Contents

1. Combinatorial methods

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

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

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

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

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

Proof. Trivial. □

Example 1.3 Let $A = [n] = \{1, ..., n\}$. Then $A + A = \{2, ..., 2n\}$ 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 $A = \{a_1, ..., a_n\}$ with $a_i < a_{i+1}$. Then $a_1 + a_1 < a_1 + a_2 < \cdots < a_1 + a_n < a_2 + a_n < \cdots < a_n + a_n$. Note this is not the only choice of increasing sequence that works, in particular, so does $a_1 + a_1 < a_1 + a_2 < a_2 + a_2 < a_2 + a_3 < a_2 + a_4 < \cdots < a_2 + a_n < a_3 + a_n < \cdots < a_n + a_n$. 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 step.

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. Note that $g \in A + B$ 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 $(A \cap B') + (A \cup B') \subseteq A + B'$.

$\square$

Proof. Assume $|A| + |B| < p + 1$, and WLOG that $1 \leq |A| \leq |B|$ and $0 \in A$ (by translation). We use induction on $|A|$. $|A| = 1$ is trivial. Let $|A| \geq 2$ and let $0 \neq a \in A$. Then since p is prime, $\{a, 2a, ..., pa\} = \mathbb{Z}/p$. 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 $|B'| = |B|$.

Now $1 \leq |A \cap B'| < |A|$ (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 $|A + B| = |A + B'| \geq |(A \cap B') + (A \cup B')| \geq |A \cap B'| + |A \cup B'| - 1 = |A| + |B| - 1$. $\square$

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. $\square$

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). $\square$

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 $\varphi : B \times (A - C) \to (A - B) \times (B - C)$, $\varphi(b, d) = (a_d - b, b - c_d)$ is injective (why?). The 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

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

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

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

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

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 $|A + B| \le K|A|$ for some $K \ge 1$. Then $\forall \ell, m \in \mathbb{N}_0$,

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

Proof (Hints).

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

□

Proof. Choose $\emptyset \ne A' \subseteq A$ which minimises $|A' + B|/|A'|$. Let the minimum value by K'. Then $|A' + B| = K'|A'|$, $K' \le K$ and $\forall A'' \subseteq A$, $|A'' + B| \ge K'|A''|$.

We claim that for every finite $C \subseteq G$, $|A' + B + C| \le K'|A' + C|$:

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', $|D + B| \ge K'|D|$. Hence,

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

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,

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

This proves the claim.

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

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

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

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

□

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's 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 $\forall \ell \geq 2$, $\ell A - A \subseteq (\ell - 1)X + A - A$:

$$\begin{aligned}\ell A - A &= A + (\ell - 1)A - A \\ &\subseteq (\ell - 2)X + 2A - A \\ &\subseteq (\ell - 2)X + X + A - A \\ &= (\ell - 1)X + A - A.\end{aligned}$$

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 $\{0, ..., p - 1\}$. Hence, $|Y| \leq p^{|X|} \leq p^{K^4}$. Finaly, $|H| \leq |Y||A - A| \leq p^{K^4}K^2|A|$ by Plunnecke's Inequality/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

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

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 **γ-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 $U = \left\{x \in G : |A\cap(x+A)| \leq \frac{1}{2}\eta|A|\right\}$. Then

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

For $0 \le i \le \lceil \log_2 \eta^{-1} \rceil$, let $Q_i = \{x \in G : |A|/2^{i+1} < |A \cap (x+A)| \le |A|/2^i\}$ and set $\delta_i = \eta^{-1} 2^{-2i}$. Then

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

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

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

Hence $\exists i_0$ such that

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

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

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

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

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

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

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

Therefore,

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

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

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

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 $|X|\ge\frac{\eta}{3}|A|$ 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 $G=(X\sqcup X,\{(x,y)\in X\times X : x-y\in P_{\eta/2^7}\})$ has at least $\frac{7}{8}|X|^2$ edges.

Let $A'=\left\{x\in X : \deg_G(x)\ge\frac{3}{4}|X|\right\}$. Clearly $|A'|\ge|X|/8$. 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

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

representations of the form $a_1-a_2-(a_3-a_4)$ with each $a_i\in A$. It follows that $\frac{\eta^3}{2^{17}}|A|^3|A'-A'|\le|A|^4$, hence $|A'-A'|\le 2^{17}\eta^{-3}|A|\le 2^{22}\eta^{-4}|A'|$, and so $|A'+A'|\le 2^{44}\eta^{-8}|A'|$. □

2. Fourier-analytic techniques

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

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

Notation 2.2 Norm and inner product notation:
- Write

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

- If Fourier support of function is restricted to $\Lambda \subseteq \widehat{G}$, 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

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

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

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

  i.e. $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$.
- 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 $\frac{1}{p} + \frac{1}{q}$, and $f \in L^p(G)$, $g \in L^q(G)$. Then

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

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

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

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

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

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 $\gamma \in \widehat{G}$, we have a corresponding character $\gamma(x) = e((\gamma.x)/p)$.
- If $G = \mathbb{Z}/N$, then any $\gamma \in \widehat{G}$ has a corresponding character $\gamma(x) = e(\gamma x/N)$.

Notation 2.9 Given a non-empty $B \subseteq G$ and $g : B \to \mathbb{C}$, 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 $x \in G$,

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

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

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

Proposition 2.12 (Fourier Inversion Formula) Let $f : G \to \mathbb{C}$. 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 Lemma 2.10. □

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

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

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 α.

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

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

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

Definition 2.16 The **balanced function** $f_A : G \to [-1,1]$ 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 $V^\perp = \{t \in \widehat{\mathbb{F}}_p^n : x.t = 0 \quad \forall x \in V\}$ 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,

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

This follows from Chernoff's inequality.

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

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

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

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

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

Proof. Exercise. □

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

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

Proof (Hints). Trivial from Plancherel's Identity. □

Proof. By Plancherel's Identity. □

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

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

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

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

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

Lemma 2.25 For all $\rho > 0$,

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

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

Proof (Hints). Use Parseval. □

Proof. By Parseval,

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

□

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

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

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

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

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

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

Theorem 2.30 (Bogolyubov's Lemma) Let $A \subseteq \mathbb{F}_p^n$ be of density α. Then there exists a subspace $V \leq \mathbb{F}_p^n$ with $\operatorname{codim}(V) \leq 2\alpha^{-2}$, 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 that if $g(x) > 0$ for all $x \in V$, then $V \subseteq 2A - 2A$.
- Let $S = \operatorname{Spec}_\rho(\mathbb{1}_A)$, with ρ for now unspecified.
- Show that $g(x) = \alpha^4 + \sum_{t \in S \setminus \{0\}} \left| \hat{\mathbb{1}}_A(t) \right|^4 e(x.t/p) + \sum_{t \notin S} \left| \hat{\mathbb{1}}_A(t) \right|^4 e(x.t/p)$.
- Find an appropriate subspace V from S, bound $g(x)$ from below in terms of ρ, and use this to determine a suitable value for ρ.

□

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

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

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

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

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

Example 2.31 The set $A = \left\{x \in \mathbb{F}_2^n : |x| \ge \frac{n}{2} + \frac{\sqrt{n}}{2}\right\}$ (where $|x|$ is number of 1s in x) has density $\ge \frac{1}{8}$ 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 α with $\sup_{t \ne 0}\left|\hat{\mathbb{1}}_A(t)\right| \ge \rho\alpha$ for some $\rho > 0$. Then there exists a subspace $V \le \mathbb{F}_p^n$ with $\operatorname{codim}(V) = 1$ and $x \in \mathbb{F}_p^n$ such that

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

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 $\hat{\mathbb{1}}_A(t) = \mathbb{E}_{j \in [p]} a_j e(-j/p)$.
- Show that $\mathbb{E}_{j \in [p]} a_j + |a_j| \ge \rho\alpha$.

□

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

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

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

Notation 2.33 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 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 $\sup_{t \neq 0}\left|\hat{\mathbb{1}}_A(t)\right| \leq \varepsilon$. Then the number of 3-APs in A differs from $\alpha^3(p^n)^2$ by at most $\varepsilon(p^n)^2$.

Proof (Hints).

- Express $T_3(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A)$ as an inner product of functions $\mathbb{F}_p^n \to \mathbb{C}$, rewrite as inner product of functions $\hat{\mathbb{F}}_p^n \to \mathbb{C}$.
- Find upper bound of the absolute value of a sub-sum of this inner product, using triangle inequality and Cauchy-Schwarz.

□

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

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

But

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

□

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 (Hints).

- Use similar proof as that of above lemma to show that $\left|T_3(\mathbb{1}_A,\mathbb{1}_A,\mathbb{1}_A) - \alpha^3\right| \leq \sup_{t\neq 0}\left|\hat{\mathbb{1}}_A(t)\right|\cdot\alpha$.
- Reason that provided $p^n \geq 2\alpha^{-2}$, we have $\sup_{t\neq 0}\left|\hat{\mathbb{1}}_A(t)\right| \geq \frac{\alpha^2}{2}$.
- Use this to iteratively generate A_1, V_1, A_2, V_2, ….
- Reason that each A_i contains no non-trivial 3 APs.
- Find an expression for maximum number of steps it takes for the density of the A_i to increase from $2^k\alpha$ to $2^{k+1}\alpha$ (in terms of k and α). Use this to deduce an upper bound for the maximum number steps it takes for the density to reach 1.
- Find lower bound for $\dim(V_m)$ where V_m is the final V_i in the sequence, use fact that iteration halted to deduce that $p^{\dim(V_m)} \leq 2\alpha^{-2}$.
- Reason that we can assume $\alpha \geq \sqrt{2}p^{-n/4}$, and conclude that $\alpha \leq 16n$.

□

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

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

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 $\left|T_3(\mathbb{1}_A,\mathbb{1}_A,\mathbb{1}_A) - \alpha^3\right| \geq \alpha^3/2$, hence

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

So by Lemma 2.32 with $\rho = \frac{\alpha}{2}$, there exists a subspace $V \leq \mathbb{F}_p^n$ of codimension 1 and $x \in \mathbb{F}_p^n$ such that $|A \cap (x+V)| \geq (\alpha + \alpha^2/4)|V|$.

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

So the density reaches 1 in at most $4\alpha^{-1}\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) = 8\alpha^{-1}$ 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. $\frac{n}{2} \leq 8\alpha^{-1}$. □

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

Proof (Hints).
- Show that we can assume $|A'| \geq \alpha(1 - \alpha/200)p$.

□

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

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

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

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

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

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

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

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

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

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 $\left|\hat{\mathbb{1}}_{A'}(t)\right| \ge \alpha^2/20$ for some $t \ne 0$. Then there exists a progression $P \subseteq [N]$ of length at least $\alpha^2\sqrt{N}/500$ such that $|A \cap P| \ge \alpha(1 + \alpha/80)|P|$.

Proof. Let $\varepsilon = \alpha^2/40\pi$ and use above lemma to partition $[p]$ into progressions P_i of length $\ge \varepsilon\sqrt{p/2} \ge \alpha^2/40\pi\frac{\sqrt{N/3}}{2} \ge \alpha^{\sqrt{N}}/500$, and $\operatorname{diam}(\varphi(P_i)) \le \varepsilon p$. Fix one x_i from each of the P_i. Then

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

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,

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

hence $\exists i$ such that

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

and so

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

$\square$

Definition 2.41 Let $\Gamma \subseteq \widehat{G}$ and $\rho > 0$. The **Bohr set** $B(\Gamma, \rho)$ is the set

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

The **rank** of $B(\Gamma, \rho)$ is $|B(\Gamma, \rho)|$, and is **width** (or **radius**) is ρ.

Example 2.42 Let $G = \mathbb{F}_p^n$, then $B(\Gamma, \rho) = \langle \Gamma \rangle^\perp$ for all sufficiently small ρ. Here, the rank gives an upper bound on $\operatorname{codim}(\langle \Gamma \rangle^\perp)$.

Lemma 2.43 Let $\Gamma \subseteq \widehat{G}$ and $|\Gamma| = d$, and let $\rho > 0$. Then

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

Proposition 2.44 (Bogolyubov's Lemma for Finite Abelian Groups) Let $A \subseteq G$ be of density $\alpha > 0$. Then there exists $\Gamma \subseteq \widehat{G}$ with $|\Gamma| \leq 2\alpha^{-2}$ such that

$$B\left(\Gamma, \frac{1}{2}\right) \subseteq A + A - (A + A).$$

Proof. Recall that

$$(\mathbb{1}_A * \mathbb{1}_A * \mathbb{1}_A * \mathbb{1}_A)(x) = \sum_{\gamma \in \widehat{G}} \left| \widehat{\mathbb{1}}_A(\gamma) \right|^4 \gamma(x)$$

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

$$\operatorname{Re}\left(\sum_{\gamma \in \widehat{G}} \left| \widehat{\mathbb{1}}_A(\gamma) \right|^4 \gamma(x) \right) = \operatorname{Re}\left(\sum_{\gamma \in \Gamma} \right) \left| \widehat{\mathbb{1}}_A(\gamma) \right|^4 \gamma(x)) + \operatorname{Re}\left(\sum_{x \notin \Gamma} \right) \left| \widehat{\mathbb{1}}_A(\gamma) \right|^4 \gamma(x))$$

and

$$\left|\operatorname{Re}\left(\sum_{\gamma\notin\Gamma}\left|\hat{\mathbb{1}}_A(\gamma)\right|^4\gamma(x)\right)\right|) \leq \sup_{\gamma\notin\Gamma}\left|\hat{\mathbb{1}}_A(\gamma)\right|^2\sum_{\gamma\notin\Gamma}\left|\hat{\mathbb{1}}_A(\gamma)\right|^2$$

$$\leq\left(\sqrt{\frac{\alpha}{2}}\cdot\alpha\right)^2\cdot\alpha=\frac{\alpha^4}{2}$$

by Parseval. □

Theorem 2.45 (Roth) Let $A\subseteq[N]$ be a set containing no non-trivial 3-APs. Then $|A| = O(N/\log\log N)$.

Proof.

□

Example 2.46 (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

All probability spaces here will be finite.

Theorem 3.1 (Khintchine's Inequality) Let $p\in[2,\infty)$. Let $X_1,...,X_n$ be independent random variables such that

$$\forall i\in[n],\quad \mathbb{P}(X_i=x_i)=\mathbb{P}(X_i=-x_i)=\frac{1}{2}$$

for some $x_1,...,x_n\in\mathbb{C}$. Then

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

Proof. Since L_p norms are nested, it suffices to prove in the case that $p=2k$ for some $k\in\mathbb{N}$. Write $X=\sum_{i=1}^n X_i$, and assume the quantity $\sum_{i=1}^n\|X_i\|_{L^\infty(\mathbb{P})}^2=\sum_{i=1}^n|x_i|^2=\sum_{i=1}^n\|X_i\|_{L^2(\mathbb{P})}^2$ is equal to 1. By Chernoff's Inequality, $\forall\theta>0$,

$$\Pr(|X|\geq\theta)\leq 4\exp(-\theta^2/4),$$

and so, since $\int_0^t P_X(s)\,\mathrm{d}s=\Pr(|X|\leq t)$,

$$\begin{aligned}\|X\|_{L^{2k}(\Pr)}^{2k}&=\int_0^\infty t^{2k}P_X(t)\,\mathrm{d}t\\&=\int_0^\infty 2kt^{2k-1}\Pr(|X|\geq t)\,\mathrm{d}t \text{ by integration by parts}\\&\leq 8k\int_0^\infty t^{2k-1}\exp(-t^2/4)\,\mathrm{d}t=:8kI(k)\end{aligned}$$

We will show by induction on k that $I(k)\leq 2^{2k}(2k)^k/4k$. Indeed, when $k=1$,

$$\int_0^\infty t\exp(-t^2/4)\,\mathrm{d}t = \left[-2\exp(-t^2/4)\right]_0^\infty = 2$$
$$= 2^{2\cdot 1}(2\cdot 1)^1/(4\cdot 1)$$

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

$$\begin{aligned}
I(k) &:= \int_0^\infty \underbrace{t^{2k-2}}_{u} \cdot \underbrace{t\exp(-t^2/4)}_{v'}\,\mathrm{d}t \\
&= \left[t^{2k-2}\cdot(-2\exp(-t^2/4))\right]_0^\infty - \int_0^\infty (2k-2)t^{2k-3}\cdot(-2\exp(-t^2/4))\,\mathrm{d}t \\
&= 4(k-1)\int_0^\infty t^{2(k-1)-1}\exp(-t^2/4)\,\mathrm{d}t \\
&= 4(k-1)I(k-1) \\
&\le \frac{4(k-1)2^{2k-1}(2(k-1))^{k-1}}{4(k-1)} \quad \text{by induction hypothesis} \\
&\le \frac{2^{2k}(2k)^k}{4k}.
\end{aligned}$$

□

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

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

Proof. Exercise. □

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

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

Proof. Let $f \in L^p(\mathbb{F}_2^n)$ and let $g(x) = \sum_{\gamma\in\Gamma} \hat{f}(\gamma)\gamma(x)$, so $g = f|_\Gamma$?. Then

$$\begin{aligned}
\left\|\hat{f}\right\|_{\ell^2(\Gamma)}^2 &= \sum_{\gamma\in\Gamma} \left|\hat{f}(\gamma)\right|^2 \\
&= \langle \hat{f}, \hat{g}\rangle_{\ell^2(\Gamma)} = \langle \hat{f}, \hat{g}\rangle_{\ell^2\left(\widehat{\mathbb{F}}_2^n\right)} \\
&= \langle f, g\rangle_{L^2(\mathbb{F}_2^n)} && \text{by Plancherel's Identity} \\
&\le \|f\|_{L^p(\mathbb{F}_2^n)}\|g\|_{L^q(\mathbb{F}_2^n)} && \text{by Holder‘s inequality.}
\end{aligned}$$

where $1/p + 1/q = 1$. By Rudin's Inequality,

$$
\begin{aligned}
\|g\|_{L^q(\mathbb{F}_2^n)} &= O\left(\sqrt{q}\cdot\|\hat{g}\|_{\ell^2(\Gamma)}\right)\\
&= O\left(\sqrt{\frac{p}{p-1}}\cdot\left\|\hat{f}\right\|_{\ell^2(\Gamma)}\right).
\end{aligned}
$$

□

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

Theorem 3.4 (Special Case of Chang's Theorem) Let $A\subseteq\mathbb{F}_2^n$ be of density of $\alpha>0$. Then

$$\forall\rho>0,\exists H\le\widehat{\mathbb{F}}_2^n:\dim(H)=O(\rho^{-2}\log\alpha^{-1})\text{ and }\mathrm{Spec}_\rho(\mathbb{1}_A)\subseteq H.$$

Proof. Let $\Gamma\subseteq\mathrm{Spec}_\rho(\mathbb{1}_A)$ be maximal linearly independent set. Let $H=\langle\mathrm{Spec}_\rho(\mathbb{1}_A)\rangle$. Clearly $\dim(H)=|\Gamma|$. By Dual Rudin, $\forall p\in(1,2]$,

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

Hence, $|\Gamma|\le O\left(\rho^{-2}\alpha^{-2}\alpha^{2/p}\frac{p}{p-1}\right)$. Setting $p=1+\left(\log\alpha^{-1}\right)^{-1}$, we obtain $|\Gamma|\le O(\rho^{-2}\alpha^{-2}(\alpha^2e^2)(\log\alpha^{-1}+1))=O(\rho^{-2}\log\alpha^{-1})$. □

Definition 3.5 Let G be a finite abelian group. $S\subseteq G$ is **dissociated** if $\sum_{s\in S}\varepsilon_s s=0$ with each $\varepsilon_s\in\{-1,0,1\}$, then $\varepsilon_s=0$ for all $s\in S$.

Example 3.6 Clearly, if $G=\mathbb{F}_2^n$, then $S\subseteq G$ is dissociated iff S is linearly independent.