

# Contents

1. Combinatorial methods .....	2
2. Fourier-analytic techniques .....	7
3. Probabilistic tools .....	7
4. Further topics .....	7

# 1. Combinatorial methods

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

*Proof.* Trivial. □

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

**Lemma.** 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.** 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.** 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** (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.** 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.** 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.** 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.** 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** (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  $(A - B) \times (B - C)$ .

□

*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.

□

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

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

**Remark.** 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.** 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** (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.

□

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

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

*Proof.*

- Observe that

$$\begin{aligned} E(A, B) &= |\{(a, a', b, b') \in A^2 \times B^2 : a + b = a' + b'\}| \\ &= \sum_{x \in G} r_{A+B}(x)^2 \end{aligned}$$

□

## 2. Fourier-analytic techniques

## 3. Probabilistic tools

## 4. Further topics