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 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, $\{a, 2a, ..., pa\} = \mathbb{Z}/p$.
- 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 $\varphi : B \times (A - C) \to (A - B) \times (B - C)$, $\varphi(b, d) = (a_d - b, b - c_d)$ 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 $\sigma(A) \coloneqq |A + A|/|A|$.

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

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

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

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 $|A + B| \leq K|A|$ 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 by 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 $\{0, ..., p - 1\}$. 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

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

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 **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 $\sum_{x \in U} |A \cap (x + A)|^2 \leq \frac{1}{2}\eta|A| \sum_{x \in G}|A \cap (x + A)| = \frac{1}{2}\eta|A|^3 = \frac{1}{2}E(A)$.
- For $0 \leq i \leq \lceil \log_2 \eta^{-1} \rceil$, let $Q_i = \left\{x \in G : |A|/2^{i+1} < |A \cap (x + A)| \leq |A|/2^i\right\}$ 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 $S = \left\{(a, b) \in A^2 : a - b \notin P_{c\eta}\right\}$. 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

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

- 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,

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

- 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

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

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

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

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

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 $\gamma(x) = e((\gamma.x)/p)$.
- 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 $g : B \to \mathbb{C}$, 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 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 the above lemma. □

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

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

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

Proof. Exercise. □

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

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

Proof (Hints). Trivial from Plancherel. □

Proof. By Plancherel. □

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

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

Example 2.24 By the previous example, if $f = \mathbb{1}_V$ with $V \leq \mathbb{F}_p^n$ a subspace, then for all $\rho \in (0, 1]$,

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

Lemma 2.25 For all $\rho > 0$,

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

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

Proof. By Parseval's identity,

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

□

Remark 2.26 In particular, if $f = \mathbb{1}_A$ for $A \subseteq G$, then $\|f\|_1 = \alpha = |A|/|G| = \|f\|_2^2$. So $\left|\operatorname{Spec}_\rho(\mathbb{1}_A)\right| \leq \rho^{-2}\alpha^{-1}$.

Definition 2.27 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 2.28 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 2.29 Given $f, g : G \to \mathbb{C}$,

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

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 2.30 $\mathbb{E}_{x+y=z+w} f(x) f(y) \overline{f(z) f(w)} = \left\|\hat{f}\right\|_{\ell^4(\widehat{G})}^4$. In particular, $\left\|\hat{\mathbb{1}}_A\right\|_{\ell^4(\widehat{G})}^4 = E(A)/|G|^3$ for any $A \subseteq G$.

Theorem 2.31 (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. 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 $V \leq \mathbb{F}_p^n$ such that $g(x) > 0$ for all $x \in V$.

Now

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

since first sum is $\geq (\rho\alpha)^4$ as $x.t = 0$ $\forall t \in S$ absolute value of each term in the second sum is $\leq \sup_{t\notin S}\left|\hat{\mathbb{1}}_A(t)\right|^2 \sum_{t\notin S}\left|\hat{\mathbb{1}}_A\right|^2 \leq \sup_{t\notin S}\left|\hat{\mathbb{1}}_A(t)\right|^2 \sum_{t\in\mathbb{F}_p^n}\left|\hat{\mathbb{1}}_A\right|^2 \leq (\rho\alpha)^2 \leq \|\mathbb{1}_A\|_2^2 = \rho^2\alpha^3$ by Parseval. So we want $\rho^2\alpha^3 \leq \frac{\alpha^4}{2}$, so set $\rho = \sqrt{a/2}$. Hence $g(x) > 0$ (in fact, $g(x) \geq \frac{\alpha^4}{2}$) for all $x \in V$, and $\operatorname{codim}(V) \leq 2\alpha^{-2}$.

Let $S = \operatorname{Spec}_\rho(\mathbb{1}_A)$ with $\rho = ...$, and let $V = \langle S\rangle^\perp$. By Lemma 2.25, $\operatorname{codim}(V) \leq |S| \leq \rho^{-2}\alpha^{-1}$. Fix $x \in V$. □

Example 2.32 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 $C \subseteq A + A$.

Lemma 2.33 Let $A \subseteq \mathbb{F}_p^n$ have density α with $\sup_{t\neq 0}\left|\hat{\mathbb{1}}_A(t)\right| \geq \rho\alpha$ for some $\rho > 0$. Then there exists a subspace $V \leq \mathbb{F}_p^n$ with $\operatorname{codim}(V) = 1$ and $x \in \mathbb{F}_p^n$ such that

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

Proof. 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 $\hat{\mathbb{1}}_A(t) = \hat{f}_A(t) = \mathbb{E}_{x\in\mathbb{F}_p^n}(\mathbb{1}_A(x) - \alpha)e(-x.t/p) = \mathbb{E}_{j\in[p]}\mathbb{E}_{x\in v_j+V}(\mathbb{1}_A(x) - \alpha)e(-j/p) = \mathbb{E}_{j\in[p]}\left(\frac{|A\cap(v_j+V)|}{|v_j+V|} - \alpha\right)e(-j/p) =: \mathbb{E}_{j\in[p]}a_j e(-j/p)$. 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 $a_j \geq \rho\alpha/2$. □

3. Probabilistic tools

4. Further topics