Part III – Introduction to Additive Combinatorics (Incomplete)

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

Lent 2024

Contents

1 Fourier-analytic techniques

Lecture 1

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

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

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

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

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

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

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

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

Indeed,

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

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

- 1_A the *characteristic function* of A, ie
$$1_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$
- μ_A the *characteristic measure* of A, ie
$$\mu_A = \alpha^{-1} 1_A$$
where $\alpha = \frac{|A|}{|G|}$.
- f_A the *balanced function* of A, ie
$$f_A(x) = 1_A(x) - \alpha$$

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

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

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

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

So

$$\widehat{\mu_V}(t) = 1_{V^\perp}(t)$$

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

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

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

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

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

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

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

Consequently,

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

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

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

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

Proof. Exercise. □

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

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

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

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

Proof.

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

□

Lecture 2

Definition 1.9. Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$, define their **convolution** $f * g : \mathbb{F}_p^n \to \mathbb{C}$ by

$$(f * g)(x) = \mathop{\mathbb{E}}_y f(y) g(x - y)$$

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

$$\begin{aligned} (1_A * 1_B)(x) &= \mathop{\mathbb{E}}_y 1_A(y) 1_B(x - y) \\ &= \frac{1}{p^n} |A \cap (x - B)| \\ &= \frac{\#\text{ ways to write } x = a + b, a \in A, b \in B}{p^n} \end{aligned}$$

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

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

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

$$\widehat{f * g}(t) = \hat{f}(t) \hat{g}(t)$$

Proof.

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

□

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

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

Proof. Observe that $(A+A)-(A+A) = \operatorname{supp}(\underbrace{1_A * 1_A * 1_{-A} * 1_{-A}}_{g})$, so we wish to find V such that $g(x) > 0$ for all $x \in V$. Let $K = \operatorname{Spec}_\rho(1_A)$ for some $\rho > 0$ and define $V = \langle K\rangle^\perp$. By Lemma 1.8, $\operatorname{codim} V \le |K| \le \rho^{-2}\alpha^{-1}$. We calculate

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

We now see that

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

and

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

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

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

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

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

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

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

the cosets of V. Then

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

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

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

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

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

as wanted. $\square$

Lecture 3

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

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

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

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

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

times

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

In absolute value, the error term is at most

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

□

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

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

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

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

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

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

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

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

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

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

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

Lecture 4

We have proved that if $A \subseteq \mathbb{F}_3^n$ only contains trivial 3APs then $|A| = O(\frac{3^n}{n})$. The largest known set in $\mathbb{F}_3^n$ with only trivial 3APs has size $\ge 2.218^n$ (Tyrrell, 2022). We will return to this later.

From now on, let G be a finite abelian group. G comes equipped with a set of **characters**, ie group homomorphisms $\gamma : G \to \mathbb{C}^\times$. Characters themselves form a group denoted $\hat{G}$ and called the **Pontryagin dual** (aka **dual group**) of G. It turns out that if G is finite abelian then $\hat{G} \cong G$ (but *non-canonically*). For instance,

- If $G = \mathbb{F}_p^n$, then $\hat{G} = \{\gamma_t : x \mapsto \omega^{x \cdot t} \mid t \in G\}$
- If $G = \mathbb{Z}/n\mathbb{Z}$, then $\hat{G} = \{\gamma_t : x \mapsto \omega^{xt} \mid t \in G\}$

The latter is a special case of the former, but again n should thought of as an asymptotic variable.

Definition 1.18. Given $f : G \to \mathbb{C}$, define its **Fourier transform** $\hat{f} : \hat{G} \to \mathbb{C}$ by

$$\hat{f}(\gamma) = \mathop{\mathbb{E}}_{x \in G} f(x)\gamma(x)$$

It is easy to verify that $f(x) = \sum_{\gamma \in \hat{G}} \hat{f}(\gamma)\overline{\gamma(x)}$. Similarly, Definitions 1.6, 1.9, Examples 1.3, 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, $L < p$ be even and $J = [-\frac{L}{2}, \frac{L}{2}] \subseteq \mathbb{F}_p$. Then for all $t \ne 0$ we have

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

See Example Sheet 1.

Theorem 1.20 (Roth)**.** Let $A \subseteq [N]$ be a set containing only trivial 3APs. Then $|A| = O(\frac{N}{\log\log N})$.

Lemma 1.21. Let $A \subseteq [N]$ of density $\alpha > 0$ containing only trivial 3APs and satisfying $N > 50\alpha^{-2}$. Let p be a prime in $[\frac{N}{3}, \frac{2N}{3}]$ and write $A' = A \cap [p] \subseteq \mathbb{F}_p$. Then either

1. $\sup_{t \ne 0} \left|\widehat{1_A}(t)\right| \ge \frac{\alpha^2}{10}$ (where the Fourier coefficients are computed in $\mathbb{F}_p$)
2. or there exists an interval J of length $\ge \frac{N}{3}$ such that

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

Proof. If $|A'| \le \alpha\left(1 - \frac{\alpha}{200}\right)p$, then

$$|A \cap [p+1, N]| \ge \alpha(N-p) + \frac{\alpha^2 p}{200} \ge \alpha\left(1 + \frac{\alpha}{400}\right)(N-p)$$

and we are in Case 2 with $J = [p+1, N]$. Let $A'' = A' \cap [\frac{p}{3}, \frac{2p}{3}]$. Note that all 3APs of the form $(x, x+d, x+2d) \in A' \times A'' \times A''$ are in fact 3APs in $[N]$ (and in particular they are trivial).
If $\left|A' \cap [\frac{p}{3}]\right|$ or $\left|A' \cap [\frac{2p}{3}, p]\right|$ were at least $\frac{2}{5}|A'|$, then we would again be in Case 2. We may therefore assume that $|A''| \geq \frac{|A'|}{5}$.
Now, as in Lemma 1.16 and Theorem 1.17 with $\alpha' = \frac{|A'|}{p}, \alpha'' = \frac{|A''|}{p}$,

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

So, as before, $\frac{\alpha'\alpha''}{2} \leq \alpha'' \sup_{t \neq 0} \left|\widehat{1_{A'}}(t)\right|$, provided $\frac{\alpha''}{p} \leq \frac{\alpha'\alpha''^2}{2}$. This holds by assumption since $p \geq \frac{N}{3}, N \geq 50\alpha^{-2}, \alpha' \geq \frac{199}{200}\alpha, \alpha'' \geq \frac{\alpha'}{5}$. $\square$

Lecture 5

We now want to convert the large Fourier coefficient into a density increment. This is harder now that the number of values of xt grows as $n \to \infty$. Compare this to the finite field case where $x \cdot t$ only take p different values regardless of n. If we can't find a single big coefficient, then we might instead be able to find an interval of coefficients whose total contribution is big.

TODO: Insert picture

Lemma 1.22. Let $m \in \mathbb{N}$ and $\phi : [m] \to \mathbb{F}_p$ be multiplication by some fixed $t \neq 0$. Given $\varepsilon > 0$, there exists a partition of $[m]$ into progressions P_i of length $\in [\frac{\varepsilon\sqrt{m}}{2}, \varepsilon\sqrt{m}]$ such that $\operatorname{diam}(\phi(P_i)) \leq \varepsilon p$.

Proof. Let $u = \lfloor\sqrt{m}\rfloor$ and consider $0, t, \ldots, ut$. By pigeonhole, find $0 \leq v < w \leq u$ such that $|wt - vt| \leq \frac{p}{u}$. Set $s = w - v \leq u$ so that $|st| \leq \frac{p}{u}$. Divide $[m]$ into residue classes mod s. Each has size at least $\left\lfloor\frac{m}{s}\right\rfloor \geq \left\lfloor\frac{m}{u}\right\rfloor$ and can be divided into progressions of the form $a, a+s, \ldots, a+ds$ with $\frac{\varepsilon u}{2} < d \leq \varepsilon u$. The diameter of each progression under ϕ is $|dst| \leq \varepsilon p$. $\square$

Lemma 1.23. Let $A \subseteq [N]$ be of density $\alpha > 0$. Let p be a prime in $[\frac{N}{3}, \frac{2N}{3}]$ and write $A' = A \cap [p]$. Suppose there exists $t \neq 0$ such that $\left|\widehat{1_A}(t)\right| \geq \frac{\alpha^2}{10}$. Then there exists a progression P of length at least $\alpha^2\frac{\sqrt{N}}{500}$ such that

$$|A \cap P| \geq \alpha\left(1 + \frac{\alpha}{50}\right)|P|$$

Proof. Let $\varepsilon = \frac{\alpha^2}{40\pi}$ and use Lemma 1.22 to partition $[p]$ into progressions P_i of length at least $\frac{\varepsilon\sqrt{p}}{2} \geq \frac{\alpha^2}{80\pi}\sqrt{\frac{N}{3}} \geq \frac{\alpha^2\sqrt{N}}{500}$ and $\operatorname{diam}\phi(P_i) \leq \varepsilon p$. Fix one x_i inside each P_i.

$$\begin{aligned}
\frac{\alpha^2}{10} &\leq \left|\widehat{f_{A'}}(t)\right| \\
&= \frac{1}{p}\left|\sum_i \sum_{x \in P_i} f_{A'}(x)\omega^{xt}\right| \\
&= \frac{1}{p}\left|\sum_i \sum_{x \in P_i} f_{A'}(x)\omega^{x_i t} + \sum_i \sum_{x \in P_i} f_{A'}(x)(\omega^{xt} - \omega^{x_i t})\right| \\
&\leq \frac{1}{p}\sum_i \left|\sum_{x \in P_i} f_{A'}(x)\omega^{x_i t}\right| + \frac{1}{p}\sum_i \sum_{x \in P_i} |f_{A'}(x)|\, 2\pi\varepsilon \\
&\leq \frac{1}{p}\sum_i \left|\sum_{x \in P_i} f_{A'}(x)\omega^{x_i t}\right| + \frac{\alpha^2}{20}
\end{aligned}$$

So

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

Since $f_{A'}$ has mean zero, there exists i such that $\sum_{x \in P_i} f_{A'}(x) \geq \frac{\alpha^2 |P_i|}{40}$. □

Proof of Roth's theorem. Put the ingredients together, Similarly to Meshulam. See Example Sheet 1 for details. □

Example 1.24 (Behrend's construction)**.** There exists a set $A \subseteq [N]$ containing non nontrivial 3APs of size at least $e^{-O(\sqrt{\log n})}$. See Example Sheet 1.

Definition 1.25. Let $\Gamma \subseteq \hat{G}$. The **Bohr set** of **frequencies** Γ and width ρ is

$$B(\Gamma, \rho) = \{x \in G \mid \forall \gamma \in \Gamma, |\gamma(x) - 1| \leq \rho\}$$

$|\Gamma|$ is the **rank** of the Bohr set.

Example 1.26. When $G = \mathbb{F}_p^n$, $B(\Gamma, \rho) = \langle\Gamma\rangle^\perp$ for all small enough ρ (depending only on p, not n).

Lemma 1.27. Let B be a Bohr set of rank d and width ρ. Then $|B| \geq \left(\frac{\rho}{2\pi}\right)^d |G|$.

Proof. See Example Sheet 2. □

Lecture 6

Lemma 1.28 (Bogolyubov)**.** Given $A \subseteq \mathbb{F}_p$ of density $\alpha > 0$, there exists $\Gamma \subseteq \widehat{\mathbb{F}_p}$ of size at most $2\alpha^{-2}$ such that $B(\Gamma, \frac{1}{2}) \subseteq (A + A) - (A + A)$.

Proof. Recall $(1_A * 1_A * 1_{-A} * 1_{-A})(x) = \sum_{t \in \widehat{\mathbb{F}_p}} \left|\widehat{1_A}(t)\right|^4 \omega^{-xt}$. Let $\Gamma = \operatorname{Spec}_{\sqrt{\frac{\alpha}{2}}}(1_A)$ and note that we have $\cos(\frac{2\pi xt}{p}) > 0$ for all $x \in B(\Gamma, \frac{1}{2})$ and $t \in \Gamma$. Hence

$$\begin{aligned}
\operatorname{Re}\sum_{t \in \widehat{\mathbb{F}_p}} \left|\widehat{1_A}(t)\right|^4 \omega^{-xt} &= \sum_{t \in \Gamma} \left|\widehat{1_A}(t)\right|^4 \cos\left(\frac{2\pi xt}{p}\right) + \sum_{t \notin \Gamma} \left|\widehat{1_A}(t)\right|^4 \cos\left(\frac{2\pi xt}{p}\right) \\
&\geq \alpha^4 - \frac{\alpha^4}{2} > 0
\end{aligned}$$

□

2 Combinatorial methods

For now, let G be an abelian group. Given $A, B \subseteq G$, we defined

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

If A and B are finite and nonempty, then

$$\max(|A|, |B|) \leq |A \pm B| \leq |A| |B|$$

Better bounds are available in certain settings.

Example 2.1. Let $V \leq \mathbb{F}_p^n$ be a subspace. Then $V + V$, so $|V + V| = |V|$. In fact, if $A \subseteq \mathbb{F}_p^n$ is such that $|A + A| = |A|$, then A is a coset of some subspace.

Example 2.2. Let $A \subseteq \mathbb{F}_p^n$ be such that $|A + A| < \frac{3}{2} |A|$. Then there exists $V \leq \mathbb{F}_p^n$ such that A is contained in a coset of V and $|V| < \frac{3}{2} |A|$. See Example Sheet 2.

Example 2.3. Let $A \subseteq \mathbb{F}_p^n$ be a set of linearly independent vectors. Then $|A + A| = \binom{|A|+1}{2}$. This is big doubling, but $|A| \leq n$ is small!
Let $A \subseteq \mathbb{F}_p^n$ be a set where each point is taken randomly with probability $p^{-\theta n} = N^{-\theta}$ where $\theta \in]\frac{1}{2}, 1]$. Then with high probability $|A + A| = (1 + o(1)) \frac{|A|^2}{2}$.

Definition 2.4. Given finite sets $A, B \subseteq G$, we define the Ruzsa distance between A and B to be

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

$d(A, B)$ is clearly nonnegative and symmetric. However, $d(A, A) \neq 0$ in general.

Lemma 2.5 (Ruzsa's triangle inequality)**.** For $A, B, C \subseteq G$ finite,

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

Proof. The inequality reduces to

$$|B| |A - C| \leq |A - B| |B - C|$$

This is true because

$$\begin{aligned} \phi : B \times (A - C) &\to (A - B) \times (B - C) \\ (b, d) &\mapsto (a_d - b, b - c_d) \end{aligned}$$

is injective, where for each $d \in A - C$ we have chosen $a_d \in A, c_d \in C$ such that $d = a_d - c_c$. □

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

$d(A, A) = \log \sigma(A)$ and $d(A, -A) = \log \delta(A)$, so Lemma 2.5 for $A, -A, -A$ tells us that $\delta(A) \leq \sigma(A)^2$.

Lecture 7

Notation. Given $A \subseteq G$ and $\ell, m \in \mathbb{N}$, write $\ell A - mA$ for the set

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

Theorem 2.7 (Plünnecke's inequality)**.** Let $A, B \subseteq G$ be finite such that $|A+B| \leq K|A|$. Then for all ℓ, m,

$$|\ell B - mB| \leq K^{\ell+m} |A|$$

ww

Idea. A should be thought of as being approximately a subspace. The assumption then says that B is efficiently contained in (a translate of) A and the conclusion now reads that B must itself have small multiples. This makes sense, since we can use multiples of A (which are not much bigger than A) to efficiently contain the multiples of B.

Proof. WLOG $|A+B| = K|A|$. Choose $A' \subseteq A$ nonempty such that the ratio $\frac{|A'+B|}{|A'|} = K'$ is minimised. Note $K' \leq K$ and $|A''+B| \geq K'|A''|$ for all $A'' \subseteq A$.

Claim. For all finite $C \subseteq G$, $|A'+B+C| \leq K'|A'+C|$.

From the claim, we show that $|A'+mB| \leq K'^m |A'|$ for all m by induction: That's true for $m = 0$. For $m+1$, the claim with $C = mB$ gives

$$|A' + (m+1)B| = |A'+B+C| \leq K'|A'+C| \leq K'^{m+1}|A'|$$

Now, by the triangle inequality,

$$|A'||\ell B - mB| \leq |A'+\ell B||A'+mB| \leq K'^\ell |A'| K'^m |A'|$$

Namely, $|\ell B - mB| \leq K'^{\ell+m}|A'| \leq K^{\ell+m}|A|$.

Proof of the claim. Do induction on C. For $C = \varnothing$, it's true. For $C' = C \cup \{x\}$ with x $\notin C$, observe that

$$\begin{aligned} A'+B+C' &= A'+B+C \cup A'+B+x \\ &= A'+B+C \cup A'+B+x \setminus D+B+x \end{aligned}$$

where $D = \{a \in A' \mid a+B+x \subseteq A'+B+C\}$. By definition of K', $|D+B| \geq K'|D|$, so

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

We now apply the same argument again, writing

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

where $E = \{a \in A' \mid a+x \in A'+C\} \subseteq D$. This time, the union is disjoint, so

$$|A'+C'| = |A'+C| + |A'| - |E| \geq |A'+C| + |A| - |D|$$

Hence $|A'+B+C'| \leq K'|A'+C'|$ which proves the claim. □

□

We are now in a position to generalise Example 2.2.

Theorem 2.8 (Freiman-Ruzsa)**.** Let $A \subseteq \mathbb{F}_p^n$ be such that $|A+A| \leq K|A|$ for some $K > 0$. Then A is contained in a subspace $H \leq \mathbb{F}_p^n$ of size $|H| \leq K^2 p^{K^4} |A|$.

Proof. Write $S = A - A$ and choose $X \subseteq A + S$ maximal such that the translates $x + A$ for $x \in X$ are disjoint.
X cannot be too large. Indeed, $\forall x \in X, x + A \subseteq 2A + S$. Hence $\bigcup_{x \in X}(x + A) \subseteq 2A + S$ and $|X||A| = \left|\bigcup_{x \in X}(x + A)\right| \leq |2A + S| \leq K^4 |A|$ by Plünnecke, namely $|X| \leq K^4$.
Now observe that $A + S \subseteq X + S$. Indeed, if $y \in A + S$, then either $y \in X \subseteq X + S$ (because $0 \in S$) or $y \notin X$, meaning that $x + A$ and $y + A$ are not disjoint (X is maximal), namely $y \in x + A - A \subseteq X + S$.
By induction, $\ell A + S \subseteq \ell X + S$ for all ℓ. Hence, writing

$$H = \langle A \rangle = \bigcup_\ell (\ell A + S) \subseteq \bigcup_\ell (\ell X + S) = \langle X \rangle + S$$

the subgroup generated by A, we see that A is contained in a subgroup of size

$$|H| \leq |\langle X \rangle| \, |S| \leq p^{|X|} K^2 |A| \leq K^2 p^{K^4} |A|$$

□

Lecture 8

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

Conjecture 1 (Polynomial Freiman-Ruzsa)**.** Let $A \subseteq \mathbb{F}_p^n$ be such that $|A + A| \leq K|A|$. Then there is a subspace $H \leq \mathbb{F}_p^n$ of size at most $C_1(K)|A|$ and $x \in \mathbb{F}_p^n$ such that $|A \cap (x + H)| \geq \frac{|A|}{C_2(K)}$ where $C_1(K)$ and $C_2(K)$ are polynomials.

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

Definition 2.10. Given an abelian group G and finite sets $A, B \subseteq G$, define **additive quadruples** to be the tuples $(a, a', b, b') \in A^2 \times B^2$ such that $a + b = a' + b'$ and the **additive energy between** A **and** B to be

$$E(A, B) = \frac{\#\{\text{additive quadruples}\}}{|A|^{\frac{3}{2}} |B|^{\frac{3}{2}}}$$

Write $E(A) = E(A, A)$ the **additive energy of** A.

Observe that, if G is finite, then

$$\begin{aligned} |A|^3 E(A) &= |G|^3 \mathop{\mathbb{E}}_{x+y=z+w} 1_A(x) 1_A(y) 1_A(z) 1_A(w) \\ &= |G|^3 \left\| \widehat{1_A} \right\|_4^4 \end{aligned}$$

Example 2.11. When $H \leq \mathbb{F}_p^n$, we have $E(H) = 1$.

Lemma 2.12. Let G be abelian and $A, B \subseteq G$ be finite. Then $E(A, B) \geq \frac{\sqrt{|A||B|}}{|A \pm B|}$.

Proof. Write $r(x) = \#\{(a,b) \in A \times B \mid a + b = x\}$ so that

$$|A|^{\frac{3}{2}} |B|^{\frac{3}{2}} E(A,B) = \#\{\text{additive quadruples}\} = \sum_x r(x)^2$$

Observe that $\sum_x r(x) = |A|\,|B|$, therefore

$$\begin{aligned} |A|^{\frac{3}{2}} |B|^{\frac{3}{2}} E(A,B) &= \sum_x r(x)^2 \\ &\geq \frac{\sum_x r(x) 1_{A+B}(x)}{\sum_x 1_{A+B}(x)^2} \text{ by Cauchy-Schwarz} \\ &= \frac{(|A|\,|B|)^2}{|A+B|} \end{aligned}$$

and similarly for $A - B$. □

In particular, if $|A + A| \leq K\,|A|$ then $E(A) \geq \frac{1}{K}$. The mantra is "Small doubling implies big energy". The converse is **not** true.

Example 2.13. Let G be your favorite family of abelian groups. Then there are constants $\eta, \theta > 0$ such that for all sufficiently large n there exists $A \subseteq G$ with $|A| = n$ satisfying $E(A) \gg \eta$ and $|A + A| \geq \theta\,|A|^2$. See Example Sheet 2.

If we can't hope for a set to have small doubling when its energy is big, we might at least be able to find a big subset with big energy.

Theorem 2.14 (Balog-Szemerédi-Gowers)**.** Let G be an abelian group and let $A \subseteq G$ be finite such that $E(A) \geq \eta$ for some $\eta > 0$. Then there exists $A' \subseteq A$ of size at least $c(\eta)\,|A|$ such that $|A' + A'| \leq C(\eta)\,|A|$ where $c(\eta)$ and $C(\eta)$ are polynomials in η.

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

Lemma 2.15. Let $A_1, \dots, A_m \subseteq [n]$ and suppose that $\sum_{i,j} |A_i \cap A_j| \geq \delta^2 n m^2$. Then there exists $X \subseteq [m]$ 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 the pairs $(i,j) \in X^2$.

Proof. Let $x_1, \dots, x_5$ be taken uniformly at random from $[n]$ and let

$$X = \{i \in [m] \mid \forall k, x_k \in A_i\}$$

Observe that $\mathbb{P}(i,j \in X) = \left(\frac{|A_i \cap A_j|}{n}\right)^5$. Hence

$$\frac{\mathbb{E}\,|X|^2}{m^2} = \mathop{\mathbb{E}}_{i,j} \mathbb{P}(i,j \in X) \geq \left(\frac{\mathbb{E}_{i,j}\,|A_i \cap A_j|}{n}\right)^5 \geq \delta^{10}$$

Call a pair **bad** if $|A_i \cap A_j| < \frac{\delta^2 n}{2}$. Note that

$$\mathbb{P}(i,j \in X \mid (i,j) \text{ bad}) = \mathbb{P}(x_1 \in A_i \cap A_j \mid (i,j) \text{ bad})^5 \leq \frac{\delta^{10}}{2^5}$$

Hence

$$\mathbb{E}[\#\{\text{bad pairs in } X^2\}] \leq \frac{\delta^{10} m^2}{2^5}$$

meaning that

$$\frac{\delta^{10} m^2}{2} + 16\,\mathbb{E}[\#\{\text{bad pairs in } X^2\}] \leq \mathbb{E}[|X|^2]$$

We can therefore find $x_1, \dots, x_5$ such that $\frac{\delta^{10} m^2}{2} + 16\#\{\text{bad pairs in } X^2\} \le |X|^2$. This both means that $|X| \ge \frac{\delta^5 m}{\sqrt{2}}$ and that

$$\#\{\text{bad pairs in } X^2\} \le \frac{|X|^2}{16} \le 10\% \, |X|^2$$

$\square$

Lecture 9

Proof of Balog-Szemerédi-Gowers. Call d a **popular difference** if we can write $d = x - y$ with $x, y \in A$ in at least $\frac{\eta|A|}{2}$ ways, ie if $r_{A-A}(d) \ge \frac{\eta|A|}{2}$.

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

$$\begin{aligned}
\eta |A|^3 &\le \sum_d r_{A-A}(d)^2 \\
&= \sum_{d \text{ popular}} r_{A-A}(d)^2 + \sum_{d \text{ unpopular}} r_{A-A}(d)^2 \\
&< \frac{\eta |A|}{2} |A|^2 + \frac{\eta |A|}{2} \sum_d r_{A-A}(d) \\
&= \eta |A|^3
\end{aligned}$$

Define a graph with vertex set A and with $x \sim y$ if $y - x$ is a popular difference. Since we have at least $\frac{\eta|A|}{2}$ popular differences, our graph has at least $\frac{\eta^2|A|^2}{4}$ (directed) edges. We have $\mathbb{E}_{x,y \in A} |N(x) \cap N(y)| \ge \frac{\eta^4|A|}{2^4}$. Indeed,

$$\begin{aligned}
\mathop{\mathbb{E}}_{x,y \in A} |N(x) \cap N(y)| &= \mathop{\mathbb{E}}_{x,y \in A} \sum_{z \in A} 1_{x \sim z} 1_{y \sim z} \\
&= \sum_{z \in A} \left(\mathop{\mathbb{E}}_{x \in A} 1_{x \sim z} \right)^2 \\
&\ge \frac{1}{|A|} \left(\sum_{z \in A} \mathop{\mathbb{E}}_{x \in A} 1_{x \sim z} \right)^2 \\
&= \frac{1}{|A|} \left(\mathop{\mathbb{E}}_{x \in A} |N(x)| \right)^2 \\
&\ge \frac{1}{|A|} \left(\frac{\eta^2 |A|}{4} \right)^2 \\
&= \frac{\eta^4 |A|}{2^4}
\end{aligned}$$

We apply Lemma 2.15 with $m = n = |A|$ and $\delta = \frac{\eta^2}{4}$ to find a subset $B \subseteq A$ of size $\ge \frac{\eta^{10}|A|}{2^{11}}$ with the property that $|N(x) \cap N(y)| \ge \frac{\eta^4|A|}{2^5}$ for at least 90% of the $x, y \in B$. But then for at least 50% of the $x \in B$ we have $|N(x) \cap N(y)| \ge \frac{\eta^4|A|}{2^5}$ for at least 80% of the $y \in B$ (else $90\% \le \mathbb{E}_{x,y \in B} 1_{(x,y) \text{ good}} < 50\% * 100\% + 50\% * 80\% = 90\%$). Call

$A' \subseteq B$ that set of such x. On one hand, $|A'| \geq \frac{|B|}{2} \geq \frac{\eta^{10}|A|}{2^{12}}$. On the other hand, if $x, y \in A'$ then at least 60% of the $z \in B$, namely at least $\frac{\eta^{10}|A|}{2^{12}}$ such z, are such that

$$|N(x) \cap N(z)|, |N(y) \cap N(z)| \geq \frac{\eta^4 |A|}{2^5}$$

We now prove an upper bound on $|A' - A'|$ by showing that each element can be written as a linear combination of distinct octuples in A. For each such z, there are at least $\left(\frac{\eta^4|A|}{2^5}\right)^2$ pairs (u, v) with $u \in N(x) \cap N(z), v \in N(y) \cap N(z)$. For each such pair (u, v), we have $x \sim u \sim z \sim v \sim y$, hence the elements $u - x, z - u, v - z, y - v$ are all popular differences and there are at least $\left(\frac{\eta|A|}{2}\right)^4$ octuples $(a_1, \ldots, a_8) \in A^8$ such that

$$u - x = a_2 - a_1, z - u = a_4 - a_3, v - z = a_6 - a_5, y - v = a_8 - a_7$$

In other words, there are at least

$$\underbrace{\frac{\eta^{10} |A|}{2^{12}}}_{z} \underbrace{\left(\frac{\eta^4 |A|}{2^5}\right)^2}_{(u,v)} \underbrace{\left(\frac{\eta |A|}{2}\right)^4}_{(a_1,\ldots,a_8)} = \frac{\eta^{22} |A|^7}{2^{26}}$$

octuples $(a_1, \ldots, a_8) \in A^8$ such that

$$y - x = (a_8 - a_7) + (a_6 - a_5) + (a_4 - a_3) + (a_2 - a_1)$$

Since distinct $y - x$ give rise to distinct octuples,

$$\frac{\eta^{22} |A|^7}{2^{26}} |A' - A'| \leq |A|^8$$

namely

$$|A' - A'| \leq \frac{2^{26}}{\eta^{22}} |A| \leq \frac{2^{38}}{\eta^{32}} |A'|$$

$\square$

3 Probabilistic tools

Proposition 3.1 (Khintchine's inequality)**.** Let $X_1, \dots, X_n$ be independent random variables taking values $\pm x_i$ with probability $\frac{1}{2}$. Then, for all $p \in [2, \infty[$,

$$\left\| \sum_i X_i \right\|_{L^p(\mathbb{P})} = O\left(\sqrt{p} \left(\sum_i \|X_i\|_{L^2(\mathbb{P})}^2 \right)^{\frac{1}{2}} \right)$$

Lecture 10

Proof. By nesting of norms, it's enough to prove it when $p = 2k$ for some integer k. Write $X = \sum_i X_i$ and WLOG assume that $\sum_i \|X_i\|_{L^2(\mathbb{P})}^2 = 1$. By Chernoff,

$$\|X\|_{L^{2k}(\mathbb{P})}^{2k} = \int_0^\infty 2kt^{2k-1} \mathbb{P}(|X| \geq t) \, dt \leq 8k \underbrace{\int_0^\infty t^{2k-1} \exp\left(-\frac{t^2}{4}\right) \, dt}_{I(k)}$$

Let's prove by induction on k that $I(k) \leq C^{2k} \frac{(2k)^k}{4k}$ for some constant $C > 0$. Indeed if $k = 1$ then

$$\int_0^\infty t \exp\left(-\frac{t^2}{4}\right) \, dt = -2 \exp\left(-\frac{t^2}{4}\right) \Big|_0^\infty = 2 \leq C^2 \frac{2}{4}$$

if $C \geq 2$. For $k > 1$,

$$\begin{aligned}
I(k) &= \int_0^\infty t^{2k-2} t \exp\left(-\frac{t^2}{4}\right) \, dt \\
&= t^{2k-2}(-2) \exp\left(-\frac{t^2}{4}\right) \Big|_0^\infty - \int_0^\infty (2k-2) t^{2k-3} (-2) \exp\left(-\frac{t^2}{4}\right) \, dt \\
&= 4(k-1) I(k-1) \\
&\leq 4(k-1) C^{2(k-1)} \frac{(2(k-1))^{k-1}}{4(k-1)} \\
&\leq C^{2k} \frac{(2k)^k}{4k}
\end{aligned}$$

if $C \geq \sqrt{2}$. □

Corollary 3.2 (Rudin's inequality)**.** Let $\Lambda \subseteq \widehat{\mathbb{F}_2^n}$ be linearly independent and $f : \mathbb{F}_2^n \to \mathbb{C}$ be such that $\hat{f}$ is supported on Λ. Then, for all $p \in [2, \infty[$,

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

Proof. See Example Sheet 2. □

Corollary 3.3 (Dual form of Rudin's inequality)**.** Let $\Lambda \subseteq \widehat{\mathbb{F}_2^n}$ be linearly independent and let $q \in]1, 2]$ Then for all $f \in L^q(\mathbb{F}_2^n)$,

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

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

$$\hat{g}(\delta) = \mathop{\mathbb{E}}_x \delta(x) \sum_{\gamma\in\Lambda} \hat{f}(\gamma)\gamma(x) = \sum_{\gamma\in\Lambda} \hat{f}(\gamma) \mathop{\mathbb{E}}_x \gamma(x)\delta(x) = 1_\Lambda(\delta)\hat{f}(\delta)$$

So $\hat{g}$ is supported on Λ and

$$\left\|\hat{f}\right\|^2_{\ell^2(\Lambda)} = \sum_{\gamma\in\Lambda} \left|\hat{f}(\gamma)\right|^2 = \sum_{\gamma\in\Lambda} \hat{f}(\gamma)\overline{\hat{g}(\gamma)} = \langle \hat{f}, \hat{g}\rangle_{\ell_2(\mathbb{F}_2^n)} = \langle f, g\rangle_{L^2(\mathbb{F}_2^n)}$$

By Hölder,

$$\langle f, g\rangle_{L^2(\mathbb{F}_2^n)} \le \|f\|_{L^q(\mathbb{F}_2^n)} \|g\|_{L^p(\mathbb{F}_2^n)}$$

where $\frac{1}{p} + \frac{1}{q} = 1$. By Rudin,

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

Putting all of this together, we get the result. □

Recall that, given $A \subseteq \mathbb{F}_2^n$ of density $\alpha > 0$, $\left|\mathrm{Spec}_\rho(1_A)\right| \le \rho^{-2}\alpha^{-1}$. This is best possible, as the example of a subspace $H \le \mathbb{F}_2^n$ shows:

$$|\mathrm{Spec}_1(1_H)| = \left|H^\perp\right| = \left(\frac{|H|}{2^n}\right)^{-1}$$

But here H is very structured! And indeed in Bogolyubov we used the bound on the size of the spectrum only to bound the size of the subspace it generated. So maybe the *dimension* of the spectrum is what we should be looking at instead of its size.

Theorem 3.4 (Special case of Chang's lemma)**.** Let $A \subseteq \mathbb{F}_2^n$ be of density $\alpha > 0$. Then for all $\rho > 0$ there exists a subspace $H \le \mathbb{F}_2^n$ of dimension $O(\rho^{-2}\log\alpha^{-1})$ such that $\mathrm{Spec}_\rho(1_A) \subseteq H$.

Proof. Let $\Lambda \subseteq \mathrm{Spec}_\rho(1_A)$ be a maximal linearly independent subset and let $H = \langle \mathrm{Spec}_\rho(1_A)\rangle$. Then $\dim H = |\Lambda|$. By Corollary 3.3, if $q \in]1, 2]$,

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

So $|\Lambda| = O\left(\frac{q}{q-1}\rho^{-2}\alpha^{\frac{2}{q}-2}\right)$. Choose $q = 1 + \log^{-1}\alpha^{-1}$ to get $|\Lambda| = O(\rho^{-2}\log\alpha^{-1})$. □

We will prove Chang's lemma in greater generality on Example Sheet 3. The key definition for the generalisation is the following.

Definition 3.5. Let G be a finite abelian group. We say $S \subseteq G$ is **dissociated** if

$$\sum_{s\in S} \varepsilon_s s = 0 \implies \varepsilon = 0$$

for all $\varepsilon \in \{-1, 0, 1\}^S$.

Note that if $G = \mathbb{F}_2^n$ then a set $S \subseteq G$ is dissociated iff it's linearly independent.

Lecture 11

Theorem 3.6 (Chang's lemma)**.** Let G be a finite abelian group and let $A \subseteq G$ be of density $\alpha > 0$. If $\Lambda \subseteq \mathrm{Spec}_\rho(1_A)$ is dissociated, then $|\Lambda| = O(\rho^{-2}\log\alpha^{-1})$.

Proof. See Example Sheet 3. □

We may bootstrap Khintchine's inequality to get the following.

Theorem 3.7 (Marcinkiewicz-Zygmund inequality)**.** Let $p \in [2, \infty[$ and $X_1, \dots, X_n \in L^p(\mathbb{P})$ be independent random variables with $\mathbb{E}\sum_i X_i = 0$. Then

$$\left\|\sum_i X_i\right\|_{L^p(\mathbb{P})} = O\left(\sqrt{p}\left\|\sum_i |X_i|^2\right\|_{L^{\frac{p}{2}}(\mathbb{P})}^{\frac{1}{2}}\right)$$

Proof. We can derive the complex-valued case from the real-valued case by taking real and imaginary parts and apply the triangle inequality.
Next assume that the distribution of the X_i is symmetric, ie $\mathbb{P}(X_i = a) = \mathbb{P}(X_i = -a)$ for all a. Partition the probability space Ω into sets $\Omega_1, \dots, \Omega_M$, writing $\mathbb{P}_j$ for the induced probability measure on Ω_j. Do it so that all X_i are symmetric and take at most two values on each Ω_j. Applying Khintchine for each $j \in [M]$,

$$\left\|\sum_i X_i\right\|_{L^p(\mathbb{P}_j)}^p = O\left(p^{\frac{p}{2}}\left(\sum_i \|X_i\|_{L^2(\mathbb{P}_j)}^2\right)^{\frac{p}{2}}\right) = O\left(p^{\frac{p}{2}}\left\|\sum_i |X_i|^2\right\|_{L^{\frac{p}{2}}(\mathbb{P}_j)}^{\frac{p}{2}}\right)$$

with the last inequality being Jensen on $x \mapsto x^{\frac{p}{2}}$. Summing over all $j \in [M]$ and taking p-th roots gives the symmetric case.
Now suppose the X_i are arbitrary. Let $Y_1, \dots, Y_n$ be such that $X_i \sim Y_i$ and $X_1, \dots, X_n$, $Y_1, \dots, Y_n$ are independent. Applying the symmetric result to $X_i - Y_i$,

$$\begin{aligned}\left\|\sum_i (X_i - Y_i)\right\|_{L^p(\mathbb{P}\times\mathbb{P})} &= O\left(\sqrt{p}\left\|\sum_i |X_i - Y_i|^2\right\|_{L^{\frac{p}{2}}(\mathbb{P}\times\mathbb{P})}^{\frac{1}{2}}\right) \\ &= O\left(\sqrt{p}\left\|\sum_i |X_i|^2\right\|_{L^{\frac{p}{2}}(\mathbb{P})}^{\frac{1}{2}}\right)\end{aligned}$$

But also

$$\left\|\sum_i X_i\right\|_{L^p(\mathbb{P})} = \left\|\sum_i X_i - \mathop{\mathbb{E}}\sum_i Y_i\right\|_{L^p(\mathbb{P})} \le \left\|\sum_i (X_i - Y_i)\right\|_{L^p(\mathbb{P}\times\mathbb{P})}$$

by convexity. □

Theorem 3.8 (Croot-Sisask Almost Periodicity)**.** Let G be a finite abelian group, let $\varepsilon > 0$ and let $p \in [2, \infty[$. Let $A, B \subseteq G$ be such that $|A + B| \le K|A|$ and let $f : G \to \mathbb{C}$. Then there exist $b \in B$ and a set $X \subseteq B - b$ such that $|X| \ge (2K)^{-O(\varepsilon^{-2}p)}|B|$ and

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

Proof. The main idea is to approximate

$$(f * \mu_A)(y) = \mathop{\mathbb{E}}_x \mu_A(x) f(y - x) = \mathop{\mathbb{E}}_{x \in A} f(y - x)$$

by $\frac{1}{k}\sum_{i=1}^k f(y-z_i)$ with the z_i sampled uniformly at random from A for some k to be chosen. For each $y \in G$, define $Z_i(y) = \tau_{-z_i}(f)(y) - (f * \mu_A)(y)$ which are independent with mean zero. So, by Marcinkiewicz-Zygmund,

$$\left\|\sum_i Z_i(y)\right\|_{L^p(\mathbb{P})}^p = O\left(p^{\frac{p}{2}}\left\|\sum_i |Z_i(y)|^2\right\|_{L^{\frac{p}{2}}(\mathbb{P})}^{\frac{p}{2}}\right) = O\left(p^{\frac{p}{2}} \mathop{\mathbb{E}}_{z_1,\dots,z_k}\left|\sum_i |Z_i(y)|^2\right|^{\frac{p}{2}}\right)$$

Lecture 12

By Hölder, picking q such that $\frac{2}{p}+\frac{1}{q}=1$,

$$\text{RHS} \le \left(\sum_i 1^q\right)^{\frac{1}{q}\frac{p}{2}}\left(\sum_i |Z_i(y)|^{2\frac{p}{2}}\right)^{\frac{2}{p}\frac{p}{2}} = k^{\frac{p}{2}-1}\sum_i |Z_i(y)|^p$$

So, for each $y \in G$,

$$\left\|\sum_i Z_i(y)\right\|_{L^p(\mathbb{P})}^p = O\left(p^{\frac{p}{2}}k^{\frac{p}{2}-1}\mathop{\mathbb{E}}_{z_1,\dots,z_k}\sum_i |Z_i(y)|^p\right)$$

Taking expectation over $y \in G$,

$$\mathop{\mathbb{E}}_y\left\|\sum_i Z_i(y)\right\|_{L^p(\mathbb{P})}^p = O\left(p^{\frac{p}{2}}k^{\frac{p}{2}-1}\mathop{\mathbb{E}}_{z_1,\dots,z_k}\sum_i \|Z_i\|_{L^p(G)}^p\right)$$

Note that

$$\|Z_i\|_{L^p(G)} \le \|\tau_{-z_i}(f)\|_{L^p(G)} + \|f * \mu_A\|_{L^p(G)} \le 2\|f\|_{L^p(G)}$$

by Young's convolution inequality ($\|f * g\|_{L^p} \le \|f\|_{L^q}\|g\|_{L^r}$ if $1+\frac{1}{p} = \frac{1}{q}+\frac{1}{r}$). It follows that

$$\mathop{\mathbb{E}}_{z_1,\dots,z_k}\mathop{\mathbb{E}}_y\left|\sum_i Z_i(y)\right|^p = O\left(p^{\frac{p}{2}}k^{\frac{p}{2}-1}\sum_i 2\|f\|_{L^p(G)}^p\right) = O\left((pk\|f\|_{L^p(G)}^2)^{\frac{p}{2}}\right)$$

Dividing by k on both sides,

$$\mathop{\mathbb{E}}_{z_1,\dots,z_k}\underbrace{\mathop{\mathbb{E}}_y\left|\mathop{\mathbb{E}}_i(\tau_{-z_i}(f)(y) - (f * \mu_A)(y))\right|^p}_{(*)} = O\left((pk^{-1}\|f\|_{L^p(G)}^2)^{\frac{p}{2}}\right)$$

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

$$L = \left\{(z_1,\dots,z_k) \mid (*) \ge \left(\frac{\varepsilon}{2}\|f\|_{L^p(G)}\right)^p\right\}$$

Observe that $\mathbb{E}(*) \le (\frac{\varepsilon}{4}\|f\|_{L^p(G)})^p = 2^{-p}(\frac{\varepsilon}{2}\|f\|_{L^p(G)})^p$. Hence Markov tells us that

$$\frac{|L^c|}{|A|^k} = \mathbb{P}\left((*) \ge \left(\frac{\varepsilon}{2}\|f\|_{L^p(G)}\right)^p\right) \le 2^{-p} \le 1 - 2^{-k}$$

Hence $|L| \ge \frac{1}{2^k}|A|^k$. Let $D = \{(b,\dots,b) \mid b \in B\} \subseteq B^k$ the diagonal. Note that $L + D \subseteq (A+B)^k$, whence $|L+D| \le \left|(A+B)^k\right| \le K^k|A|^k \le (2K)^k|L|$. By Lemma 2.12,

$$\#\{\text{additive quadruples between } L \text{ and } D\} \ge \frac{|D|^2|L|}{(2K)^k}$$

So there are at least $\frac{|D|^2}{(2K)^k}$ pairs $(d_1, d_2) \in D \times D$ such that $r_{L-L}(d_1 - d_2) > 0$ (rewrite additive quadruples $\ell_1 + d_1 = \ell_2 + d_2$ as $d_1 - d_2 = \ell_2 - \ell_1$ and double-count). In particular, there exists $b \in B$ and $X \subseteq B - b$ of size $|X| \geq \frac{|D|}{(2K)^k}$ such that $\forall i, \ell_1(x) - \ell_2(x) = x$. We are now done: By the triangle inequality, for each $x \in X$,

$$\begin{aligned}
\|\tau_{-x}(f * \mu_A) - f * \mu_A\|_{L^p(G)} \leq & \left\| \tau_{-x}(f * \mu_A - \mathop{\mathbb{E}}_i \tau_{-\ell_2(x)}(f)) \right\|_{L^p(G)} \\
& + \left\| \tau_{-x} \mathop{\mathbb{E}}_i \tau_{-\ell_2(x)}(f) - f * \mu_A \right\|_{L^p(G)} \\
\leq & \left\| \tau_{-x}(f * \mu_A - \mathop{\mathbb{E}}_i \tau_{-\ell_2(x)}(f)) \right\|_{L^p(G)} \\
& + \left\| \mathop{\mathbb{E}}_i \tau_{-\ell_1(x)}(f) - f * \mu_A \right\|_{L^p(G)} \\
\leq & \varepsilon \|f\|_{L^p(G)} \quad \text{by definition of } L
\end{aligned}$$

□

Theorem 3.9 (Polynomial Bogolyubov)**.** Let $A \subseteq \mathbb{F}_p^n$ 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 $V \subseteq A + A - (A + A)$.

Proof. See Example Sheet 3. □

Theorem 3.10 (Schoen, Shkredov)**.** Let $p \neq 5$ and let $A \subseteq \mathbb{F}_p^n$ be a set containing no nontrivial solution to $x_1 + x_2 + x_3 + x_4 + x_5 = 5y$. Then $|A| = \exp(-\Omega(n^{\frac{1}{5}})) \left|\mathbb{F}_p^n\right|$.

Proof. Let α be the density of A. Partition A into $A_1 \cup A_2$ where $|A_1| = \left\lfloor \frac{\alpha}{2} p^n \right\rfloor, |A_2| = \left\lceil \frac{\alpha}{2} p^n \right\rceil$. By averaging, find z 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 $V \leq \mathbb{F}_p^n$ of codimension $O(\log^4 \alpha^{-1})$ such that $V \subseteq A' + A' - (A' + A')$. Hence

$$2z + V \subseteq 2z + A' + A' - (A' + A') \subseteq A_1 + A_1 + A_2 + A_2$$

Consequently, $(5 \cdot A - A) \cap (2z + V) = \varnothing$. Else there would be $x, y \in A, a_1, a_1' \in A_1, a_2, a_2' \in A_2$ such that $5y - x = a_1 + a_1' + a_2 + a_2'$ which would yield a nontrivial solution since A_1, A_2 are disjoint. If 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 nonempty. Therefore

$$2|A| = \sum_{w \in V^\perp} |A \cap (w + V)| + |5 \cdot A \cap (w + 2z + V)| \leq \left|V^\perp\right| \sup_{w \in V^\perp} |A \cap (w + V)|$$

So there exists $w \in V^\perp$ such that $|A \cap (w + V)| \geq \frac{2|A|}{|V^\perp|} = 2\alpha V$. The set $A \cap (w + V) \subseteq w + V$ has density at least 2α and contains no nontrivial solution.
After t steps, we obtain a subspace W of codimension $O(t \log^4 \alpha^{-1})$ and w such that $|A \cap (w + W)| \geq 2^t \alpha |W|$. Arguing as in the proof of Theorem 1.17 yields the result. □

We get a similar bound in $\mathbb{F}_n$ where Behrend's construction offers a comparable lower bound.

4 Further topics

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

Theorem 4.1 (Ellenberg-Gijswijt, based on Croot-Lev-Pach)**.** Let $A \subseteq \mathbb{F}_3^n$ be a set containing no nontrivial 3AP. 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 $\mathbb{F}_3$-vector space 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 write V_n^d for the corresponding vector space. Set $m_d = \dim V_n^d = \left|M_n^d\right|$.

Lemma 4.2. Let $A \subseteq \mathbb{F}_3^n$ and suppose $P \in V_n^d$ is such that $P(a + a') = 0$ for all $a, a' \in A$ distinct. Then

$$|\{a \in A \mid P(2a) \neq 0\}| \leq 2m_{\frac{d}{2}}$$

Proof. Every $P \in V_n^d$ can be written as a linear combination of monomials from M_n^d. So

$$P(x + y) = \sum_{\substack{m,m' \in M_n^d \\ \deg m + \deg m' \leq d}} c_{m,m'} m(x) m'(y)$$

for some coefficients $c_{m,m'}$. Since at least one of m, m' has degree $\leq \frac{d}{2}$, we can write

$$P(x + y) = \sum_{m \in M_n^{\frac{d}{2}}} m(x) F_m(y) + \sum_{m' \in M_n^{\frac{d}{2}}} m'(y) G_{m'}(x)$$

where $F_m, G_{m'}$ are polynomials. Viewing P as an $|A| \times |A|$-matrix, we see that it can be written as a sum of at most $2m_{\frac{d}{2}}$ rank 1 matrices. Hence $\operatorname{rank} P \leq 2m_{\frac{d}{2}}$. But P is a diagonal matrix by assumption. Hence

$$|\{a \in A \mid P(2a) \neq 0\}| = \operatorname{rank} P \leq 2m_{\frac{d}{2}}$$

□

Proposition 4.3. Let $A \subseteq \mathbb{F}_3^n$ be a set containing no nontrivial 3AP. Then $|A| \leq 3m_{\frac{2n}{3}}$.

Proof. Let $d \in [1, 2n]$ be an integer to be chosen later. Let W be the subspace of V_n^d that vanish on $2 \cdot A^c$. Clearly,

$$\dim W \geq \dim V_n^d - |2 \cdot A^c| = m_d - (3^n - |A|)$$

We claim that there is $P \in W$ such that $|\operatorname{supp} P| \geq \dim W$. Indeed, pick $P \in W$ with maximal support. If $|\operatorname{supp} P| < \dim W$, then there is a nonzero $Q \in W$ vanishing on $\operatorname{supp} P$, in which case P and Q have disjoint support and

$$\operatorname{supp}(P + Q)) \operatorname{supp} P \cup \operatorname{supp} Q \supsetneq \operatorname{supp} P$$

contradicting the maximality of P.
By assumption, $\{a + a' \mid a, a' \in A, a \neq a'\}$ and $2 \cdot A$ are disjoint. So any polynomial vanishing on $2 \cdot A^c$ also vanishes on $\{a + a' \mid a, a' \in A, a \neq a'\}$. By Lemma 4.2,

$$|\operatorname{supp} P| = |\{x \mid P(x) \neq 0\}| = |\{a \in A \mid P(2a) \neq 0\}| \leq 2m_{\frac{d}{2}}$$

Putting everything together,

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

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

$$|A| \leq (3^n - m_d) + 2m_{\frac{d}{2}} = m_{2n-d} + 2m_{\frac{d}{2}} = 3m_{\frac{2n}{3}}$$

□

We do **not** know of a comparable bound for 4APs. Fourier-analytic techniques also fail.

Example 4.4. Recall from Lemma 1.16 that

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

But it is impossible to bound

$$\left|T_4(1_A, 1_A, 1_A, 1_A) - \alpha^4\right| = \left|\mathop{\mathbb{E}}_{x,d} 1_A(x)1_A(x+d)1_A(x+2d)1_A(x+3d) - \alpha^4\right|$$

by $\sup_{t\neq 0}\left|\widehat{1_A}(t)\right|$. Indeed, consider $Q = \{x \in \mathbb{F}_p^n \mid x \cdot x = 0\}$. By Question 2.ii on Example Sheet 1, $\frac{|Q|}{p^n} = \frac{1}{p} + O(p^{-\frac{n}{2}})$ and $\sup_{t\neq 0}\left|\widehat{1_A}(t)\right| = O(p^{-\frac{n}{2}})$. But, given a 3AP $x, x+d, x+2d \in Q$, we automatically have $x + 3d \in Q$ because of the following identity:

$$x \cdot x - 3(x+d) \cdot (x+d) + 3(x+2d) \cdot (x+2d) - (x+3d) \cdot (x+3d)$$

So $T_4(1_A, 1_A, 1_A, 1_A) = T_3(1_A, 1_A, 1_A) = \alpha^3 + o(1)$ by Lemma 1.16.

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

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

Question 3.i on Example Sheet 1 showed that $\|f\|_{U^2} = \left\|\hat{f}\right\|_{\ell^4}$, so this is indeed a norm. Question 3.ii asserted the following.

Lemma 4.6. Let $f_1, f_2, f_3 : G \to \mathbb{C}$. Then

$$\begin{aligned} |T_3(f_1, f_2, f_3)| \leq & \|f_1\|_{L^2} \|f_2\|_{U^2} \|f_3\|_{U^2}, \\ & \|f_1\|_{U^2} \|f_2\|_{L^2} \|f_3\|_{U^2}, \\ & \|f_1\|_{U^2} \|f_2\|_{U^2} \|f_3\|_{L^2} \end{aligned}$$

In particular,

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

Note that

$$\sup_\gamma \left|\hat{f}(\gamma)\right|^4 \leq \sum_\gamma \left|\hat{f}(\gamma)\right|^4 \leq \sup_\gamma \left|\hat{f}(\gamma)\right|^2 \sum_\gamma \left|\hat{f}(\gamma)\right|^2$$

Thus, by Parseval,

$$\left\|\hat{f}\right\|_{\infty} \leq \|f\|_{U^2} \leq \left\|\hat{f}\right\|_{\infty}^{\frac{1}{2}} \|f\|_{L^2}^{\frac{1}{2}}$$

Moreover, if $f = f_A = 1_A - \alpha$, then

$$T_3(f,f,f) = T_3(1_A - \alpha, 1_A - \alpha, 1_A - \alpha) = T_3(1_A, 1_A, 1_A) - \alpha^3$$

We could therefore reformulate the first step in the proof of Meshulam's theorem (Theorem 1.17) as follows:
If $p^n \geq 2\alpha^{-2}$, then

$$\frac{\alpha^3}{2} \leq |T_3(1_A, 1_A, 1_A) - \alpha| \leq \|f_A\|_{U^2}$$

by Lemma 4.6.

Lecture 13

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 which A has increased density.

Theorem 4.7 (U^2 inverse theorem)**.** Let $f : \mathbb{F}_p^n \to \mathbb{C}$ satisfy $\|f\|_\infty \leq 1$ and $\|f\|_{U^2} \geq \delta$ for some $\delta > 0$. Then there exists b such that $\left|\mathbb{E}_x f(x)\omega^{x\cdot b}\right| \geq \delta^2$.
In other words, $|\langle f, \phi\rangle| \geq \delta^2$ for $\phi(x) = \omega^{x\cdot b}$ and we say that "f correlates with a linear function".

Proof. We have seen that $\|f\|_{U^2}^2 \leq \left\|\hat{f}\right\|_\infty \|f\|_2 \leq \left\|\hat{f}\right\|_\infty$. So $\delta^2 \leq \left\|\hat{f}\right\|_\infty = |\mathbb{E}_x f(x)\omega^{x\cdot n}|$ for some b. □

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

$$\|f\|_{U^3}^8 = \mathop{\mathbb{E}}_{x,a,b,c} f(x)\overline{f(x+a)f(x+b)f(x+c)}$$

$$f(x+a+b)f(x+a+c)f(x+b+c)\overline{f(x+a+b+c)}$$

$$= \mathop{\mathbb{E}}_{x,h_1,h_2,h_3} \prod_{\varepsilon\in\{0,1\}^3} \mathrm{conj}^{|\varepsilon|} f(x+\varepsilon\cdot h)$$

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

Definition 4.9. Given functions $f_\varepsilon : G \to \mathbb{C}$ for $\varepsilon \in \{0,1\}^3$, define the **Gowers U^3-inner product** by

$$\langle f\rangle_{U^3} = \mathop{\mathbb{E}}_{h} \|\Delta_h f\|_{U^2}^4$$

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

Lemma 4.10 (Gowers-Cauchy-Schwarz)**.** Given $f_\varepsilon : G \to \mathbb{C}$ for $\varepsilon \in \{0,1\}^3$,

$$|\langle f\rangle_{U^3}| \leq \prod_{\varepsilon} \|f_\varepsilon\|_{U^3}$$

Proof. See Example Sheet 3. □

Setting $f_\varepsilon = \begin{cases} f & \text{if } \varepsilon_0 = 0 \\ 1 & \text{if } \varepsilon_0 = 1 \end{cases}$, the LHS equals $\|f\|_{U^2}^4$. Hence $\|f\|_{U^2} \leq \|f\|_{U^3}$.

Proposition 4.11. Let $f : G \to \mathbb{C}$ with $\|f\|_\infty \leq 1$. Then

$$|T_4(f,f,f,f)| \leq \|f\|_{U^3}$$

Proof. Reparametrising, we have

$$\begin{aligned}
T_4(f,f,f,f) &= \mathop{\mathbb{E}}_{a,b,c,d} \underbrace{f(3a+2b+c)}_{=:f_1(a,b,c)} \underbrace{f(2a+b-d)}_{=:f_2(a,b,d)} \underbrace{f(a-c-2d)}_{=:f_3(a,c,d)} \underbrace{f(-b-2c-3d)}_{=:f_4(b,c,d)} \\
&= \mathop{\mathbb{E}}_{a,b,c} f_1(a,b,c) \mathop{\mathbb{E}}_{d} f_2(a,b,d) f_3(a,c,d) f_4(b,c,d)
\end{aligned}$$

So

$$\begin{aligned}
|T_4(f,f,f,f)|^2 &\leq \mathop{\mathbb{E}}_{a,b,c} \left| \mathop{\mathbb{E}}_{d} f_2(a,b,d) f_3(a,c,d) f_4(b,c,d) \right|^2 \\
&= \mathop{\mathbb{E}}_{d,d',a,b} f_2(a,b,d)\overline{f_2(a,b,d')} \mathop{\mathbb{E}}_{c} f_3(a,c,d) f_4(b,c,d) \overline{f_3(a,c,d') f_4(b,c,d')}
\end{aligned}$$

Hence

$$\begin{aligned}
|T_4(f,f,f,f)|^4 &\leq \mathop{\mathbb{E}}_{d,d',a,b} \left| \mathop{\mathbb{E}}_{c} f_3(a,c,d) f_4(b,c,d) \overline{f_3(a,c,d') f_4(b,c,d')} \right|^2 \\
&= \mathop{\mathbb{E}}_{c,c',d,d',a} f_3(a,c,d) \overline{f_3(a,c,d') f_3(a,c',d)} f_3(a,c',d') \\
&\quad \mathop{\mathbb{E}}_{b} f_4(b,c,d) \overline{f_4(b,c,d'), f_4(b,c',d)} f_4(b,c',d')
\end{aligned}$$

Finally,

$$\begin{aligned}
|T_4(f,f,f,f)|^8 &\leq \mathop{\mathbb{E}}_{c,c',d,d',a} \left| \mathop{\mathbb{E}}_{b} f_4(b,c,d) \overline{f_4(b,c,d'), f_4(b,c',d)} f_4(b,c',d') \right|^2 \\
&= \mathop{\mathbb{E}}_{b,b',c,c',d,d'} f_4(b,c,d) \overline{f_4(b,c,d'), f_4(b,c',d)} f_4(b,c',d') \\
&\quad \overline{f_4(b',c,d)} f_4(b',c,d'), f_4(b',c',d) \overline{f_4(b',c',d')} \\
&= \|f\|_{U^3}^8
\end{aligned}$$

□

One might hope to generalise Meshulam's theorem (Theorem 1.17) as follows.

Theorem 4.12 (Szemerédi for 4APs)**.** Let $A \subseteq \mathbb{F}_p^n$ be a set containing no nontrivial 4APs. Then $|A| = o(p^n)$.

Idea. By Proposition 4.11 with $f = f_A = 1_A - \alpha$,

$$T_4(1_A, 1_A, 1_A, 1_A) - \alpha^4 = T_4(f_A, f_A, f_A, f_A) + \underbrace{\dots + \dots + \dots}_{\text{controlled by } \|f_A\|_{U^2}} + \underbrace{\dots + \dots + \dots}_{\text{explicit}}$$

Hence, and since $\|f_A\|_{U^2} \le \|f_A\|_{U^3}$,

$$\left|T_4(1_A, 1_A, 1_A, 1_A) - \alpha^4\right| \le 14 \|f_A\|_{U^3}$$

so if A contains no nontrivial 4AP and $p^n \ge 2\alpha^{-3}$ then $\frac{\alpha^4}{2} \le 14 \|f_A\|_{U^3}$.

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

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

Theorem 4.14 (U^3 inverse theorem)**.** Let $f : \mathbb{F}_p^n \to \mathbb{C}$ satisfying $\|f\|_\infty \le 1$ and $\|f\|_{U^3} \ge \delta$ for some $\delta > 0$. Then there exists a symmetric matrix M with entries in $\mathbb{F}_p$ and $b \in \mathbb{F}_p^n$ such that

$$\left| \mathop{\mathbb{E}}_x f(x) \omega^{x^\perp M x + b^\perp x} \right| \ge c_p(\delta)$$

where c_p is a polynomial.
In other words, $|\langle f, \phi \rangle| \ge c_p(\delta)$ for $\phi(x) = \omega^{x^\perp M x + b^\perp x}$ and we say that "f correlates with a quadratic phase function".

Proof sketch. Suppose $\|f\|_{U^3} \ge \delta$.

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

Proposition 4.15. Let $f : \mathbb{F}_p^n \to \mathbb{C}$ satisfy $\|f\|_\infty \le 1$ and $\|f\|_{U^3} \ge \delta$ for some $\delta > 0$. Suppose that $\left|\mathbb{F}_p^n\right| = \Omega_\delta(1)$. Then there exists $S \subseteq \mathbb{F}_p^n$ of density $\Omega_\delta(1)$ and a function $\phi : S \to \mathbb{F}_p^n$ such that

1. $\left|\widehat{\Delta_h} f(\phi(h))\right| = \Omega_\delta(1)$
2. There are at least $\Omega_\delta(\left|\mathbb{F}_p^n\right|^2)$ additive quadruples $(s_1, s_2, s_3, s_4) \in S^4$ (namely $s_1 + s_2 = s_3 + s_4$) such that $\phi(s_1) + \phi(s_2) = \phi(s_3) + \phi(s_4)$.

Step 2: "Strong linearity"
If S and ϕ are as above, then there is an affine map $\psi : \mathbb{F}_p^n \to \widehat{\mathbb{F}_p^n}$ 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 there exists a $n \times n$ matrix with entries in $\mathbb{F}_p$ and $b \in \mathbb{F}_p^n$ such that the map $\psi : \mathbb{F}_p^n \to \widehat{\mathbb{F}_p^n}$ satisfies $\psi(x) = \phi(x)$ for $\Omega_\delta(\left|\mathbb{F}_p^n\right|)$ elements x of S

Proof. Consider the graph $\Gamma = \{(h, \phi(h)) \mid h \in S\} \subseteq \mathbb{F}_p^n \times \widehat{\mathbb{F}_p^n}$. By Proposition 4.15, Γ has $\Omega_\delta(\left|\mathbb{F}_p^n\right|)$ additive quadruples. By Balog-Szemerédi-Gowers (Theorem 2.14), there exists $\Gamma' \subseteq \Gamma$ with $|\Gamma'| = \Omega_\delta(|\Gamma|) = \Omega_\delta(\left|\mathbb{F}_p^n\right|)$ and $|\Gamma' + \Gamma'| = O_\delta(|\Gamma'|)$. Denote by

$\pi : \mathbb{F}_p^n \times \widehat{\mathbb{F}_p^n} \to \mathbb{F}_p^n$ the projection onto the first factor. Define $S' = \pi(\Gamma')$ and note that $|S'| = |\Gamma'| = \Omega_\delta(|\mathbb{F}_p^n|)$. By Freiman-Ruzsa (Theorem 2.8) applied to $\Gamma' \subseteq \mathbb{F}_p^n \times \widehat{\mathbb{F}_p^n}$, there exists a subspace $H \leq \mathbb{F}_p^n \times \widehat{\mathbb{F}_p^n}$ with $|H| = \Omega_\delta(|\Gamma'|) = \Omega_\delta(|\mathbb{F}_p^n|)$ such that $\Gamma' \subseteq H$. By construction, $S' \subseteq \pi(H)$. Moreover,

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

We may pick H^* a transversal of $\ker \pi \restriction_H$ and partition H into cosets of H^*. π is injective on each coset. By averaging, there 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 $S'' = \pi(\Gamma'')$. Now, $\pi \restriction_{x+H^*}$ is a bijection onto its image $V = \operatorname{im} \pi \restriction_{x+H^*}$. Thus we have an affine map $\psi : V \to \widehat{\mathbb{F}_p^n}$ such that $(h, \psi(h)) \in \Gamma''$ for all $h \in S''$. $\square$

Step 3: Symmetry argument
Having obtained $\psi(x) = Mx + b$ for some matrix M and vector b such that $(h, Mh + b) \in \Gamma''$ for all $h \in S''$, we need to turn M into a symmetric matrix in preparation of Step 4.

Step 4: "Integrating"

Proposition 4.17. Suppose f, M, b are as in Step 3 and $\mathbb{E}_h \left|\widehat{\Delta_h} f(Mh + b)\right|^2 = \Omega_\delta(1)$. If $p > 2$, then there exists $b' \in \mathbb{F}_p^n$ such that $\mathbb{E}_x\, f(x) \omega^{x^T \frac{M+M^T}{2} x + b'^T x} = \Omega_\delta(1)$.

Proof. See Example Sheet 3. $\square$

$\square$