k \notin K} |\widehat{1}_A(t)|^2 \sum_t |\widehat{1}_A(t)|^2.$$

By Parseval's identity we get

$$|(2)| \leq (\rho\alpha)^2 \|1_A\|_2^2 = \rho^2\alpha^3.$$

So pick ρ such that $\rho^2\alpha^3 \leq \alpha^4/2$ (for example $\rho = \sqrt{\alpha/2}$) This gives $\text{codim}(V) \leq 2\alpha^{-2}$. □

Example 1.14. The set $A = \{x \in \mathbb{F}_2^n : |x| \geq \frac{n}{2} + \frac{\sqrt{n}}{2}\}$ has density at least $1/4$ and there is no coset C of any subspace of codimension \sqrt{n} such that $C \subset A + A$. We'll see this on example sheet 1.

Lemma : 1.15

Let $A \subset \mathbb{F}_p^n$ of density α be such that $\exists t \neq 0$ in $\text{Spec}_\rho(1_A)$. Then there exists $V \leq \mathbb{F}_p^n$ of codimension 1 and exists $x \in \mathbb{F}_p^n$ such that $|A \cap (x + V)| \geq \alpha(1 + \rho/2)|V|$.

Proof. Let $t \neq 0$ be such that $|\widehat{1}_A(t)| \geq \rho\alpha$, and let $V = \langle t \rangle^\perp$. Write $v_j + V$ for $j \in [p] = \{1, 2, \dots, p\}$ for the cosets of V such that $v_j + V = \{x \in \mathbb{F}_p^n : x \cdot t = j\}$. Then $\widehat{1}_A(t) = \widehat{f}_A(t) = \mathbb{E}_{x \in \mathbb{F}_p^n} (1_A(x) - \alpha)\omega^{x \cdot t} = \underbrace{\mathbb{E}_{j \in [p]} \mathbb{E}_{x \in v_j + V} (1_A(x) - \alpha)\omega^j}_{=: a_j}$ where $a_j = \frac{|A \cap (v_j + V)|}{|v_j + V|} - \alpha$. By the triangle inequality $\mathbb{E}_{j \in [p]} |a_j| \geq \rho\alpha$. Since $\mathbb{E}_{j \in [p]} a_j = 0$, $\mathbb{E}_{j \in [p]} (a_j + |a_j|) \geq \rho\alpha$ implies that there exists $j \in [p]$ such that $a_j + |a_j| \geq \rho\alpha$ therefore $a_j \geq \rho \frac{\alpha}{2}$. \square

Lecture 3

Lemma : 1.16

Let $p \geq 3$ and $A \subset \mathbb{F}_p^n$ has density $\alpha > 0$. Let A be such that $\sup_{k \neq 0} |\widehat{1}_A(t)| = o(1)$. Then A contains $(\alpha^3 + o(1))(p^n)^2$ 3-term arithmetic progressions.

Notation:

- 3-AP = 3-term arithmetic progression.
- Write $2 \cdot A = \{2a : a \in A\}$. It's important to distinguish this from $2A = A + A = \{a + a' : a, a' \in A\}$.

Proof. The number of 3-APs in A is $(p^n)^2$ times

$$\begin{aligned} T_3(1_A, 1_A, 1_A) &= \mathbb{E}_{x,d} [\widehat{1}_A(x) \widehat{1}_A(\underbrace{x+d}_y) \widehat{1}_A(x+2d)] \\ &= \mathbb{E}_{x,y} [\widehat{1}_A(x) \widehat{1}_A(y) \widehat{1}_A(2y-x)] = \mathbb{E}_y [\widehat{1}_A(y) \widehat{1}_A * \widehat{1}_A(2y)] \\ &= \langle \widehat{1}_{2 \cdot A}, \widehat{1}_A * \widehat{1}_A \rangle. \end{aligned}$$

By Plancharel's identity we get taht this is equal to

$$\langle \widehat{1}_{2 \cdot A}, \widehat{1}_A * \widehat{1}_A \rangle = \langle \widehat{1}_{2 \cdot A}, \widehat{1}_A \cdot \widehat{1}_A \rangle = \alpha^3 + \underbrace{\sum_{t \neq 0} \widehat{1}_A(t)^2 \overline{\widehat{1}_{2 \cdot A}(t)}}_{(1)}$$

. In absolute value, the sum above is

$$|(1)| \leq \sup_{t \neq 0} |\widehat{1}_A(t)| \sum_{t \neq 0} |\widehat{1}_A(t) \cdot \overline{\widehat{1}_{2 \cdot A}(t)}|$$

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

By Parseval this becomes

$$|(1)| \leq \sup_{t \neq 0} |\widehat{1}_A(t)| \cdot \alpha^{1/2} \cdot \alpha^{1/2}.$$

□

We shall combine these observations to prove the following:

Theorem : 1.17 - Meshulam

Let $A \subset \mathbb{F}_p^n$, $p \geq 3$, be a set containing no nontrivial 3-AP. Then $|A| = O\left(\frac{p^n}{n \log p}\right)$.

Proof. By assumption, $T_3(1_A, 1_A, 1_A) = \frac{\alpha}{p^n}$ but as in lemma 1.16 $T_3(1_A, 1_A, 1_A) = \alpha^3 + \sum_{t \neq 0} \widehat{1}_A(t)^2 \widehat{1}_{2 \cdot A}(t)$.

Observation:

Provided that $p^n \geq 2\alpha^{-2}$, we have

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

That is $\sup_{t \neq 0} |\widehat{1}_A(t)| \geq \frac{\alpha^2}{2}$.

By lemma 1.15 with $\rho = \frac{\alpha}{2}$ there exists $V \leq \mathbb{F}_p^n$ of codimension 1 and $x \in \mathbb{F}_p^n$ such that

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

We iterate this observation. Let $A_0 = A$, $V_0 = \mathbb{F}_p^n$, $\alpha_0 = \frac{|A_0|}{|V_0|} = \alpha$.

At step i we are given a set $A_{i-1} \subset V_{i-1}$ of density α_{i-1} with no nontrivial 3-APs.

Provided that $p^{\dim(V_{i-1})} \geq 2\alpha_{i-1}^{-2}$ there exists $V_i \leq V_{i-1}$ of codimension 1 and $x_i \in V_{i-1}$ such that

$$|A_{i-1} \cap (x_i + V_i)| \geq \left(\alpha_{i-1} + \frac{\alpha_{i-1}^2}{4}\right) |V_{i-1}|.$$

Set $A_i = A_{i-1} - x_i$. This set will be 3-AP-free because we're shifting a 3-AP-free set. Note that $\alpha_i \geq \alpha_{i-1} + \frac{\alpha_{i-1}^2}{4}$. Through this iteration, the density of A increases from α to 2α in at most $4\alpha^{-1}$ steps. From 2α to 4α in at most $2\alpha^{-1}$ steps,..., and reaches 1 in at most $4\alpha^{-1}(1 + 1/2 + 1/4 + \dots) = 8\alpha^{-1}$.

The argument must therefore end with $\dim(V_i) \geq n - 8\alpha^{-1}$ at which point we must've had $p^{\dim(V_i)} < 2\alpha_i^{-2} \leq 2\alpha^{-2}$. But we may assume that $\alpha \geq \sqrt{2}p^{-n/4}$ whence $p^{n-8\alpha^{-1}} \leq p^{n/2}$ or $n/2 \leq 8\alpha^{-1}$. \square

Lecture 4

Last time we proved that if $A \subset \mathbb{F}_3^n$ contains no non-trivial 3-APs, then $|A| = O(\frac{3^n}{n})$.

The largest known subset of \mathbb{F}_3^n containing no non-trivial 3-APs has size $\geq (2.218)^n$ due to Tyrrell (2022) - we'll return to this later.

From now on, let G be a finite abelian group. G comes equipped with a set of **characters**, i.e. group homomorphisms $\gamma : G \rightarrow \mathbb{C}^\times$, which themselves form a group, denoted by \widehat{G} , and is referred to as the **dual** of G .

It turns out that if G is finite abelian, then $\widehat{G} = G$.

For instance, if $G \simeq \mathbb{F}_p^n$, then $\widehat{G} = \{\gamma_t : x \mapsto \omega^{x \cdot t}, t \in G\}$. If $G = \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ (not p-adics!), then $\widehat{G} = \{\gamma_t : x \mapsto \omega^{xt}, t \in G\}$.

Definition 1.18. Given $f : G \rightarrow \mathbb{C}$ define its **Fourier transform** $\widehat{f} : \widehat{G} \rightarrow \mathbb{C}$ by

$$\widehat{f}(\gamma) = \mathbb{E}_{x \in G} f(x)\gamma(x) \quad \forall \gamma \in \widehat{G}.$$

It is easy to verify that

$$f(x) = \sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma) \overline{\gamma(x)}.$$

You may also check that definitions 1.6, 1.9; examples 1.3 and 1.10; and lemmas 1.5, 1.8, 1.11 go through in this more general context.

Example 1.19. Let p be a prime, let $L \leq p-1$ be even and consider $J = \left[-\frac{L}{2}, \frac{L}{2}\right] \subset \mathbb{Z}_p$.

Then $\forall t \neq 0$ we have $|\widehat{1}_J(t)| \leq \min\{\frac{L+1}{p}, \frac{1}{2|t|}\}$. We'll see this in Example Sheet 1.

Theorem : 1.20. (Roth)

Let $A \subset [N]$ be a set containing no nontrivial 3-APs. Then $|A| = O\left(\frac{N}{\log \log N}\right)$.

Lemma : 1.21

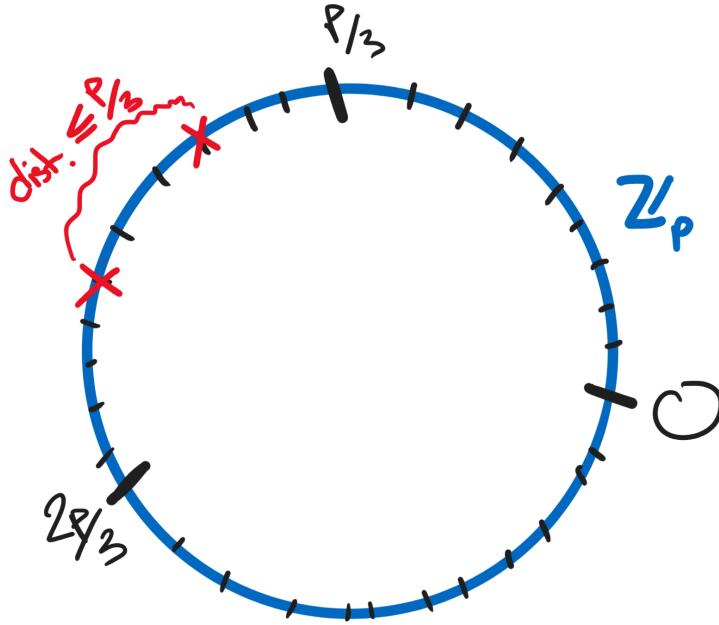
Let $A \subset [N]$ be of density $\alpha > 0$ satisfying $N > 50\alpha^{-2}$, containing no non-trivial 3-APs. Let p be a prime in $[\frac{N}{3}, \frac{2N}{3}]$ and write $A' = A \cap [p] \subset \mathbb{Z}_p$. Then either:

(i) $\sup_{t \neq 0} |\widehat{1_{A'}}(t)| \geq \frac{\alpha^2}{10}$ (where the Fourier coefficient is computed in \mathbb{Z}_p), or

(ii) There exists an interval $J \subset [N]$ of length $\geq \frac{N}{3}$ such that

$$|A \cap J| \geq \alpha \left(1 + \frac{\alpha}{400}\right) |J|.$$

Proof. We may assume that $|A'| = |A \cap [p]| \geq \alpha(1 - \frac{\alpha}{200})p$ since otherwise $|A \cap [p+1, N]| \geq \alpha(N-p) + \frac{\alpha^2 p}{200} \geq \alpha(1 + \frac{\alpha}{400})(N-p)$ so we would be in case (ii) with $J = [p+1, N]$. Let $A'' = A' \cap [\frac{p}{3}, \frac{2p}{3}]$. Note that all 3-APs of the form $(x, x+d, x+2d) \in A' \times A'' \times A''$ are in fact proper APs in $[N]$.



Note that because distance is less than $p/3$, there's no wrapping around!

If $|A' \cap [\frac{p}{3}]|$ or $|A' \cap [\frac{2p}{3}, p]|$ are at least $\frac{2}{5}|A'|$ we are again in case (ii).

We may assume that $|A''| \geq \frac{|A'|}{5}$. Now, as in lemma 1.16 and theorem 1.17, with $\alpha' = \frac{|A'|}{p}$, $\alpha'' = \frac{|A''|}{p}$ we have

$$\frac{\alpha''}{p} = \frac{|A''|}{p^2} = T_3(1_{A'}, 1_{A''}, 1_{A''}) = \alpha'(\alpha'')^2 + \sum_{t \neq 0} \widehat{1_{A'}}(t) \widehat{1_{A''}}(t) \overline{\widehat{1_{2 \cdot A''}}(t)}.$$

So as before $\frac{\alpha'(\alpha'')^2}{2} \leq \sup_{t \neq 0} |\widehat{1}_{A'}(t)|\alpha''$ provided that $\frac{\alpha''}{p} \leq \frac{\alpha'(\alpha'')^2}{2}$ which holds by assumption. \square

Lecture 5

We must convert the large Fourier coefficient into a density increment.

Lemma : 1.22

Let $m \in \mathbb{N}$ and let $\phi : [m] \rightarrow \mathbb{Z}_p$ taking $x \mapsto xt$ for some fixed $t \neq 0$. Given $\varepsilon > 0 \exists$ partition of $[m]$ into progressions P_i of length in $\left[\varepsilon \frac{\sqrt{m}}{2}, \varepsilon \sqrt{m}\right]$ such that $\text{diam}(\phi(P_i)) = \max_{x,y \in P_i} |\phi(x) - \phi(y)| \leq \varepsilon p$ for all i .

Proof. Let $u = \lfloor \sqrt{m} \rfloor$ and consider $0, t, 2t, \dots, ut$. By the pigeonhole principle we can find $0 \leq v < w \leq u$ such that $|wt - vt| \leq p/u$.

Divide $[m]$ into residue classes mod s , where $s = w - v$ (so $|st| \leq p/u$). Each of size at least $m/s \geq m/u$. But each residue class can be divided into progressions of the form $a, a + s, a + 2s, \dots, a + ds$ with $\frac{\varepsilon u}{2} < d \leq \varepsilon u$. The diameter of the image of each progression under φ is $|dst| < \varepsilon p$. \square

Lemma : 1.23

Let $A \subset [N]$ of density α . Let $p \in [\frac{N}{3}, \frac{2N}{3}]$ and $A' = A \cap [p] \subset \mathbb{Z}_p$. Suppose there exists $t \neq 0$ such that $|\widehat{1}_{A'}(t)| \geq \frac{\alpha^2}{10}$. Then there exists a progression P of length at least $\frac{\alpha^2 \sqrt{N}}{500}$ such that $|A \cap P| \geq \alpha(1 + \frac{\alpha}{80})|P|$.

Proof. Let $\varepsilon = \frac{\alpha^2}{40\pi}$, and use lemma 1.22 to partition $[p]$ into progressions P_i of length at least $\frac{\varepsilon \sqrt{p}}{2} \geq \frac{\alpha^2}{40\pi} \frac{\sqrt{\frac{N}{3}}}{2} \geq \frac{\alpha^2 \sqrt{N}}{500}$. The diameter $\phi(P_i) \leq \varepsilon p$. Fix one x_i from each P_i we have

$$\frac{\alpha^2}{10} \leq |\widehat{1}_{A'}(t)| = |\widehat{f}_{A'}(t)| = \frac{1}{p} \left| \sum_i \sum_{x \in P_i} f_{A'}(x) \omega^{xt} \right|.$$

We have

$$\begin{aligned} \frac{1}{p} \left| \sum_i \sum_{x \in P_i} f_{A'}(x) \omega^{xt} \right| &= \frac{1}{p} \left| \sum_i \sum_{x \in P_i} f_{A'}(x) \omega^{x_i t} \sum_i \sum_{x \in P_i} f_{A'}(x) (\omega^{xt} - \omega^{x_i t}) \right| \\ &\leq \frac{1}{p} \sum_i \left| \sum_{x \in P_i} f_{A'}(x) \right| + \frac{1}{p} \sum_i \sum_{x \in P_i} \underbrace{|f_{A'}(x)|}_{\leq 1} 2\pi\varepsilon \end{aligned} \quad (1)$$

since $|t(x_i - x)| \leq \varepsilon p$ for all $x \in P_i$. We have that

$$\frac{1}{p} \left| \sum_i \sum_{x \in P_i} f_{A'}(x) \omega^{xt} \right| \leq \frac{1}{p} \sum_i \left| \sum_{x \in P_i} f_{A'}(x) \right| + \frac{\alpha^2}{20}.$$

So we have

$$\frac{1}{p} \sum_i \left| \sum_{x \in P_i} f_{A'}(x) \right| \geq \frac{\alpha^2}{20}.$$

Since $f_{A'}$ has mean 0, we have

$$\sum_i \left(\left| \sum_{x \in P_i} f_{A'}(x) \right| + \sum_{x \in P_i} f_{A'}(x) \right) \geq \frac{\alpha^2 p}{20}.$$

So there exists i such that $\left| \sum_{x \in P_i} f_{A'}(x) \right| + \sum_{x \in P_i} f_{A'}(x) \geq \frac{\alpha^2 |P_i|}{40}$ and so $\sum_{x \in P_i} f_{A'}(x) \geq \frac{\alpha^2 |P_i|}{80}$. \square

We'll put these together to prove theorem 1.20 in the example sheet.

Behrend's Example 1.24. There exists a set $A \subset [N]$ containing no non-trivial 3-APs of size

$$|A| \geq C \exp(-c\sqrt{\log N})N$$

where c, C are absolute constants.

Definition 1.25. Let $\Gamma \subset \widehat{G}$ and $\rho > 0$. By the **Bohr set** $B(\Gamma, \rho)$ we mean $B(\Gamma, \rho) = \{x \in G : |\gamma(x) - 1| \leq \rho \forall \gamma \in \Gamma\}$. We call $|\Gamma|$ the **rank** and ρ the **radius** of the Bohr set.

Example 1.26. When $G = \mathbb{F}_p^n$, $B(\Gamma, \rho) = \langle \Gamma \rangle^\perp$ for all $\rho < 1$ (for $p = 3$).

Lemma : 1.27

Let $\Gamma \subset \widehat{G}$ be of size d , and let $\rho > 0$. Then $|B(\Gamma, \rho)| \geq \left(\frac{\rho}{2\pi}\right)^d |G|$.

Proof. We'll see this in example sheet 2. \square

Lemma : Bogolyubov's again

Given $A \subset \mathbb{Z}_p$ of density $\alpha > 0$, there exists $\Gamma \subset \widehat{\mathbb{Z}}_p$ of size at most $2\alpha^{-2}$ such that $B(\Gamma, \frac{1}{2}) \subset A + A - A - A$.

Lecture 6

Proof. Recall $1_A * 1_A * 1_{-A} * 1_{-A}(x) = \sum_{t \in \widehat{\mathbb{Z}}_p} |\widehat{1}_A(t)|^4 \omega^{-xt}$. Let $\Gamma = \text{Spec}_{\sqrt{\alpha/2}}(1_A)$ and note that for all $x \in B(\Gamma, \frac{1}{2})$ and $t \in \Gamma$, $\cos(\frac{2\pi xt}{p}) > 0$. Hence $\text{Re}(\sum_{t \in \widehat{\mathbb{Z}}_p} |\widehat{1}_A(t)|^4 \omega^{-xt}) = \underbrace{\sum_{t \in \Gamma} |\widehat{1}_A(t)|^4 \cos(\frac{2\pi xt}{p})}_{\geq \alpha^4} + \underbrace{\sum_{t \notin \Gamma} |\widehat{1}_A(t)|^4 \cos(\frac{2\pi xt}{p})}_{(1)}$. In absolute value we have

$$|(1)| \leq \sup |\widehat{1}_A(t)|^2 \sum |\widehat{1}_A(t)|^2 \leq (\sqrt{\frac{\alpha}{2}} \cdot \alpha)^2 \cdot \alpha = \frac{\alpha^4}{2}.$$

□

Chapter 2: Combinatorial Methods

Lecture 6

For now, let G be an abelian group. Given $A, B \subset G$. We defined $A \pm B = \{a \pm b : a \in A, b \in B\}$. If A and B are finite, then

$$\max\{|A|, |B|\} \leq |A \pm B| \leq |A| \cdot |B|.$$

(better bounds are available in certain settings)

Example 2.1. Let $V \leq \mathbb{F}_p^n$ be a subspace, then $V + V = V$. So $|V + V| = |V|$. In fact, if $A \subset \mathbb{F}_p^n$ such that $|A + A| = |A|$ then A must be a coset of a subspace.

Example 2.2. Let $A \subset \mathbb{F}_p^n$ be such that $|A + A| < \frac{3}{2}|A|$. Then $\exists V \leq \mathbb{F}_p^n$ such that $A \subset V$ and $|V| \leq \frac{3}{2}|A|$. We'll see this in example sheet 2 (**check, it may be wrong**)

Example 2.3. Let $A \subset \mathbb{F}_p^n$ be a set of linearly independent vectors. Then $A + A$ has size $\binom{|A|}{2}$. But $|A| \leq n$ (small!)

Let $A \subset \mathbb{F}_p^n$ be a set chosen at random with probability $p^{-\theta n}$ for some $\theta \in (\frac{1}{2}, 1]$. Then with high probability $|A + A| = (1 - o(1)) \frac{|A|^2}{2}$.

Definition 2.4. Given finite sets $A, B \subset G$ we define the **Ruzsa distance** $d(A, B)$ between A and B by

$$d(A, B) = \log \left(\frac{|A - B|}{\sqrt{|A| \cdot |B|}} \right).$$

$d(A, B)$ is clearly non-negative and symmetric.

Lemma : 2.5 - (Ruzsa's Triangle Inequality)

Given finite sets $A, B, C \subset G$, we have:

$$d(A, C) \leq d(A, B) + d(B, C).$$

Proof. Observe that $|B| \cdot |A - C| \leq |A - B| \cdot |B - C|$. Indeed, writing each $d \in A - C$ as $d = a_d - c_d$ for some $a_d \in A, c_d \in C$. The map $\phi : B \times (A - C) \rightarrow (A - B) \times (B - C)$ via $(b, d) \mapsto (a_d - b, b - c_d)$. You can easily check that this is injective. The triangle inequality follows from the definition of d . \square

Definition 2.6. Given a finite set $A \subset G$ we write $\sigma(A) = \frac{|A + A|}{|A|}$ for the **doubling constant** and $\delta(A) = \frac{|A - A|}{|A|}$ for the **difference constant** of A .

Lemma 2.5 tells us for example that

$$d(A, A) \leq d(A, -A) + d(-A, A)$$

So

$$\log(\delta(A)) \leq 2 \log(\sigma(A))$$

Therefore $\delta(A) \leq \sigma(A)^2$ or $|A - A| \leq \frac{|A + A|^2}{|A|}$.

Notation: Given $A \subset G$ and $l, m \in \mathbb{N}_0$. Write $lA - mA$ for the set

$$\underbrace{A + A + \cdots + A}_{l\text{-times}} - \underbrace{A - A - \cdots - A}_{m\text{-times}}$$

Theorem : 2.7 - Plünnecke's Inequality

Let $A, B \subset G$ be finite sets such that $|A + B| \leq K|A|$ for some $K > 0$. Then for any $l, m \in \mathbb{N}_0$, $|lB - mB| \leq K^{l+m}|A|$.

Proof. WLOG assume that $|A + B| = K|A|$. Choose a nonempty subset $A' \subset A$ such that the ratio $\frac{|A' + B|}{|A'|}$ is minimized, and call this minimal ratio K' . Then $|A' + B| = K'|A|$, $K' \leq K$ and $|A'' + B| \geq K'|A''|$ for $A'' \subset A$.

Claim: For any finite $C \subset G$, $|A' + B + C| \leq K'|A' + C|$. (finishing the proof in Lecture 7:) We first show that $|A' + mB| \leq K'^m|A'|$ for all $m \in \mathbb{N}_0$. We do this by induction: $m = 0 \checkmark$, $m = 1 \checkmark$. Suppose $m > 1$ and the result holds for $m - 1$. By the claim with $C = (m - 1)B$ we get

$$|A' + mB| = |A' + B + (m - 1)B| \leq K'|A' + (m - 1)B| \leq K'^{m-1}|A'| \quad \checkmark$$

As in the proof of Ruzsa's triangle inequality, $|A'| \cdot |lB - mB| \leq |A' + lB| \cdot |A' + mB| \leq K^n|A'| \cdot K'^m|A'|$ Therefore $|lB - mB| \leq K^{n+m}|A'| \leq K^{l+m}|A|$.

We now prove the claim by induction on $|C|$.

$|C| = 1 \checkmark$ Suppose the claim holds for C and consider $C' = C \cup \{x\}$ for some $x \notin C$.

Observe $A' + B + C' = (A' + B + C) \cup (A' + B + x)$ and in fact $A' + B + C' = (A' + B + C) \cup ((A' + B + x) \setminus (D + B + x))$ where $D = \{a \in A' : a + B + x \subset A' + B + C\}$. By definition of K' , $|D + B| \geq K'|D|$ therefore

$$\begin{aligned} |A' + B + C'| &\leq |A' + B + C| + |(A' + B + x) \setminus (D + B + x)| \\ &\leq |A' + B + C| + |A' + B| - |D + B| \\ &\leq K'|A' + C| + K'|A'| - K'|D| \\ &= K'(|A' + C| + |A'| - |D|) \end{aligned}$$

We apply the same argument again, writing

$$A' + C' = (A' + C) \cup ((A' + x) \setminus (E + x))$$

where $E = \{a \in A' : a + x \in A' + C\} \subset D$. We conclude that $|A' + C'| = |A' + C| + |A'| - |E| \geq |A' + C| + |A'| - |D|$. So $|A' + B + C'| \leq K'(|A' + C| + |A'| - |D|) \leq K'|A' + C'|$ which concludes the proof of our theorem. \square

Lecture 7

We are now in a position to generalize example 2.2.

Theorem : Frieman-Ruzsa Theorem 2.8.

Let $A \subset \mathbb{F}_p^n$ be such that $|A + A| \leq K|A|$ (i.e. $\sigma(A) \leq K$) for some $K > 0$. Then A is contained in a coset of a subspace $H \leq \mathbb{F}_p^n$ of size $|H| \leq K^2 p^{K^4} |A|$.

Proof. Choose $X \subset 2A - A$ maximal such that the translates $x + A$ for $x \in X$ are disjoint. X cannot be too large because for all $x \in X$, $x + A \subset 3A - A$ and by Plunnecke, $|3A - A| \leq K^4 |A|$ but the translates $x + A$ for $x \in X$ are disjoint and each of size $|A|$ so

$$|X| \cdot |A| = |\cup_{x \in X} (x + A)| \leq |3A - A|$$

Therefore $|X| \leq K^4$. We now show that

$$2A - A \subset X + A - A \tag{*}$$

Indeed, if $y \in 2A - A$ and $y \notin X$, then $(y + A) \cap (x + A) \neq \emptyset$ for some $x \in X$ by maximality of X . So $y \in X + A - A$. If $y \in X$ then it's clear. It follows by induction from (*) that for all $l \geq 2$

$$lA - A \subset (l-1)X + A - A \tag{**}$$

(since $lA - A = A + (l-1)A - A \stackrel{hi}{\subset} A + (l-2)X + A - A = (l-2)X + 2A - A \stackrel{(*)}{\subset} (l-1)X + A - A$). Now let H be the subgroup of \mathbb{F}_p^n generated by A , which we can write as

$$H \subset \bigcup_{l \geq 1} (lA - A) \stackrel{(**)}{\subset} Y + A - A.$$

where Y is the subgroup generated by X . Then $|Y| \leq p^{|X|} \leq p^{K^4}$ so

$$|H| \leq |Y + A - A| = |Y| \cdot |A - A| \leq p^{K^4} K^2 |A|.$$

□

Lecture 8

Example 2.9. Let $A = H \cup R \subset \mathbb{F}_p^n$ where $H \leq \mathbb{F}_p^n$ is a subspace of dimension d with $k << d << n - K$ and R consists of $K - 1$ linearly independent vectors in H^\perp . Then $|A| = |H \cup R| \sim |H|$ and $|A + A| = |(H \cup R) + (H \cup R)| = |(H + H) \cup (H + R) \cup (R + R)| \sim K|H|$ but any subspace $V \leq \mathbb{F}_p^n$ containing A must have size $\geq p^{d+(K-1)} = |H|p^{K-1} \sim |A|p^{k-1}$, where the constant is exponential in K .

Conjecture : 2.10 Polynomial Frieman-Ruzsa

Let $A \subset \mathbb{F}_p^n$ such that $|A + A| \leq K|A|$. Then there is a subspace $H \leq \mathbb{F}_p^n$ of size at most $C_1(K) \leq A$ such that for some $x \in \mathbb{F}_p^n$, $|A \cap (x + H)| \geq \frac{|A|}{C_2(K)}$, where $C_1(K)$ and $C_2(K)$ are polynomial in K .

For $p = 2$, this is now a theorem.

Definition 2.11. Given an abelian group G and finite sets $A, B \subset G$, define the **additive energy** between A and B to be

$$E(A, B) = \frac{\#\{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}}{|A|^{3/2} |B|^{3/2}}.$$

We refer to quadruples $(a, a', b, b') \in A \times A \times B \times B$ such that $a + b = a' + b'$ as **additive quadruples**.

Observe that if G is finite, then

$$|A|^3 E(A, A) = |G|^3 \mathbb{E}_{x+y=z+w} [1_A(x)1_A(y)1_A(z)1_A(w)] = |G|^3 \|\widehat{1_A}\|_4^4$$

This comes from example sheet 1.

Example 2.12. When $H \leq \mathbb{F}_p^n$, then $E(V, V) = 1$

Lemma : 2.13

Let G be abelian and let $A, B \subset G$ be finite. Then $E(A, B) \geq \frac{\sqrt{|A| \cdot |B|}}{|A + B|}$.

Proof. Note that

$$|A|^{3/2} |B|^{3/2} E(A, B) = \#\{(a, a', b, b') \in A^2 \times B^2 : a + b = a' + b'\} = \sum_{x \in G} r_{A+B}(x)^2.$$

where $r_{A+B}(x) = \#\text{ways of writing } x \text{ as } a+b \text{ with } a \in A, b \in B$. Observe that $\sum_{x \in G} r_{A+B}(x) = |A| \cdot |B|$. So

$$|A|^{3/2} |B|^{3/2} E(A, B) = \sum_{x \in G} r_{A+B}(x)^2 \geq \frac{(\sum_{x \in G} r_{A+B}(x))^2}{\sum_{x \in G} 1_{A+B}(x)} = \frac{(|A| \cdot |B|)^2}{|A + B|}.$$

Therefore

$$E(A, B) \geq \frac{\sqrt{|A| \cdot |B|}}{|A + B|}.$$

□

In particular if $A \subset G$ such that $|A + A| \leq K|A|$, then $E(A) \geq \frac{1}{K}$. The converse is NOT true.

Example 2.14. Let G be your favorite class of abelian group. Then there exists constants $\eta, \theta > 0$ such that for all sufficiently large n , there exists $A \subset G$ with $|A| = n$ satisfying $E(A, A) \geq \eta$ and $|A + A| \geq \theta|A|^2$. We'll see this in ExSheet2.

Theorem : 2.15 (Balog-Szemeredi-Gowers)

Let G be an abelian group, and let $A \subset G$ be finite such that $E(A, A) \geq \eta$ for some $\eta > 0$. Then $\exists A' \subset A$ of size at least $c(\eta)|A|$ such that $|A' + A'| \leq C(\eta)|A|$ where $c(\eta)$ and $C(\eta)$ are polynomial in η .

We first prove a technical lemma, using a method known as "dependent random choice".

Lemma : 2.16

Let $A_1, A_2, \dots, A_m \subset [n]$ and suppose that $\sum_{i,j} |A_i \cap A_j| \geq \delta^2 nm^2$. Then there exists $X \subset [m]$ of size at least $\frac{\delta^5 m}{\sqrt{2}}$ such that $|A_i \cap A_j| \geq \frac{\delta^2 n}{2}$ for at least 90% of pairs $(i, j) \in X^2$.

Proof. Let x_1, x_2, x_3, x_4, x_5 be random from $[n]$, and let $X = \{i \in [m] : x_j \in A_i \forall j \in [5]\}$. Observe that if $|A_i \cap A_j| = \gamma n$, then $\mathbb{P}((i, j) \in X^2) = \gamma^5$ and hence (by convexity)

$$\mathbb{E}|X^2| = \sum_{i,j} \mathbb{P}((i, j) \in X^2) \geq \delta^{10} m^2.$$

Let us call a pair (i, j) "bad" if $|A_i \cap A_j| < \frac{\delta^2 n}{2}$. As before, $\mathbb{E}(\#\text{bad pairs in } X^2) \leq \frac{\delta^{10}}{2^5} m^2$.

Hence $\mathbb{E}(|X^2| - 16\#\text{bad pairs in } X^2) \geq \frac{\delta^{10}}{2^5} m^2$. So there must be a choice of x_1, x_2, x_3, x_4, x_5 such that $|X| \geq \frac{\delta^5 m}{\sqrt{2}}$ and the proportion of bad pairs in X^2 is at most $\frac{1}{16} < 10\%$. □

Lecture 9

Proof of BSG. We call a difference d "popular" if d can be written as $d = x - y$ with $x, y \in A$ in at least $\eta \frac{|A|}{2}$ ways. i.e. $r_{A-A}(d) \geq \eta \frac{|A|}{2}$.

There must be at least $\eta \frac{|A|}{2}$ popular differences, because if not,

$$\eta |A|^3 \leq \sum_d r_{A-A}(d)^2 = \sum_{d-\text{pop}} r_{A-A}(d)^2 + \sum_{d-\text{unpop}} r_{A-A}(d)^2 < \eta \frac{|A|}{2} |A|^2 + \eta \frac{|A|}{2} \sum_{d-\text{unpop}} r_{A-A}(d)$$

So

$$\eta |A|^3 < \eta \frac{|A|}{2} |A|^2 + \eta \frac{|A|}{2} |A - A| \leq \eta \frac{|A|}{2} |A|^2 + \eta \frac{|A|}{2} |A|^2.$$

and this gives a contradiction.

Define a graph with vertex set A , joining x and y by an edge if and only if $y - x$ is a popular difference. Then $\mathbb{E}_{x \in A} [|N(x)|] = \frac{1}{|A|} \sum_{x \in A} |\underbrace{N(x)}_{\#y:y \sim x}| \geq \frac{\eta |A|}{2}$. We can also have $\mathbb{E}_{x,y \in A} |N(x) \cap N(y)| \geq \frac{\eta^2 |A|}{4}$. Indeed,

$$\begin{aligned} \mathbb{E}_{x,y \in A} [|N(x) \cap N(y)|] &= \mathbb{E}_{x,y \in A} \left[\sum_{z \in A} 1_{N(x)}(z) 1_{N(y)}(z) \right] = \sum_{z \in A} \left(\mathbb{E}_{x \in A} 1_{N(x)}(z) \right)^2 \\ &\geq \frac{1}{|A|} \left(\sum_{z \in A} \mathbb{E}_{x \in A} 1_{N(x)}(z) \right)^2 = \frac{1}{|A|} \left(\mathbb{E}_{x \in A} |N(x)| \right)^2 \\ &\geq \frac{1}{|A|} \left(\frac{\eta |A|}{2} \right)^2. \end{aligned}$$

We apply lemma 2.16 with $m = n = |A|$ and $\delta^2 = \frac{\eta^2}{4}$ to find a subset $A' \subset A$ of size $\geq \eta^{10} \frac{|A|}{2^{11}}$ with the property that $|N(x) \cap N(y)| \geq \frac{\eta^2 |A|}{8}$ for at least 90% of $(x, y) \in A'^2$. But then for at least 10% of $x \in A'$, $|N(x) \cap N(y)| \geq \frac{\eta^2 |A|}{8}$ for at least 80% of $y \in A'$. Hence there exists $A'' \cap A'$ of size $\geq \eta^{10} \frac{|A|}{2^{15}}$ such that for all $x \in A''$ at least 80% of $z \in A'$ satisfy $|N(x) \cap N(z)| \geq \frac{\eta^2 |A|}{8}$.

Let $x, y \in A''$ then there are at least $\frac{\eta^{10} |A|}{2^{12}}$ many $z \in A'$ such that $|N(x) \cap N(y)| \geq \frac{\eta^2 |A|}{8}$ and $|N(y) \cap N(z)| \geq \frac{\eta^2 |A|}{8}$. We shall prove an upper bound on $|A'' - A''|$ by showing that each element of $A'' - A''$ can be written as a linear combination of distinct octuples from A . For each such z , there are at least $\left(\frac{\eta^2 |A|}{8} \right)^2$ pairs (u, v) such that $u \in N(x) \cap N(y)$ and

$v \in N(y) \cap N(z)$.

For each such pair (u, v) , the elements $u - x, z - u, v - z, y - v$ are all popular differences.

Hence, for each pair (u, v) there are at least $\left(\frac{\eta|A|}{2}\right)^4$ octuples $(a_1, a_2, \dots, a_8) \in A^8$ such that $u - x = a_2 - a_1, v - z = a_6 - a_5, z - u = a_4 - a_3, y - v = a_8 - a_7$. In other words, there are at least

$$\underbrace{\left(\frac{\eta^{10}|A|}{2^{12}}\right)}_z \cdot \underbrace{\left(\frac{\eta^2|A|}{8}\right)}_{u,v} \cdot \underbrace{\left(\frac{\eta|A|}{2}\right)}_{a_1,\dots,a_8} = \frac{\eta^{18}}{2^{22}}|A|^7$$

octuples $(a_1, \dots, a_8) \in A^8$ such that $y - x = \underbrace{a_2 - a_1}_{u-x} + \underbrace{a_4 - a_3}_{z-u} + \underbrace{a_6 - a_5}_{v-z} + \underbrace{a_8 - a_7}_{y-v}$. But distinct $y - x$ give rise to distinct octuples

$$\frac{\eta^{18}}{2^{22}}|A|^7 \cdot |A'' - A''| \leq |A|^8.$$

Hence

$$|A'' - A''| \leq 2^{22}\eta^{-18}|A| \leq 2^{27}\eta^{-28}|A''|.$$

$|A'' + A''|$ follows from Plunnecke. \square

Chapter 3: Probabilistic Tools

Lecture 9

Proposition : 3.1 (Khintchine's inequality)

Let X_1, X_2, \dots, X_n be independent random variables, taking values $\pm x_i$ with probability $1/2$ for all i . Then for all $p \in [2, \infty)$ we have

$$\left\| \sum_{i=1}^n X_i \right\|_{L^p(\mathbb{P})} = O \left(p^{1/2} \left(\sum_{i=1}^n \|X_i\|_{L^2(\mathbb{P})}^2 \right)^{1/2} \right).$$

The constant doesn't depend on p .

Proof. By nesting of norms, it suffices to prove the case $p = 2k$ with $k \in \mathbb{N}$. Write $X = \sum_{i=1}^n X_i$ and wlog assume that $\sum_{i=1}^n \|X_i\|_\infty^2 = \sum_{i=1}^n \|X_i\|_2^2 = 1$. By Chernoff (example 1.3) $\forall \theta \geq 0, \mathbb{P}(|X| \geq \theta) \leq 4 \exp(-\theta^2/4)$ so

$$\|X\|_{L^{2k}(\mathbb{P})}^{2k} = \int_0^\infty 2kt^{2k-1} \mathbb{P}[|X| \geq t] dt \leq 8k \underbrace{\int_0^\infty t^{2k-1} \exp(-t^2/4) dt}_{=I(k)}.$$

We shall prove by induction on k that $I(k) \leq \frac{C^{2k}(2k)^k}{4k}$.

If $k = 1$, then $\int_0^\infty t \exp\left(-\frac{t^2}{4}\right) dt = [-2 \exp(-t^2/4)]_0^\infty = 2 \leq \frac{C^2 \cdot 2}{4}$ if $C \geq 2$.

For $k > 1$, doing integration by parts yields

$$\begin{aligned}
I(k) &= \int_0^\infty t^{2k-2} \cdot t \exp(-t^2/4) dt \\
&= [t^{2k-2}(-2) \exp(-t^2/4)]_0^\infty - \int_0^\infty (2k-2)t^{2k-3}(-2) \exp(-t^2/4) dt \\
&= 4(k-1) \int_0^\infty t^{2(k-1)-1} \exp(-t^2/4) dt \\
&= 4(k-1)I(k-1)
\end{aligned}$$

By the inductive hypothesis we have

$$I(k) \leq \frac{4(k-1)C^{2(k-1)}(2(k-1))^{k-1}}{4(k-1)}$$

If $C \geq \sqrt{2}$ we get the desired conclusion. \square

Lecture 10

Corollary : 3.2 - Rudin's inequality

Let $\Lambda \subset \widehat{\mathbb{F}_2^n}$ be a linearly independent set and let $p \in [2, \infty)$. Then for all $\widehat{f} \in \ell^2(\Lambda)$ (i.e. $\widehat{f} : \Lambda \rightarrow \mathbb{C}$) we have

$$\left\| \sum_{\gamma \in \Lambda} \widehat{f}(\gamma) \gamma \right\|_{L^p(\mathbb{F}_2^n)} = O\left(\sqrt{p} \cdot \|\widehat{f}\|_{\ell^2(\Lambda)}\right).$$

Corollary : 3.3 - Dual form of Rudin's inequality

Let $\Lambda \subset \widehat{\mathbb{F}_2^n}$ be a linearly independent set and let $p \in (1, 2]$ then for all $f \in L^p(\mathbb{F}_2^n)$,

$$\|\widehat{f}\|_{\ell^2(\Lambda)} = O\left(\sqrt{\frac{p}{p-1}} \cdot \|f\|_{L^p(\mathbb{F}_2^n)}\right)$$

Proof. Let $f \in L^p(\mathbb{F}_2^n)$ and write $g = \sum_{\gamma \in \Lambda} \widehat{f}(\gamma) \gamma$. Then

$$\|\widehat{f}\|_{\ell^2(\Lambda)}^2 = \sum_{\gamma \in \Lambda} |\widehat{f}(\gamma)|^2 \stackrel{?}{=} \sum_{\gamma \in \Lambda} \widehat{f}(\gamma) \overline{\widehat{g}(\gamma)} = \langle \widehat{f}, \widehat{g} \rangle_{\ell^2(\Lambda)} = \langle \widehat{f}, \widehat{g} \rangle_{\ell^2(\mathbb{F}_2^n)}$$

By Plancharel, this is $\langle f, g \rangle_{L^2(\mathbb{F}_2^n)}$. By Holder, $\langle f, g \rangle_{L^2(\mathbb{F}_2^n)} \leq \|f\|_{L^p(\mathbb{F}_2^n)} \|g\|_{L^{p'}(\mathbb{F}_2^n)}$ where $\frac{1}{p} + \frac{1}{p'} = 1$. By Rudin's inequality with p' :

$$\|g\|_{L^{p'}(\mathbb{F}_2^n)} = O\left(\sqrt{p'} \|\widehat{g}\|_{\ell^2(\Lambda)}\right) = O\left(\sqrt{\frac{p}{p-1}} \|\widehat{f}\|_{\ell^2(\Lambda)}\right).$$

So

$$\|\widehat{f}\|_{\ell^2(\Lambda)}^2 = \|f\|_{L^p(\mathbb{F}_2^n)} O\left(\sqrt{\frac{p}{p-1}} \|\widehat{f}\|_{\ell^2(\Lambda)}\right)$$

The result follows after dividing on both sides by $\|\widehat{f}\|_{\ell^2(\Lambda)}$. \square

Recall that given $A \subset \mathbb{F}_2^n$ of density $\alpha > 0$, $|Spec_\rho(1_A)| \leq \rho^{-2} \alpha^{-1}$. This is best possible, as the example of a subspace $H \leq \mathbb{F}_2^n$ shows: $Spec_1(1_H) = H^\perp$ so $|Spec_1(1_H)| = |H^\perp| = \frac{|\mathbb{F}_2^n|}{|H|} = \alpha^{-1}$.

Theorem : 3.4. - Special case of Chang's

Let $A \subset \mathbb{F}_2^n$ be a set of density $\alpha > 0$. Then for all $\rho > 0$, there exists a subspace $H \leq \mathbb{F}_2^n$ of dimension at most $O(\rho^{-2} \log(\alpha^{-1}))$ such that $H \supset Spec_\rho(1_A)$.

Proof. Let $\Lambda \subset Spec_\rho(1_A)$ be a maximal linearly independent subset of $Spec_\rho(1_A)$ and let $H = \langle Spec_\rho(1_A) \rangle$. Then $\dim(H) = |\Lambda|$. By corollary 3.3, $\forall p \in (1, 2]$,

$$|\Lambda|(\rho\alpha)^2 \leq \sum_{\gamma \in \Lambda} |\widehat{1}_A(\gamma)|^2 = \|\widehat{1}_A\|_{\ell^2(\Lambda)}^2 = O\left(\frac{p}{p-1} \|1_A\|_{L^p(\mathbb{F}_2^n)}^2\right).$$

We have $\|1_A\|_{L^p(\mathbb{F}_2^n)}^2 = \left(\mathbb{E}_y |1_A(y)|^p\right)^{2/p} = \alpha^{2/p}$. So $|\Lambda| \leq \rho^{-2} \alpha^{-2} O\left(\frac{p}{p-1} \alpha^{2/p}\right)$.

Choose $p = 1 + (\log(\alpha^{-1}))^{-1}$ to get $|\Lambda| = O(\rho^{-2} \log(\alpha^{-1}))$. \square

Definition 3.5. Let G be a finite abelian group. We say $S \subset G$ is **dissociated** if $\sum_{s \in S} \varepsilon_s s = 0$ for some $\varepsilon_s \in \{-1, 0, 1\}^{|S|}$, then $\varepsilon \equiv 0$.

Note that if $G = \mathbb{F}_2^n$, then a set $S \subset G$ is dissociated if and only if it is linearly independent.

Lecture 11

Theorem : 3.6 - Chang's Theorem

Let G be a finite abelian group, and let $A \subset G$ of density $\alpha > 0$. If $\Lambda \subset Spec_\rho(1_A)$ is dissociated, then $|\Lambda| = O(\rho^{-2} \log(\alpha^{-1}))$.

We may bootstrap Khintchine's inequality to obtain the following:

Theorem : 3.7 - Marcinkiewicz-Zygmund inequality

Let $p \in [2, \infty)$, and let $X_1, X_2, \dots, X_n \in L^p(\mathbb{P})$ be independent random variables with $\mathbb{E}[\sum_{i=1}^n X_i] = 0$. Then $\|\sum_{i=1}^n X_i\|_{L^p(\mathbb{P})} = O\left(p^{1/2} \|\sum_{i=1}^n |X_i|^2\|_{L^{p/2}(\mathbb{P})}^{1/2}\right)$.

Proof. For \mathbb{C} -valued random variables, the result follows from the real case by taking real and imaginary parts and applying the triangle inequality.

Next, assume the distribution of the X_i 's is symmetric i.e. $\mathbb{P}(X_i = a) = \mathbb{P}(X_i = -a)$ for all $a \in \mathbb{R}$. Partition the probability space Ω into sets $\Omega_1, \Omega_2, \dots, \Omega_M$ writing \mathbb{P}_j for the induced measure on Ω_j such that all X_i 's are symmetric and take at most 2 values on each Ω_j .

Applying Khintchine for each $j \in [M]$ we get

$$\left\| \sum_{i=1}^n X_i \right\|_{L^p(\mathbb{P}_j)}^p = O \left(p^{p/2} \left(\sum_{i=1}^n \|X_i\|_{L^2(\mathbb{P}_j)}^2 \right)^{p/2} \right) = O \left(p^{p/2} \left\| \sum_{i=1}^n |X_i|^2 \right\|_{L^{p/2}(\mathbb{P}_j)}^{p/2} \right).$$

So sum over all $j \in [M]$ and take the p -th root to get the symmetric case.

Now suppose X_i 's are arbitrary and let Y_1, \dots, Y_n be such that $X_i \sim Y_i$ and $X_1, X_2, \dots, X_n, Y_1, \dots, Y_n$ are independent. Applying the symmetric result to $X_i - Y_i$ we get

$$\begin{aligned} \left\| \sum_{i=1}^n (X_i - Y_i) \right\|_{L^p(\mathbb{P} \times \mathbb{P})} &= O \left(p^{1/2} \left\| \sum_{i=1}^n |X_i - Y_i|^2 \right\|_{L^{p/2}(\mathbb{P} \times \mathbb{P})}^{1/2} \right) \\ &= O \left(p^{1/2} \left\| \sum_{i=1}^n |X_i|^2 \right\|_{L^{p/2}(\mathbb{P})}^{1/2} \right) \end{aligned}$$

But also

$$\left\| \sum_{i=1}^n X_i \right\|_{L^p(\mathbb{P})} = \left\| \sum_{i=1}^n X_i - \mathbb{E} \sum_{i=1}^n Y_i \right\|_{L^p(\mathbb{P})} \leq \left\| \sum_{i=1}^n (X_i - Y_i) \right\|_{L^p(\mathbb{P} \times \mathbb{P})}$$

by complexity. \square

Theorem : 3.8 - Croot-Sisask Almost Periodicity

Let G be a finite abelian group, $\varepsilon > 0$, and $p \in [2, \infty)$. Let $A, B \subset G$ be such that $|A + B| \leq K|A|$ and let $F : G \rightarrow \mathbb{C}$. Then, there exists $b \in B$ and $X \subset B - b$ such that $|X| \geq (2K)^{-O(\varepsilon^{-2}p)}|B|$ and

$$\|\tau_x(f * \mu_A) - f * \mu_A\|_{L^p(G)} \leq \varepsilon \|f\|_{L^p(G)}$$

for all $x \in X$ where $\tau_x g(y) = g(y + x)$ and μ_A is the characteristic measure of A .

Proof. The main idea is to approximate $f * \mu_A(y) = \mathbb{E}_x \mu_A(x)f(y - x) = \mathbb{E}_{x \in A} f(y - x)$ by $\frac{1}{k} \sum_{i=1}^k f(y - Z_i)$ with Z_i sampled independently at random from A (say $Z = (Z_1, \dots, Z_k)$), for some choice of k . For each $y \in G$ define $Z_i(y) = \tau_{-Z_i}(f)(y) - f * \mu_A(y)$. For fixed $y \in G$

these are independent and have mean zero, so by Marcinkiewicz-Zygmund,

$$\begin{aligned} \left\| \sum_{i=1}^k Z_i(y) \right\|_{L^p(\mathbb{P})}^p &= O \left(p^{p/2} \left\| \sum_{i=1}^k |Z_i(y)|^2 \right\|_{L^{p/2}(\mathbb{P})}^{p/2} \right) \\ &= O \left(p^{p/2} \mathbb{E} \underbrace{\left| \sum_{i=1}^k |Z_i(y)|^2 \right|}_{(1)}^{p/2} \right) \end{aligned}$$

Using Holder with $\frac{2}{p} + \frac{1}{p'} = 1$, we have

$$(1) \leq \left(\sum_{i=1}^k 1^{p'} \right)^{1/p' \cdot 2} \left(\sum_{i=1}^k |Z_i(y)|^{2 \cdot p/2} \right)^{2/p \cdot p/2} = k^{p/2-1} \sum_{i=1}^k |Z_i(y)|^p.$$

So for each $y \in G$,

$$\left\| \sum_{i=1}^k Z_i(y) \right\|_{L^p(\mathbb{P})}^p = O \left(p^{p/2} k^{p/2-1} \mathbb{E} \sum_{i=1}^k |Z_i(y)|^p \right).$$

Lecture 12

Summing over $y \in G$,

$$\mathbb{E}_{y \in G} \left\| \sum_{i=1}^k Z_i(y) \right\|_{L^p(\mathbb{P})}^p = O \left(p^{p/2} k^{p/2-1} \mathbb{E} \sum_{i=1}^k \mathbb{E}_{y \in G} |Z_i(y)|^p \right)$$

with $\left(\mathbb{E}_{y \in G} |Z_i(y)|^p \right)^{1/p} = \|Z_i\|_{L^p(\mathbb{P})} \leq \underbrace{\|\tau_{-Z_i}(f)\|_{L^p(G)}}_{=\|f\|_{L^p(G)}} + \underbrace{\|f * \mu_A\|_{L^p(G)}}_{\leq \|f\|_{L^p(G)}}$. Here we're using Young's

convolution inequality: If $1 + \frac{1}{r} = \frac{1}{q} + \frac{1}{p}$ then $\|f * g\|_r \leq \|f\|_p \|g\|_q$. It follows that

$$\begin{aligned} \mathbb{E}_{Z \in A^k} \mathbb{E}_{y \in G} \left| \sum_{i=1}^k Z_i(y) \right|^p &= O \left(p^{p/2} k^{p/2-1} \mathbb{E}_{Z \in A^k} \sum_{i=1}^k 2 \|f\|_{L^p(G)}^p \right) \\ &= O \left(p^{p/2} k^{p/2} \|f\|_{L^p(G)}^p \right) \\ &= O \left((pk \|f\|_{L^p(G)}^2)^{\frac{p}{2}} \right) \end{aligned}$$

This implies

$$\underbrace{\mathbb{E}_{Z \in A^k} \mathbb{E}_{y \in G} \left| \frac{1}{k} \sum_{i=1}^k [\tau_{-Z_i}(f)(y) - f * \mu_A(y)] \right|^p}_{(*)} = O \left((pk^{-1} \|f\|_{L^p(G)}^2)^{\frac{p}{2}} \right).$$

Choose $k = O(\varepsilon^{-2}p)$ such that the RHS is at most $\left(\frac{\varepsilon}{4}\|f\|_{L^p(G)}\right)^p$. Write

$$L = \left\{ (Z_1, \dots, Z_k) \in A^k : (\star) \leq \left(\frac{\varepsilon}{2}\|f\|_{L^p(G)}\right)^p \right\}$$

By Markov since $\mathbb{E}(\star) \leq \left(\frac{\varepsilon}{2}\|f\|_{L^p(G)}\right)^p = 2^{-p} \left(\frac{\varepsilon}{2}\|f\|_{L^p(G)}\right)^p$.

$$\frac{|L|}{|A|^k} = \mathbb{P}\left((\star) \geq \left(\frac{\varepsilon}{2}\|f\|_{L^p(G)}\right)^p\right) \leq \mathbb{P}((\star) \geq 2^p \mathbb{E}(\star)) \leq 2^{-p}.$$

This implies that $\frac{|L|}{|A|^k} \geq 2^{-p}$ so in particular $|L| \geq \frac{1}{2}|A|^k$. Let $D = \underbrace{\{(b, b, \dots, b) : b \in B\}}_{k\text{-times}}$, so $L + D \subset (A + B)^k$ thus

$$|L + D| \leq |(A + B)^k| \leq (K|A|)^k = k^k|A|^k \leq (2K)^k|L|$$

since $|L| \geq \frac{1}{2}|A|^k$.

By lemma 2.13, $E(L+D, L+D) \geq \frac{|D|^2|L|}{(2K)^k}$, so there are at least $\frac{|D|^2}{(2K)^k}$ pairs $(b_1, b_2) \in D \times D$ such that $r_{L-L}(b_1 - b_2) > 0$. In particular, there exists $b \in B$ and $X \subset X - b$ of size $|X| \geq \frac{|B|}{(2K)^k}$ such that $r_{L-L}(x) > 0$ for all $x \in X$. In other words, for all $x \in X$ there exist $l_1(x), l_2(x) \in L$ such that $\forall i \in [k], l_1(x)_i = l_2(x)_i + x$ ($_i$ means i -th coordinate).

By the triangle inequality for each $x \in X$

$$\begin{aligned} \|\tau_{-x}(f * \mu_A) - f * \mu_A\|_{L^p(G)} &\leq \left\| \tau_{-x}(f * \mu_A) - \tau_{-x} \left(\frac{1}{k} \sum_{i=1}^k \tau_{-l_2(x)_i}(f) \right) \right\|_{L^p(G)} \\ &\quad + \left\| \tau_{-x} \left(\frac{1}{k} \sum_{i=1}^k \tau_{-l_2(x)_i}(f) \right) - f * \mu_A \right\|_{L^p(G)} \\ &\leq \left\| f * \mu_A - \frac{1}{k} \sum_{i=1}^k \tau_{-l_2(x)_i}(f) \right\|_{L^p(G)} + \left\| \frac{1}{k} \sum_{i=1}^k \tau_{-x-l_2(x)_i}(f) - f * \mu_A \right\|_{L^p(G)} \\ &\leq 2\frac{\varepsilon}{2}\|f\|_{L^p(G)} \end{aligned}$$

by the definition of L . □

Theorem : 3.9 - Bogolyubov, due to Sanders

Let $A \subset \mathbb{F}_p^n$ be a set of density $\alpha > 0$. Then there exists a subspace $V \leq \mathbb{F}_p^n$ of codimension $O(\log^4(\alpha^{-1}))$ such that $V \subset A + A - A - A$.

Proof. Ex Sheet 3. Chang & Croot-Sisask. □

Theorem : 3.10 - due to Schoen and Shkredov

Let $p \neq 5$ and $A \subset \mathbb{F}_p^n$. Suppose that A contains no non-trivial solutions to the equation $x_1 + x_2 + x_3 + x_4 + x_5 = 5y$ i.e. no solutions such that $y \neq x_i$ for some $i \in [5]$. Then $|A| = \exp(-\Omega_p(\log |\mathbb{F}_p^n|^{\frac{1}{5}}))|\mathbb{F}_p^n|$.

Lecture 13

Proof. Let $\alpha = \frac{|A|}{|\mathbb{F}_p^n|}$ and partition A into $A_1 \cup A_2$ with $|A_1| = \left\lfloor \frac{\alpha}{2} p^n \right\rfloor$ and $|A_2| = \left\lceil \frac{\alpha}{2} p^n \right\rceil$. By

averaging $\exists z \in \mathbb{F}_p^n$ such that $|A_1 \cap (z - A_2)| \geq \frac{\alpha^2}{4} p^n$. Let $A' = A_1 \cap (z - A_2)$. By theorem 3.9 there exists a subspace $V \leq \mathbb{F}_p^n$ of codimension $O(\log^4(\alpha^{-1}))$ such that $A' + A' - A' - A' \supset V$ and hence $2z + V \subset 2z + A' + A' - A' - A' \subset A_1 + A_1 + A_2 + A_2$.

Consequently, $(5 \cdot A - A) \cap (2z + V) = \emptyset$, for if there were $x, y \in A$ such that $5y - x \in 2z + V$, then we would be able to write $5y - x \in 2z + V$, then we would be able to write $5y - x$ as $a_1 + a'_1 + a_2 + a'_2$ with $a_1, a'_1 \in A_1$ and $a_2, a'_2 \in A_2$ which since A_1 and A_2 are disjoint would yield a nontrivial solution.

It follows that for all $w \in \mathbb{F}_p^n$, at most one of $|A \cap (w + V)|$ and $5 \cdot A \cap (w + 2z + V)$ can be non-empty. Therefore, $2|A| = \sum_{w \in V^\perp} |A \cap (w + V)| + |5 \cdot A \cap (w + 2z + V)| \leq |V^\perp| \sup_{w \in V^\perp} |A \cap (w + V)|$.

So there exists $w \in V^\perp$ such that $|A \cap (w + V)| \geq \frac{2|A|}{|V^\perp|} = \frac{2\alpha|\mathbb{F}_p^n|}{|\mathbb{F}_p^n|/|V|} = 2\alpha|V|$.

The set $A \cap (w + V) \subset w + V$ of density $\geq 2\alpha$, or equivalently $(A - w) \cap V \subset V$ of density $\geq 2\alpha$, containing no non-trivial solutions to $x_1 + x_2 + x_3 + x_4 + x_5 = 5y$.

After t iterations we obtain a subspace W of codimension $O(t \log^4(\alpha^{-1}))$ and $w \in \mathbb{F}_p^n$ such that $|A \cap (w + W)| \geq 2^t \alpha |W|$. Arguing as in the proof of theorem 1.17 yields the result. \square

A similar bound in \mathbb{Z}_N where Behrend's construction offers a comparable lower bound.

Chapter IV - Further Topics

Lecture 13

In \mathbb{F}_p^n we can do much better, even for 3-APs.

Theorem : 4.1 (due to Ellenberg-Gijswijt based on Croot-Lev-Pach)

Let $A \subset \mathbb{F}_3^n$ be a set containing no non-trivial 3-APs. Then $|A| = o(2.765^n)$

Let M_n be the set of monomials in x_1, \dots, x_n whose degree in each variable is at most 2. Let V_n be the vector space over \mathbb{F}_3 generated by M_n . For any $d \in [0, 2n]$, write M_n^d for the set of monomials in M_n of (total) degree at most d , and V_n^d for the corresponding vector space. Set m_d for the dimension of V_n^d i.e. $|M_n^d|$.

Lemma : 4.2

Let $A \subset \mathbb{F}_3^n$ and suppose $P \in V_n^d$ is such that $P(a + a') = 0$ for all $a \neq a' \in A$. Then $|\{a \in A : P(2a) \neq 0\}| \leq 2m_{d/2}$.

Proof. Every $P \in V_n^d$ can be written as a linear combination of monomials from M_n^d , so $P(x + y) = \sum_{\deg(mm') \leq d} c_{m,m'} m(x)m'(y)$ for some coefficients $c_{m,m'}$.

Since at least one of m, m' has to have degree at most $\frac{d}{2}$, we can write $P(x + y) = \sum_{m \in M_n^{d/2}} m(x)F_m(y) + \sum_{m' \in M_n^{d/2}} m'(y)G_{m'}(x)$ where $(F_m)_{m \in M_n^{d/2}}, (G_{m'})_{m' \in M_n^{d/2}}$ are polynomials.

Viewing $(P(x + y))_{x,y \in A}$ as an $|A| \times |A|$ matrix C , we see that C can be written as a sum of at most $2m_{d/2}$ matrices of rank at most 1. Hence $\text{rank}(C) \leq 2m_{d/2}$. But C is a diagonal matrix by assumption, whose rank equals $|\{a \in A : P(2a) \neq 0\}|$. \square

Proposition : 4.3

Let $A \subset \mathbb{F}_3^n$ be a set containing no non-trivial 3-APs. Then $|A| \leq 3m_{\frac{2n}{3}}$

Lecture 14

Proof. Let $d \in [1, 2n]$ to be chosen later. Let W be the subspace of V_n^d which vanish on $(2 \cdot A)^C$. Clearly, $\dim(W) \geq \dim(V_n^d) - |(2 \cdot A)^C| = m_d - (3^n - |2 \cdot A|)$.

Claim that there is $P \in W$ such that $|\text{supp}(P)| \geq \dim(W)$. Indeed, pick $P \in W$ with maximal support. If $|\text{supp}(P)| < \dim(W)$ then there would be a nonzero $Q \in W$ vanishing on $\text{supp}(P)$, in which case $\text{supp}(P + Q) \supsetneq \text{supp}(P)$, contradicting our choice of P .

By assumption $\{a + a' : a \neq a' \in A\} \cap 2 \cdot A = \emptyset$. So any polynomial that vanishes $(2 \cdot A)^C$ also vanishes on $\{a + a' : a \neq a' \in A\}$.

By lemma 4.2 therefore

$$|\text{supp}(P)| = |\{x \in \mathbb{F}_3^n : P(x) \neq 0\}| = |\{a \in A : P(2a) \neq 0\}| \leq 2m_{\frac{d}{2}}.$$

Putting everything together we have

$$m_d - (3^n - |A|) \leq \dim(W) \leq |\text{supp}(P)| \leq 2m_{\frac{d}{2}}$$

thus $|A| \leq (3^n - m_d) + 2m_{\frac{d}{2}}$. But the monomials in $M_n \setminus M_n^d$ are in bijection with those of degree at most $2n - d$ (via $x_1^{\alpha_1} \dots x_n^{\alpha_n} \mapsto x_1^{2-\alpha_1} \dots x_n^{2-\alpha_n}$) thus $3^n - m_d = m_{2n-d}$. Thus setting $d = \frac{4n}{3}$ yields $|A| \leq 3m_{\frac{2n}{3}}$. \square

We'll deduce Theorem 4.1 on sheet 3. We do not know of a comparable bound for 4-APs. Fourier-analytic techniques also fail.

Example 4.4. Recall from lemma 1.16 that $|T_3(1_A, 1_A, 1_A) - \alpha^3| \leq \sup_{t \neq 0} |\widehat{1}_A(t)|$.

But it is impossible to bound $|T_4(1_A, 1_A, 1_A, 1_A) - \alpha^4| = |\mathbb{E}_{x,d} 1_A(x) 1_A(x+d) 1_A(x+2d) 1_A(x+3d) - \alpha^4|$ by $\sup_{t \neq 0} |\widehat{1}_A(t)|$. Indeed, consider $Q = \{x \in \mathbb{F}_p^n : x \cdot x = 0\}$. By problem 2 (ii) on

sheet 1 we know that $\frac{|Q|}{p^n} = \frac{1}{p} + O(p^{-\frac{n}{2}})$ and $\sup_{t \neq 0} |\widehat{1}_Q(t)| = O(p^{-\frac{n}{2}})$.

But given a 3-AP $x, x+d, x+2d$ in Q , we automatically have that $x+3d \in Q$.

$$\forall x, d \in \mathbb{F}_p^n, x \cdot x - 3(x+d) \cdot (x+d) + 3(x+2d) \cdot (x+2d) - (x+3d) \cdot (x+3d) = 0$$

So $T_4(1_A, 1_A, 1_A, 1_A) = T_3(1_A, 1_A, 1_A) = \alpha^3 + o(1)$.

Definition 4.5. Given $f : G \rightarrow \mathbb{C}$ with G finite abelian define its **U^2 -norm** by the formula

$$\|f\|_{U^2(G)}^4 = \mathbb{E}_{x,a,b \in G} f(x) \overline{f(x+a)} \overline{f(x+b)} f(x+a+b).$$

Problem 3(i) on sheet 1 showed that $\|f\|_{U^2(G)} = \|\widehat{f}\|_{\ell^4(G)}$, so this is indeed a norm. Problem 3(ii) asserted the following.

Lemma : 4.6

Let $f_1, f_2, f_3 : G \rightarrow \mathbb{C}$. Then $|T_3(f_1, f_2, f_3)| \leq \min_{i \in [3]} \|f_i\|_{U^2(G)} \prod_{j \neq i} \|f_j\|_{L^\infty(G)}$.

Note that

$$\sup_{\gamma \in \widehat{G}} |\widehat{f}(\gamma)|^4 \leq \sum_{\gamma \in \widehat{G}} |\widehat{f}(\gamma)|^4 \leq \sup_{\gamma \in \widehat{G}} |\widehat{f}(\gamma)|^2 \sum_{\gamma \in \widehat{G}} |\widehat{f}(\gamma)|^2.$$

By Parseval, $\|\widehat{f}\|_{\ell^\infty(\widehat{G})} \leq \|\widehat{f}\|_{\ell^4(\widehat{G})} = \|f\|_{U^2(G)} \leq \|\widehat{f}\|_{\ell^\infty(G)}^{\frac{1}{2}} \cdot \|f\|_{L^2(G)}^{\frac{1}{2}}$.

Moreover, if $f = f_A = 1_A - \alpha$, then $T_3(f, f, f) = T_3(1_A - \alpha, 1_A - \alpha, 1_A - \alpha) = T_3(1_A, 1_A, 1_A) - \alpha^3$ plus three terms of the form $(-\alpha) \mathbb{E}_{x,d} 1_A(x+d) 1_A(x+2d) = \alpha^3$ plus three terms of the form $(-\alpha)^2 \mathbb{E}_{x,d} 1_A(x+3d) = \alpha^3$. So $T_3(f, f, f) = T_3(1_A, 1_A, 1_A) - \alpha^3$. We could therefore reformulate the first step in the proof of Meshulam's theorem as follows:

If $p^n \geq 2\alpha^{-2}$ then $\frac{\alpha^3}{2} \leq |T_3(1_A, 1_A, 1_A) - \alpha^3| \leq \|f_A\|_{U^2(G)}$ by lemma 4.6.

Lecture 15

Recasting theorem 1.17: IF $p^n \geq 2\alpha^{-2}$, then

$$\frac{\alpha^3}{2} \leq \left| \frac{\alpha}{p^n} - \alpha^3 \right| = |T_3(f_A, f_A, f_A)| \leq \|f_A\|_{U^2}.$$

It remains to show that if $\|f_A\|_{U^2}$ is not too small then there exists a subspace $V \leq \mathbb{F}_p^n$ of bounded codimension on A has increased density.

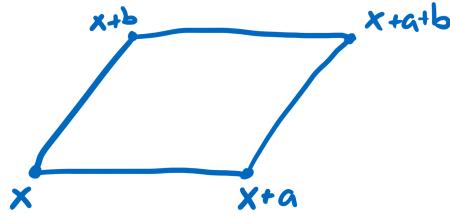
Theorem : 4.7 - U^2 -Inverse

Let $f : \mathbb{F}_p^n \rightarrow \mathbb{C}$ satisfy $\|f\|_\infty \leq 1$ and $\|f\|_{U^2} \geq \delta$ for some $\delta \geq 0$. Then $\exists b \in \mathbb{F}_p^n$ such that $|\mathbb{E}_x f(x) \omega^{x \cdot b}| \geq \delta^2$.

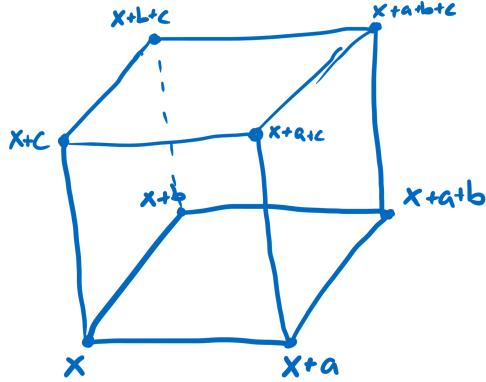
In other words, $|\langle f, \phi \rangle| \geq \delta^2$ for $\phi(x) = \omega^{x \cdot b}$ and we say " f correlates a linear function".

Proof. We've seen that $\|f\|_{U^2}^2 \leq \|\widehat{f}\|_{\ell^\infty} \cdot \|f\|_2 \leq \|\widehat{f}\|_{\ell^\infty}$, so $\delta^2 \leq \|\widehat{f}\|_{\ell^\infty} = \mathbb{E}_x f(x) \omega^{x \cdot b}$ for some $b \in \mathbb{F}_p^n$. \square

We can visualize the U^2 norm as a parallelogram:



We can extend this to the U^3 norm (soon to be defined) by adding an extra dimension:



Definition 4.8. Given $f : G \rightarrow \mathbb{C}$ with G finite abelian, define its U^3 -norm by

$$\begin{aligned} \|f\|_{U^3(G)}^8 &= \mathbb{E}_{x,a,b,c \in G} f(x) \overline{f(x+a)f(x+b)f(x+c)} f(x+a+b) f(x+a+c) f(x+b+c) \overline{f(x+a+b+c)} \\ &= \mathbb{E}_{x,h_1,h_2,h_3} \prod_{\varepsilon \in \{0,1\}^3} \mathcal{C}^{|\varepsilon|} f(x + \varepsilon \cdot h). \end{aligned}$$

where $\mathcal{C}g(X) = \overline{g(X)}$ and $|\varepsilon| = \#\text{1s in } \varepsilon$.

It's easy to verify that $\|f\|_{U^3(G)}^8 = \mathbb{E}_h \|\Delta_h f\|_{U^2(G)}^4$ where $\Delta_h f(x) = f(x) \overline{f(x+h)}$.

Definition 4.9. Given functions $f_\varepsilon : G \rightarrow \mathbb{C}$ for $\varepsilon = \{0,1\}^3$, define the **Gowers inner-product** by $\langle (f_\varepsilon)_{\varepsilon \in \{0,1\}^3} \rangle_{U^3(G)} = \mathbb{E}_{x,h_1,h_2,h_3} \prod_{\varepsilon \in \{0,1\}^3} \mathcal{C}^{|\varepsilon|} f_\varepsilon(x + \varepsilon \cdot h)$.

Observe that $\langle f, \dots, f \rangle_{U^3(G)} = \|f\|_{U^3(G)}^8$.

Lemma : 4.10 - Gowers-Cauchy-Schwarz Inequality

Given $f_\varepsilon : G \rightarrow \mathbb{C}$ for $\varepsilon \in \{0, 1\}^3$ $|\langle (f_\varepsilon)_{\varepsilon \in \{0,1\}^3} \rangle_{U^3(G)}| \leq \prod_{\varepsilon \in \{0,1\}^3} \|f_\varepsilon\|_{U^3(G)}$

Proof. ExSheet 3. □

Setting $f_\varepsilon = f$ for $\varepsilon \in \{0, 1\}^2 \times \{0\}$ and $f_\varepsilon = 1$ otherwise. The LHS equals $\|f\|_{U^2(G)}^4$ so $\|f\|_{U^2(G)} \leq \|f\|_{U^3(G)}$.

Proposition : 4.11

Let $f : G \rightarrow \mathbb{C}$ with $\|f\|_{L^\infty(G)} \leq 1$. Then $|T_4(f, f, f, f)| \leq \|f\|_{U^3(G)}$.

Proof. It's long. Apply Cauchy-Schwarz 3 times. □

One might hope to generalize Meshulam's theorem as follows:

Theorem : 4.12 - Szemerédi's (for progressions of length 4)

Let $A \subset \mathbb{F}_p^n$ be a set containing no non-trivial 4-APs. Then $|A| = o(p^n)$.

Idea: By proposition 4.11 with $f = f_A$. $T_4(1_A, 1_A, 1_A, 1_A) - \alpha^4 = T_4(f_A, f_A, f_A, f_A)$ plus terms in which one and three of the inputs are equal to f_A , each of which is controlled $\|f_A\|_{U^2}$. Hence $|T_4(1_A, 1_A, 1_A, 1_A) - \alpha^4| \leq 14\|f_A\|_{U^3}$ since $\|\cdot\|_{U^2} \leq \|\cdot\|_{U^3}$. So if A contains no nontrivial 4-APs and $p^n \geq 2\alpha^{-3}$ then $\frac{\alpha^4}{2} \leq 14\|f_A\|_{U^3}$.

Lecture 16

What can we say about functions whose U^3 -norm is large?

Example 4.13. Let M be an $n \times n$ (symmetric) matrix with entries in \mathbb{F}_p . Then $f(x) = \omega^{x^T M x}$ satisfies $\|f\|_{U^3} = 1$.

Theorem : 4.14 - U^3 -Inverse Theorem

Let $f : \mathbb{F}_p^n \rightarrow \mathbb{C}$ satisfying $\|f\|_\infty \leq 1$ and $\|f\|_{U^3} \geq \delta$ for some $\delta > 0$. Then there exists a symmetric $n \times n$ matrix M with entries in \mathbb{F}_p and $b \in \mathbb{F}_p^n$ such that $|\mathbb{E}_x f(x) \omega^{x^T M x + b^T x}| \geq c(\delta)$ where $c(\delta)$ is a polynomial in δ (depending on p).

In other words, $|\langle f, \phi \rangle| \geq c(\delta)$ for $\phi(x) = \omega^{x^T M x + b^T x}$ and we say " f correlates with a quadratic phase function".

Proof Sketch. Suppose $\|f\|_{U^3} \geq \delta$.

Step 1: "Weak linearity". If $\|f\|_{U^3}^8 = \mathbb{E}_h \|\Delta_h f\|_{U^2}^4 \geq \delta^8$ then for at least a $\frac{\delta^8}{2}$ -proportion of $h \in \mathbb{F}_p^n$, $\|\Delta_h f\|_{U^2}^4 \geq \frac{\delta^8}{2}$, for each such $h \in \mathbb{F}_p^n$, $\exists t_n$ such that $|\widehat{\Delta_h f}(t_n)|^2 \geq \frac{\delta^8}{2}$. Working a tiny bit harder, one can obtain the following:

Proposition : 4.15

Let $f : \mathbb{F}_p^n \rightarrow \mathbb{C}$ satisfy $\|f\|_\infty \leq 1$ and $\|f\|_{U^3} \geq \delta$ for some $\delta > 0$. Suppose that $|\mathbb{F}_p^n| = \Omega_\delta(1)$. Then there exists a subset $S \subset \mathbb{F}_p^n$ with $\frac{|S|}{|\mathbb{F}_p^n|} = \Omega_\delta(1)$ and a function $\phi : S \rightarrow \mathbb{F}_p^n$ such that:

- (i) $|\widehat{\Delta_h f}(\phi(h))| = \Omega_\delta(1)$.
- (ii) There are at least $\Omega_\delta(|\mathbb{F}_p^n|^3)$ additive quadruples $(s_1, s_2, s_3, s_4) \in S^4$ and $\phi(s_1) + \phi(s_2) = \phi(s_3) + \phi(s_4)$.

Step 2: "Strong linearity"

If S and ϕ as above, then there's a linear map $\Psi : \mathbb{F}_p^n \rightarrow \widehat{\mathbb{F}_p^n}$ which coincides with ϕ for many elements of S . More precisely,

Proposition : 4.16

Let S and ϕ be given by Proposition 4.15. Then $\exists n \times n$ matrix M with entries in \mathbb{F}_p and $b \in \mathbb{F}_p^n$ such that the map $\psi : \mathbb{F}_p^n \rightarrow \widehat{\mathbb{F}_p^n}$ via $x \mapsto Mx + b$ satisfies $\Psi(x) = \phi(x)$ for $\Omega_\delta(|\mathbb{F}_p^n|)$ elements $x \in S$.

Proof. Consider the graph $\Gamma = \{(h, \phi(h)) : h \in S\} \subset \mathbb{F}_p^n \times \widehat{\mathbb{F}_p^n}$. By proposition 4.15, Γ has $\Omega_\delta(|\mathbb{F}_p^n|)$ additive quadruples. By the Balog-Szemerédi-Gowers theorem we have $\exists \Gamma' \subset \Gamma$ with $|\Gamma'| = \Omega_\delta(|\Gamma|) = \Omega_\delta(|\mathbb{F}_p^n|)$ and $|\Gamma' + \Gamma'| = O_\delta(|\Gamma'|)$.

Define S' by $\Gamma' = \{(h, \phi(h)) : h \in S'\}$ and note that $|S'| = \Omega_\delta(|\mathbb{F}_p^n|)$. By the Freiman-Ruzsa theorem applied to $\Gamma' \subset \mathbb{F}_p^n \times \widehat{\mathbb{F}_p^n}$, \exists subspace $H \leq \mathbb{F}_p^n \times \widehat{\mathbb{F}_p^n}$ with $|H| = O_\delta(|\Gamma'|) = O_\delta(|\mathbb{F}_p^n|)$ such that $\Gamma' \subset H$.

Denote by $\pi : \mathbb{F}_p^n \times \widehat{\mathbb{F}_p^n} \rightarrow \mathbb{F}_p^n$ the projection onto the first n coordinates. By construction, $\pi(H) \supset S'$. Moreover, since $|S'| = \Omega_\delta(|\mathbb{F}_p^n|)$,

$$|\ker(\pi|_H)| = \frac{|H|}{|Im(\pi|_H)|} \leq \frac{O_\delta(|\mathbb{F}_p^n|)}{|S'|} = O_\delta(1).$$

We may thus partition H into $O_\delta(1)$ cosets of $H^* = \ker(\pi|_H)$ such that π is injective on each coset. By averaging, $\exists x + H^*$ such that $|\Gamma' \cap (x + H^*)| = \Omega_\delta(|\Gamma'|) = \Omega_\delta(|\mathbb{F}_p^n|)$. Set $\Gamma'' = \Gamma' \cap (x + H^*)$ and define S'' accordingly.

Now $\pi|_{x+H^*}$ is both injective and surjective onto its image. $V = \text{Im}(\pi|_{x+H^*})$. But this means that \exists affine linear map $\Psi : V \rightarrow \widehat{\mathbb{F}_p^n}$ such that $(h, \Psi(h)) \in \Gamma''$ for all $h \in S''$. \square

Step 3: "The symmetry argument"

Having obtained $\Psi(x) = Mx + b$ for some matrix M and vectors b such that $(h, Mh + b) \in \Gamma'' \forall h \in S''$ we need to turn M into a symmetric matrix in preparation for step 4.

Step 4: "Integrating"

Proposition : 4.18

Suppose f, M, b are as in step 3 and $\mathbb{E}_h |\widehat{\Delta_h f}(Mh + b)|^2 = \Omega_\delta(1)$. Then KOMPLETOJE