Contents

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 $A = [n] = \{1, ..., n\}$. Then $A + A = \{2, ..., 2n\}$ 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 $A = \{a_1, ..., a_n\}$ 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. 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 $1 \le |A| \le |B|$ 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 $1 \le |A| \le |B|$ and $0 \in A$ (by translation).
- Use induction on $|A|$. $|A| = 1$ is trivial.
- Let $|A| \ge 2$ and let $0 \ne a \in A$. Then since p is prime, $\{a, 2a, ..., pa\} = \mathbb{Z}/p$.
- There exists $m \ge 0$ such that $ma \in B$ but $(m+1)a \notin B$ (why?). Let $B' = B - ma$, so $0 \in B'$, $a \notin B'$ and $|B'| = |B|$.
- $1 \le |A \cap B'| < |A|$ (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 $|A + B| = |A + B'| \ge |(A \cap B') + (A \cup B')| \ge |A \cap B'| + |A \cup B'| - 1 = |A| + |B| - 1$.

□

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 $|A + A| \le \frac{3}{2}|A|$. Then there exists a subspace $V \subseteq \mathbb{F}_p^n$ such that $|V| \le \frac{3}{2}|A|$ 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

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

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 $\varphi : B \times (A-C) \to (A-B) \times (B-C)$, $\varphi(b,d) = (a_d - b, b - c_d)$ is injective (why?).
- Triangle inequality now follows from definition of Ruzsa distance.

□

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

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

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

2. Fourier-analytic techniques

3. Probabilistic tools

4. Further topics