Sum Product Theorems and Applications (Spring 2022, Weikun He)

Ajorda Jiao

Contents

Theorem 0.1 (Erdös-Szemerédi Theorem)
There exists an absolute constant $c > 0$, such that for every finite set $A \subseteq \mathbb{R}$,

$$\max \{\sharp(A+A), \sharp AA\} \geqslant c(\sharp A)^{1+c}.$$

§1 Basic additive combinatorics

$(E, +)$ abelian group. $A, B \subseteq E$.

Notation 1.1. $A + B \coloneqq \{a + b : a \in A, b \in B\}$.

> **Question 1.2** (Freiman)**.** If $\sharp(A + A) \leqslant K\sharp A$, for some parameter K, what can we say about A?

Observation 1.3. If A is a **arithmetic progression**, then $\sharp(A + A) \leqslant 2\sharp A$. If A is a **generalized A.P.** of **rank** r, i.e.

$$A = \{a_0 + t_1 d_1 + \cdots + t_r d_r : \forall i, 1 \leqslant t_i \leqslant N_i\},$$

then $\sharp(A + A) \leqslant 2^r \sharp A$.

Freiman Type Theorem If $\sharp(A + A) \leqslant K\sharp A$, then exists

(i) $P \subseteq E$ is a generalized arithmetic progression of rank $O_K(1)$, $\sharp P = O_K(\sharp A)$.

(ii) $X \subseteq E$ finite, $\sharp X = O_K(1)$.

Such that $A \subseteq P + X$.

Theorem 1.4 (Szemerédi)
$A \subseteq \mathbb{N}$ with positive upper density, then A contains arbitrarily long A.P.

Lemma 1.5 (Ruzsa Triangle Inequality)
$A, B, C \subseteq (E, +)$ finite, then

$$\sharp(A - C)\sharp B \leqslant \sharp(A - B)\sharp(B - C).$$

Proof. Construct a map $(A - C) \times B \to (A - B) \times (B - C), (x, b) \mapsto (a_x - b, b - c_x)$, where $x = a_x - b_x$ is a typical decomposition, this map is an injective. ☐

Definition 1.6. Define the **Ruzsa distance** between A, B by

$$d(A, B) = \log \frac{\sharp(A - B)}{(\sharp A)^{\frac{1}{2}} (\sharp B)^{\frac{1}{2}}}.$$

Lemma 1.7 (Ruzsa Covering Lemma)
$A, B \subseteq (E, +)$ finite, $K \geqslant 1$. If $\sharp(A+B) \leqslant K\sharp A$, then $\exists X \subseteq E, \sharp X \leqslant K$, such that $B \subset A - A + X$.

Proof. Let $X \subseteq B$ be the maximal set such that $(x+A)_{x\in X}$ is pointwise disjoint. $\square$

Notation 1.8. $\mathbb{O}(K)$ denotes some subset of cardinality $\leqslant K$.

Remark 1.9 — Ruzsa Covering Lemma $\iff B \subseteq A - A + \mathbb{O}\left(\frac{\sharp(A+B)}{\sharp A}\right)$.

Proposition 1.10 (Plünnecke-Ruzsa Inequality)
$A, B \subseteq E$ finite, $K \geqslant 1$. If $\sharp(A+B) \leqslant K\sharp A$, then $\forall k, l \geqslant 0$, we have

$$\sharp\left(\sum_k B - \sum_l B\right) \leqslant K^{k+l}\sharp A,$$

where $\sum_k B \coloneqq \underbrace{B + B + \cdots + B}_{k\ B\text{s}}$.

Lemma 1.11 (Petridis)
If $\sharp(A+B) \leqslant K\sharp A$, then $\exists A_0 \subseteq A$, such that for every $C \subset E$ finite,

$$\sharp(C + A_0 + B) \leqslant K\sharp(C + A_0).$$

Proof. Let $K_0 \coloneqq \inf_{A'\subseteq A} \frac{\sharp(A'+B)}{\sharp A'} \leqslant K$ and $A_0 \subseteq A$ such that $K_0 = \frac{\sharp(A_0+B)}{\sharp A_0}$. Applying induction to $\sharp C$, consider $C' = C \cup \{c\}$, where $c \notin C$. WLOG, assume $c = 0$. Then

$$\sharp(C' + A_0 + B) = \sharp(C + A_0 + B) + \sharp(A_0 + B) - \sharp((C + A_0 + B) \cap (A_0 + B)).$$

Observe that $((C + A_0) \cap A_0) + B \subseteq (C + A_0 + B) \cap (A_0 + B)$. By assumption,

$$(C + A_0) \cap A_0 \subseteq A \implies \sharp((C + A_0) \cap A_0) + B \geqslant K_0\sharp((C + A_0) \cap A_0).$$

Hence by inductive assumption,

$$\sharp(C' + A_0 + B) \leqslant K_0(\sharp(C + A_0) + \sharp A_0 - \sharp((C + A_0) \cap A_0)) = K_0\sharp(C' + A_0).$$

$\square$

Proof of Plünnecke-Ruzsa Inequality 1.10. Applying lemma, we have

$$\sharp(B + A_0) \leqslant K\sharp A_0, \quad \sharp(B + B + A_0) \leqslant K\sharp(B + A_0) \leqslant K^2\sharp A_0, \quad \cdots.$$

Hence, $\sharp\left(\sum_k B + A_0\right) \leqslant K^k\sharp A_0$. Finally, applying Ruzsa triangle inequality, we have

$$\sharp\left(\sum_k B - \sum_l B\right) \leqslant \frac{\sharp\left(\sum_k B + A_0\right)\sharp\left(\sum_l B + A_0\right)}{\sharp A_0} \leqslant K^{k+l}\sharp A_0 \leqslant K^{k+l}\sharp A.$$

$\square$

Question 1.12. If E is not an abelian group, does the arguments still hold?

Answer Ruzsa triangle inequality, Ruzsa covering lemma, Petridis lemma still hold, but Plünnecke-Ruzsa inequality **fails**. See the following examples.

Example 1.13

G non abelian group. Take $A = H \cup \{a\}$, where H is a subgroup of G and $a \notin H$. Then $AA = H \cup aH \cup Ha \cup \{a\}$. Assume $\sharp H = N$, then $\sharp(AA) \leqslant 3N + 1 \leqslant \sharp A$. Consider $AAA \supseteq HaH$, if $aHa^{-1} \cap H = \{1\}$, then $\sharp(HaH) = N^2$. Explicitly, we can choose $G = S_{N+1}$, $H = \langle(123 \cdots N)\rangle$ and $a = (N\ (N+1))$. Hence for any $N > 0$, there exists A such that $\sharp(AA) \leqslant 3\sharp A$ but $\sharp(AAA) \geqslant N\sharp A$.

§2 Sum-product theorems

Let $(E, 0, 1, +, \cdot)$ be a ring, $A \subseteq E$ finite set, $K \geqslant 1$ parameter.
Let $E^\times = \{\text{invertible elements in } E\}$.

Definition 2.1. Let $R(A, K) \coloneqq \{x \in E : \sharp(A + xA) \leqslant K\sharp A\}$.

The following lemma shows that $R(A, K)$ has an "almost" ring structure.

Lemma 2.2

The following holds:

1. If $x \in R(A, K) \cap E^\times$, then $x^{-1} \in R(A, K)$.
2. If $1, x, y \in R(A, K)$, then $x + y, x - y, xy \in R(A, K^{O(1)})$, where $O(1) = 8$ is enough.

Proof. 1. Trivial.

2. If $x, y \in R(A, K)$, by Ruzsa covering lemma, we have

$$xA \subseteq A - A + \mathbb{O}(K), \quad yA \subseteq A - A + \mathbb{O}(K).$$

then $A + (x + y)A \subseteq \sum_3 A - \sum_2 A + \mathbb{O}(K^2)$. Because $1 \in R(A, K)$, hence by P-R, we have $\sharp\left(\sum_3 A - \sum_2 A\right) \leqslant K^5\sharp A$. Then $\sharp(A + (x + y)A) \leqslant K^7\sharp A$. Similarly, we can prove $\sharp(A + xyA) \leqslant K^8\sharp A$.

□

Notation 2.3. For $s \in \mathbb{N}$, let $\sum_{\leqslant s} A = \bigcup\limits_{1 \leqslant k \leqslant s} \sum_k A$, let $\prod_{\leqslant s} A = \bigcup\limits_{1 \leqslant k \leqslant s} \prod_k A$. Let

$$\langle A \rangle_s = \sum_{\leqslant s} \prod_{\leqslant s} A - \sum_{\leqslant s} \prod_{\leqslant s} A.$$

Notation 2.4. $O_s(1)$ denotes a constant which just depend on s.

Lemma 2.5 (Ring Version of P-R)

Assume $\sharp(A+AA) \leqslant K\sharp A$, then $\sharp\left\langle A\right\rangle_s \leqslant K^{O_s(1)}\sharp A$.

Remark 2.6 — $\sharp(A+A) \leqslant K\sharp A$ and $\sharp(AA) \leqslant K\sharp A$ do not imply $\sharp(A+AA) \leqslant K^{O(1)}\sharp A$. For a counter example, we consider $A = \sqrt{-1}\mathbb{F}_p \subseteq \mathbb{F}_p[\sqrt{-1}]$ for some $p = 4k+3$ and $K = 1$, then $\sharp(A+AA) = p^2 = p\sharp A$.

Proof. By R-covering, we have $AA \subseteq A - A + \mathbb{O}(K)$. Let $X = \mathbb{O}(K)$, note that X could be chose in AA. Because $A \subseteq R(A,K)$ and $1 \in R(A,K^2)$ for $\sharp A \geqslant 2$, then $AA \subseteq R(A, K^{O(1)})$. Then

$$AAA \subseteq AA - AA + \bigcup_{x\in X} xA \subseteq \sum_2 A - \sum_2 A + \mathbb{O}(K^2) + \bigcup_{x\in X}(A - A + \mathbb{O}(K^{O(1)})),$$

hence $AAA \subseteq \sum_3 A - \sum_3 A + \mathbb{O}(K^{O(1)})$. By induction, we can prove the theorem. $\square$

As the consequence of this lemma, we have $\left\langle A\right\rangle_s \subseteq R(A, K^{O_s(1)})$ if $A \subseteq R(A,K)$.

From now on, let E be a field, $A \subset E$ finite, $K \geqslant 1$.

Notation 2.7. Denote $f \ll g$ if there is an absolute constant $C > 0$ such that $f \ll Cg$.

Theorem 2.8 (Sum-Product Theorem in Fields)

Assume $\sharp(A+AA) \leqslant K\sharp A$, then

(1) either $\sharp A \ll K^{10000}$.

(2) or $\exists$ finite subfield F, such that $A \subseteq F$ and $\sharp F \ll K^{10000}\sharp A$.

Remark 2.9 — If $E = \mathbb{R}$, then for every $A \subseteq \mathbb{R}$, $\sharp(A+AA) \geqslant (\sharp A)^{1+\frac{1}{10000}}$.

Lemma 2.10

For any $x \in E$, if $\sharp(A+xA) < (\sharp A)^2$, then $x \in \frac{A-A}{(A-A)\setminus\{0\}}$.

Proof of Theorem 2.8. Let $F = \frac{A-A}{(A-A)\setminus\{0\}}$. Consider $K = (\sharp A)^{\frac{1}{10000}}$, the lemma shows that $R(A, K^{9999}) \subseteq F$. By assumption, $A \subseteq R(A,K)$, hence $A \subseteq R(A,K^2)$ by P-R if $\sharp A \geqslant 2$. By "almost" ring structure, we have $A - A \subseteq R(A, K^{20})$ and $((A-A)\setminus\{0\})^{-1} \subseteq R(A,K^{20})$, hence $F \subseteq R(A, K^{200})$. Furthermore, $F+F, FF \subseteq R(A, K^{2000}) \subseteq F$. Hence F is a finite field.

Now, we estimate $\sharp F$. There are two methods. One way is to consider a map

$$F \times (A \setminus \{0\}) \to (AA - AA) \times (AA - AA), \quad (x,a) \mapsto (au_x, bv_x),$$

where $u_x, v_x \in A - A$ are typical of writing $x = \frac{u_x}{v_x}$. The map is injective, hence $(\sharp F)(\sharp A - 1) \leqslant (\sharp(AA-AA))^2 \leqslant K^4(\sharp A)^2$ by P-R.

Another way is to use energy argument, see definition 3.1. Consider

$$(\sharp A)^4 = \sum_{x\in F} \sharp\left\{a, b, a', b' \in A : ax + b = a'x + b'\right\} \geqslant \sum_{x\in F} \frac{(\sharp A)^4}{\sharp(A + xA)} \geqslant \sharp F \frac{(\sharp A)^3}{K^{200}}.$$

Hence $\sharp F \leqslant K^{200} \sharp A$. $\square$

Corollary 2.11

If $\sharp(AA) \leqslant K\sharp A, \sharp(A + A) \leqslant K\sharp A$, then

(1) either $\sharp A \ll K^{O(1)}$.

(2) or $\exists$ finite subfield F, $\exists a \in E$, such that $\sharp(A \cap aF) \gg \frac{\sharp A}{K^{O(1)}}$ and $\sharp F \ll K^{O(1)}\sharp A$.

Lemma 2.12 (Katz-Tao Lemma)

Assume $\sharp(A + A) \leqslant K\sharp A, \sharp(A + A) \leqslant K\sharp A$. Then $\exists A' \subseteq A$ such that

$$\sharp A' \gg \frac{1}{K^{O(1)}}\sharp A \quad \text{and} \quad \sharp(A'A' - A'A') \ll K^{O(1)}\sharp A'.$$

Proof of Corollary 2.11 assuming Lemma 2.12. Take such A' in lemma, we choose $a \in A' \setminus \{0\}$, let $B = a^{-1}A'$. Then $1 \in B$ and $B - BB \subseteq BB - BB$, hence $\sharp(B - BB) \leqslant K^{O(1)}\sharp B$. Then $\sharp(B + BB) \leqslant K^{O(1)}\sharp B$ by P-R and R-covering. Applying Theorem 2.8 to B, the corollary follows. $\square$

Notation 2.13. Denote $f \lesssim g$ if $f \ll K^{O(1)}g$, denote $f \approx g$ if $f \lesssim g$ and $g \lesssim f$.

Proof of Katz-Tao Lemma 2.12. Consider the function $\varphi = \sum_{a\in A} \mathbb{1}_{aA}$ defined on AA. Endowing AA with counting measure, then

$$(\sharp A)^4 = \|\varphi\|_1^2 \leqslant \|\varphi\|_2^2 \|1\|_2^2 = \sharp(AA) \left\| \sum_{a,b\in A} \mathbb{1}_{aA\cap bA} \right\|_1 \leqslant K\sharp A \sum_{a,b\in A} \sharp(aA \cap bA).$$

Therefore, $\exists b \in A$ such that $\frac{1}{\sharp A}\sum_{a\in A} \sharp(aA \cap bA) \geqslant \frac{\sharp A}{K}$. Consider

$$A' := \left\{a \in A : \sharp(aA \cap bA) \geqslant \frac{\sharp A}{2K}\right\},$$

then $\sharp A' \geqslant \frac{\sharp A}{2K}$. Hence for every $a \in A'$, by R-triangle,

$$\sharp(aA + bA) \leqslant \frac{\sharp(aA + aA \cap bA)\sharp(bA - aA \cap bA)}{\sharp(aA \cap bA)} \lesssim \frac{\sharp(A + A)\sharp(A - A)}{\sharp A} \lesssim \sharp A.$$

By R-covering, $aA \subseteq bA - bA + \mathbb{O}(K^{O(1)})$. Then for every $a_1, a_2, a_3, a_4 \in A$,

$$(a_1a_2 - a_3a_4)A \subseteq b^2 \left(\sum_4 A - \sum_4 A\right) + \mathbb{O}(K^{O(1)}).$$

Let $d = a_1 a_2 - a_3 a_4$, then $dA \subseteq \bigcup_{x\in X} \left(b^2 \left(\sum_4 A - \sum_4 A\right) + x\right)$ where $\sharp X \lesssim 1$. Then $\exists x$ such that $\sharp \left(dA \cap \left(b^2 \left(\sum_4 A - \sum_4 A\right) + x\right)\right) \gtrsim \sharp A$. Hence

$$\sharp \left\{ u \in A - A : du \in b^2 \left(\sum_8 A - \sum_8 A \right) \right\} \gtrsim \sharp A.$$

Consider $F = b^2 \frac{\sum_8 A - \sum_8 B}{(A-A)\setminus\{0\}}$, then $\sharp F \leqslant \sharp(A-A)\sharp(\sum_8 A - \sum_8 A) \lesssim (\sharp A)^2$. On the other hand, $\sharp F \gtrsim \sharp A \sharp(A'A' - A'A')$ by the former deduction. Hence $\sharp(A'A' - A'A') \lesssim \sharp A$. $\square$

§3 More additive combinatorics

$(E, +)$ abelian group.

Definition 3.1. For $A, B \subseteq (E, +)$, define the **additive energy** between A, B

$$\mathscr{E}_+(A, B) := \sharp \left\{ (a, b, a', b') \in A \times B \times A \times B : a + b = a' + b' \right\}.$$

The trivial bound of energy is

$$\sharp A \sharp B \leqslant \mathscr{E}_+(A, B) \leqslant (\sharp A)^{\frac{3}{2}} (\sharp B)^{\frac{3}{2}}.$$

Let $r = \mathbb{1}_A * \mathbb{1}_B$, then $r(y) = \sharp \left\{ (a, b) \in A \times B : a + b = y \right\}$. Endowing E with the counting measure, then

$$\mathscr{E}_+(A, B) = \sum_{y \in A+B} r(y)^2 = \left\| \mathbb{1}_A * \mathbb{1}_B \right\|_2^2.$$

Note that $\left\| \mathbb{1}_A * \mathbb{1}_B \right\|_1 = \left\| \mathbb{1}_A \right\|_1 \left\| \mathbb{1}_B \right\|_1 = \sharp A \sharp B$. By Cauchy-Schwarz,

$$\mathscr{E}_+(A, B) = \left\| \mathbb{1}_A * \mathbb{1}_B \right\|_2^2 \geqslant \frac{\left\| \mathbb{1}_A * \mathbb{1}_B \right\|_1^2}{\sharp \operatorname{supp} \mathbb{1}_A * \mathbb{1}_B} = \frac{(\sharp A)^2 (\sharp B)^2}{\sharp (A + B)}.$$

This inequality shows that if A and B have a small sum set, then the additive energy between A, B is big.

Remark 3.2 — The converse is **not** true. See the following example.

Example 3.3

Let $A = \{0, 1, 2, \cdots, N-1\} \cup \left\{ N, 2N, \cdots, N^2 \right\}$, then $\sharp A = 2N$. We have $\sharp(A + A) \asymp N^2$ and $\mathscr{E}_+(A, A) \geqslant \mathscr{E}_+(\{0, \cdots, N-1\}, \{0, \cdots, N-1\}) \geqslant \frac{N^2}{2N} \gg N^3$. They both attain the trivial upper bound up to a constant.

Theorem 3.4 (Balog-Szemerédi-Gowers)

The following are equivalent, the parameter $K_i > 0$ differs from each other by at most a polynomial dependence:

(i) $\mathscr{E}_+(A, B) \geqslant \frac{1}{K_1} (\sharp A)^{\frac{3}{2}} (\sharp B)^{\frac{3}{2}}$.

(ii) $\exists A' \subseteq A, B' \subseteq B$ with $\sharp A' \geqslant \frac{\sharp A}{K_2}, \sharp B' \geqslant \frac{\sharp B}{K_2}$, such that $\sharp(A' + B') \leqslant K_2 (\sharp A)^{\frac{1}{2}} (\sharp B)^{\frac{1}{2}}$.

(iii) $\exists G \subseteq A \times B$ with $\sharp G \geqslant \frac{1}{K_3} \sharp A \sharp B$ such that $\sharp(A \overset{G}{+} B) \leqslant K_3 (\sharp A)^{\frac{1}{2}} (\sharp B)^{\frac{1}{2}}$, where $A \overset{G}{+} B := \{ a + b : (a, b) \in G \}$.

Proof. (ii) $\Longrightarrow$ (i): Trivial.

(i) $\Longrightarrow$ (iii): Let $Y = \left\{ y : r(y) \geqslant \frac{(\sharp A)^{\frac{1}{2}}(\sharp B)^{\frac{1}{2}}}{2K_1} \right\}$, $G = \{(a,b) \in A \times B : a + b \in Y\}$, then $A \overset{G}{+} B = Y$. The bound of energy $\mathscr{E}_+(A,B) \geqslant \frac{1}{K_1}(\sharp A)^{\frac{3}{2}}(\sharp B)^{\frac{3}{2}}$ immediately gives that $\sharp G \geqslant \frac{1}{2K_1}\sharp A \sharp B$. Besides,

$$\sharp Y \frac{\sharp A \sharp B}{4K_1^2} \leqslant \sum_{y \in Y} r(y)^2 \leqslant (\sharp A)^{\frac{3}{2}}(\sharp B)^{\frac{3}{2}},$$

hence $\sharp Y \ll K_1^2 (\sharp A)^{\frac{1}{2}}(\sharp B)^{\frac{1}{2}}$. $\square$