

# Contents

1. Combinatorial methods .....	2
2. Fourier-analytic techniques .....	10
3. Probabilistic tools .....	19
4. Further topics .....	19

# 1. Combinatorial methods

**Definition 1.1** Let  $G$  be an abelian group and  $A, B \subseteq G$ . The **sumset** of  $A$  and  $B$  is

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

The **difference set** of  $A$  and  $B$  is

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

**Proposition 1.2**  $\max\{|A|, |B|\} \leq |A + B| \leq |A| \cdot |B|$ .

*Proof.* Trivial. □

**Example 1.3** Let  $A = [n] = \{1, \dots, n\}$ . Then  $A + A = \{2, \dots, 2n\}$  so  $|A + A| = 2|A| - 1$ .

**Lemma 1.4** Let  $A \subseteq \mathbb{Z}$  be finite. Then  $|A + A| \geq 2|A| - 1$  with equality iff  $A$  is an arithmetic progression.

*Proof (Hints).* Consider two sequences in  $A + A$  which are strictly increasing and of the same length. □

*Proof.*

- Let  $A = \{a_1, \dots, a_n\}$  with  $a_i < a_{i+1}$ . Then  $a_1 + a_1 < a_1 + a_2 < \dots < a_1 + a_n < a_2 + a_n < \dots < a_n + a_n$ .
- Note this is not the only choice of increasing sequence that works, in particular, so does  $a_1 + a_1 < a_1 + a_2 < a_2 + a_2 < a_2 + a_3 < a_2 + a_4 < \dots < a_2 + a_n < a_3 + a_n < \dots < a_n + a_n$ .
- So when equality holds, all these sequences must be the same. In particular,  $a_2 + a_i = a_1 + a_{i+1}$  for all  $i$ .

□

**Lemma 1.5** If  $A, B \subseteq \mathbb{Z}$ , then  $|A + B| \geq |A| + |B| - 1$  with equality iff  $A$  and  $B$  are arithmetic progressions with the same common difference.

*Proof (Hints).* Similar to above, consider 4 sequences in  $A + B$  which are strictly increasing and of the same length. □

**Example 1.6** Let  $A, B \subseteq \mathbb{Z}/p$  for  $p$  prime. If  $|A| + |B| \geq p + 1$ , then  $A + B = \mathbb{Z}/p$ .

*Proof (Hints).* Consider  $A \cap (g - B)$  for  $g \in \mathbb{Z}/p$ . □

*Proof.*

- $g \in A + B$  iff  $A \cap (g - B) \neq \emptyset$  where  $(g - B = \{g\} - B)$ .
- Let  $g \in \mathbb{Z}/p$ , then use inclusion-exclusion on  $|A \cap (g - B)|$  to conclude result.

□

**Theorem 1.7** (Cauchy-Davenport) Let  $p$  be prime,  $A, B \subseteq \mathbb{Z}/p$  be non-empty. Then

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

*Proof (Hints).*

- Assume  $|A| + |B| < p + 1$ , and WLOG that  $1 \leq |A| \leq |B|$  and  $0 \in A$  (by translation).
- Induct on  $|A|$ .
- Let  $a \in A$ , find  $B'$  such that  $0 \in B'$ ,  $a \notin B'$  and  $|B'| = |B|$  (use fact that  $p$  is prime).
- Apply induction with  $A \cap B'$  and  $A \cup B'$ , while reasoning that  $(A \cap B') + (A \cup B') \subseteq A + B'$ .

□

*Proof.*

- Assume  $|A| + |B| < p + 1$ , and WLOG that  $1 \leq |A| \leq |B|$  and  $0 \in A$  (by translation).
- Use induction on  $|A|$ .  $|A| = 1$  is trivial.
- Let  $|A| \geq 2$  and let  $0 \neq a \in A$ . Then since  $p$  is prime,  $\{a, 2a, \dots, pa\} = \mathbb{Z}/p$ .
- There exists  $m \geq 0$  such that  $ma \in B$  but  $(m+1)a \notin B$  (why?). Let  $B' = B - ma$ , so  $0 \in B'$ ,  $a \notin B'$  and  $|B'| = |B|$ .
- $1 \leq |A \cap B'| < |A|$  (why?) so the inductive hypothesis applies to  $A \cap B'$  and  $A \cup B'$ .
- Since  $(A \cap B') + (A \cup B') \subseteq A + B'$  (why?), we have  $|A + B| = |A + B'| \geq |(A \cap B') + (A \cup B')| \geq |A \cap B'| + |A \cup B'| - 1 = |A| + |B| - 1$ .

□

**Example 1.8** Cauchy-Davenport does not hold general abelian groups (e.g.  $\mathbb{Z}/n$  for  $n$  composite): for example, let  $A = B = \{0, 2, 4\} \subseteq \mathbb{Z}/6$ , then  $A + B = \{0, 2, 4\}$  so  $|A + B| = 3 < \min\{6, |A| + |B| - 1\}$ .

**Example 1.9** Fix a small prime  $p$  and let  $V \subseteq \mathbb{F}_p^n$  be a subspace. Then  $V + V = V$ , so  $|V + V| = |V|$ . In fact, if  $A \subseteq \mathbb{F}_p^n$  satisfies  $|A + A| = |A|$ , then  $A$  is an affine subspace (a coset of a subspace).

*Proof.* If  $0 \in A$ , then  $A \subseteq A + A$ , so  $A = A + A$ . General result follows by considering translation of  $A$ . □

**Example 1.10** Let  $A \subseteq \mathbb{F}_p^n$  satisfy  $|A + A| \leq \frac{3}{2} |A|$ . Then there exists a subspace  $V \subseteq \mathbb{F}_p^n$  such that  $|V| \leq \frac{3}{2} |A|$  and  $A$  is contained in a coset of  $V$ .

*Proof.* Exercise (sheet 1). □

**Definition 1.11** Let  $A, B \subseteq G$  be finite subsets of an abelian group  $G$ . The **Ruzsa distance** between  $A$  and  $B$  is

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

**Lemma 1.12** (Ruzsa Triangle Inequality) Let  $A, B, C \subseteq G$  be finite. Then

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

*Proof (Hints).* Consider a certain map from  $B \times (A - C)$  to  $(A - B) \times (B - C)$ .  $\square$

*Proof.*

- Note that  $|B| |A - C| \leq |A - B| |B - C|$ . Indeed, writing each  $d \in A - C$  as  $d = a_d - c_d$  with  $a_d \in A$ ,  $c_d \in C$ , the map  $\varphi : B \times (A - C) \rightarrow (A - B) \times (B - C)$ ,  $\varphi(b, d) = (a_d - b, b - c_d)$  is injective (why?).
- Triangle inequality now follows from definition of Ruzsa distance.

$\square$

**Definition 1.13** The **doubling constant** of finite  $A \subseteq G$  is  $\sigma(A) := |A + A|/|A|$ .

**Definition 1.14** The **difference constant** of finite  $A \subseteq G$  is  $\delta(A) := |A - A|/|A|$ .

**Remark 1.15** The Ruzsa triangle inequality shows that

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

So  $\delta(A) \leq \sigma(A)^2$ , i.e.  $|A - A| \leq |A + A|^2/|A|$ .

**Notation 1.16** Let  $A \subseteq G$ ,  $\ell, m \in \mathbb{N}_0$ . Then

$$\ell A + mA := \underbrace{A + \dots + A}_{\ell \text{ times}} - \underbrace{A - \dots - A}_{m \text{ times}}$$

This is referred to as the **iterated sum and difference set**.

**Theorem 1.17** (Plunnecke's Inequality) Let  $A, B \subseteq G$  be finite and  $|A + B| \leq K|A|$  for some  $K \geq 1$ . Then  $\forall \ell, m \in \mathbb{N}_0$ ,

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

*Proof (Hints).*

- Let  $A' \subseteq A$  minimise  $|A' + B|/|A'|$  with value  $K'$ .
- Show that for every finite  $C \subseteq G$ ,  $|A' + B + C| \leq K'|A + C|$  by induction on  $|C|$  (note two sets need to be written as disjoint unions here).
- Show that  $\forall m \in \mathbb{N}_0$ ,  $|A' + mB| \leq (K')^m|A'|$  by induction.
- Use Ruzsa triangle inequality to conclude result.

$\square$

*Proof.*

- Choose  $\emptyset \neq A' \subseteq A$  which minimises  $|A' + B|/|A'|$ . Let the minimum value be  $K'$ .
- Then  $|A' + B| = K'|A'|$ ,  $K' \leq K$  and  $\forall A'' \subseteq A$ ,  $|A'' + B| \geq K'|A''|$ .
- Claim: for every finite  $C \subseteq G$ ,  $|A' + B + C| \leq K'|A' + C|$ :
  - Use induction on  $|C|$ .  $|C| = 1$  is true by definition of  $K'$ .
  - Let claim be true for  $C$ , consider  $C' = C \cup \{x\}$  for  $x \notin C$ .
  - $A' + B + C' = (A' + B + C) \cup ((A' + B + x) - (D + B + x))$ , where  $D = \{a \in A' : a + B + x \subseteq A' + B + C\}$ .
  - By definition of  $K'$ ,  $|D + B| \geq K'|D|$ . Hence,

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

- Applying this argument a second time, write  $A' + C' = (A' + C) \cup ((A' + x) - (E + x))$ , where  $E = \{a \in A' : a + x \in A' + C\} \subseteq D$ .
- Finally,

$$\begin{aligned}
|A' + C'| &= |A' + C| + |A' + x| - |E + x| \\
&\geq |A' + C| + |A'| - |D|.
\end{aligned}$$

- We first show that  $\forall m \in \mathbb{N}_0$ ,  $|A' + mB| \leq (K')^m |A'|$  by induction:
  - $m = 0$  is trivial,  $m = 1$  is true by assumption.
  - Suppose  $m - 1 \geq 1$  is true. By the claim with  $C = (m - 1)B$ , we have

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

- As in the proof of Ruzsa's triangle inequality,  $\forall \ell, m \in \mathbb{N}_0$ ,

$$|A'| | \ell B - mB | \leq |A' + \ell B| |A' + mB| \leq (K')^\ell |A'| (K')^m |A'| = (K')^{\ell+m} |A'|^2.$$

□

**Theorem 1.18** (Freiman-Ruzsa) Let  $A \subseteq \mathbb{F}_p^n$  and  $|A + A| \leq K|A|$ . Then  $A$  is contained in a subspace  $H \subseteq \mathbb{F}_p^n$  with  $|H| \leq K^2 p^{K^4} |A|$ .

*Proof (Hints).*

- Let  $X \subseteq 2A - A$  be of maximal size such that all  $x + A$ ,  $x \in X$ , are disjoint.
- Use Plunnecke's inequality to obtain an upper bound on  $|X||A|$ .
- Show that  $\forall \ell \geq 2$ ,  $\ell A - A \subseteq (\ell - 1)X + A - A$  by induction.
- Let  $H$  be subgroup generated by  $A$ . By writing  $H$  as an infinite union, show that  $H \subseteq Y + A - A$ , where  $Y$  is subgroup generated by  $X$ .
- Find an upper bound for  $|Y|$ , conclude using Plunnecke inequality.

□

*Proof.*

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

$$|X||A| = \left| \bigcup_{x \in X} (x + A) \right| \leq |3A - A| \leq K^4 |A|.$$

Hence  $|X| \leq K^4$ .

- We next show that  $2A - A \subseteq X + A - A$ . Indeed, if,  $y \in 2A - A$  and  $y \notin X$ , then by maximality of  $X$ , then  $(y + A) \cap (x + A) \neq \emptyset$  for some  $x \in X$ . If  $y \in X$ , then  $y \in X + A - A$ .

- It follows from above, by induction, that  $\forall \ell \geq 2$ ,  $\ell A - A \subseteq (\ell - 1)X + A - A$ :  
 $\ell A - A = A + (\ell - 1)A - A \subseteq (\ell - 2)X + 2A - A \subseteq (\ell - 2)X + X + A - A = (\ell - 1)X + A - A$ .
- Now, let  $H \subseteq \mathbb{F}_p^n$  be the subgroup generated by  $A$ :

$$H = \bigcup_{\ell \geq 1} (\ell A - A) \subseteq Y + A - A$$

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

- Every element of  $Y$  can be written as a sum of  $|X|$  elements of  $X$  with coefficients in  $\{0, \dots, p-1\}$ . Hence,  $|Y| \leq p^{|X|} \leq p^{K^4}$ .
- Hence  $|H| \leq |Y||A - A| \leq p^{K^4} K^2 |A|$  by Plunnecke/Ruzsa triangle inequality.

□

**Example 1.19** Let  $A = V \cup R$ , where  $V \subseteq \mathbb{F}_p^n$  is a subspace with  $\dim(V) = d = n/K$  satisfying  $K \ll d \ll n - K$ , and  $R$  consists of  $K - 1$  linearly independent vectors not in  $V$ . Then  $|A| = |V \cup R| = |V| + |R| = p^{n/K} + K - 1 \approx p^{n/K} = |V|$ .

Now  $|A + A| = |(V \cup R) + (V \cup R)| = |V \cup (V + R) \cup 2R| \approx K|V| \approx K|A|$  (since  $V \cup (V + R)$  gives  $K$  cosets of  $V$ ). But any subspace  $H \subseteq \mathbb{F}_p^n$  containing  $A$  must have size at least  $p^{n/K+(K-1)} \approx |V|p^K$ . Hence, the exponential dependence on  $K$  in Freiman-Ruzsa is necessary.

**Theorem 1.20** (Polynomial Freiman-Ruzsa Theorem) Let  $A \subseteq \mathbb{F}_p^n$  be such that  $|A + A| \leq K|A|$ . Then there exists a subspace  $H \subseteq \mathbb{F}_p^n$  of size at most  $C_1(K)|A|$  such that for some  $x \in \mathbb{F}_p^n$ ,

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

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

*Proof.* Very difficult (took Green, Gowers and Tao to prove it).

□

**Definition 1.21** Given  $A, B \subseteq G$  for an abelian group  $G$ , the **additive energy** between  $A$  and  $B$  is

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

**Additive quadruples**  $(a, a', b, b')$  are those such that  $a + b = a' + b'$ . Write  $E(A)$  for  $E(A, A)$ .

**Example 1.22** Let  $V \subseteq \mathbb{F}_p^n$  be a subspace. Then  $E(V) = |V|^3$ . On the other hand, if  $A \subseteq \mathbb{Z}/p$  is chosen at random from  $\mathbb{Z}/p$  (where each  $a \in \mathbb{Z}/p$  is included with probability  $\alpha > 0$ ), with high probability,  $E(A) = \alpha^4 p^3 = \alpha |A|^3$ .

**Definition 1.23** For  $A, B \subseteq G$ , the **representation function** is  $r_{A+B}(x) := |\{(a, b) \in A \times B : a + b = x\}| = |A \cap (x - B)|$ .

**Lemma 1.24** Let  $\emptyset \neq A, B \subseteq G$  for an abelian group  $G$ . Then

$$E(A, B) \geq \frac{|A|^2|B|^2}{|A \pm B|}.$$

*Proof (Hints).*

- Show that using Cauchy-Schwarz that

$$E(A, B) = \sum_{x \in G} r_{A+B}(x)^2 \geq \frac{\left(\sum_{x \in G} r_{A+B}(x)\right)^2}{|A+B|}.$$

- By using indicator functions, show that  $\sum_{x \in G} r_{A+B}(x) = |A||B|$ .

□

*Proof.* Observe that

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

But now

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

Note that the same argument works for  $|A - B|$ .

□

**Corollary 1.25** If  $|A + A| \leq K|A|$ , then  $E(A) \geq \frac{|A|^4}{|A+A|} \geq \frac{|A|^3}{K}$ . So if  $A$  has small doubling constant, then it has large additive energy.

*Proof (Hints).* Trivial.

□

*Proof.* Trivial.

□

**Example 1.26** The converse of the above lemma does not hold: e.g. let  $G$  be a (class of) abelian group(s). Then there exist constants  $\theta, \eta > 0$  such that for all  $n$  large enough, there exists  $A \subseteq G$  with  $|A| \geq n$  satisfying  $E(A) \geq \eta|A|^3$ , and  $|A + A| \geq \theta|A|^2$ .

**Definition 1.27** Given  $A \subseteq G$  and  $\gamma > 0$ , let  $P_\gamma := \{x \in G : |A \cap (x + A)| \geq \gamma|A|\}$  be the set of  $\gamma$ -popular differences of  $A$ .

**Lemma 1.28** Let  $A \subseteq G$  be finite such that  $E(A) = \eta|A|^3$  for some  $\eta > 0$ . Then  $\forall c > 0$ , there is a subset  $X \subseteq A$  with  $|X| \geq \frac{\eta}{3}|A|$  such that for all  $(16c)$ -proportion of pairs  $(a, b) \in X^2$ ,  $a - b \in P_{c\eta}$ .

*Proof.*

- We use a technique called “dependent random choice”.
- Let  $U = \{x \in G : |A \cap (x + A)| \leq \frac{1}{2}\eta|A|\}$ .
- Then  $\sum_{x \in U} |A \cap (x + A)|^2 \leq \frac{1}{2}\eta|A| \sum_{x \in G} |A \cap (x + A)| = \frac{1}{2}\eta|A|^3 = \frac{1}{2}E(A)$ .
- For  $0 \leq i \leq \lceil \log_2 \eta^{-1} \rceil$ , let  $Q_i = \{x \in G : |A|/2^{i+1} < |A \cap (x + A)| \leq |A|/2^i\}$  and set  $\delta_i = \eta^{-1}2^{-2i}$ .
- Then

$$\begin{aligned}
\sum_{i=0}^{\lceil \log_2 \eta^{-1} \rceil} \delta_i |Q_i| &= \sum_i \frac{|Q_i|}{\eta 2^{2i}} \\
&= \frac{1}{\eta|A|^2} \sum_i \frac{|A|^2}{2^{2i}} |Q_i| \\
&= \frac{1}{\eta|A|^2} \sum_i \frac{|A|^2}{2^{2i}} \sum_{x \notin U} \mathbb{1}_{\{|A|/2^{i+1} < |A \cap (x + A)| \leq |A|/2^i\}} \\
&\geq \frac{1}{\eta|A|^2} \sum_{x \notin U} |A \cap (x + A)|^2 \\
&\geq \frac{1}{\eta|A|^2} \cdot \frac{1}{2}E(A) = \frac{1}{2}|A|.
\end{aligned}$$

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

$$\begin{aligned}
\sum_i \sum_{(a,b) \in S} |(A - a) \cap (A - b) \cap Q_i| &\leq \sum_{(a,b) \in S} |(A - a) \cap (A - b)| \\
&= \sum_{(a,b) \in S} |A \cap (a - b + A)| \\
&\leq \sum_{(a,b) \in S} c\eta|A| \quad \text{by definition of } S \\
&= |S|c\eta|A| \\
&\leq c\eta|A|^3 = 2c\eta|A|^2 \cdot \frac{1}{2}|A| \\
&\leq 2c\eta|A|^2 \sum_i \delta_i |Q_i| \quad \text{by above inequality.}
\end{aligned}$$

- Hence  $\exists i_0$  such that

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

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



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

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

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

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

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

- Therefore,

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

- So  $\exists x \in Q$  such that  $|X(x)|^2 \geq \frac{\lambda^2}{8}|A|^2$ , so  $|X| \geq \frac{\lambda}{\sqrt{8}}|A| \geq \frac{\eta}{3}|A|$  and  $|T(x)| \leq 16c|X|^2$ .

□

**Theorem 1.29** (Balog-Szemerédi-Gowers, Schoen) Let  $A \subseteq G$  be finite such that  $E(A) \geq \eta|A|^3$  for some  $\eta > 0$ . Then there exists  $A' \subseteq A$  with  $|A'| \geq c_1(\eta)|A|$  such that  $|A' + A'| \leq |A|/c_2(\eta)$ , where  $c_1(\eta)$  and  $c_2(\eta)$  are both polynomial in  $\eta$ .

*Proof.*

- The idea is to find  $A' \subseteq A$  such that  $\forall a, b \in A'$ ,  $a - b$  has many representations as  $(a_1 - a_2) + (a_3 - a_4)$  with each  $a_i \in A$ .
- Apply the above lemma with  $c = 2^{-7}$  to obtain  $X \subseteq A$  with  $|X| \geq \frac{\eta}{3}|A|$  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  $G = (X \sqcup X, \{(x, y) \in X \times X : x - y \in P_{\eta/2^7}\})$  has at least  $\frac{7}{8}|X|^2$  edges.
- Let  $A' = \{x \in X : \deg_G(x) \geq \frac{3}{4}|X|\}$ . Clearly  $|A'| \geq |X|/8$ .
- For any  $a, b \in A'$ , there are at least  $|X|/2$  elements  $y \in X$  such that  $(a, y), (b, y) \in E(G)$  (so  $a - y, b - y \in P_{\eta/2^7}$ ). Hence  $a - b = (a - y) - (b - y)$  has at least

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

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

- It follows that  $\frac{\eta^3}{2^{17}}|A|^3|A' - A'| \leq |A|^4$ , hence  $|A' - A'| \leq 2^{17}\eta^{-3}|A| \leq 2^{22}\eta^{-4}|A'|$ , and so  $|A' + A'| \leq 2^{44}\eta^{-8}|A'|$ .

□

## 2. Fourier-analytic techniques

In this chapter, assume that  $G$  is a *finite* abelian group.

**Definition 2.1** The group  $\hat{G}$  of **characters** of  $G$  is the group of homomorphisms  $\gamma : G \rightarrow \mathbb{C}^\times$ . In fact,  $\hat{G}$  is isomorphic to  $G$ .

**Notation 2.2** Norm and inner product notation:

- Write

$$\begin{aligned}\|f\|_q &= \|f\|_{L^q(G)} = (\mathbb{E}_{x \in G} |f(x)|^q)^{1/q}, \\ \|\hat{f}\|_q &= \|\hat{f}\|_{\ell^q(\hat{G})} = \left( \sum_{\gamma \in \hat{G}} |\hat{f}(\gamma)|^q \right)^{1/q}, \\ \langle f, g \rangle_{L^2(G)} &= \mathbb{E}_{x \in G} f(x) \overline{g(x)}, \\ \langle f, g \rangle_{\ell^2(\hat{G})} &= \sum_{\gamma \in \hat{G}} \hat{f}(\gamma) \overline{\hat{g}(\gamma)}\end{aligned}$$

- If Fourier support of function is restricted to  $\Lambda \subseteq \hat{G}$ , write  $\|\hat{f}\|_{\ell^q(\Lambda)} = \left( \sum_{\gamma \in \Lambda} |\hat{f}(\gamma)|^q \right)^{1/q}$ .

**Notation 2.3** Asymptotic notation:

- Write  $f(n) = O(g(n))$  if

$$\exists C > 0 : \forall n \in \mathbb{N}, \quad |f(n)| \leq C|g(n)|.$$

- Write  $f(n) = o(g(n))$  if

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} : \forall n \geq N, |f(n)| \leq \varepsilon|g(n)|,$$

$$\text{i.e. } \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0.$$

- Write  $f(n) = \Omega(g(n))$  if  $g(n) = O(f(n))$ .
- If the implied constant depends on a fixed parameter, this may be indicated by a subscript, e.g.  $\exp(pn^2) = O_p(\exp(n^2))$ .

**Theorem 2.4** (Hölder's Inequality) Let  $p, q \in [1, \infty]$  with  $\frac{1}{p} + \frac{1}{q} = 1$ , and  $f \in L^p(G)$ ,  $g \in L^q(G)$ . Then

$$\|fg\|_1 \leq \|f\|_p \|g\|_q.$$

**Theorem 2.5** (Cauchy-Schwarz Inequality) For  $f, g \in L^2(G)$ , we have

$$\langle f, g \rangle_{L^2(G)} \leq \|f\|_2 \|g\|_2.$$

Note this is a special case of Hölder's inequality with  $p = q = 2$ .

**Theorem 2.6** (Young's Convolution Inequality) Let  $p, q, r \in [1, \infty]$ ,  $\frac{1}{p} + \frac{1}{q} = \frac{1}{r}$ ,  $f \in L^p(G)$ ,  $g \in L^q(G)$ . Then

$$\|f * g\|_r \leq \|f\|_p \|g\|_q.$$

**Notation 2.7**  $e(y)$  denotes the function  $e^{2\pi i y}$ .

**Example 2.8**

- Let  $G = \mathbb{F}_p^n$ , then for any  $\gamma \in \hat{G}$ , we have a corresponding character  $\gamma(x) = e((\gamma \cdot x)/p)$ .
- If  $G = \mathbb{Z}/N$ , then any  $\gamma \in \hat{G}$  has a corresponding character  $\gamma(x) = e(\gamma x/N)$ .

**Notation 2.9** Given a non-empty  $B \subseteq G$  and  $g : B \rightarrow \mathbb{C}$ , write  $\mathbb{E}_{x \in B} g(x)$  for  $\frac{1}{|B|} \sum_{x \in B} g(x)$ . If  $B = G$ , we may simply write  $\mathbb{E}$  instead of  $\mathbb{E}_{x \in B}$ .

**Lemma 2.10** For all  $\gamma \in \hat{G}$ ,

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

and for all  $x \in G$ ,

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

*Proof (Hints).*

- For  $1 \neq \gamma \in \hat{G}$ , consider  $y \in G$  with  $\gamma(y) \neq 1$ .
- For  $0 \neq x \in G$ , by considering  $G/\langle x \rangle$ , show by contradiction that there is  $\gamma \in \hat{G}$  with  $\gamma(x) \neq 1$ .

□

*Proof.* The first case for both equations is trivial. Let  $1 \neq \gamma \in \hat{G}$ . Then  $\exists y \in G$  with  $\gamma(y) \neq 1$ . So

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

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

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

**Definition 2.11** Given  $f : G \rightarrow \mathbb{C}$ , define the **Fourier transform** of  $f$  to be

$$\begin{aligned} \hat{f} : \hat{G} &\rightarrow \mathbb{C}, \\ \gamma &\mapsto \mathbb{E}_{x \in G} f(x) \overline{\gamma(x)}. \end{aligned}$$

**Proposition 2.12** (Fourier Inversion Formula) Let  $f : G \rightarrow \mathbb{C}$ . Then for all  $x \in G$ ,

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

*Proof (Hints).* Straightforward. □

*Proof.* We have

$$\begin{aligned} \sum_{\gamma \in \widehat{G}} \hat{f}(\gamma) \gamma(x) &= \sum_{\gamma \in \widehat{G}} \mathbb{E}_{y \in G} f(y) \overline{\gamma(y)} \gamma(x) \\ &= \mathbb{E}_{y \in G} f(y) \sum_{\gamma \in \widehat{G}} \gamma(x - y) \\ &= f(x) \end{aligned}$$

by the above lemma. □

**Definition 2.13** For  $A \subseteq G$ , the **indicator** (or **characteristic**) function of  $A$  is

$$\begin{aligned} \mathbb{1}_A : G &\rightarrow \{0, 1\}, \\ x &\mapsto \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}. \end{aligned}$$

**Definition 2.14**  $\hat{\mathbb{1}}_A(1) = \mathbb{E}_{x \in G} \mathbb{1}_A(x) \cdot 1 = |A|/|G|$  is the **density** of  $A$  in  $G$ . This is often denoted by  $\alpha$ .

**Definition 2.15** Given  $\emptyset \neq A \subseteq G$ , the **characteristic measure**  $\mu_A : G \rightarrow [0, |G|]$  is defined by

$$\mu_A(x) := \alpha^{-1} \mathbb{1}_A(x).$$

Note that  $\mathbb{E}_{x \in G} \mu_A(x) = 1 = \hat{\mu}_A(1)$ .

**Definition 2.16** The **balanced function**  $f_A : G \rightarrow [-1, 1]$  of  $A$  is given by

$$f_A(x) = \mathbb{1}_A(x) - \alpha.$$

Note that  $\mathbb{E}_{x \in G} f_A(x) = 0 = \hat{f}_A(1)$ .

**Example 2.17** Let  $V \leq \mathbb{F}_p^n$  be a subspace. Then for  $t \in \widehat{\mathbb{F}}_p^n$ ,

$$\begin{aligned} \hat{\mathbb{1}}_V(t) &= \mathbb{E}_{x \in \mathbb{F}_p^n} \mathbb{1}_V(x) e(-x.t/p) \\ &= \frac{|V|}{p^n} \mathbb{1}_{V^\perp}(t). \end{aligned}$$

where  $V^\perp = \{t \in \widehat{\mathbb{F}}_p^n : x.t = 0 \ \forall x \in V\}$  is the **annihilator** of  $V$ . Hence,  $\hat{\mathbb{1}}_V = \mu_{V^\perp}$ .

**Example 2.18** Let  $R \subseteq G$  be such that each  $x \in G$  lies in  $R$  independently with probability  $\frac{1}{2}$ . Then with high probability,

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

This follows from Chernoff's inequality.

**Theorem 2.19** (Chernoff's Inequality) Given complex-valued independent random variables  $X_1, \dots, X_n$  with mean 0, for all  $\theta > 0$ , we have

$$\Pr \left[ \left| \sum_{i=1}^n X_i \right| \geq \theta \sqrt{\sum_{i=1}^n \|X_i\|_{L^\infty(\text{Pr})}^2} \right] \leq 4 \exp(-\theta^2/4).$$

**Example 2.20** Let  $Q = \{x \in \mathbb{F}_p^n : x.x = 0\}$  with  $p > 2$ . Then  $|Q|/p^n = \frac{1}{p} + O(p^{-n/2})$  and  $\sup_{t \neq 0} |\hat{\mathbb{1}}_Q(t)| = O(p^{-n/2})$ .

**Lemma 2.21** (Plancherel's Identity) For all  $f, g : G \rightarrow \mathbb{C}$ ,

$$\langle f, g \rangle = \langle \hat{f}, \hat{g} \rangle.$$

*Proof.* Exercise. □

**Corollary 2.22** (Parseval's Identity) For all  $f, g : G \rightarrow \mathbb{C}$ ,

$$\|f\|_{L^2(G)}^2 = \|\hat{f}\|_{L^2(\hat{G})}^2.$$

*Proof (Hints).* Trivial from Plancherel. □

*Proof.* By Plancherel. □

**Definition 2.23** Let  $\rho > 0$  and  $f : G \rightarrow \mathbb{C}$ . The  **$\rho$ -large Fourier spectrum** of  $f$  is

$$\text{Spec}_\rho(f) := \left\{ \gamma \in \hat{G} : |\hat{f}(\gamma)| \geq \rho \|f\|_1 \right\}.$$

**Example 2.24** Let  $A \subseteq G$ , then  $\|f\|_1 = \alpha = |A|/|G|$ , so

$$\text{Spec}_\rho(\mathbb{1}_A) = \left\{ t \in \hat{\mathbb{F}}_p^n : |\hat{\mathbb{1}}_V(t)| \geq \rho \alpha \right\}.$$

In particular, if  $V \leq \mathbb{F}_p^n$  is a subspace, then by [Example 2.17](#),  $\text{Spec}_\rho(\mathbb{1}_V) = V^\perp$  for all  $\rho \in (0, 1]$ .

**Lemma 2.25** For all  $\rho > 0$ ,

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

In particular, if  $f = \mathbb{1}_A$  for  $A \subseteq G$ , then  $\|f\|_1 = \alpha = |A|/|G| = \|f\|_2^2$ . So  $|\text{Spec}_\rho(\mathbb{1}_A)| \leq \rho^{-2} \alpha^{-1}$ .

*Proof (Hints).* Use Parseval's identity. □

*Proof.* By Parseval's identity,

$$\begin{aligned}
\|f\|_2^2 &= \|\hat{f}\|_2^2 = \sum_{\gamma \in \hat{G}} |\hat{f}(\gamma)|^2 \\
&\geq \sum_{\gamma \in \text{Spec}_\rho(f)} |\hat{f}(\gamma)|^2 \\
&\geq |\text{Spec}_\rho(f)| (\rho \|f\|_1)^2.
\end{aligned}$$

□

**Definition 2.26** The **convolution** of  $f, g : G \rightarrow \mathbb{C}$  is

$$\begin{aligned}
f * g &: G \rightarrow \mathbb{C}, \\
x &\mapsto \mathbb{E}_{y \in G} f(y)g(x - y).
\end{aligned}$$

**Example 2.27** Given  $A, B \subseteq G$ ,

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

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

**Lemma 2.28** Given  $f, g : G \rightarrow \mathbb{C}$ ,

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

*Proof (Hints).* Straightforward. □

*Proof.* We have

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

□

**Example 2.29**  $\mathbb{E}_{x+y=z+w} f(x) f(y) \overline{f(z)} \overline{f(w)} = \|\hat{f}\|_{\ell^4(\hat{G})}^4$ . In particular,  $\|\hat{\mathbb{1}}_A\|_{\ell^4(\hat{G})}^4 = E(A)/|G|^3$  for any  $A \subseteq G$ .

**Theorem 2.30** (Bogolyubov's Lemma) Let  $A \subseteq \mathbb{F}_p^n$  be of density  $\alpha$ . Then there exists a subspace  $V \leq \mathbb{F}_p^n$  with  $\text{codim}(V) \leq 2\alpha^{-2}$ , such that  $V \subseteq A + A - A - A$ .

*Proof (Hints).*

- Let  $g = \mathbb{1}_A * \mathbb{1}_A * \mathbb{1}_{-A} * \mathbb{1}_{-A}$ , reason reason that if  $g(x) > 0$  for all  $x \in V$ , then  $V \subseteq 2A - 2A$ .
- Let  $S = \text{Spec}_\rho(\mathbb{1}_A)$ , with  $\rho$  for now unspecified.
- Show that  $g(x) = \alpha^4 + \sum_{t \in S \setminus \{0\}} |\hat{\mathbb{1}}_A(t)|^4 e(x.t/p) + \sum_{t \notin S} |\hat{\mathbb{1}}_A(t)|^4 e(x.t/p)$ .
- Find an appropriate subspace  $V$  from  $S$ , bound  $g(x)$  from below in terms of  $\rho$ , and use this to determine a suitable value for  $\rho$ .

□

*Proof.* Observe  $2A - 2A = \text{supp}(g)$  where  $g = \mathbb{1}_A * \mathbb{1}_A * \mathbb{1}_{-A} * \mathbb{1}_{-A}$ , so we want to find  $V \leq \mathbb{F}_p^n$  such that  $g(x) > 0$  for all  $x \in V$ . Let  $S = \text{Spec}_\rho(\mathbb{1}_A)$  with  $\rho$  a constant to be specified later, and let  $V = \langle S \rangle^\perp$ . By [Lemma 2.25](#),  $\text{codim}(V) = \dim \langle S \rangle \leq |S| \leq \rho^{-2} \alpha^{-1}$ . Fix  $x \in V$ . Now

$$\begin{aligned}
g(x) &= \sum_{t \in \hat{\mathbb{F}}_p^n} \hat{g}(t) e(x.t/p) \\
&= \sum_{t \in \hat{\mathbb{F}}_p^n} |\hat{\mathbb{1}}_A(t)|^4 e(x.t/p) \quad \text{by [Lemma 2.28](#)} \\
&= \alpha^4 + \sum_{t \neq 0} |\hat{\mathbb{1}}_A(t)|^4 e(x.t/p) \\
&= \alpha^4 + \sum_{t \in S \setminus \{0\}} |\hat{\mathbb{1}}_A(t)|^4 e(x.t/p) + \sum_{t \notin S} |\hat{\mathbb{1}}_A(t)|^4 e(x.t/p)
\end{aligned}$$

Each term in the first sum is non-negative, since  $\forall t \in S, x.t = 0$ . The absolute value of the second sum is bounded above, by the triangle inequality, by

$$\begin{aligned}
\sum_{t \notin S} |\hat{\mathbb{1}}_A(t)|^4 &\leq \sup_{t \notin S} |\hat{\mathbb{1}}_A(t)|^2 \sum_{t \notin S} |\hat{\mathbb{1}}_A(t)|^2 \\
&\leq \sup_{t \notin S} |\hat{\mathbb{1}}_A(t)|^2 \sum_{t \in \hat{\mathbb{F}}_p^n} |\hat{\mathbb{1}}_A(t)|^2 \\
&\leq (\rho \alpha)^2 \|\mathbb{1}_A\|_2^2 = \rho^2 \alpha^3
\end{aligned}$$

by [Example 2.24](#) and Parseval's identity. Note the second sum must be real since all other terms in the equation are. So we have  $g(x) \geq \alpha^4 - \rho^2 \alpha^3$ . Thus, it is sufficient that  $\rho^2 \alpha^3 \leq \frac{\alpha^4}{2}$ , so set  $\rho = \sqrt{\alpha/2}$ . Hence  $g(x) > 0$  (in fact,  $g(x) \geq \frac{\alpha^4}{2}$ ) for all  $x \in V$ , and  $\text{codim}(V) \leq 2\alpha^{-2}$ . □

**Example 2.31** The set  $A = \left\{ x \in \mathbb{F}_2^n : |x| \geq \frac{n}{2} + \frac{\sqrt{n}}{2} \right\}$  (where  $|x|$  is 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  $C \subseteq A + A$ . Hence, the  $2A - 2A$  part of Bogolyubov's lemma is necessary:  $2A$  is not sufficient.

**Lemma 2.32** Let  $A \subseteq \mathbb{F}_p^n$  have density  $\alpha$  with  $\sup_{t \neq 0} |\hat{\mathbb{1}}_A(t)| \geq \rho \alpha$  for some  $\rho > 0$ . Then there exists a subspace  $V \leq \mathbb{F}_p^n$  with  $\text{codim}(V) = 1$  and  $x \in \mathbb{F}_p^n$  such that

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

*Proof (Hints).*

- Let  $V = \langle t \rangle^\perp$  for some suitable  $t$  (can determine later).
- Define  $a_j = \frac{|A \cap (v_j + V)|}{|v_j + V|} - \alpha$  for each  $j \in [p]$ , where  $x.v_j = j$ .
- Show that  $\hat{1}_A(t) = \mathbb{E}_{j \in [p]} a_j e(-j/p)$ .
- Show that  $\mathbb{E}_{j \in [p]} a_j + |a_j| \geq \rho\alpha$ .

□

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

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

By the triangle inequality,  $\mathbb{E}_{j \in [p]} |a_j| \geq \rho\alpha$ . Note that  $\mathbb{E}_{j \in [p]} a_j = 0$ . So  $\mathbb{E}_{j \in [p]} a_j + |a_j| \geq \rho\alpha$ , so  $\exists j \in [p]$  such that  $a_j + |a_j| \geq \rho\alpha$ , hence  $a_j \geq \rho\alpha/2$ . So take  $x = v_j$ . □

**Notation 2.33** Given  $f, g, h : G \rightarrow \mathbb{C}$ , write

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

**Notation 2.34** Given  $A \subseteq G$ , write  $2 \cdot A = \{2a : a \in A\}$ . Note this is not the same as  $2A = A + A$ .

**Lemma 2.35** Let  $p \geq 3$  and  $A \subseteq \mathbb{F}_p^n$  be of density  $\alpha > 0$ , such that  $\sup_{t \neq 0} |\hat{1}_A(t)| \leq \varepsilon$ . Then the number of 3-APs in  $A$  differs from  $\alpha^3(p^n)^2$  by at most  $\varepsilon(p^n)^2$ .

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

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

By Plancherel's identity and [Lemma 2.28](#), this is equal to



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

But

$$\begin{aligned}
\left| \sum_{t \neq 0} \hat{\mathbb{1}}_{2 \cdot A}(t) \overline{\hat{\mathbb{1}}_A(t)}^2 \right| &\leq \sup_{t \neq 0} |\hat{\mathbb{1}}_A(t)| \sum_{t \neq 0} |\hat{\mathbb{1}}_{2 \cdot A}(t)| |\hat{\mathbb{1}}_A(t)| \\
&\leq \sup_{t \neq 0} |\hat{\mathbb{1}}_A(t)| \left( \sum_t |\hat{\mathbb{1}}_{2 \cdot A}(t)|^2 \sum_t |\hat{\mathbb{1}}_A(t)|^2 \right)^{1/2} \quad \text{by Cauchy-Schwarz} \\
&\leq \varepsilon \|\hat{\mathbb{1}}_{2 \cdot A}\|_2 \|\hat{\mathbb{1}}_A\|_2 \\
&= \varepsilon \cdot \alpha \quad \text{by Parseval.}
\end{aligned}$$

□

**Theorem 2.36** (Meshulam) Let  $A \subseteq \mathbb{F}_p^n$  be a set containing no non-trivial 3-APs. Then  $|A| = O(p^n / \log p^n)$ , i.e.  $\alpha = O(1/n)$ .

*Proof.* By assumption,  $T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) = |A| / ((p^n)^2) = \alpha / p^n$ . By the proof of the above lemma,

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

So provided that  $p^n \geq 2\alpha^{-2}$ , we have  $T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) \leq \alpha^3/2$ . So we have

$$\sup_{t \neq 0} |\hat{\mathbb{1}}_A(t)| \geq \frac{\alpha^2}{2}$$

So by (find lemma) with  $\rho = \frac{\alpha}{2}$ , there exists a subspace  $V = \mathbb{F}_p^n$  of codimension 1 and  $x \in \mathbb{F}_p^n$  such that  $|A \cap (x + V)| \geq (\alpha + \alpha^2/4)|V|$ .

We iterate this observation: let  $A_0 = A$ ,  $V_0 = \mathbb{F}_p^n$ ,  $\alpha_0 = |A_0|/|V_0|$ . At this  $i$ -th step, we are given a set  $A_{i-1} \subseteq V_{i-1}$  of density  $\alpha_{i-1}$  with no non-trivial 3-APs. Provided that  $p^{\dim(V_{i-1})} \geq 2\alpha_{i-1}^{-2}$ , there exists a subspace  $V_i \leq V_{i-1}$  of codimension 1 and  $x_i \in V_{i-1}$  such that

$$|(A - x_i) \cap V_i| = |A \cap (x_i + V_i)| \geq (\alpha_{i-1} + \alpha_{i-1}^2/4)|V_i|$$

So set  $A_i = (A - x_i) \cap V_i$ .  $A_i$  has density  $\alpha_i \geq \alpha_{i-1} + \alpha_{i-1}^2/4$ , and contains no non-trivial 3-APs (since the translate  $A - x_i$  contains no non-trivial 3-APs). Through this iteration, the density increases:

- from  $\alpha$  to  $2\alpha$  in at most  $\alpha/(\alpha^2/4) = 4\alpha^{-1}$  steps,
- from  $2\alpha$  to  $4\alpha$  in at most  $(2\alpha)/((2\alpha)^2/4) = 2\alpha^{-1}$  steps.
- and so on, ...

So the density reaches 1 in at most  $4\alpha^{-1}(1 + \frac{1}{2} + \frac{1}{4} + \dots) = 8\alpha^{-1}$  steps. The iteration 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 iterated again.

But we may assume that  $\alpha \geq \sqrt{2}p^{-n/4}$  (since otherwise we would be done), so  $\alpha^{-2} < \frac{1}{2}p^{n/2}$ , whence  $p^{n-8\alpha^{-1}} \leq p^{n/2}$ , i.e.  $\frac{n}{2} \leq 8\alpha^{-1}$ .  $\square$

**Remark 2.37** The current largest known subset of  $\mathbb{F}_3^n$  containing no non-trivial 3-APs has size  $2.2202^n$ .

**Lemma 2.38** Let  $A \subseteq [N]$  be of density  $\alpha > 0$  and contain no non-trivial 3-APs, with  $N > 50\alpha^{-2}$ . Let  $p$  be a prime with  $p \in [N/3, 2N/3]$ , and write  $A' = A \cap [p] \subseteq \mathbb{Z}/p$ . Then one of the following holds:

1.  $\sup_{t \neq 0} |\hat{1}_{A'}(t)| = \alpha^2/10$  (where the Fourier coefficient is computed in  $\mathbb{Z}/p$ ).
2. There exists an interval  $J \subseteq [N]$  of length  $N/3$  such that  $|A \cap J| \geq \alpha(1 + \alpha/400)|J|$ .

*Proof.* TODO: fill in details in proof.

We may assume that  $|A'| = |A \cap [p]| \geq \alpha(1 - \alpha/200)p$ , since otherwise  $|A \cap [p+1, N]| \geq \alpha N - (\alpha(1 - \alpha/200)p) = \alpha(N - p) + \frac{\alpha^2}{200}p \geq (\alpha + \alpha^2/400)(N - p)$  since  $p \geq N/3$ , which implies case 2 with  $J = [p+1, N]$ .

Let  $A'' = A' \cap [p/3, 2p/3]$ . Note that all 3-APs of the form  $(x, x+d, x+2d) \in A' \times A'' \times A''$  are in fact APs in  $[N]$ . If  $|A' \cap [p/3]|$  or  $|A' \cap [2p/3, p]|$  is at least  $\frac{2}{5}|A'|$ , then again we are in case 2. So we may assume that  $|A''| \geq |A'|/5$ . Now as in above lemmas, we have

$$\frac{\alpha''}{p} = \frac{|A''|}{p^2} = T_3(1_{A'}, 1_{A''}, 1_{A''}) = \alpha'(\alpha'')^2 + \sum_t \overline{\hat{1}_{A'}(t)} \hat{1}_{A''}(t) \hat{1}_{2 \cdot A''}(t)$$

where  $\alpha' = |A'|/p$  and  $\alpha'' = |A''|/p$ . So as before,

$$\frac{\alpha' \alpha''}{2} \leq \sup_{t \neq 0} |\hat{1}_{A'}(t)| \cdot \alpha''$$

provided that  $\alpha''/p \leq \frac{1}{2}\alpha'(\alpha'')^2$ , i.e.  $2/p \leq \alpha' \alpha''$  (check this inequality indeed holds). Hence,  $\sup_{t \neq 0} |\hat{1}_{A'}(t)| \geq \frac{\alpha' \alpha''}{2} \geq \frac{1}{2}\alpha(1 - \alpha/200)^2 \cdot \frac{2}{5} \geq \alpha^2/10$ . TODO: constants need to change somewhere here.  $\square$

**Lemma 2.39** Let  $m \in \mathbb{N}$ , and let  $\varphi : [m] \rightarrow \mathbb{Z}/p$  be given by  $\varphi(x) = tx$  for some  $t \neq 0$ . Given  $\varepsilon > 0$ , there exists a partition of  $[m]$  into progressions  $P_i$  of length  $\ell_i \in [\varepsilon\sqrt{m}/2, \varepsilon\sqrt{m}]$ , such that

$$\forall i, \quad \text{diam}(\varphi(P_i)) = \max_{x, y \in P_i} |\varphi(x) - \varphi(y)| \leq \varepsilon p$$

(where  $|\varphi(x) - \varphi(y)|$  views  $\varphi(x), \varphi(y) \in \{0, \dots, p-1\}$ ).

*Proof.* Let  $u = \lfloor \sqrt{m} \rfloor$  and consider  $0, t, \dots, ut$ . By the pigeonhole principle, there exists  $0 \leq v < w \leq u$  such that  $|wt - vt| = |(w-v)t| \leq p/u$ . Set  $s = w - v$ , so  $|st| \leq p/u$ . Divide  $[m]$  into residue classes mod  $s$ , each of which has size at least  $m/s \geq m/u$ .

But each residue class can be divided into APs of the form  $a, a+s, \dots, a+ds$  with  $\varepsilon u/2 < d \leq \varepsilon u$ . The diameter of the image of each progression under  $\varphi$  is  $|dst| \leq dp/u \leq \varepsilon up/u = \varepsilon p$ . □

**Lemma 2.40** Let  $A \subseteq [N]$  be of density  $\alpha > 0$ , let  $p$  be prime with  $p \in [N/3, 2N/3]$ , and write  $A' = A \cap [p] \subseteq \mathbb{Z}/p$ . Suppose that  $|\hat{1}_{A'}(t)| \geq \alpha^2/10$  for some  $t \neq 0$ . Then there exists a progression  $P \subseteq [N]$  of length at least  $\alpha^2 \sqrt{N}/500$  such that  $|A \cap P| \geq \alpha(1 + \alpha/80)|P|$ .

*Proof.* □

**Theorem 2.41** (Roth) Let  $A \subseteq [N]$  be a set containing no non-trivial 3-APs. Then  $|A| = O(N/\log \log N)$ .

*Proof.* □

**Example 2.42** (Behrend's Example) There exists a set  $A \subseteq [N]$  of size  $|A| \geq \exp(-c\sqrt{\log N})N$  containing no non-trivial 3-APs. □

### 3. Probabilistic tools

### 4. Further topics