

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

Ajorda Jiao

Contents

1	Basic additive combinatorics	2
2	Sum-product theorems	4
3	More additive combinatorics	7
4	Product Theorem	9

Theorem 0.1 (Erdős-Szemerédi Theorem)

There exists an absolute constant $c > 0$, such that for every finite set $A \subseteq \mathbb{R}$,

$$\max \{\#(A + A), \#AA\} \geq c(\#A)^{1+c}.$$

§1 Basic additive combinatorics

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

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

Question 1.2 (Freiman). If $\#(A + A) \leq K\#A$, for some parameter K , what can we say about A ?

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

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

then $\#(A + A) \leq 2^r \#A$.

Freiman Type Theorem If $\#(A + A) \leq K\#A$, then exists

- (i) $P \subseteq E$ is a generalized arithmetic progression of rank $O_K(1)$, $\#P = O_K(\#A)$.
- (ii) $X \subseteq E$ finite, $\#X = O_K(1)$.

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

$$\#(A - C)\#B \leq \#(A - B)\#(B - C).$$

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

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

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

Lemma 1.7 (Ruzsa Covering Lemma)

$A, B \subseteq (E, +)$ finite, $K \geq 1$. If $\#(A + B) \leq K\#A$, then $\exists X \subseteq E, \#X \leq K$, 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 $\leq K$.

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

Proposition 1.10 (Plünnecke-Ruzsa Inequality)

$A, B \subseteq E$ finite, $K \geq 1$. If $\#(A + B) \leq K\#A$, then $\forall k, l \geq 0$, we have

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

where $\sum_k B := \underbrace{B + B + \dots + B}_{k \text{ times}}$.

Lemma 1.11 (Petridis)

If $\#(A + B) \leq K\#A$, then $\exists A_0 \subseteq A$, such that for every $C \subset E$ finite,

$$\#(C + A_0 + B) \leq K\#(C + A_0).$$

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

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

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

$$(C + A_0) \cap A_0 \subseteq A \implies \#((C + A_0) \cap A_0) + B \geq K_0\#((C + A_0) \cap A_0).$$

Hence by inductive assumption,

$$\#(C' + A_0 + B) \leq K_0(\#(C + A_0) + \#A_0 - \#((C + A_0) \cap A_0)) = K_0\#(C' + A_0).$$

\square

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

$$\#(B + A_0) \leq K\#A_0, \quad \#(B + B + A_0) \leq K\#(B + A_0) \leq K^2\#A_0, \quad \dots$$

Hence, $\#(\sum_k B + A_0) \leq K^k\#A_0$. Finally, applying Ruzsa triangle inequality, we have

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

\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 $\#H = N$, then $\#(AA) \leq 3N + 1 \leq \#A$. Consider $AAA \supseteq HaH$, if $aHa^{-1} \cap H = \{1\}$, then $\#(HaH) = N^2$. 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 $\#(AA) \leq 3\#A$ but $\#(AAA) \geq N\#A$.

§2 Sum-product theorems

Let $(E, 0, 1, +, \cdot)$ be a ring, $A \subseteq E$ finite set, $K \geq 1$ parameter.

Let $E^\times = \{\text{invertible elements in } E\}$.

Definition 2.1. Let $R(A, K) := \{x \in E : \#(A + xA) \leq K\#A\}$.

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

Lemma 2.2

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 $\#(\sum_3 A - \sum_2 A) \leq K^5\#A$. Then $\#(A + (x + y)A) \leq K^7\#A$. Similarly, we can prove $\#(A + xyA) \leq K^8\#A$.

□

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

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

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

Lemma 2.5 (Ring Version of P-R)

Assume $\#(A + AA) \leq K\#A$, then $\#\langle A \rangle_s \leq K^{O_s(1)}\#A$.

Remark 2.6 — $\#(A + A) \leq K\#A$ and $\#(AA) \leq K\#A$ do not imply $\#(A + AA) \leq K^{O(1)}\#A$. 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 $\#(A + AA) = p^2 = p\#A$.

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

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

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

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

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

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

Theorem 2.8 (Sum-Product Theorem in Fields)

Assume $\#(A + AA) \leq K\#A$, then

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

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

Lemma 2.10

For any $x \in E$, if $\#(A + xA) < (\#A)^2$, 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 $K = (\#A)^{\frac{1}{10000}}$, 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 $\#A \geq 2$. 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 $\#F$. There are two methods. One way is to consider a map

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

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

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

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

Hence $\#F \leq K^{200}\#A$. \square

Corollary 2.11

If $\#(AA) \leq K\#A$, $\#(A+A) \leq K\#A$, then

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

Lemma 2.12 (Katz-Tao Lemma)

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

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

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 $\#(B - BB) \leq K^{O(1)}\#B$. Then $\#(B + BB) \leq K^{O(1)}\#B$ 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

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

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

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

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

$$\#(aA + bA) \leq \frac{\#(aA + aA \cap bA) \#(bA - aA \cap bA)}{\#(aA \cap bA)} \lesssim \frac{\#(A+A) \#(A-A)}{\#A} \lesssim \#A.$$

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

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

Let $d = a_1a_2 - a_3a_4$, then $dA \subseteq \bigcup_{x \in X} (b^2 (\sum_4 A - \sum_4 A) + x)$ where $\#X \lesssim 1$. Then $\exists x$ such that $\#(dA \cap (b^2 (\sum_4 A - \sum_4 A) + x)) \gtrsim \#A$. Hence

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

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

§3 More additive combinatorics

$(E, +)$ abelian group.

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

$$\mathcal{E}_+(A, B) := \# \{ (a, b, a', b') \in A \times B \times A \times B : a + b = a' + b' \}.$$

The trivial bound of energy is

$$\#A\#B \leq \mathcal{E}_+(A, B) \leq (\#A)^{\frac{3}{2}}(\#B)^{\frac{3}{2}}.$$

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

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

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

$$\mathcal{E}_+(A, B) = \|\mathbb{1}_A * \mathbb{1}_B\|_2^2 \geq \frac{\|\mathbb{1}_A * \mathbb{1}_B\|_1^2}{\# \text{supp } \mathbb{1}_A * \mathbb{1}_B} = \frac{(\#A)^2(\#B)^2}{\#(A+B)}.$$

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 $A = \{0, 1, 2, \dots, N-1\} \cup \{N, 2N, \dots, N^2\}$, then $\#A = 2N$. We have $\#(A+A) \asymp N^2$ and $\mathcal{E}_+(A, A) \geq \mathcal{E}_+(\{0, \dots, N-1\}, \{0, \dots, N-1\}) \geq \frac{N^2}{2N} \gg N^3$. 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) $\mathcal{E}_+(A, B) \geq \frac{1}{K_1}(\#A)^{\frac{3}{2}}(\#B)^{\frac{3}{2}}$.
- (ii) $\exists A' \subseteq A, B' \subseteq B$ with $\#A' \geq \frac{\#A}{K_2}, \#B' \geq \frac{\#B}{K_2}$, such that $\#(A'+B') \leq K_2(\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}}$.
- (iii) $\exists G \subseteq A \times B$ with $\#G \geq \frac{1}{K_3}\#A\#B$ such that $\#(A+B)^G \leq K_3(\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}}$, where $A+B^G := \{a+b : (a, b) \in G\}$.

Proof. (ii) \implies (i): Trivial.

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

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

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

For proving (iii) \implies (ii), we need some more preparations. \square

Theorem 3.5 (Multiplicative Balog-Szemerédi-Gowers)

For every group (H, \cdot) , $A, B \subseteq H$ finite sets. The following are equivalent, the parameter $K_i > 0$ differs from each other by at most a polynomial dependence:

- (i) $\mathcal{E}_+(A, B) \geq \frac{1}{K_1}(\#A)^{\frac{3}{2}}(\#B)^{\frac{3}{2}}$.
- (ii) $\exists A' \subseteq A, B' \subseteq B$ with $\#A' \geq \frac{\#A}{K_2}, \#B' \geq \frac{\#B}{K_2}$, such that $\#(A'B') \leq K_2(\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}}$.
- (iii) $\exists G \subseteq A \times B$ with $\#G \geq \frac{1}{K_3}\#A\#B$ such that $\#(A \overset{G}{\cdot} B) \leq K_3(\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}}$, where $A \overset{G}{\cdot} B := \{ab : (a, b) \in G\}$.

Theorem 3.6 (Graph-Theoretic B-S-G)

Let A, B be finite sets, $G \subseteq A \times B$. Assume $\#G \geq \frac{1}{K}\#A\#B$. Then exists $A' \subseteq A, B' \subseteq B$, $\#A' \gtrsim \#A, \#B' \gtrsim \#B$. And for every $a' \in A', b' \in B'$,

$$\#\{(a, b) \in A \times B : (a', b), (a, b'), (a, b') \in G\} \gtrsim \#A\#B.$$

Proof of BSG assuming graph BSG. Let A', B' be given by graph B-S-G, for every $x \in A' \cdot B'$,

$$r_3(x) = \#\{(y_1, y_2, y_3) \in (A \overset{G}{\cdot} B)^3 : x = y_1 y_2^{-1} y_3\} \gtrsim \#A\#B.$$

Then

$$\#(A' \cdot B') \leq \frac{\#(A \overset{G}{\cdot} B)^3}{\#A\#B} \lesssim (\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}}.$$

\square

Notation 3.7. For $a \in A$, let $B(a) := \{b \in B : (a, b) \in G\}$.

Proof of graph BSG. Let $A_1 := \{a \in A : \#B(a) \geq \frac{\#B}{2K}\}$, then $\#A \geq \frac{\#A}{2K}$. Then

$$\sum_{a, a' \in A_1} \#B(a) \cap B(a') = \sum_{b \in B} \left(\sum_{a \in A_1} \mathbb{1}_{B(a)}(b) \right)^2 \geq \frac{(\sum_{a \in A_1} \#B(a))^2}{\#B} \geq \frac{1}{4K^2}(\#A)^2 \#B.$$

Set $\varepsilon = \frac{1}{32K}$, let

$$U = \left\{ (a, a') \in A_1 \times A_1 : \#B(a) \cap B(a') \leq \frac{\varepsilon}{4K^2} \#B \right\}.$$

Idea: we want $A' \subseteq A, B' \subseteq B$ such that:

- (i) $\#A' \gtrsim \#A, \#B' \gtrsim \#B$,
- (ii) $\forall a \in A', \#A_1^U(a) := \#\{a' \in A_1 : (a, a') \in U\} \leq \frac{\#A_1}{8K}$.
- (iii) $\forall b \in B', \#A_1(b) \geq \frac{\#A_1}{4K}$.

This is enough, but condition (ii) is too much. Instead, we want $A' \subseteq A_2 \subseteq A_1, B' \subseteq B$ such that

$$(i) \#A' \gtrsim \#A, \#B' \geq \#B,$$

$$(ii) \forall a \in A', \#A_2^U(a) \leq \frac{\#A_2}{8K}.$$

$$(iii) \forall b \in B', \#A_2(b) \geq \frac{\#A_2}{4K}.$$

Candidate $A_2 = A_1(b)$ for some $b \in B$. Notice that

$$\sum_{b \in B} \#(A_1(b) \times A_1(b)) = \sum_{a, a' \in A_1} \#(B(a) \cap B(a')) \geq \frac{(\#A_1)^2 \#B}{4K^2},$$

$$\sum_{b \in B} \#(A_1(b) \times A_1(b) \cap U) = \sum_{(a, a') \in U} \#(B(a) \cap B(a')) \leq \frac{\varepsilon(\#A_1)^2 \#B}{4K^2}.$$

Hence $\exists b \in B$, write $A_2 = A_1(b)$ such that

$$\#(A_2 \times A_2) - \frac{1}{2\varepsilon} \#(A_2 \times A_2 \cap U) \geq \frac{(\#A_1)^2}{8K^2}.$$

Then $\#A_2 \geq \frac{\#A_1}{2\sqrt{2}K}$ and $\#(U \cap (A_2 \times A_2)) \leq 2\varepsilon(\#A_2)^2$. Let $A' = \{a \in A' : \#A_2^U(a) \leq \frac{\#A_2}{8K}\}$, by

$$\sum_{a \in A_2} \#A_2^U(a) = \#(U \cap (A_2 \times A_2)) \leq \frac{(\#A_2)^2}{16K},$$

it shows $\#A' \gtrsim \#A$. Let $B' = \{b \in B' : \#A_2(b) \geq \frac{\#A_2}{4K}\}$, then

$$\sum_{b \in B} \#A_2(b) = \sum_{a \in A_2 \subseteq A_1} \#B(a) \geq \frac{\#A_2 \#A}{2K},$$

hence $\#B' \geq \frac{\#B}{4K}$. □

§4 Product Theorem

Let (G, \cdot) be a group, $A \subseteq G$ finite subset.

Notation 4.1. Let $\prod_k A = \underbrace{AA \cdots A}_{k \text{ times}}, A^{-1} = \{a^{-1} : a \in A\}.$

Lemma 4.2

1. If $\#(AAA) \leq K\#A$, then $\#\prod_3(A \cup \{1\} \cup A^{-1}) \ll K^3\#A$.
2. If $\#\prod_3(A \cup \{1\} \cup A^{-1}) \leq K\#A$, then for every $k \geq 3$,

$$\#\prod_k(A \cup \{1\} \cup A^{-1}) \leq K^{k-2}\#A.$$

Proof.

1. By Ruzsa-triangle,

$$\#(AAA^{-1}) \leq \frac{\#(AAA)\#(A^{-1}A^{-1})}{\#A^{-1}} \leq K^2\#A,$$

$$\#(AA^{-1}A) \leq \frac{\#(AA^{-1}A^{-1})\#(AA)}{\#A} \leq K^3\#A,$$

The result follow.

2. Assume $1 \in A = A^{-1}$, the statement follows by Ruzsa-triangle. □

Definition 4.3. Finite set $A \subseteq G$ is called a K -approximate subgroup, if

- (i) $1 \in A, A^{-1} = A$,
- (ii) $\exists X \subseteq G, \#X \leq K$, such that $AA \subseteq XA$.

Lemma 4.4 (Reformulation of lemma 4.2)

If $\#(AAA) \leq \#A$, then $B = \prod_2(A \cup \{1\} \cup A^{-1})$ is a $O(K^{O(1)})$ -approximate subgroup.

Problem 4A. Does $\#(AAA) \leq K\#(AA)$ implies $\#\prod_k A \leq K^{O_k(1)}\#A$.

Theorem 4.5 (Helfgott)

$\forall \delta > 0, \exists \varepsilon > 0$, let $G = \text{SL}(2, \mathbb{F}_p)$, p is a prime number. Let $A \subseteq G, \langle A \rangle = G$, then either

- (1) $\#(AAA) \geq c(\#A)^{1+\varepsilon}$,
- (2) or $\#A \geq p^{3-\delta}$.

Theorem 4.6 (Equivalent formulation of Helfgott's Theorem)

If $A \subseteq G = \text{SL}(2, \mathbb{F}_p)$ is a K -approximate subgroup, then either

- (i) $\langle A \rangle \neq G$.
- (ii) or $\#A \lesssim 1$.
- (iii) or $\#A \gtrsim \#G$.

Exercise 4.7. Prove two statements above are equivalent.

Remark 4.8 — $\text{PSL}(2, \mathbb{F}_p)$ is a simple group for $p > 5$.

Remark 4.9 — Such result does not hold for abelian group.

Lemma 4.10 (Orbit-Stabalizer Formula)

$A \curvearrowright X$, then for every $x \in X$, we have

$$\#A \leq \#(A.x)\#(\text{Stab}(x) \cap A^{-1}A).$$

Remark 4.11 — If A is a subgroup, then identity holds.

Definition 4.12. $T \subseteq \text{SL}(2, \overline{\mathbb{F}}_p)$ is called a torus if $T = g \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix} g^{-1}$ for some $g \in \text{SL}(2, \overline{\mathbb{F}}_p)$.

Lemma 4.13

Assume A is K -approximate subgroup, $\exists T \subseteq \text{SL}(2, \overline{\mathbb{F}}_p)$ a torus such that

$$\#(T \cap AA) \gtrsim \# \text{tr}(A) - 2,$$

where $\text{tr}(A) = \{\text{tr}(a) : a \in A\}$.

Proof. Consider $B \subseteq A$ with $\#B = \# \text{tr}(A) - 2$, $\pm 2 \notin \text{tr}(B)$ and $\text{tr}(b), b \in B$ are pairwise distinct. Consider the conjugation, we have

$$\#B\#A = \sum_{b \in B} \# \{aba^{-1} : a \in A\} \#(C_G(b) \cap AA) \leq \#(AAA) \max_{b \in B} \#(C_G(b) \cap AA),$$

hence there are some $b \in B$ such that $\#(C_G(b) \cap AA) \geq \frac{\#B}{K}$. □

Definition 4.14. An affine variety over $\overline{\mathbb{F}}_p$ of complexity $\leq M$ is $V \subseteq \overline{\mathbb{F}}_p^n$,

$$V = \{ \underline{x} \in \overline{\mathbb{F}}_p^n : f_1(\underline{x}) = \dots = f_s(\underline{x}) = 0 \},$$

where $f_1, \dots, f_s \in \overline{\mathbb{F}}_p[x_1, x_2, \dots, x_n]$ and $s, n, \deg f_1, \dots, \deg f_s \leq M$.

Proposition 4.15

$G = \text{SL}(2, \overline{\mathbb{F}}_p)$, $V \subseteq G$ a proper subvariety of complexity $\leq M$. $A \subseteq \text{SL}(2, \overline{\mathbb{F}}_p)$ Assume $\langle A \rangle = \text{SL}(2, \overline{\mathbb{F}}_p)$, then $\exists g \in \prod_m (\{1\} \cup A)$, such that $g \notin V$, where m depends only on M .

Remark 4.16 — $\text{SL}(2, \overline{\mathbb{F}}_p)$ is not Zariski dense in G , i.e., \exists proper subvariety V such that $\text{SL}(2, \overline{\mathbb{F}}_p) \subseteq V$, hence we need an additional condition on complexity.