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. □

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

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 $K_0 := \inf_{A'\subseteq A} \frac{\sharp(A'+B)}{\sharp A'} \leqslant K$ 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,

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

□

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

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

□

> **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

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 $\sharp(A + xyA) \leqslant K^8\sharp A$.

$\square$

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 $\sharp\langle A\rangle_s \leqslant K^{O_s(1)}\sharp A$.

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. □

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, $A \subset E$ finite, $K \geqslant 1$.

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

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

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. ☐

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 $d = a_1a_2 - a_3a_4$, 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 $\sharp(A'A' - A'A') \lesssim \sharp A$. ☐

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

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

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) $\implies$ (i): Trivial.

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

For proving (iii) $\Longrightarrow$ (ii), we need some more preparations. □

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

(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 $\sharp(A \overset{G}{\cdot} B) \leqslant K_3(\sharp A)^{\frac{1}{2}}(\sharp B)^{\frac{1}{2}}$, where $A \overset{G}{\cdot} B \coloneqq \{ab : (a,b) \in G\}$.

Theorem 3.6 (Graph-Theoretic B-S-G)
Let A, B be finite sets, $G \subseteq A \times B$. Assume $\sharp G \geqslant \frac{1}{K}\sharp A\sharp B$. Then exists $A' \subseteq A, B' \subseteq B'$, $\sharp A' \gtrsim \sharp A, \sharp B' \gtrsim \sharp B$. And for every $a' \in A', b' \in B'$,

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

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

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

Then

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

□

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

Proof of graph BSG. Let $A_1 \coloneqq \sharp\left\{a \in A : \sharp B(a) \geqslant \frac{\sharp B}{2K}\right\}$, then $\sharp A \geqslant \frac{\sharp A}{2K}$. Then

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

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

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

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

(i) $\sharp A' \gtrsim \sharp A, \sharp B' \geqslant \sharp B$,

(ii) $\forall a \in A', \sharp A_1^U(a) \coloneqq \sharp\{a' \in A_1 : (a,a') \in U\} \leqslant \frac{\sharp A_1}{8K}$.

(iii) $\forall b \in B', \sharp A_1(b) \geqslant \frac{\sharp A_1}{4K}$.

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) $\sharp A' \gtrsim \sharp A, \sharp B' \geqslant \sharp B$,

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

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

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

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

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

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

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

Then $\sharp A_2 \geqslant \frac{\sharp A_1}{2\sqrt{2}K}$ and $\sharp(U \cap (A_2 \times A_2)) \leqslant 2\varepsilon(\sharp A_2)^2$. Let $A' = \left\{a \in A' : \sharp A_2^U(a) \leqslant \frac{\sharp A_2}{8K}\right\}$, by

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

it shows $\sharp A' \gtrsim \sharp A$. Let $B' = \left\{b \in B', \sharp A_2(b) \geqslant \frac{\sharp A_2}{4K}\right\}$, then

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

hence $\sharp B' \geqslant \frac{\sharp B}{4K}$. □

§4 Product Theorem

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

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

Lemma 4.2

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

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

Proof.

1. By Ruzsa-triangle,
$$\sharp(AAA^{-1}) \leqslant \frac{\sharp(AAA)\sharp(A^{-1}A^{-1})}{\sharp A^{-1}} \leqslant K^2\sharp A,$$
$$\sharp(AA^{-1}A) \leqslant \frac{\sharp(AA^{-1}A^{-1})\sharp(AA)}{\sharp A} \leqslant K^3\sharp A,$$
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) $\exists X \subseteq G, \sharp X \leqslant K$, such that $AA \subseteq XA$.

Lemma 4.4 (Reformulation of lemma 4.2)
If $\sharp(AAA) \leqslant \sharp A$, then $B = \prod_2(A \cup \{1\} \cup A^{-1})$ is a $O(K^{O(1)})$-approximate subgroup.

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

Theorem 4.5 (Helfgott)
$\forall \delta > 0, \exists \varepsilon > 0$, let $G = \mathrm{SL}(2, \mathbb{F}_p), p$ is a prime number. Let $A \subseteq G, \langle A \rangle = G$, then either

(1) $\sharp(AAA) \geqslant c(\sharp A)^{1+\varepsilon}$,

(2) or $\sharp A \geqslant p^{3-\delta}$.

Theorem 4.6 (Equivalent formulation of Helfgott's Theorem)
If $A \subseteq G = \mathrm{SL}(2, \mathbb{F}_p)$ is a K-approximate subgroup, then either

(i) $\langle A \rangle \neq G$.

(ii) or $\sharp A \lesssim 1$.

(iii) or $\sharp A \gtrsim \sharp G$.

Exercise 4.7. Prove two statements above are equivalent.

Remark 4.8 — $\mathrm{PSL}(2, \mathbb{F}_p)$ 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

$$\sharp A \leqslant \sharp(A.x)\sharp(\mathrm{Stab}(x) \cap A^{-1}A).$$

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

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

Lemma 4.13
Assume A is K-approximate subgroup, $\exists T \subseteq \mathrm{SL}(2, \overline{\mathbb{F}}_p)$ a torus such that

$$\sharp(T \cap AA) \gtrsim \sharp\,\mathrm{tr}(A) - 2,$$

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

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

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

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

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

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

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

Proposition 4.15 (Escape from Subvarieties)
$\forall M > 0, \exists p_0 = p_0(M)$, such that for every $p > p_0$ prime, $G = \mathrm{SL}(2, \overline{\mathbb{F}}_p)$, $V \subseteq G$ a proper subvariety of complexity $\leqslant M$. $A \subseteq \mathrm{SL}(2, \mathbb{F}_p)$, assume $\langle A \rangle = \mathrm{SL}(2, \mathbb{F}_p)$, then $\exists g \in \prod_m(\{1\} \cup A)$, such that $g \notin V$, where m depends only on M.

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

Definition 4.17. An affine subvariety V is **irreducible** if V can not be written as $V = V_1 \cup V_2$ where V_1, V_2 are both subvarieties and $V_1, V_2 \neq V$.

Definition 4.18. **Krull dimension** of a subvariety V is defined as

$$\dim V := \max\left\{k : \exists V_1 \subsetneqq V_2 \subsetneqq \cdots \subsetneqq V_k \subseteq V, V_1, \cdots, V_k \text{ irreducible}\right\}.$$

Proof. $G = \left\{(x_{11}, x_{12}, x_{21}, x_{22}) \in \overline{\mathbb{F}}_p^4 : x_{11}x_{22} - x_{12}x_{21} = 1\right\}$ is of complexity 4. Let

$$\overline{\mathbb{F}}_p[G] := \overline{\mathbb{F}}_p[x_{11}, \cdots, x_{22}]/(\det \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} - 1).$$

For every $V \subseteq G$ subvariety, with complexity $\leqslant M$, let

$$I_V := \left\{f \in \overline{\mathbb{F}}_p[G] : \forall x \in V, f(x) = 0\right\},$$

which is an ideal. There exists $d = d(M)$ such that $I = I_V \cap \overline{\mathbb{F}}_p[G]_{\deg \leqslant d} = I_V$. Consider $G \curvearrowright \overline{\mathbb{F}}_p[G]$ given by $(g.f)(\cdot) = f(g^{-1}\cdot)$. Hence $G \curvearrowright \overline{\mathbb{F}}_p[G]_{\deg \leqslant d}$, let $m = \dim \overline{\mathbb{F}}_p[G]_{\deg \leqslant d}$. Assume for a contradiction, $\prod_m (A \cup \{1\}) \subseteq V$. Then there exists $g_1, \cdots, g_s \in \prod_m (A \cup \{1\})$ such that

$$J = I + g_1^{-1} I + \cdots + g_s^{-1} I$$

is $\langle A \rangle$-invariant. Let $H = \{g \in G : g.I = I\}$, then

1. H is a subgroup, $A \subseteq H$.
2. $H \subseteq V$. Indeed, $\forall h \in H, f \in I$, $h^{-1}.f \in J$. Hence $\exists f_0, f_1, \cdots, f_s \in I$, such that

   $$h^{-1} f = f_0 + g_1^{-1} f_1 + \cdots + g_s^{-1} f_s.$$

   Take $x = 1_G$, we have $h \in V$.
3. Complexity of H is $O_M(1)$.

By a Schwarz-Zippel (Long-Weil) theorem, we have

$$\sharp(H \cap \mathrm{SL}_2(\mathbb{F}_p)) \ll_M p^{\dim H} \ll_M p^{\dim V}.$$

But $\sharp \langle A \rangle \asymp p^3$, if V is proper, then $\dim V < \dim G = 3$. A contradiction. $\square$

Proof of Theorem 4.6. We separate the proof into following four steps.

I. $\exists T \subseteq G$ torus such that $\sharp(T \cap AA) \gtrsim \sharp \operatorname{tr}(A) - 2$.

II. There exists some integers of $O(1)$ such that $\sharp \operatorname{tr}(\prod_{O(1)} A) \gg (\sharp A)^{\frac{1}{3}}$.

III. T torus, finite $V \subseteq T$, then $\exists g \in \prod_{O(1)} A$ such that one of the following holds:
   (1) $\sharp VVV \geqslant K \sharp V$.
   (2) $\sharp \operatorname{tr}(\prod_{20} V g \prod_{20} V g^{-1}) \geqslant K \sharp V$.
   (3) $\sharp V \lesssim 1$.
   (4) $\sharp V \gtrsim p$.

IV. T torus, finite $V \subseteq T$, then $\exists g \in \prod_{O(1)} A$ such that $\sharp(V g V g^{-1} V) \gg (\sharp V)^3$.

After those four steps, we can prove the theorem. Applying II, we have $\sharp \operatorname{tr} \prod_{O(1)} A \gg (\sharp A)^{\frac{1}{3}}$. By I, there is T torus, let $V = T \cap \prod_{O(1)} A$, such that $\sharp V \gtrsim (\sharp A)^{\frac{1}{3}}$. For every $g \in \prod_{O(1)} A$, we have $\sharp \operatorname{tr}(\prod_{O(1)} A) \geqslant \sharp \operatorname{tr}(\prod_{20} V g \prod_{20} V g^{-1})$. By I, there is some $V' = T' \cap \prod_{O(1)} A$ such that

$$\sharp V' \gtrsim \max\left\{\sharp \operatorname{tr}(\prod_{20} V g \prod_{20} V g^{-1}), \sharp VVV\right\}.$$

By IV, there exists $h \in \prod_{O(1)} A$, such that

$$\sharp A \gtrsim \sharp \prod_{O(1)} A \gg \sharp(V' h V' h^{-1} V') \gg (\sharp V')^3.$$

Hence, $\max\left\{\sharp\, \mathrm{tr}(\prod_{20} V g \prod_{20} V g^{-1}), \sharp VVV\right\} \lesssim (\sharp A)^{\frac{1}{3}}$. By III, there exists $g \in \prod_{O(1)} A$ such that $\sharp V \lesssim 1$ or $\sharp V \gtrsim p$. Which shows that $\sharp A \lesssim 1$ or $\sharp A \gtrsim p^3$. □

Proof of II. For every $g, h \in G$, consider

$$\Phi_{g,h} : G \to (\overline{F}_p)^3, \quad x \mapsto (\mathrm{tr}(x), \mathrm{tr}(gx), \mathrm{tr}(hx)).$$

Then

$$\begin{aligned} &\{(g,h) \in G \times G : \Phi_{g,h} \text{ has fiber of positive dimension}\} \\ = &\{(g,h) \in G \times G : \Phi_{g,h} \text{ has fiber of } \sharp > 2\} \end{aligned}$$

is a proper subvariety of $G \times G$ of complexity $O(1)$. By "escape"(4.15), there exists $g, h \in \prod_{O(1)}(A \cup \{1\})$ such that each fiber of $\Phi_{g,h}$ has $\sharp \leqslant 2$, hence $\sharp A \ll (\sharp\, \mathrm{tr}(\prod_{O(1)} A))^3$. □

Proof of IV. For every $g \in G$, consider

$$\phi_g : T^3 \to G, \quad (x, y, z) \mapsto xgyg^{-1}z.$$

Then

$$\{g \in G : \phi_g \text{ has fiber of positive dimension}\}$$

is a proper subvariety of G of complexity $O(1)$. By "escape"(4.15), there exists $g \in \prod_{O(1)}(A \cup \{1\})$ such that each fiber of ϕ_g is of 0-dimensional. Because the complexity is of $O(1)$, hence each fiber of ϕ_g is of $\sharp \leqslant O(1)$. Therefore, $\sharp \phi_g(V^3) \gg (\sharp V)^3$. □

Proof of III. Assume $V \subseteq T = \left\{\begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}\right\}, g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then

$$\mathrm{tr}\left(\begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} y & 0 \\ 0 & y^{-1} \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1}\right) = ad \cdot w(xy) - bc \cdot w(xy^{-1}),$$

where $w(x) = x + x^{-1}$. Then the statement is equivalent to the following proposition. □

Proposition 4.19

$\widehat{V} \subseteq \overline{\mathbb{F}}_p^{\times}, a_1, a_2 \in \overline{\mathbb{F}}_p^{\times}$, assume $\widehat{V}$ is K-approximate subgroup of $\overline{\mathbb{F}}_p$ and

$$\left\{a_1 w(xy) + a_2 w(xy^{-1}) : x, y \in \prod_{20} \widehat{V}\right\} \leqslant K \sharp \widehat{V},$$

then either $\sharp \widehat{V} \lesssim 1$ or $\sharp \widehat{V} \gtrsim p$.

Proof. We just prove a special case of $a_1 = a_2 = 1$. Let $E = \left\{(w(xy), w(xy^{-1})) : x, y \in \widehat{V}\right\}$, by assumption, $\sharp(w(\prod_2 \widehat{V}) \overset{E}{+} w(\prod_2 \widehat{V})) \lesssim \sharp \widehat{V}$. At the same time, $\sharp E \gg (\sharp \widehat{V})^2$, hence by B-S-G(3.4) and P-R, there exists $V' \subseteq \prod_2 \widehat{V}, \sharp V' \gtrsim \sharp \widehat{V}$ such that

$$\sharp(w(V') + w(V')) \lesssim \sharp \widehat{V}.$$

Notice that $w(x)w(y) = w(xy) + w(xy^{-1})$, then $w(V')w(V') \leqslant K \sharp \widehat{V}$. By sum-product, either $\sharp w(V') \lesssim 1$ or $\sharp w(A') \gtrsim p$. □

Exercise 4.20. Prove the general cases.

§5 Expansion in $\mathrm{SL}(2, \mathbb{F}_p)$

Let $S \subseteq \mathrm{SL}(2, \mathbb{Z})$ be a finite subset, $S = S^{-1}$. Let $G_p = \mathrm{SL}(2, \mathbb{F}_p) = \mathrm{SL}(2, \mathbb{Z})/\ker \pi_p$, where

$$\pi_p : \mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{F}_p)$$

is the projection by $\mod p$. Let $\Gamma = \mathrm{SL}(2, \mathbb{Z})$, then there is a natural action $\Gamma \curvearrowright G_p$. Consider **Koopman representation** $\Gamma \curvearrowright L^2(G_p)$ given by

$$\gamma \mapsto T_p(\gamma) \in U(L^2(G_p)), \quad T_p(\gamma) f(\,\cdot\,) = f(\gamma^{-1} \cdot).$$

Let $\chi_S = \frac{1}{\sharp S} \mathbb{1}_S$, define

$$T_p(\chi_S) f(\,\cdot\,) = \frac{1}{\sharp S} \sum_{\gamma \in S} f(\gamma^{-1} \cdot) = \chi_S * f,$$

then $T_p(\chi_S) \in \mathrm{End}(L^2(G_p))$.

Remark 5.1 — If $S = S^{-1}$, then $T_p(\chi_S)$ is self-adjoint.

Consider the spectrum of $T_p(\chi_S)$. Note that $\|T_p(\chi_S)\| \leqslant 1$ and $1 \in \mathrm{Spec}(T_p(\chi_S))$. Let

$$L_0^2(G_p) := \mathbb{1}_G^{\perp} = \left\{ f \in L^2(G_p) : \int f = 0 \right\},$$

then $T_{p,0}(\chi_S) : L_0^2(G_p) \to L_0^2(G_p)$.

Theorem 5.2 (Uniform Expansion in $\mathrm{SL}(2, \mathbb{F}_p)$, Bourgain-Gamburd)
Assume $\langle S \rangle \subseteq \mathrm{SL}(2, \mathbb{Z})$ is not virtually solvable, then $\{T_{p,0}(\chi_S)\}_p$ has a **uniform spectral gap**, i.e., there exists $c > 0$, such that for every p prime,

$$\mathrm{Spec}(T_{p,0}(\chi_S)) \cap [1 - c, 1] = \varnothing.$$

Exercise 5.3. Prove that the conclusion is equivalent to $\exists \varepsilon > 0$, such that $\forall p$ prime, for every $f \in L_0^2(G_p)$, there exists $s \in S$,

$$\|f - T_p(s) f\| \geqslant \varepsilon \|f\|.$$

(We say $\oplus_p L_0^2(G_p)$ has no almost invariant vector).

Remark 5.4 — As a consequence of the exercise, let $S' \subseteq \langle S \rangle$ be a finite symmetric set, if $\{T_p(\chi_{S'})\}_p$ has a uniform spectral gap, then $\{T_p(\chi_S)\}_p$ has a uniform spectral gap.

Proposition 5.5 (Tits Alternative for $\mathrm{SL}(2,\mathbb{Z})$)

$\Gamma' \subseteq \mathrm{SL}(2,\mathbb{Z})$ subgroup, then

(1) either Γ' contains non-abelian free subgroup,

(2) or Γ' is virtually solvable.

Proof. Consider $\Gamma(3) = \ker \pi_3 = \{g \in \mathrm{SL}(2,\mathbb{Z}) : g \equiv 1 \bmod 3\}$, then $[\Gamma : \Gamma(3)] < \infty$. Note that $\Gamma(3) = \pi_1(\mathbb{H}/\Gamma(3))$ which is a free group. By Nielson-Schreien's argument, $\Gamma' \cap \Gamma(3) \subseteq \Gamma(3)$ is of finite index and hence is also a free group. Then, $\Gamma' \cap \Gamma(3) = 1, \mathbb{Z}$, or a non-abelian free group. $\square$

Remark 5.6 — Finite index subgroup of finite generated group is also finite generated.