Introduction to Additive Combinatorics

Daniel Naylor

December 3, 2024

Contents

Lecture 1

1 Combinatorial methods

Definition 1.1 (Sumset)**.** Let G be an abelian group. Given $A, B \subseteq G$, define the *sumset* $A + B$ to be

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

and the *difference set* $A - B$ to be

$$A - B := \{a + b : a \in A, b \in B\}.$$

If A and B are finite, then certainly

$$\max\{|A|, |B|\} \leq |A + B| \leq |A||B|.$$

Example 1.2. Let $A = [n] := \{1, 2, \dots, n\} \subseteq \mathbb{Z}$. Then

$$|A + A| = |\{2, \dots, 2n\}| = 2n - 1 = 2|A| - 1.$$

Lemma 1.3. Assuming that:

- $A \subseteq \mathbb{Z}$ is finite.

Then $|A + A| \geq 2|A| - 1$, with equality if and only if A is an arithmetic progression.

Proof. Let $A = \{a_1, a_2, \dots, a_n\}$ with $a_1 < a_2 < \dots < a_n$. Then

$$a_1 + a_1 < a_1 + a_2 < a_1 + a_2 < \dots < a_1 + a_n < a_2 + a_n < \dots < a_n + a_n,$$

so $|A + A| \geq 2|A| - 1$. But we could also have written

$$a_1 + a_1 < a_1 + a_2 < a_2 + a_2 < a_2 + a_3 < a_2 + a_4 < \dots < a_2 + a_n < a_3 + a_n < \dots < a_n + a_n.$$

When $|A + A| = 2|A| - 1$, these two orderings must be the same. So $a_2 + a_i = a_1 + a_{i+1}$ for all $i = 2, \dots, n - 1$. □

Exercise: If $A, B \subseteq \mathbb{Z}$, then $|A + B| \geq |A| + |B| - 1$ with equality if and only if A and B are arithmetic progressions with the same common difference.

Example 1.4. Let $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ with p prime. Then $|A + B| \geq p + 1 \implies A + B = \mathbb{Z}/p\mathbb{Z}$. Indeed, $g \in A + B \iff A \cap (g - B) \neq \emptyset$ (note that $g - B$ means $\{g\} - B$). But $\forall g \in \mathbb{Z}/p\mathbb{Z}$,

$$|A \cap (g - B)| = |A| + |g - B| - |A \cup (g - B)| \geq |A| + |B| - p \geq 1.$$

Theorem 1.5 (Cauchy-Davenport)**.** Assuming that:

- p is a prime
- $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ nonempty

Then
$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof. Assume $|A|+|B| \leq p+1$. Without loss of generality assume that $1 \leq |A| \leq |B|$ and that $0 \in A$. Apply induction on $|A|$. The case $|A| = 1$ is trivial. Suppose $|A| \geq 2$, and let $0 \neq a \in A$.

Since $\{a, 2a, 3a, \dots, (p-1)a, pa\} = \mathbb{Z}/p\mathbb{Z}$ and $|A| + |B| \leq p + 1$, there must exist $m \geq 0$ such that $ma \in B$ but $(m + 1)a \notin B$. Let $B' = B - ma$, so $0 \in B'$, $a \notin B'$, $|B'| = |B|$.

But $1 \leq |A \cap B'| < |A|$, so the inductive hypothesis applies to $A \cap B'$ and $A \cup B'$. Since
$$(A \cap B') + (A \cup B') \subseteq A + B',$$
we have
$$|A + B| = |A + B'| \geq |(A \cap B') + (A \cup B')| \geq |A \cap B'| + |A \cup B'| + 1 = |A| + |B| + 1. \qquad \square$$

This fails for general abelian groups (or even general cyclic groups).

Example 1.6. Let p be (fixed, small) prime, and let $V \leq \mathbb{F}_p^n$ be a subspace. Then $V + V = V$, so $|V + V| = |V|$. In fact, if $A \subseteq \mathbb{F}_p^n$ is such that $|A + A| = |A|$, then A must be a coset of a subspace.

Example 1.7. Let $A \subseteq \mathbb{F}_p^n$ be such that $|A + A| < \frac{3}{2}|A|$. Then there exists $V \leq \mathbb{F}_p^n$ a subspace such that $|V| < \frac{3}{2}|A|$ and A is contained in a coset of V. See Example Sheet 1.

Definition 1.8 (Ruzsa distance)**.** Given finite sets $A, B \subseteq G$, we define the *Ruzsa distance* $d(A, B)$ between A and B by
$$d(A, B) = \log \frac{|A - B|}{\sqrt{|A||B|}}$$

Lecture 2

Note that this is symmetric, but is not necessarily non-negative, so we cannot prove that it is a metric. It does, however, satisfy triangle inequality:

Lemma 1.9 (Ruzsa's triangle inequality)**.** Assuming that:

- $A, B, C \subseteq G$ finite

Then

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

Proof. Observe that

$$|B| \cdot |A - C| \le |A - B| \cdot |B - C|.$$

Indeed, writing each $d \in A - C$ as $d = a_d - c_d$ with $a_d \in A$, $c_d \in C$, the map

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

is injective. The triangle inequality now follows from the definition. □

Definition 1.10 (Doubling / difference constant)**.** Given a finite $A \subseteq G$, we write

$$\sigma(A) := \frac{|A + A|}{|A|}$$

for the *doubling constant* of A and

$$\delta(A) := \frac{|A - A|}{|A|}$$

for the *difference constant* of A.

Then Lemma 1.9 shows, for example, that

$$\log \delta(A) = d(A, A) \le d(A, -A) + d(-A, A) = 2 \log \sigma(A).$$

So $\delta(A) \le \sigma(A)^2$, or $|A - A| \le \frac{|A+A|^2}{|A|}$.

Notation. Given $A \subseteq G$ and $l, m \in \mathbb{N}_0$, we write

$$lA - mA := \underbrace{A + A + \cdots + A}_{l \text{ times}} - \underbrace{A - A - \cdots - A}_{m \text{ times}}.$$

Theorem 1.11 (Plúnnecke's Inequality)**.** Assuming that:

- $A, B \subseteq G$ are finite sets
- $|A + B| \le K|A|$ for some $K \ge 1$

Then $\forall l, m \in \mathbb{N}_0$,

$$|lB - mB| \le K^{l+m}|A|.$$

Proof. Choose a non-empty subset $A' \subseteq A$ such that the ratio $\frac{|A'+B|}{|A'|}$ is minimised, and call this ratio K'. Then $|A'+B| = K'|A'|$, $K' \leq K$, and $\forall A'' \subseteq A$, $|A''+B| \geq K'|A''|$.

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

Let's complete the proof of the theorem assuming the claim. We first show that $\forall m \in \mathbb{N}_0$, $|A'+mB| \leq K'^m|A'|$. Indeed, the case $m=0$ is trivial, and $m=1$ is true by assumption. Suppose $m>1$ and the inequality holds for $m-1$. By the claim with $C=(m-1)B$, we get

$$|A'+mB| = |A'+B+(m-1)B| \leq K'|A'+(m-1)B| \leq K'^m|A'|.$$

But as in the proof of Ruzsa's triangle inequality, $\forall l, m \in \mathbb{N}_0$, we can show

$$|A'||lB-mB| \leq |A'+lB||A'+mB| \leq K'^l|A'|K'^m|A'| = K'^{l+m}|A'|^2.$$

Hence $|lB-mB| \leq K'^{l+m}|A'| \leq K'^{l+m}|A|$, which completes the proof (assuming the claim).

We now prove the claim by induction on $|C|$. When $|C|=1$ the statement follows from the assumptions. Suppose the claim is true for C, and consider $C' = C \cup \{x\}$ for some $x \notin C$. Observe that

$$A'+B+C' = (A'+B+C) + ((A'+B+x) \setminus (D+B+x))$$

with $D = \{a \in A' : a+B+x \subseteq A'+B+X\}$.

By definition of K', $|D+B| \geq K'|D|$, so

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

We apply this argument a second time, writing

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

where $E = \{a \in A' : a+x \in A'+C\} \subseteq D$. We conclude that

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

so

$$|A'+B+C'| \leq K'(|A'+C| + |A'| - |D|) \leq K'|A'+C'|,$$

proving the claim. □

We are now in a position to generalise Example 1.7.

Theorem 1.12 (Freiman-Ruzsa)**.** Assuming that:

- $A \subseteq \mathbb{F}_p^n$

- $|A+A| \leq K|A|$ (i.e. $\sigma(A) \leq K$)

Then A is contained in a subspace $H \leq \mathbb{F}_p^n$ of size $|H| \leq K^2 p^{K^4}|A|$.

Lecture 3

Proof. Choose $X \subseteq 2A-A$ maximal such that the translates $x+A$ with $x \in X$ are disjoint. Such a set X cannot be too large: $\forall x \in X$, $x+A \subseteq 3A-A$, so by Plúnnecke's Inequality, since $|3A-A| \leq K^4|A|$,

$$|X||A| = \left|\bigcup_{x\in X}(x+A)\right| \leq |3A-A|.$$

So $|X| \leq K^4$. We next show

$$2A - A \subseteq X + A - A. \tag{$*$}$$

Indeed, if $y \in 2A-A$ and $y \notin X$, then by maximality of X, $y+A \cap x+A \neq \emptyset$ for some $x \in X$ (and if $y \in X$, then clearly $y \in X+A-A$).

It follows from $(*)$ by induction that $\forall l \geq 2$,

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

since

$$lA - A = A + \underbrace{(l-1)A - A}_{\subseteq (l-2)X+A-A} \subseteq (l-2)X + \underbrace{2A - A} \subseteq X + A - A \subseteq (l-1)X + A - A.$$

Now let $H \leq \mathbb{F}_p^n$ be the subgroup generated by A, which we can write as

$$H = \bigcup_{l\geq 1}(lA - A) \overset{(**)}{\subseteq} Y + A - A$$

where $Y \leq \mathbb{F}_p^n$ is the subgroup generated by X.

But every element of Y can be written as a sum of $|X|$ elements of X with coefficients amongst $0, 1, \ldots, p-1$, hence $|Y| \leq p^{|X|} \leq p^{K^4}$. To conclude, note that

$$|U| \leq |Y||A-A| \leq p^{K^4} \leq p^{K^4}K^2|A|,$$

where we use Plúnnecke's Inequality or even Ruzsa's triangle inequality. □

Example 1.13. Let $A = V \cup R$ where $V \leq \mathbb{F}_p^n$ is a subspace of dimension $K \ll d \ll n-K$ and R consists of $K-1$ linearly independent vectors not in V.
Then

$$|A| = |V \cup R| = |V| + |R| = p^{n/k} + K - 1 \sim p^{n/k} = |V|$$

and

$$|A+A| = |(V \cup R) + (V \cup R)| = |V \cup (V+R) \cup (R+R)| \sim K|V|.$$

But any subspace $K \le \mathbb{F}_p^n$ containing A must have size at least $p^{n/K+(K-1)} \sim |V| \cdot p^K$, so the exponential dependence on K is necessary.

Theorem 1.14 (Polynomial Freiman-Ruzsa, due to Gowers–Green–Manners–Tao 2024)**.** Assuming that:

- $A \subseteq \mathbb{F}_p^n$
- $|A+A| \le K|A|$

Then there exists a subspace $K \le \mathbb{F}_p^n$ of size at most $C_1(K)|A|$ such that for some $x \in \mathbb{F}_p^n$,

$$|A \cap (x+K)| \ge \frac{|A|}{C_2(K)},$$

where $C_1(K)$ and $C_2(K)$ are polynomial in K.

Proof. Omitted, because the techniques are not relevant to other parts of the course. See Entropy Methods in Combinatorics next term. □

Definition 1.15. Given $A, B \subseteq G$ we define the *additive energy* between A and B to be

$$E(A,B) = |\{(a,a',b,b') \in A \times A \times B \times B : a+b = a'+b'\}|.$$

We refer to the quadruples (a,a',b,b') such that $a+b=a'+b'$ as *additive quadruples.*

Example 1.16. Let $V \le \mathbb{F}_p^n$ be a subspace. Then $E(V) = E(V,V) = |V|^3$.
On the other hand, if $A \subseteq \mathbb{Z}/p\mathbb{Z}$ is chosen at random from $\mathbb{Z}/p\mathbb{Z}$ (each element chosen independently with probability $\alpha > 0$), then with high probability

$$E(A) = E(A,A) = \alpha^4 p^3 = \alpha|A|^3.$$

Lemma 1.17. Assuming that:

- $A, B \subseteq G$
- both non-empty

Then

$$E(A,B) \ge \frac{|A|^2|B|^2}{|A+B|}.$$

Proof. Define $r_{A+B}(x) = |\{(a,b) \in A \times B : a+b = x\}|$ (and notice that this is the same as $|A \cap (x-B)|$). Observe that

$$\begin{aligned} E(A,B) &= |\{(a,a',b,b') \in A^2 \times B^2 : a+b = a'+b'\}| \\ &= \sum_{x \in G} r_{A+B}(x)^2 \\ &= \sum_{x \in A+B} r_{A+B}(x)^2 \\ &\ge \frac{\left(\sum_{x \in A+B} r_{A+B}(x)\right)^2}{|A+B|} && \text{by Cauchy-Schwarz} \end{aligned}$$

but

$$\begin{aligned} \sum_{x \in G} |A \cup (x-B)| &= \sum_{x \in G} \sum_{y \in G} \mathbb{1}_A(y) \mathbb{1}_{x-B}(y) \\ &= \sum_{x \in G} \sum_{y \in G} \mathbb{1}_A(y) \mathbb{1}_B(x-y) \\ &= |A||B| \end{aligned}$$

(As usual, $\mathbb{1}_A$ here means the indicator function). □

Lecture 4

In particular, if $|A+A| \le K|A|$, then

$$E(A) = E(A,A) \ge \frac{|A|^4}{|A+A|} \ge \frac{|A|^3}{K}.$$

The converse is *not* true.

Example 1.18. Let G be your favourite (class of) abelian group(s). Then there exist constants $\theta, \eta > 0$ such that for all sufficiently large n, there exists $A \subseteq G$, with $|A| \ge n$ satisfying $E(A) \ge \eta |A|^3$ and $|A+A| \ge \theta |A|^2$.

Theorem 1.19 (Balog–Szemeredi–Gowers, Schoen)**.** Assuming that:

- $A \subseteq G$ is finite
- $E(A) \ge \eta |A|^3$ for some $\eta > 0$

Then there exists $A' \subseteq A$ of size at least $c_1(\eta)|A|$ such that $|A' + A'| \le \frac{|A'|}{c_2(\eta)}$, where $c_1(\eta)$ and $c_2(\eta)$ are polynomial in η.

Idea: Find $A' \subseteq A$ such that $\forall a, b \in A'$ such that $a-b$ has many representations as $(a_1 - a_2) + (a_3 - a_4)$ with $a_i \in A$.

We first prove a technical lemma, using a technique called "dependent random choice".

Definition 1.20 (gamma-popular differences)**.** Given $A \subseteq G$ and $\gamma > 0$, let

$$P_\gamma = \{x \in G : |A \cap (x + A)| \geq \gamma |A|\}$$

be the set of *γ-popular differences* of A.

Lemma 1.21. Assuming that:

- $A \subseteq G$ is finite
- $E(A) \geq \eta |A|^3$
- $c > 0$

Then there is a subset $X \subseteq A$ of size $|X| \geq \eta |A|/3$ such that for all but a $(16c)$-proportion of pairs $(a, b) \in X^2$, $a - b \in P_{c\eta}$.

Proof. Let $U = \{x \in G : |A \cap (x + A)| \leq \frac{1}{2}\eta |A|\}$. Then

$$\begin{aligned} \sum_{x \in U} |A \cap (x + A)|^2 &= \frac{1}{2}\eta |A| \sum_x |A \cap (x + A)| \\ &= \frac{1}{2}\eta |A|^3 \\ &= \frac{1}{2}E(A) \end{aligned}$$

For $0 \leq i \leq \lceil \log_2 \eta^{-1} \rceil$, let

$$Q_i = \left\{x \in G : \frac{|A|}{2^{i+1}} < |A \cap (x + A)| \leq \frac{|A|}{2^i}\right\},$$

and set $\delta_i = \eta^{-1}2^{-2i}$. Then

$$\begin{aligned}
\sum_i \delta_i |Q_i| &= \sum_i \frac{|Q_i|}{\eta^{2^{2i}}} \\
&= \frac{1}{\eta|A|^2} \sum_i \frac{|A|^2}{2^{2i}} |Q_i| \\
&= \frac{1}{\eta|A|^2} \sum_i \frac{|A|^2}{2^{2i}} \sum_{x \notin U} \mathbb{1}_{\left\{ \frac{|A|}{2^{i+1}} < |A \cap (x+A)| \le \frac{|A|}{2^i} \right\}} \\
&\ge \frac{1}{\eta|A|^2} \sum_{x \notin U} |A \cap (x+A)|^2 \\
&\ge \frac{1}{\eta|A|^2} \cdot \frac{1}{2} E(A) && \left(\sum_{x \in U} |A \cap (x+A)|^2 \le \frac{1}{2} E(A) \right) \\
&= \frac{1}{2}|A| && (*)
\end{aligned}$$

Let $S = \{(a,b) \in A^2 : a - b \notin P_{c\eta}\}$. Then

$$\begin{aligned}
\sum_i \sum_{(a,b) \in S} |(A-a) \cap (A-b) \cap Q_i| &\le \sum_{(a,b) \in S} \underbrace{\underbrace{|(A-a) \cap (A-b)|}_{=|A \cap (a-b+A)| \le c\eta|A|}}_{\text{by definition of } S} \\
&\le |S| \cdot c\eta|A| \\
&\le c\eta|A|^3 \\
&\le 2c\eta|A|^2 \cdot \frac{1}{2}|A| \\
&\overset{(*)}{\le} 2c\eta|A|^2 \sum_i \delta_i |Q_i|
\end{aligned}$$

Hence there exists i_0 such that

$$\sum_{(a,b) \in S} |(A-a) \cap (A-b) \cap Q_{i_0}| \le 2c\eta|A|^2 \delta_{i_0} |Q_{i_0}|.$$

Let $Q = Q_{i_0}$, $\delta = \delta_{i_0}$, $\lambda = 2^{-i_0}$. So

$$\sum_{(a,b) \in S} |(A-a) \cap (A-b) \cap Q| \le 2c\eta\delta|A|^2|Q|. \qquad (**)$$

Lecture 5 Find x such that $X = |A \cap (A+x)|$ is large.

Given $x \in G$, let $X(x) = A \cap (x+A)$. Then

$$\mathbb{E}_{x \in Q}|X(x)| = \frac{1}{|Q|} \sum_{x \in Q} |A \cap (x+A)| \ge \frac{1}{2}\lambda|A|.$$

Let $T(x) = \{(a,b) \in X(x)^2 : a - b \notin P_{c\eta}\}$. Then

$$\begin{aligned}
\mathbb{E}_{X\in Q}|T(x)| &= \mathbb{E}_{x\in Q}|\{(a,b) \in (A \cap (\underbrace{x}_{x\in A-a\cap A-b} + A))^2 : a - b \notin P_{c\eta}\}| \\
&= \frac{1}{|Q|}\sum_{x\in Q} |\{(a,b) \in S : x \in A - a \cap A - b\}| \\
&= \frac{1}{|Q|}\sum_{(a,b)\in S} |(A-a) \cap (A-b) \cap Q| \\
&\le \frac{1}{|Q|} 2c\eta|A|^2\delta|Q| \\
&= 2c\eta\delta|A|^2 \\
&= 2c\lambda^2|A|^2
\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathbb{E}_{x\in Q}|X(x)|^2 - (16c)^{-1}|T(x)| &\overset{\text{C-S}}{\le} (\mathbb{E}_{x\in Q}|X(x)|)^2 - (16c)^{-1}\mathbb{E}_{x\in Q}|T(x)| \\
&\le \left(\frac{\lambda}{2}\right)^2 |A|^2 - (16c)^{-1} 2c\lambda^2|A|^2 \\
&= \left(\frac{\lambda^2}{4} - \frac{\lambda^2}{8}\right)|A|^2 \\
&= \frac{\lambda^2}{8}|A|
\end{aligned}$$

So there exists $x \in Q$ such that $|X(x)|^2 \ge \frac{\lambda^2}{8}|A|^2$, in which case we have

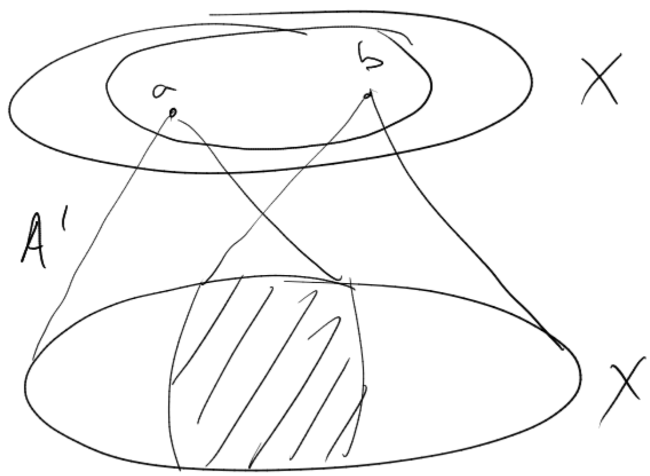
$$|X| \ge \frac{\lambda}{\sqrt{8}}|A| \ge \frac{\eta}{3}|A|$$

and $|T(x)| \le 16c|X|^2$. □

Proof of Theorem 1.19. Given $A \subseteq G$ with $E(A) \ge \eta|A|^3$, apply Lemma 1.21 with $c = 2^{-7}$ to otain $X \subseteq A$ of size $|X| \ge \frac{\eta}{3}|A|$ such that for all but $\frac{1}{8}$ of pairs $(a,b) \in X^2$, $a - b \in P_{\eta/2^7}$. In particular, the bipartite graph

$$G = (X \dot\cup X, \{(x,y) \in X \times X : x - y \in P_{\eta/2^7}\})$$

has at least $\frac{7}{8}|X|^2$ edges. Let $A' = \left\{x \in X : \deg(x) \ge \frac{3}{4}|X|\right\}$.



Clearly, $|A'| \geq \frac{|X|}{8}$. For any $a, b \in A'$, there are at least $\frac{|X|}{2}$ elements $y \in X$ such that $(a, y), (b, y) \in E(G)$ $(a - y, b - y \in P_{\eta/2^7})$.

Thus $a - b = (a - y) - (b - y)$ has at least

$$\underbrace{\frac{\eta}{6}|A|}_{\text{choices for } y} \cdot \frac{\eta}{2^7}|A| \cdot \frac{\eta}{2^7}|A| \geq \frac{\eta^3}{2^{17}}|A|^3$$

representations of the form $a_1 - a_2 - (a_3 - a_4)$ with $a_i \in A$.

It follows that

$$\begin{aligned} \frac{\eta^3}{2^{17}}|A|^3|A' - A'| &\leq |A|^4 \\ \implies |A' - A'| &\leq 2^{17}\eta^{-3}|A| \\ &\leq 2^{22}\eta^{-4}|A'| \end{aligned}$$

Thus $|A' + A'| \leq 2^{44}\eta^{-8}|A'|$. $\square$

2 Fourier-analytic techniques

In this chapter we will assume that G is *finite* abelian.

G comes equipped with a group $\hat{G}$ of characters, i.e. homomorphisms $\gamma : G \to \mathbb{C}$. In fact, $\hat{G}$ is isomorphic to G.

See Representation Theory notes for more information about characters and proofs of this as well as some of the facts below.

Example 2.1.

(i) If $G = \mathbb{F}_p^n$, then for any $\gamma \in \hat{G} = \mathbb{F}_p^n$, we have an associated character $\gamma(x) = e(\gamma \cdot x/p)$, where $e(y) = e^{2\pi i y}$.

(ii) If $G = \mathbb{Z}/N\mathbb{Z}$, then any $\gamma \in \widehat{G} = \mathbb{Z}/N\mathbb{Z}$ can be associated to a character $\gamma(x) = e(\gamma x/N)$.

Notation. Given $B \subseteq G$ nonempty, and any function $g : B \to \mathbb{C}$, let

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

Lemma 2.2. Assuming that:

- $\gamma \in \widehat{G}$

Then

$$\mathbb{E}_{x \in G} \gamma(x) = \begin{cases} 1 & \text{if } \gamma = 1 \\ 0 & \text{otherwise} \end{cases},$$

and for all $x \in G$,

$$\sum_{\gamma \in \widehat{G}} \gamma(x) = \begin{cases} |\widehat{G}| & \text{if } x = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Proof. The first equality in eqch case is trivial. Suppose $\gamma \neq 1$. Then there exists $y \in G$ with $\gamma(y) \neq 1$. Then

$$\begin{aligned} \gamma(y) \mathbb{E}_{z \in G} \gamma(z) &= \mathbb{E}_{z \in G} \gamma(y + z) \\ &= \mathbb{E}_{z' \in G} \gamma(z') \end{aligned}$$

So $\mathbb{E}_{z \in G} \gamma(z) = 0$.

For the second part, note that given $x \neq 0$, there must by $\gamma \in \widehat{G}$ such that $\gamma(x) \neq 1$, for otherwise $\widehat{G}$ would act trivially on $\langle x \rangle$, hence would also be the dual group for $G/\langle x \rangle$, a contradiction. □

Definition 2.3 (Fourier transform)**.** Given $f : G \to \mathbb{C}$, define its *Fourier transform* $\hat{f} : \widehat{G} \to \mathbb{C}$ by
$$\hat{f}(\gamma) = \mathbb{E}_{x\in G} f(x)\overline{\gamma(x)}.$$

Lecture 6

It is easy to verify the inversion formula: for all $x \in G$,
$$f(x) = \sum_{\gamma\in\widehat{G}} \widehat{f}(\gamma)\gamma(x).$$

Indeed,
$$\begin{aligned}\sum_{\gamma\in\widehat{G}} \widehat{f}(\gamma)\gamma(x) &= \sum_{\gamma\in\widehat{G}} \mathbb{E}_{y\in G} f(y)\overline{\gamma(y)}\gamma(x) \\ &= \mathbb{E}_{y\in G} f(y) \underbrace{\sum_{\gamma\in\widehat{G}} \gamma(x-y)}_{=|G| \text{ iff } x=y} \\ &= f(x) && \text{by Lemma 2.2}\end{aligned}$$

Given $A \subseteq G$, the *indicator* or *characteristic function* of A, $\mathbb{1}_A : G \to \{0,1\}$ is defined as usual.

Note that
$$\widehat{\mathbb{1}_A}(1) = \mathbb{E}_{x\in G} \mathbb{1}_A(x) 1(x) = \frac{|A|}{|G|}.$$

The *density* of A in G (often denoted by α).

Definition (Characteristic measure)**.** Given non-empty $A \subseteq G$, the *characteristic measure* $\mu_A : G \to [0,|G|]$ is defined by $\mu_A(x) = \alpha^{-1}\mathbb{1}_A(x)$.
Note that $\mathbb{E}_{x\in G}\mu_A(x) = 1 = \widehat{\mu_A}(1)$.

Definition (Balanced function)**.** The *balanced function* $f_A : G \to [-1,1]$ is given by $f_A(x) = \mathbb{1}_A(x) - \alpha$. Note that $\mathbb{E}_{x\in G} f_A(x) = 0 = \widehat{f_A}(1)$.

Example 2.4. Let $V \le \mathbb{F}_p^n$ be a subspace. Then for $t \in \widehat{\mathbb{F}_p^n}$, we have
$$\begin{aligned}\widehat{\mathbb{1}_V}(t) &= \mathbb{E}_{x\in\mathbb{F}_p^n} \mathbb{1}_V(x) e\left(-\frac{x\cdot t}{p}\right) \\ &= \frac{|V|}{p^n}\mathbb{1}_{V^\perp}(t)\end{aligned}$$
where $V^\perp = \{t \in \widehat{\mathbb{F}_p^n} : x\cdot t = 0\ \forall x \in V\}$ is the *annihilator* of V. In other words, $\widehat{\mathbb{1}_V}(t) = \mu_{V^\perp}(t)$.

Example 2.5. Let $R \subseteq G$ be such that each $x \in G$ lies in R independently with probability $\frac{1}{2}$. Then with high probability

$$\sup_{\gamma \neq 1} |\widehat{\mathbb{1}_R}(\gamma)| = O\left(\sqrt{\frac{\log |G|}{|G|}}\right).$$

This follows from *Chernoff's inequality*: Given $\mathbb{C}$-valued independent random variables $X_1, X_2, \ldots, X_n$ with mean 0, then for all $\theta > 0$, we have

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

Example 2.6. Let $Q = \{x \in \mathbb{F}_p^n : x \cdot x = 0\} \subseteq \mathbb{F}_p^n$ with $p > 2$. Then

$$\frac{|Q|}{p^n} = \frac{1}{p} + O(p^{-\frac{n}{2}})$$

and $\sup_{t \neq 0} |\widehat{\mathbb{1}_Q}(t)| = O(p^{-\frac{n}{2}})$.

Given $f, g : G \to \mathbb{C}$, we write

$$\langle f, g \rangle = \mathbb{E}_{x \in G} f(x)\overline{g(x)} \qquad \text{and} \qquad \langle \widehat{f}, \widehat{g} \rangle = \sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma)\overline{\widehat{g}(\gamma)}.$$

Consequently,

$$\|f\|_{L^2(G)}^2 = \mathbb{E}_{x \in G} |f(x)|^2 \qquad \text{and} \qquad \left\|\widehat{f}\right\|_{l^2(\widehat{G})}^2 = \sum_{\gamma \in \widehat{G}} |\widehat{f}(\gamma)|^2.$$

Lemma 2.7. Assuming that:

- $f, g : G \to \mathbb{C}$

Then

(i) $\|f\|_{L^2(G)}^2 = \left\|\widehat{f}\right\|_{l^2(\widehat{G})}^2$ (Parseval's identity)

(ii) $\langle f, g \rangle = \langle \widehat{f}, \widehat{g} \rangle$ (Plancherel's identity)

Proof. Exercise (hopefully easy). □

Definition 2.8 (Spectrum)**.** Let $1 \geq \rho > 0$ and $f : G \to \mathbb{C}$. Define the *ρ-large spectrum of f* to be

$$\mathrm{Spec}_\rho(f) = \{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geq \rho \|f\|_1\}.$$

Example 2.9. By Example 2.4, if $f = \mathbb{1}_V$ with $V \leq \mathbb{F}_p^n$, then $\forall \rho > 0$,

$$\mathrm{Spec}_\rho(\mathbb{1}_V) = \left\{ t \in \widehat{\mathbb{F}_p^n} : |\widehat{\mathbb{1}_V}(t)| \geq \rho \frac{|V|}{p^n} \right\} = V^\perp.$$

Lemma 2.10. Assuming that:

- $\rho > 0$

Then

$$|\mathrm{Spec}_\rho(f)| \leq \rho^{-2} \frac{\|f\|_2^2}{\|f\|_1^2}.$$

Proof. By Parseval's identity,

$$\begin{aligned}
\|f\|_2^2 &= \left\| \widehat{f} \right\|_2^2 \\
&= \sum_{\gamma \in \widehat{G}} |\widehat{f}(\gamma)|^2 \\
&\geq \sum_{\gamma \in \mathrm{Spec}_\rho(f)} |\widehat{f}(\gamma)|^2 \\
&\geq |\mathrm{Spec}_\rho(f)| (\rho \|f\|_1)^2
\end{aligned}$$

□

In particular, if $f = \mathbb{1}_A$ for $A \subseteq G$, then

$$\|f\|_1 = \alpha = \frac{|A|}{|G|} = \|f\|_2^2,$$

Lecture 7 so $|\mathrm{Spec}_\rho(\mathbb{1}_A)| \leq \rho^{-2}\alpha^{-1}$.

Definition 2.11 (Convolution)**.** Given $f, g : G \to \mathbb{C}$, we define their *convolution* $f * g : G \to \mathbb{C}$ by

$$f * g(x) = \mathbb{E}_{y \in G} f(y) g(x - y) \qquad \forall x \in G.$$

Example 2.12. Given $A, B \subseteq G$,

$$\mathbb{1}_A * \mathbb{1}_B(x) = \mathbb{E}_{y \in G} \mathbb{1}_A(y) \mathbb{1}_B(x-y) = \mathbb{E}_{y \in G} \mathbb{1}_A(y) \mathbb{1}_{x-B}(y) = \frac{|A \cap (x-B)|}{|G|} = \frac{1}{|G|} r_{A+B}(x).$$

In particular, $\mathrm{supp}(\mathbb{1}_A * \mathbb{1}_B) = A + B$.

Lemma 2.13. Assuming that:

- $f, g : G \to \mathbb{C}$

Then

$$\widehat{f * g}(\gamma) = \widehat{f}(\gamma)\widehat{g}(\gamma) \forall \gamma \in \widehat{G}.$$

Proof.

$$\begin{aligned}
\widehat{f * g}(\gamma) &= \mathbb{E}_{x \in G} f * g(x) \overline{\gamma(x)} \\
&= \mathbb{E}_{x \in G} \mathbb{E}_{[\in y]} G f(y) g(\underbrace{x-y}_{u}) \overline{\gamma(x)} \\
&= \mathbb{E}_{u \in G} \mathbb{E}_{[\in y]} G f(y) g(u) \overline{\gamma(u+y)} \\
&= \widehat{f}(\gamma)\widehat{g}(\gamma)
\end{aligned}$$

□

Example 2.14.

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

In particular,

$$\|\widehat{\mathbb{1}_A}\|^4_{l^4(\widehat{G})} = \frac{E(A)}{|G|^3}$$

for any $A \subseteq G$.

Theorem 2.15 (Bogolyubov's lemma)**.** Assuming that:

- $A \subseteq \mathbb{F}_p^n$ be a set of density α

Then there exists $V \le \mathbb{F}_p^n$ of codimension $\le 2\alpha^{-2}$ such that $V \subseteq A + A - A - A$.

Proof. Observe

$$2A - 2A = \mathrm{supp}(\underbrace{\mathbb{1}_A * \mathbb{1}_A * \mathbb{1}_{-A} * \mathbb{1}_{-A}}_{=:g}),$$

so wish to find $V \leq \mathbb{F}_p^n$ such that $g(x) > 0$ for all $x \in V$. Let $S = \mathrm{Spec}_\rho(\mathbb{1}_A)$ with $\rho = \sqrt{\frac{\alpha}{2}}$ and let $V = \langle S \rangle^\perp$. By Lemma 2.10, $\mathrm{codim}(V) \leq |S| \leq \rho^{-2}\alpha^{-1}$. Fix $x \in V$.

$$\begin{aligned}
g(x) &= \sum_{t \in \widehat{\mathbb{F}_p^n}} \widehat{g}(t) e(x \cdot t/p) \\
&= \sum_{t \in \widehat{\mathbb{F}_p^n}} |\widehat{\mathbb{1}_A}(t)|^4 e(x \cdot t/p) && \text{by Lemma 2.13} \\
&= \alpha^4 + \sum_{t \neq 0} |\widehat{\mathbb{1}_A}(t)|^4 e(x \cdot t/p) \\
&= \alpha^4 + \underbrace{\sum_{t \in S \setminus \{0\}} |\widehat{\mathbb{1}_A}(t)|^4 e(x \cdot t/p)}_{(1)} + \underbrace{\sum_{t \notin S} |\widehat{\mathbb{1}_A}(t)|^4 e(x \cdot t/p)}_{(2)}
\end{aligned}$$

Note $(1) \geq (\rho\alpha)^4$ since $x \cdot t = 0$ for all $t \in S$ and

$$\begin{aligned}
|(2)| &\leq \sup_{t \notin S} |\widehat{\mathbb{1}_A}(t)|^2 \sum_{t \notin S} |\widehat{\mathbb{1}_A}|^2 \\
&\leq \sup_{t \in S} |\widehat{\mathbb{1}_A}(t)|^2 \sum_{t \notin S} |\widehat{\mathbb{1}_A}|^2 \\
&\leq (\rho\alpha)^2 \|\mathbb{1}_A\|_2^2 && \text{by Parseval's identity} \\
&= \rho^2 \alpha^3
\end{aligned}$$

hence $g(x) > 0$ (in fact, $\geq \frac{\alpha^4}{2}$) for all $x \in V$ and $\mathrm{codim}(V) \leq 2\alpha^{-2}$. □

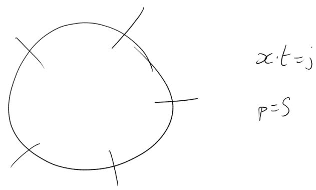
Example 2.16. The set $A = \{x \in \mathbb{F}_2^n : |x| \geq \frac{n}{2} + \frac{\sqrt{n}}{2}\}$ (where $|x|$ counts the number of 1s in x) has density $\geq \frac{1}{8}$, but there is no coset C of any subspace of codimension $\sqrt{n}$ such that $C \subseteq A + A (= A - A)$.

Lemma 2.17. Assuming that:

- $A \subseteq \mathbb{F}_p^n$ of density α
- $\rho > 0$
- $\sup_{t \neq 0} |\widehat{\mathbb{1}_A}(t)| \geq \rho\alpha$

Then there exists $V \leq \mathbb{F}_p^n$ of codimension 1 and $x \in \mathbb{F}_p^n$ such that

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



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

$$\begin{aligned}
\widehat{\mathbb{1}_A}(t) &= \widehat{f_A}(t) \\
&= \mathbb{E}_{x \in \mathbb{F}_p^n} (\mathbb{1}_A(x) - \alpha) e(-x \cdot t/p) \\
&= \mathbb{E}_{j \in [p]} \mathbb{E}_{x \in v_j + V} (\mathbb{1}_A(x) - \alpha) e(-j/p) \\
&= \mathbb{E}_{j \in [p]} \left(\underbrace{\frac{|A \cap (v_j + V)|}{|v_j + V|} - \alpha}_{= a_j} \right) e(-j/p)
\end{aligned}$$

By triangle inequality, $\mathbb{E}_{j \in [p]} |a_j| \ge \rho\alpha$. But note that $\mathbb{E}_{j \in [p]} a_j = 0$ so $\mathbb{E}_{j \in [p]} a_j + |a_j| \ge \rho\alpha$, hence there exists $j \in [p]$ such that $a_j + |a_j| \ge \rho\alpha$. Then $a_j \ge \frac{\rho\alpha}{2}$. □

Lecture 8

Notation. Given $f, g, h : G \to \mathbb{C}$, write

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

Notation. Given $A \subseteq G$, write

$$2 \cdot A = \{2a : a \in A\},$$

to be distinguished from $2A = A + A = \{a + a' : a, a' \in A\}$.

Lemma 2.18. Assuming that:

- $p \ge 3$ prime
- $A \subseteq \mathbb{F}_p^n$ of density $\alpha > 0$
- $\sup_{t \neq 0} |\widehat{\mathbb{1}_A}(t)| \le \varepsilon$

Then the number of 3-term arithmetic progressions in A differs from $\alpha^3 (p^n)^2$ by at most $\varepsilon (p^n)^2$.

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

$$\begin{aligned}
T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) &= \mathbb{E}_{x,d\in\mathbb{F}_p^n} \mathbb{1}_A(x)\mathbb{1}_(x+d)\mathbb{1}_A(x+2d) \\
&= \mathbb{E}_{x,y\in\mathbb{F}_p^n} \mathbb{1}_A(x)\mathbb{1}_A(y)\mathbb{1}_A(2y-x) \\
&= \mathbb{E}_{y\in G}\mathbb{1}_A(y)\mathbb{E}_{x\in G}\mathbb{1}_A(x)\mathbb{1}_A(2y-x) \\
&= \mathbb{E}_{y\in G}\mathbb{1}_A(y)\mathbb{1}_A * \mathbb{1}_A(2y) \\
&= \langle \mathbb{1}_{2\cdot A}, \mathbb{1}_A * \mathbb{1}_A \rangle
\end{aligned}$$

By Plancherel's identity and Lemma 2.13, we have

$$\begin{aligned}
&= \langle \widehat{\mathbb{1}_{2\cdot A}}, \widehat{\mathbb{1}_A}^2 \rangle \\
&= \sum_t \widehat{\mathbb{1}_{2\cdot A}}(t)\overline{\widehat{\mathbb{1}_A}(t)^2} \\
&= \alpha^3 + \sum_{t\neq 0} \widehat{\mathbb{1}_{2\cdot A}}(t)\overline{\widehat{\mathbb{1}_A}(t)^2}
\end{aligned}$$

but

$$\begin{aligned}
\left| \sum_{t\neq 0} \widehat{\mathbb{1}_{2\cdot A}}(t)\widehat{\mathbb{1}_A}(t)^2 \right| &\le \sup_{t\neq 0} |\widehat{\mathbb{1}_A}(t)| \sum_{t\neq 0} |\widehat{\mathbb{1}_{2\cdot A}}(t)||\widehat{\mathbb{1}_A}(t)| \\
&\overset{\text{CS}}{\le} \sup_{t\neq 0} |\widehat{\mathbb{1}_A}(t)| \left(\sum_t |\widehat{\mathbb{1}_{2\cdot A}}(t)|^2 \sum_t |\widehat{\mathbb{1}_A}(t)|^2 \right)^{\frac{1}{2}} \\
&\le \varepsilon \|\widehat{\mathbb{1}_{2\cdot A}}\|_2 \|\widehat{\mathbb{1}_A}\|_2 \\
&= \varepsilon \cdot \alpha
\end{aligned}$$

by Parseval's identity. □

Theorem 2.19 (Meshulam's Theorem)**.** Assuming that:

- $A \subseteq \mathbb{F}_p^n$ a set containing no non-trivial 3 term arithmetic progressions

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

Proof. By assumption,

$$T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) = \frac{|A|}{(p^n)^2} = \frac{\alpha}{p^n}.$$

But as in (the proof of) Lemma 2.18,

$$|T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) - \alpha^3| \le \sup_{t\neq 0} |\widehat{\mathbb{1}_A}(t)| \cdot \alpha,$$

so provided $p^n \geq 2\alpha^{-2}$, i.e. $T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) \leq \frac{\alpha^3}{2}$ we have $\sup_{t \neq 0} |\widehat{\mathbb{1}_A}(t)| \geq \frac{\alpha^2}{2}$.

So by Lemma 2.17 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 $A_0 = A$, $V_0 = \mathbb{F}_p^n$, $\alpha_0 = \frac{|A_0|}{|V_0|}$. At the i-th step, we are given a set $A_{i-1} \subseteq V_{i-1}$ of density α_{i-1} with no non-trivial 3 term arithmetic progressions. Provided that $p^{\dim(V_{i-1})} \geq 2\alpha_{i-1}^{-2}$, there exists $V_i \leq V_{i-1}$ of codimension 1, $x_i \in V_{i-1}$ such that

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

Set $A_i = (A - x_i) \cap V_i \subseteq V_i$, has density $\geq \alpha_{i-1} + \frac{(\alpha_{i-1})^2}{4}$, and is free of non-trivial 3 term arithmetic progressions.

Through this iteration, the density increases from α to 2α in at most $\frac{\alpha}{\left(\frac{\alpha^2}{4}\right)} = 4 \cdot \alpha^{-1}$ steps.

2α to 4α in at most $\frac{2\alpha}{\left(\frac{(2\alpha)^2}{4}\right)} = 2\alpha^{-1}$ steps and so on.

So reaches 1 in at most

$$4\alpha^{-1} \left(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots\right) \leq 8\alpha^{-1}$$

steps. The argument must end with $\dim(V_i) \geq n - 8\alpha^{-1}$, at which point we must have had $p^{\dim(V_i)} < 2\alpha_{i-1}^2 \leq 2\alpha^{-2}$, or else we could have continued.

But we may assume that $\alpha \geq \sqrt{2} p^{-\frac{n}{4}}$ (or $\alpha^{-2} < 2p^{\frac{n}{2}}$) whence $p^{n - 8\alpha^{-1}} \leq p^{\frac{n}{2}}$, or $\frac{n}{2} \leq 2\alpha^{-1}$. $\square$

At the time of writing, the largest known subset of $\mathbb{F}_3^n$ containing no non-trivial 3 term arithmetic progressions has size $(2.2202)^n$.

We will prove an upper bound of the form $(2.756)^n$.

Theorem 2.20 (Roth's theorem)**.** Assuming that:

- $A \subseteq [N] = \{1, \ldots, N\}$
- A contains no non-trivial 3 term arithmetic progressions

Then $|A| = O\left(\frac{N}{\log \log N}\right)$.

Lecture 9

Example 2.21 (Behrend's example)**.** There exists $A \subseteq [N]$ of size at least $|A| \geq \exp(-c\sqrt{\log N})N$ containing no non-trivial 3 term arithmetic progressions.

Lemma 2.22. Assuming that:

- $A \subseteq [N]$ of density $\alpha > 0$
- $N > 50\alpha^{-2}$
- A contains no non-trivial 3 term arithmetic progressions
- p a prime in $\left[\frac{N}{3}, \frac{2N}{3}\right]$
- let $A' = A \cap [p] \subseteq \mathbb{Z}/p\mathbb{Z}$

Then one of the following holds:

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

(ii) There exists an interval $J \subseteq [N]$ of length $\ge \frac{N}{3}$ such that $|A \cap J| \ge \alpha\left(1 + \frac{\alpha}{400}\right)|J|$

Proof. We may assume that $|A'| = |A \cap [p]| \ge \alpha\left(1 - \frac{\alpha}{200}\right)p$ since otherwise

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

so we would be in Case (ii) with $J = [p+1, N]$. Let $A'' = A' \cap \left[\frac{p}{3}, \frac{2p}{3}\right]$. Note that all 3 term arithmetic progressions of the form $(x, x+d, x+2d) \in A' \times A'' \times A''$ are in fact arithmetic progressions in $[N]$.

If $|A' \cap \left[\frac{p}{3}\right]|$ or $|A' \cap \left[\frac{2p}{3}, p\right]|$ were at least $\frac{2}{5}|A'|$, we would again be in case (ii). So we may assume that $|A''| \ge \frac{|A'|}{5}$.

Now as in Lemma 2.18 and Theorem 2.19,

$$\frac{\alpha''}{p} = \frac{|A''|}{p^2}$$

$$\begin{aligned} &T_3(\mathbb{1}_{A'}, \mathbb{1}_{A''}, \mathbb{1}_{A''}) \\ &\qquad = \alpha'(\alpha'')^2 + \sum_t \overline{\widehat{\mathbb{1}_{A'}}(t)\widehat{\mathbb{1}_{A''}}(t)}\widehat{\mathbb{1}_{2 \cdot A''}}(t) \end{aligned}$$

where $\alpha' = \frac{|A'|}{p}$ and $\alpha'' = \frac{|A''|}{p}$. So as before,

$$\frac{\alpha'\alpha''}{2} \le \sup_{t \neq 0} |\mathbb{1}_{A'}(t)| \cdot \alpha'',$$

provided that $\frac{\alpha''}{p} \le \frac{1}{2}\alpha'(\alpha'')^2$, i.e. $\frac{2}{p} \le \alpha'\alpha''$. (Check this is satisfied).

Hence

$$\sup_{t\neq 0}|\widehat{\mathbb{1}_{A'}}(t)| \ge \frac{\alpha'\alpha''}{2} \ge \frac{1}{2}\left(\alpha\left(1-\frac{\alpha}{200}\right)\right)^2 \cdot \frac{2}{5} \ge \frac{\alpha^2}{10}.$$

□

Lemma 2.23. Assuming that:

- $m \in \mathbb{N}$
- $\varphi : [m] \to \mathbb{Z}/p\mathbb{Z}$ be given by $x \mapsto tx$ for some $t \neq 0$
- $\varepsilon > 0$

Then there exists a partition of $[m]$ into progressions P_i of length $l_i \in \left[\frac{\varepsilon\sqrt{m}}{2}, \varepsilon\sqrt{m}\right]$ such that

$$\operatorname{diam}(\varphi(P_i)) = \max_{x,y\in P_i} |\varphi(x) - \varphi(y)| \le \varepsilon p$$

for all i.

Proof. Let $u = \lfloor\sqrt{m}\rfloor$ and consider $0, t, 2t, \dots, ut$. By Pigeonhole, there exists $0 \le v < w \le u$such that $|wt - vt| = |(w-v)t| \le \frac{p}{u}$. Set $s = w - v$, so $|st| \le \frac{p}{u}$. Divide $[m]$ into residue classes modulo s, each of which has size at least $\frac{m}{s} \ge \frac{m}{4}$. But each residue class can be divided into arithmetic progressions of the form $a, a+s, \dots, a+ds$ with $\varepsilon\frac{u}{2} < d \le \varepsilon u$. The diameter of the image of each progression under φ is $|dst| \le d\frac{p}{u} \le \varepsilon u \frac{p}{u} = \varepsilon p$. □

Lemma 2.24. Assuming that:

- $A \subseteq [N]$ of density $\alpha > 0$
- p a prime in $\left[\frac{N}{3}, \frac{2N}{3}\right]$
- let $A' = A \cap [p] \subseteq \mathbb{Z}/p\mathbb{Z}$
- $|\widehat{\mathbb{1}_{A'}}(t)| \ge \frac{\alpha^2}{20}$ for some $t \neq 0$

Then there exists a progression $P \subseteq [N]$ of length at least $\alpha^2\frac{\sqrt{N}}{500}$ such that $|A \cap P| \ge \alpha\left(1 + \frac{\alpha}{80}\right)|P|$.

Lecture 10

Proof. Let $\varepsilon = \frac{\alpha^2}{40\pi}$, and use Lemma 2.23 to partition $[p]$ into progressions P_i of length

$$\ge \varepsilon\sqrt{\frac{p}{2}} \ge \frac{\alpha^2}{40\pi}\frac{\sqrt{\frac{N}{3}}}{2} \ge \frac{\alpha^2\sqrt{N}}{500}$$

and $\operatorname{diam}(\varphi(P_i)) \le \varepsilon p$. Fix one x_i from each of the P_i. Then

$$\begin{aligned}
\frac{\alpha^2}{20} &\le |\widehat{f_{A'}}(t)| \\
&= \left| \frac{1}{p} \sum_i \sum_{x \in P_i} f_{A'}(x) e(-xt/p) \right| \\
&= \frac{1}{p} \left| \sum_i \sum_{x \in P_i} f_{A'}(x) e(-x_i t/p) + \sum_i \sum_{x \in P_i} f_{A'}(x)(e(-xt/p) - e(-x_i t/p)) \right| \\
&\le \frac{1}{p} \sum_i \left| \sum_{x \in P_i} f_{A'}(x) \right| + \frac{1}{p} \sum_i \sum_{x \in P_i} |f_{A'}(x)| \underbrace{|e(-xt/p) - e(-x_i t/p)|}_{\substack{\le 2\pi\varepsilon \\ \text{since } |t(x - x_i)| \le \varepsilon p}}
\end{aligned}$$

So

$$\sum_i \left| \sum_{x \in P_i} f_{A'}(x) \right| \ge \frac{\alpha^2}{40} p.$$

Since $f_{A'}$ has mean zero,

$$\sum_i \left(\left| \sum_{x \in P_i} f_{A'}(x) \right| + \sum_{x \in P_i} f_{A'}(x) \right) \ge \frac{\alpha^2}{40} p,$$

hence there exists i such that

$$\left| \sum_{x \in P_i} f_{A'}(x) \right| + \sum_{x \in P_i} f_{A'}(x) \ge \frac{\alpha^2}{80} |P_i|$$

and so

$$\sum_{x \in P_i} f_{A'}(x) \ge \frac{\alpha^2}{160} |P_i|. \qquad \square$$

Definition 2.25 (Bohr set)**.** Let $\Gamma \subseteq \widehat{G}$ and $\rho > 0$. By the *Bohr set* $B(\Gamma, \rho)$ we mean the set

$$B(\Gamma, \rho) = \{x \in G : |\gamma(x) - 1| < \rho \ \forall \gamma \in \Gamma\}.$$

We call $|\Gamma|$ the *rank* of $B(\Gamma, \rho)$, and ρ its *width* or *radius*.

Example 2.26. When $G = \mathbb{F}_p^n$, then $B(\Gamma, \rho) = \langle \Gamma \rangle^\perp$ for all sufficiently small ρ.

Lemma 2.27. Assuming that:

- $\Gamma \subseteq \widehat{G}$ of size d
- $\rho > 0$

Then

$$|B(\Gamma,\rho)| \geq \left(\frac{\rho}{8}\right)^d |G|.$$

Proposition 2.28 (Bogolyubov in a general finite abelian group)**.** Assuming that:

- $A \subseteq G$ of density $\alpha > 0$

Then there exists $\Gamma \subseteq \widehat{G}$ of size at most $2\alpha^{-2}$ such that $A + A - A - A \supseteq B(\Gamma, \rho)$.

Proof. Recall $\mathbb{1}_A * \mathbb{1}_A * \mathbb{1}_{-A} * \mathbb{1}_{-A}(x) = \sum_{\gamma \in \widehat{G}} |\widehat{\mathbb{1}_A}(\gamma)|^4 \gamma(x)$.

Let $\Gamma \in \mathrm{Spec}_{\sqrt{\frac{\alpha}{2}}}(\mathbb{1}_A)$, and note that, for $x \in B\left(\Gamma, \frac{1}{2}\right)$ and $\gamma \in \Gamma$, $\mathrm{Re}(\gamma(x)) > 0$. Hence, for $x \in B\left(\Gamma, \frac{1}{2}\right)$,

$$\mathrm{Re} \sum_{\gamma \in \widehat{G}} |\widehat{\mathbb{1}_A}(\gamma)|^4 \gamma(x) = \underbrace{\mathrm{Re} \sum_{\gamma \in \Gamma} |\widehat{\mathbb{1}_A}(\gamma)|^4 \gamma(x)}_{\geq \alpha^4} + \mathrm{Re} \sum_{\gamma \notin \Gamma} |\widehat{\mathbb{1}_A}(\gamma)|^4 \gamma(x)$$

and

$$\left| \mathrm{Re} \sum_{\gamma \notin \Gamma} |\widehat{\mathbb{1}_A}(\gamma)|^4 \gamma(x) \right| \leq \sup_{\gamma \notin \Gamma} |\widehat{\mathbb{1}_A}(\gamma)|^2 \sum_{\gamma \notin \Gamma} |\widehat{\mathbb{1}_A}(\gamma)|^2 \leq \left(\sqrt{\frac{\alpha}{2}} \cdot \alpha\right)^2 \cdot \alpha = \frac{\alpha^4}{2}.$$

□

3 Probabilistic Tools

All probability spaces in this course will be finite.

Theorem 3.1 (Khintchine's inequality)**.** Assuming that:

- $p \in [2, \infty)$
- $X_1, X_2, \dots, X_n$ independent random variables
- $\mathbb{P}(X_i = x_i) = \frac{1}{2} = \mathbb{P}(X_i = -x_i)$

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

Proof. By nesting of norms, it suffices to prove the case $p = 2k$ for some $k \in \mathbb{N}$. Write $X = \sum_{i=1}^n X_i$, and assume $\sum_{i=1}^n \|X_i\|_{L^\infty(\mathbb{P})}^2 = 1$. Note that in fact $\sum_{i=1}^n \|X_i\|_{L^2(\mathbb{P})}^2 = \sum_{i=1}^n \|X_i\|_{L^\infty(\mathbb{P})}^2$, hence
Lecture 11 $\sum_{i=1}^n \|X_i\|_{L^2(\mathbb{P})}^2 = 1$.

By Chernoff's inequality (Example 2.5), for all $\theta > 0$ we have
$$\mathbb{P}(|X| \ge \theta) \le 4 \exp\left(-\frac{\theta^2}{4} \right),$$
and so using the fact that $\mathbb{P}(|X| \le t) = \int_0^t \rho_X(s) \mathrm{d}s$ we have
$$\begin{aligned} \|X\|_{L^{2k}(\mathbb{P})}^{2k} &= \int_0^\infty t^{2k} \rho_X(t) \mathrm{d}t \\ &= \int_0^\infty 2kt^{2k-1} \mathbb{P}(|X| \ge t) \mathrm{d}t && \text{integration by parts} \\ &\le \underbrace{\int_0^\infty 8kt^{2k-1} \exp\left(-\frac{t^2}{4} \right) \mathrm{d}t}_{=: I(K)} \end{aligned}$$

We shall show by induction on k that $I(K) \le 2^{2k} \frac{(2k)^k}{4k}$. Indeed, when $k = 1$,
$$\int_0^\infty t \exp\left(-\frac{t^2}{4} \right) \mathrm{d}t = \left[-2 \exp\left(-\frac{t^2}{4} \right) \right]_0^\infty = 2 \le 2.$$

For $k > 1$, integrate by parts to find that

$$\begin{aligned}
I(K) &= \int_0^\infty \underbrace{t^{2k-2}}_{u} \cdot \underbrace{t\exp\left(-\frac{t^2}{4}\right)}_{v} \mathrm{d}t \\
&= \left[t^{2k-2} \cdot \left(-2\exp\left(-\frac{t^2}{4}\right)\right)\right]_0^\infty - \int_0^\infty (2k-2)t^{2k-3}\left(-2\exp\left(-\frac{t^2}{4}\right)\right) \mathrm{d}t \\
&= 4(k-1)\int_0^\infty t^{2(k-1)-1}\exp\left(-\frac{t^2}{4}\right) \mathrm{d}t \\
&= 4(k-1)I(K-1) \\
&\leq 4(k-1)2^{2(k-1)}\frac{(2(k-1))^{k-1}}{4(k-1)} \\
&\leq 2^{2k}\frac{(2k)^k}{4k}
\end{aligned}$$

□

Corollary 3.2 (Rudin's Inequality)**.** Let $F \subseteq \widehat{\mathbb{F}_2^n}$ be a linearly independent set and let $p \in [2, \infty)$. Then $\widehat{f} \in l^2(\Gamma)$,

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

Corollary 3.3. Let $\Gamma \subseteq \widehat{\mathbb{F}_2^n}$ be a linearly independent set and let $p \in (1, 2]$. Then for all $f \in L^p(\mathbb{F}_2^n)$,

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

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

$$\begin{aligned}
\|\widehat{f}\|_{l^2(\Gamma)}^2 &= \sum_{\gamma\in\Gamma} |\widehat{f}(\gamma)|^2 \\
&= \langle \widehat{f}, \widehat{g} \rangle_{l^2(\widehat{\mathbb{F}_2^n})} \\
&= \langle f, g \rangle_{L^2(\mathbb{F}_2^n)} && \text{by Plancherel's identity}
\end{aligned}$$

which is bounded above by $\|f\|_{L^p(\mathbb{F}_2^n)}\|g\|_{L^{p'}(\mathbb{F}_2^n)}$ where $\frac{1}{p} + \frac{1}{p'} = 1$, using Hölder's inequality.

By Rudin's inequality,

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

□

Recall that given $A \subseteq \mathbb{F}_2^n$ of density $\alpha > 0$, we had $|\operatorname{Spec}_\rho(\mathbb{1}_A) \le \rho^{-2}\alpha^{-1}$. This is best possible as the example of a subspace shows. However, in this case the large spectrum is highly structured.

Theorem 3.4 (Special case of Chang's Theorem)**.** Assuming that:

- $A \subseteq \mathbb{F}_2^n$ of density $\alpha > 0$
- $\rho > 0$

Then there exists $H \le \widehat{\mathbb{F}_2^n}$ of dimension $O(\rho^{-2}\log\alpha^{-1})$ such that $H \supseteq \operatorname{Spec}_\rho(\mathbb{1}_A)$.

Proof. Let $\Gamma \subseteq \operatorname{Spec}_\rho(\mathbb{1}_A)$ be a maximal linearly independent set. Let $H = \langle \operatorname{Spec}_\rho(\mathbb{1}_A)\rangle$. Clearly $\dim(H) = |\Gamma|$. By Corollary 3.3, for all $p \in (1, 2]$,

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

so

$$|\Gamma| = O\left(\rho^{-2}\alpha^{-2}\alpha^{2/p}\frac{p}{p-1}\right).$$

Set $p = 1 + (\log\alpha^{-1})^{-1}$ to get $|\Gamma| = O(\rho^{-2}\alpha^{-2}(\alpha^2 \cdot e^2)(\log\alpha^{-1} + 1))$. □

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

Lecture 12 Clearly, if $G = \mathbb{F}_2^n$, then $S \subseteq G$ is dissociated if and only if it is linearly independent.

Theorem 3.6 (Chang's Theorem)**.** Assuming that:

- G a finite abelian group
- $A \subseteq G$ be of density $\alpha > 0$
- $\Lambda \supseteq \operatorname{Spec}_\rho(\mathbb{1}_A)$ 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)**.** Assuming that:

- $p \in [2, \infty)$
- $X_1, X_2, \dots, X_n \in {}^p(\mathbb{P})$ independent random variables
- $\mathbb{E}\sum_{i=1}^n X_i = 0$

Then

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

Proof. First 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 $\Omega_1, \Omega_2, \ldots, \Omega_M$, write $\mathbb{P}_j$ for the induced measure on Ω_j such that all X_i's are symmetric and take at most 2 values. By Khintchine's inequality, for each $j \in [M]$,

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

so summing over all j and taking p-th roots gives the symmetric case. Now suppose the X_i's are arbitrary, and let $Y_1, \ldots, Y_n$ be such that $Y_i \sim X_i$ and $X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots, Y_n$ are all independent. Applying the symmetric case to $X_i - Y_i$,

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

But then

$$\begin{aligned}\left\|\sum_{i=1}^{n} X_i\right\|_{L^p(\mathbb{P})} = \left\|\sum_{i=1}^{n} X_i - \underbrace{\mathbb{E}^Y\sum_{i=1}^{n} Y_i}_{=0}\right\|_{L^p(\mathbb{P})}^{p} &\\ &= \mathbb{E}^X\left|\sum X_i - \mathbb{E}^Y\sum Y_i\right|^p\\ &= \mathbb{E}^X\left|\mathbb{E}^Y\sum(X_i - Y_i)\right|^p\\ &\le \mathbb{E}^X\mathbb{E}^Y\left|\sum(X_i - Y_i)\right|^p \qquad \text{by Jensen say}\\ &= \left\|\sum(X_i - Y_i)\right\|_{L^p(\mathbb{P}\times\mathbb{P})}^p\end{aligned}$$

concluding the proof. ∎

Theorem 3.8 (Croot-Sisask almost periodicity)**.** Assuming that:

- G a finite abelian group
- $\varepsilon > 0$
- $p \in [2, \infty)$
- $A, B \subseteq G$ are such that $|A + B| \le K|A|$
- $f : G \to \mathbb{C}$

Then there exists $b \in B$ and a set $X \subseteq B - b$ such that $|X| \ge 2^{-1}K^{-O(\varepsilon^{-2}p)}|B|$ and

$$\|\tau_x f * \mu_A - f * \mu_A\|_{L^p(G)} \le \varepsilon \|f\|_{L^p(G)} \qquad \forall x \in X,$$

where $\tau_x g(y) = g(y + x)$ for all $y \in G$, and as a reminder, μ_A is the characteristic measure of A.

Proof. The main idea is to approximate

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

by $\frac{1}{m}\sum_{i=1}^m f(y - z_i)$, where z_i are sampled independently and uniformly from A, and m is to be chosen later.

For each $y \in G$, define $Z_i(y) = \tau_{-zi} f(y) - f * \mu_A(y)$. For each $y \in G$, these are independent random variables with mean 0, so by Marcinkiewicz-Zygmund,

$$\begin{aligned}
\left\|\sum_{i=1}^m Z_i(y)\right\|_{L^p(\mathbb{P})}^p &= O\left(p^{p/2}\left\|\sum_{i=1}^m |Z_i(y)|^2\right\|_{L^{p/2}(\mathbb{P})}^{p/2}\right) \\
&= O\left(p^{p/2}\mathbb{E}_{(z_1,\dots,z_m)\in A^m}\left|\sum_{i=1}^m |Z_i(y)|^2\right|^{p/2}\right)
\end{aligned}$$

By Hölder with $\frac{1}{p'} + \frac{2}{p} = 1$, we get

$$\begin{aligned}
\left|\sum_{i=1}^m |Z_i(y)|^2\right|^{p/2} &\le \left(\sum_{i=1}^m 1^{p'}\right)^{\frac{1}{p'}\cdot\frac{p}{2}} \left(\sum_{i=1}^m |Z_i(y)|^{2\cdot p/2}\right)^{\frac{2}{p}\cdot\frac{p}{2}} \\
&\le \left(\sum_{i=1}^m 1^{p'}\right)^{\frac{p}{2}-1} \left(\sum_{i=1}^m |Z_i(y)|^{2\cdot p/2}\right)^{\frac{2}{p}\cdot\frac{p}{2}} \\
&= m^{p/2-1}\sum_{i=1}^m |Z_i(y)|^p
\end{aligned}$$

so

$$\left\|\sum_{i=1}^m Z_i(y)\right\|_{L^p(\mathbb{P})}^p = O\left(p^{p/2}m^{p/2-1}\mathbb{E}_{(z_1,\dots,z_m)\in A^m}\sum_{i=1}^m |Z_i(y)|^p\right).$$

Summing over all $y \in G$, we have

$$\mathbb{E}_{y\in G}\left\|\sum_{i=1}^m Z_i(y)\right\|_{L^p(\mathbb{P})}^p = O\left(p^{p/2}m^{p/2-1}\mathbb{E}_{(z_1,\dots,z_m)\in A^m}\sum_{i=1}^m \mathbb{E}_{y\in G}|Z_i(y)|^p\right)$$

with

$$\begin{aligned}(\mathbb{E}_{y\in G}|Z_i(y)|^p)^{\frac{1}{p}} &= \|Z_i\|_{L^p(G)} \\ &= \|\tau_{-z_i}f - f * \mu_A\|_{L^p(G)} \\ &\le, \|\tau_{-z_i}f\|_{L^p(G)} + \|f * \mu_A\|_{L^p(G)} \\ &\le \|f\|_{L^p(G)} + \|f\|_{L^q(G)}\|\mu_A\|_{L^1(G)} \\ &\le 2\|f\|_{L^p(G)}\end{aligned}$$

Lecture 13 by Young / Hölder ($\|f * g\|_{L^r(G)} \le \|f\|_{L^p(G)}\|g\|_{L^q(G)}$ where $1 + \frac{1}{r} = \frac{1}{p} + \frac{1}{q}$).

So we have

$$\mathbb{E}_{(z_1,\dots,z_m)\in A^m}\mathbb{E}_{y\in G}\left|\sum_{i=1}^m Z_i(y)\right|^p = O\left(p^{p/2}m^{p/2-1}\sum_{i=1}^m (2\|f\|_{L^p(G)})^p\right) = O((4p)^{p/2}m^{p/2}\|f\|_{L^p(G)}^p).$$

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

$$\mathbb{E}_{(z_1,\dots,z_m)\in A^m}\underbrace{\mathbb{E}_{y\in G}\left|\frac{1}{m}\sum_{i=1}^m \tau_{-zi}f(y) - f * \mu_A(y)\right|^p}_{=(*)} = O((4p)^{p/2}m^{p/2}\|f\|_{L^p(G)}^p) = \left(\frac{\varepsilon}{4}\|f\|_{L^p(G)}\right)^p.$$

Write

$$L = \left\{z = (z_1, \dots, z_m) \in A^m : (*) \le \left(\frac{\varepsilon}{2}\|f\|_{L^p(G)}\right)^p\right\}.$$

By Markov inequality, since

$$\mathbb{E}(*) \le \left(\frac{\varepsilon}{4}\|f\|_{L^p(G)}\right)^p = 2^{-p}\left(\frac{\varepsilon}{2}\|f\|_{L^p(G)}\right)^p,$$

we have

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

so $|L| \ge \left(1 - \frac{1}{2^p}\right)|A|^m \ge \frac{1}{2}|A|^m$. Let

$$D = \{\underbrace{(b, b, \dots, b)}_{m} : b \in B\}.$$

Now $L + D \subseteq (A + B)^m$, whence

$$|L + D| \le |A + B|^m \le K^m|A|^m \le 2K^m|L|.$$

By Lemma 1.17,

$$E(L, D) \geq \frac{|L|^2|D|^2}{|L + D|} \geq \frac{1}{2}K^{-m}|D|^2|L|$$

so there are at least $\frac{|D|^2}{2K^m}$ pairs $(d_1, d_2) \in D \times D$ such that $r_{L-L}(d_2 - d_1) > 0$. In particular, there exists $b \in ub$ and $X \subseteq B - b$ of size $|X| \geq \frac{|D|}{2K^m} = \frac{|B|}{2K^m}$ such that for all $x \in X$, there exists $l_2(x) \in L$ such that for all $i \in [m]$, $l_1(x)_i - l_2(x)_i = x$. But then for each $x \in X$, by the triangle inequality,

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

by definion of L. □

Theorem 3.9 (Bogolyubov again, after Sanders)**.** Assuming that:

- $A \subseteq \mathbb{F}_p^n$ of density $\alpha > 0$

Then there exists a subspace $V \leq \mathbb{F}_p^n$ of codimension $O(\log^4 \alpha^{-1})$ such tht $V \subseteq A + A - A - A$.

Almost periodicity is also a key ingredient in recent work of Kelley and Meka, showing that any $A \subseteq [N]$ containing no non-trivial 3 term arithmetic progressions has size $|A| \leq \exp(-C \log^{\frac{1}{11}} N)N$.

4 Further Topics

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

Theorem 4.1 (Ellenberg-Gijswijt, following Croot-Lev-Pach)**.** Assuming that:

- $A \subseteq \mathbb{F}_3^n$ contains no non-trivial 3 term arithmetic progressions

Then $|A| = o(2.756)^n$.

Notation. Let M_n be the set of monomials in $x_1, \dots, x_2$ whose degree in each variable is at most 2. Let V_n be the vector space over $\mathbb{F}_3$ whose basis is 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 $m_d = \dim(V_n^d) = |M_n^d|$.

Lemma 4.2. Assuming that:

- $A \subseteq \mathbb{F}_3^n$
- $P \in V_n^d$ is a polynomial
- $P(a + a') = 0$ for all $a \neq a' \in A$

Then
$$|\{a \in A : P(2a) \neq 0\}| \le 2m_{d/2}.$$

Lecture 14

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

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

for some coefficients $c_{m,m'}$. Clearly at least one of m, m' must have degree $\le \frac{d}{2}$, whence

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

for some families of polynomials $(F_m)_{m \in M_n^{d/2}}$, $(G_{m'})_{m' \in M_n^{d/2}}$.

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

Proposition 4.3. Assuming that:

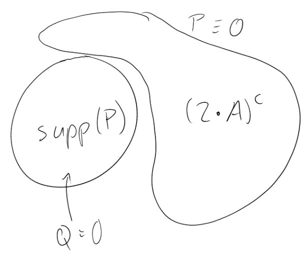
- $A \subseteq \mathbb{F}_3^n$ a set containing no non-trivial 3 term arithmetic progressions

Then $|A| \leq 3m_{2n/3}$.

Proof. Let $d \in [0, 2n]$ be an integer to be determined later. Let W be the space of polynomials in V_n^d that vanish on $(2 \cdot A)^c$. We have

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

We claim that there exists $P \in W$ such that $|\operatorname{supp}(P)| \geq \dim(W)$. Indeed, pick $P \in W$ with maximal support. If $|\operatorname{supp}(P)| < \dim(W)$, then there would be a non-zero polynomial $Q \in W$ vanishing on $\operatorname{supp}(P)$, in which case $\operatorname{supp}(P + Q) \supsetneq \operatorname{supp}(P)$, contradicting the choice of P.



Now by assumption,

$$\{a + a' : a \neq a' \in A\} \cap 2 \cdot A = \emptyset.$$

So any polynomial that vanishes on $(2 \cdot A)^c$ vanishes on $\{a + a' : a \neq a' \in A\}$. By Lemma 4.2 we now have that,

$$\begin{aligned} |A| - (3^n - m_d) &= m_d - (3^n - |A|) \\ &\leq \dim(W) \\ &\leq |\operatorname{supp}(P)| \\ &= |\{x \in \mathbb{F}_3^n : P(x) \neq 0\}| \\ &= |\{a \in A : P(2a) \neq 0\}| \\ &\leq 2m_{d/2} \end{aligned}$$

Hence $|A| \geq 3^n - m_d + 2m_{d/2}$. But the monomials in $M_n \setminus M_n^d$ are in bijection with the ones in M_{2n-d} via $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mapsto x_1^{2-\alpha_1} \cdots x_n^{2-\alpha_n}$, whence $3^n - m_d = m_{2n-d}$. Thus setting $d = \frac{4n}{3}$, we have $|A| \leq m_{2n/3} + 2m_{2n/3} = 3m_{2n/3}$. □

You will prove Theorem 4.1 on Example Sheet 3.

We do not have at present a comparable bound for 4 term arithmetic progressions. Fourier techniques also fail.

Example 4.4. Recall from Lemma 2.18 that given $A \subseteq G$,

$$|T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) - \alpha^3| \ge \sup_{\gamma \neq 1} |\widehat{\mathbb{1}_A}(\gamma)|.$$

But it is impossible to bound

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

by $\sup_{\gamma \neq 1} |\widehat{\mathbb{1}_A}(\gamma)|$. Indeed, consider $Q = \{x \in \mathbb{F}_p^n : x \cdot x = 0\}$. By Problem 11(ii) on Sheet 1,

$$\frac{|Q|}{p^n} = \frac{1}{p} + O(p^{-n/2})$$

and

$$\sup_{t \neq 0} |\widehat{\mathbb{1}_Q}(t)| = O(p^{-n/2}).$$

But given a 3 term arithmetic progression $x, x+d, x+2d \in Q$, by the identity

$$x^2 - 3(x+d)^2 + 3(x+2d)^2 - (x+3d)^2 = 0 \qquad \forall x, d,$$

$x + 3d$ automatically lies in Q, so

$$T_4(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) = T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) = \left(\frac{1}{p}\right)^3 + O(p^{-n/2})$$

which is not close to $\left(\frac{1}{p}\right)^4$.

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

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

Problem 1(i) on Sheet 2 showed that $\|f\|_{U^2(G)} = \|\widehat{f}\|_{l^4(\widehat{G})}$, so this is indeed a norm.

Problem 1(ii) asserted the following:

Lemma 4.6. Assuming that:

- $f_1, f_2, f_3 : G \to \mathbb{C}$

Then

$$|T_3(f_1, f_2, f_3)| \le \min_{i \in [3]} \|f_i\|_{U^2(G)} \cdot \prod_{j \neq i} \|f_j\|_{L^\infty(G)}.$$

Note that

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

and thus by Parseval's identity,

$$\|f\|_{U^2(G)}^4 = \|\widehat{f}\|_{l^\infty(\widehat{G})}^4 \le \|\widehat{f}\|_{l^\infty(\widehat{G})}^2 \|f\|_{L^2(G)}^2.$$

Lecture 15

Hence

$$\|\widehat{f}\|_{l^\infty(\widehat{G})} \le \|\widehat{f}\|_{l^4(\widehat{G})} = \|f\|_{U^2(G)} \le \|\widehat{f}\|_{l^\infty(\widehat{G})}^{\frac{1}{2}} \|f\|_{L^2(G)}^{\frac{1}{2}}.$$

Moreover, if $f = f_A A = \mathbb{1}_A - \alpha$, then

$$T_3(f,f,f) = T_3(\mathbb{1}_A - \alpha, \mathbb{1}_A - \alpha, \mathbb{1}_A - \alpha) = T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) - \alpha^3.$$

We may therefore reformulate the first step in the proof of Meshulam's Theorem as follows: if $p^n \ge 2\alpha^{-2}$, then by Section 4,

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

It remains to show that if $\|f_A A\|_{U^2(\mathbb{F}_p^n)}$ is non-trivial, then there exists a subspace $V \le \mathbb{F}_p^n$ of bounded codimension on which A has increased density.

Theorem 4.7 (U^2 Inverse Theorem)**.** Assuming that:

- $f : \mathbb{F}_p^n \to \mathbb{C}$
- $\|f\|_{L^\infty(\mathbb{F}_p^n)} \le 1$
- $\delta > 1$
- $\|f\|_{U^2(\mathbb{F}_p^n)} \ge \delta$

Then there exists $b \in \mathbb{F}_p^n$ such that

$$|\mathbb{E}_{x\in\mathbb{F}_p^n} f(x) e(-x\cdot b/p)| \ge \delta^2.$$

In other words, $|\langle f, \phi\rangle| \ge \delta^2$ for $\phi(x) = e(-x\cdot b/p)$ and we say "f correlates with a linear phase function".

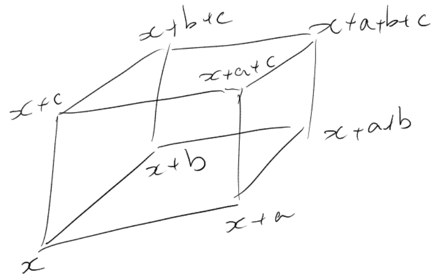
Proof. We have seen that

$$\|f\|_{U^2(\mathbb{F}_p^n)}^2 \le \|\widehat{f}\|_{l^\infty(\widehat{\mathbb{F}_p^n})} \|f\|_{L^2(\mathbb{F}_p^n)} \le \|\widehat{f}\|_{l^\infty(\widehat{\mathbb{F}_p^n})},$$

so

$$\delta^2 \le \|\widehat{f}\|_{l^\infty(\widehat{\mathbb{F}_p^n})} = \sup_{t\in\widehat{\mathbb{F}_p^n}} |\mathbb{E}_x f(x) e(-x\cdot t/p)|.$$

□



Definition 4.8 (U^3 norm)**.** Given $f : G \to \mathbb{C}$, define its U^3 *norm* by

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

where $\mathcal{C}g(x) = \overline{g(x)}$ and $|\varepsilon|$ denotes the number of ones in ε.

It is easy to verify that $\mathbb{E}_{c\in G}\|\Delta_c f\|^4_{U^2(G)}$ where $\Delta_c g(x) = g(x)\overline{g(x+c)}$.

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

$$\langle (f_\varepsilon)_{\varepsilon\in\{0,1\}^3}\rangle_{U^3(G)} = \mathbb{E}_{x,h_1,h_2,h_3\in G} \prod_{\varepsilon\in\{0,1\}^3} \mathcal{C}^{|\varepsilon|} f_\varepsilon(x+\varepsilon\cdot\mathbf{h}).$$

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

Lemma 4.10 (Gowers–Cauchy–Schwarz Inequality)**.** Assuming that:

- $f_\varepsilon : G \to \mathbb{C}$, $\varepsilon \in \{0,1\}^3$

Then

$$|\langle (f_\varepsilon)_{\varepsilon\in\{0,1\}^3}\rangle_{U^3(G)} \le \prod_{\varepsilon\in\{0,1\}^3} \|f_\varepsilon\|_{U^3(G)}.$$

Setting $f_\varepsilon = f$ for $\varepsilon \in \{0,1\}^2 \times \{0\}$ and $f_\varepsilon = 1$ otherwise, it follows that $\|f\|^4_{U^2(G)} \le \|f\|_{U^3(G)}{}^4$ hence $\|f\|_{U^2(G)} \le \|f\|_{U^3(G)}$.

Proposition 4.11. Assuming that:

- $f_1, f_2, f_3, f_4 : \mathbb{F}_5^n \to \mathbb{C}$

Then
$$T_4(f_1, f_2, f_3, f_4) \le \min_{i \in [4]} \|f_i\|_{U^3(G)} \prod_{j \neq i} \|f_j\|_{L^\infty(\mathbb{F}_5^n)}.$$

Proof. We additionally assume $f = f_1 = f_2 = f_3 = f_4$ to make the proof easier to follow, but the same ideas are used for the general case. We additionally assume $\|f\|_{L^\infty(\mathbb{F}_5^n)} \le 1$, by rescaling, since the inequality is homogeneous.

Reparametrising, we have

$$\begin{aligned}
T_4(f,f,f,f) &= \mathbb{E}_{a,b,c,d \in \mathbb{F}_5^n} f(3a+2b+c) f(2a+b-d) f(a-c-2d) f(-b-2c-3d) \\
|T_4(f,f,f,f)|^8 &\le \left(\mathbb{E}_{a,b,c} |\mathbb{E}_d f(2a+b-d) f(a-c-2d) f(-b-2c-3d)|^2 \right)^4 \\
&= \Big(\mathbb{E}_{d,d'} \mathbb{E}_{a,b} f(2a+b+d) \overline{f(2a+b-d')} \\
&\qquad \mathbb{E}_c f(a-c-2d) \overline{f(a-c-2d')} f(-b-2c-3d) \overline{f(-b-2c-3d')} \Big)^4 \\
&\le \left(\mathbb{E}_{d,d'} \mathbb{E}_{a,b} |\mathbb{E}_c f(a-c-2d) \overline{f(a-c-2d')} f(-b-2c-3d) \overline{f(-b-2c-3d')}|^2 \right)^2 \\
&= \Big(\mathbb{E}_{c,c',d,d'} \mathbb{E}_a f(a-c-2d) \overline{f(a-c'-2d) f(a-c-2d')} f(a-c'-2d') \\
&\qquad \mathbb{E}_b f(-b-2c-3d) \overline{f(-b-2c'-3d) f(-b-2c-3d')} f(-b-2c'-3d') \Big)^2 \\
&\le \mathbb{E}_{c,c',d,d',a} |\mathbb{E}_b f(-b-2c-3d) \overline{f(-b-2c'-3d) f(-b-2c-3d')} f(-b-2c'-3d')|^2 \\
&= \mathbb{E}_{b,b',c,c',d,d'} f(-b-2c-3d) \overline{f(-b'-2c-3d) f(-b-2c'-3d)} f(-b'-2c'-3d) \\
&\qquad \overline{f(-b-2c-3d')} f(-b'-2c-3d') f(-b-2c'-3d') \overline{f(-b'-2c'-3d')}
\end{aligned}$$
□

Lecture 16

Theorem 4.12 (Szemerédi's Theorem for 4-APs)**.** Assuming that:

- $A \subseteq \mathbb{F}_5^n$ a set containing no non-trivial 4 term arithmetic progressions

Then $|A| = o(5^n)$.

Idea: By Proposition 4.11 with $f = f_A = \mathbb{1}_A - \alpha$,

$$T_4(\underbrace{\mathbb{1}_A}_{f_A+\alpha}, \underbrace{\mathbb{1}_A}_{f_A+\alpha}, \underbrace{\mathbb{1}_A}_{f_A+\alpha}, \underbrace{\mathbb{1}_A}_{f_A+\alpha}) - \alpha^4 = T_4(f_A, f_A, f_A, f_A) + \cdots$$

where $\cdots$ consists of 14 other terms in which between one and three of the inputs are equal to f_A.

These are controlled by
$$\|f_A\|_{U^2(\mathbb{F}_5^n)} \le \|f_A\|_{U^3(G)},$$
whence
$$|T_4(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) - \alpha^4| \le 15\|f_A\|_{U^3(G)}.$$
So if A contains no non-trivial 4 term arithmetic progressions and $5^n > 2\alpha^{-3}$, then $\|f_A\|_{U^3(G)} \ge \frac{\alpha^4}{30}$.

What can we say about functions with large U^3 norm?

Example 4.13. Let M be an $n \times n$ symmetric matrix with entries in $\mathbb{F}_5$. Then $f(x) = e(x^\top Mx/5)$ satisfies $\|f\|_{U^3(G)} = 1$.

Theorem 4.14 (U^3 inverse theorem)**.** Assuming that:

- $f : \mathbb{F}_5^n \to \mathbb{C}$
- $\|f\|_{L^\infty(\mathbb{F}_5^n)} \le 1$
- $\|f\|_{U^3(G)} \ge \delta$ for some $\delta > 0$

Then there exists a symmetric $n \times n$ matrix M with entries in $\mathbb{F}_5$ and $b \in \mathbb{F}_5^n$ such that
$$|\mathbb{E}_x f(x) e((x^\top Mx + b^\top x)/p)| \ge c(\delta)$$
where $c(\delta)$ is a polynomial in δ. In other words, $|\langle f, \phi\rangle| \ge c(\delta)$ for $\phi(x) = e((x^\top Mx + b^\top x)/p)$ and we say "f correlates with a quadratic phase function".

Proof (sketch). Let $\Delta_h f(x)$ denote $f(x)\overline{f(x+h)}$.

$\|f\|_{U^3(G)} = (\mathbb{E}_h \|\Delta_h f\|_{U^2}^4)^{\frac{1}{8}}$.

STEP 1: Weak linearity. See reference.

STEP 2: Strong linearity. We will spend the rest of the lecture discussing this in detail.

STEP 3: Symmetry argument. Problem 8 on Sheet 3.

STEP 4: Integration step. Problem 9 on Sheet 3.

STEP 1: If $\|f\|_{U^3(G)}{}^8 = \mathbb{E}_h \|\Delta_h\|_{U^2}^4 \ge \delta^8$, then for at least a $\frac{\delta^8}{2}$-proportion of $h \in \mathbb{F}_5^n$, $\frac{\delta^8}{2} \le \|\Delta_h f\|_{U^2}^4 \le \|\widehat{\Delta_h f}\|_{l^\infty}^2$. So for each such $h \in \mathbb{F}_5^n$, there exists t_h such that $|\widehat{\Delta_h f}(t_h)|^2 \ge \frac{\delta^8}{2}$.

Proposition 4.15. Assuming that:

- $f : \mathbb{F}_5^n \to \mathbb{C}$

- $\|f\|_\infty \le 1$
- $\|f\|_{U^3(G)} \ge \delta$
- $|\mathbb{F}_5^n| = \Omega_\delta(1)$

Then there exists $S \subseteq \mathbb{F}_5^n$ with $|S| = \Omega_\delta(|\mathbb{F}_5^n|)$ and a function $\phi : S \to \widehat{\mathbb{F}_5^n}$ such that

(i) $|\widehat{\Delta_h f}(\phi(h))| = \Omega_\delta(1)$;

(ii) There are at least $\Omega_\delta(|\mathbb{F}_5^n|^3)$ quadruples $(s_1, s_2, s_3, s_4) \in S^4$ such that $s_1 + s_2 = s_3 + s_4$ and $\phi(s_1) + \phi(s_2) + \phi(s_4)$.

STEP 2: If S and ϕ are as above, then there is a linear function $\psi : \mathbb{F}_5^n \to \widehat{\mathbb{F}_5^n}$ which coincides with ϕ for many elements of S.

Proposition 4.16. Assuming that:

- S and ϕ given as in Proposition 4.15

Then there exists $n \times n$ matrix M with entries in $\mathbb{F}_5$ and $b \in \mathbb{F}_5^n$ such that $\psi(x) = Mx + b$ ($\psi : \mathbb{F}_5^n \to \widehat{\mathbb{F}_5^n}$) satisfies $\psi(x) = \phi(x)$ for $\Omega_\delta(|\mathbb{F}_5^n|)$ elements $x \in S$.

Proof. Consider the graph of ϕ, $\Gamma = \{(h, \phi(h)) : h \in S\} \subseteq \mathbb{F}_5^n \times \widehat{\mathbb{F}_5^n}$. By Proposition 4.15, Γ has $\Omega_\delta(|\mathbb{F}_5^n|^3)$ additive quadruples.

By Balog–Szemeredi–Gowers, Schoen, there exists $\Gamma' \subseteq \Gamma$ with $|\Gamma'| = \Omega_\delta(|\Gamma|) = \Omega_\delta(|\mathbb{F}_5^n|)$ and $|\Gamma' + \Gamma'| = O_\delta(|\Gamma'|)$. udefine $S' \subseteq S$ by $\Gamma' = \{(h, \phi(h)) : h \in S'\}$ and note $|S'| = \Omega_\delta(|\mathbb{F}_5^n|)$.

By Freiman-Ruzsa applied to $\Gamma' \subseteq \mathbb{F}_5^n \times \widehat{\mathbb{F}_5^n}$, there exists a subspace $H \le \mathbb{F}_5^n \times \widehat{\mathbb{F}_5^n}$ with $|H| = O_\delta(|\Gamma'|) = O_\delta(|\mathbb{F}_5^n|)$ such that $\Gamma' \subseteq H$.

Denote by $\pi : \mathbb{F}_5^n \times \widehat{\mathbb{F}_5^n} \to \mathbb{F}_5^n$ the projection onto the first n coordinates. By construction, $\pi(H) \supseteq S'$. Moreover, since $|S'| = \Omega_\delta(|\mathbb{F}_5^n|)$,

$$|\ker(\pi|_H)| = \frac{|H|}{|\operatorname{Im}(\pi|_H)|} = \frac{O_\delta(|\mathbb{F}_5^n|)}{|S'|} = O_\delta(1).$$

We may thus partition H into $O_\delta(1)$ cosets of some subspace H^* such that $\pi|_H$ is injective on each coset. By averaging, there exists a coset $x + H^*$ such that

$$|\Gamma' \cap (x + H^*)| = \Omega_\delta(|\Gamma'|) = \Omega_\delta(|\mathbb{F}_5^n|).$$

Set $\Gamma'' = \Gamma' \cap (x + H^*)$, and define S'' accordingly.

Now $\pi|_{x+^*}$ is injective and surjective onto $V := \operatorname{Im}(\pi|_{x+H^*})$. This means there is an affine linear map $\psi : V \to \widehat{\mathbb{F}_5^n}$ such that $(h, \psi(h)) \in \Gamma''$ for all $h \in S''$. □

Then do steps 3 and 4. □

Index