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

Ajorda Jiao

Contents

Notation

$O(1)$	Absolute constant.
$O_s(1)$	A constant only depend on s.
$\mathbb{O}(m)$	A subset with cardinality at most m.
K	A parameter at least 1. Always denote a bound of cardinality increasing under sum or product.
$f \ll g$	There exists an absolute constant $C > 0$ such that $f \leqslant Cg$.
$f \asymp g$	$f \ll g$ and $g \ll f$.
$f \ll_s g$	There exists an constant C_s depending on s such that $f \leqslant C_s g$.
$f \lesssim g$	There exists $C = C(K) > 0$ with at most a polynomial dependence on K such that $f \leqslant Cg$.
$f \sim g$	$f \lesssim g$ and $g \lesssim f$.
$R(A, K)$	See Definition 2.1.
$\#A$	Cardinality of A.
$\lvert A\rvert$	Lebesgue measure of A.
$A^{(\delta)}$	δ-neighborhood of A.
$\mathcal{N}_\delta(A)$	δ-covering number of A.
$R_\delta(A, K)$	See Definition 6.10.
$\lVert\cdot\rVert, \lVert\cdot\rVert_p$	L^2 norm and general L^p norm, usually take $p = 1, \infty$.
$\mu \boxplus \nu$	Additive convolution of measures on $\mathbb{R}$.
$\mu \boxminus \nu$	Subtractive convolution of measures on $\mathbb{R}$.
$\mu * \nu$	Multiplicative convolution of measures in a group or on $\mathbb{R}$.

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

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

§1 Basic additive combinatorics

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

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

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

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

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

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

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

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

(ii) $X \subset E$ finite, $\#X = O_K(1)$.

Such that $A \subset P + X$.

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

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

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

Proof. Construct a map $(A-C) \times B \to (A-B) \times (B-C)$, $(x,b) \mapsto (a_x - b, b - c_x)$, where a_x, c_x are fixed way of writing $x = a_x - c_x$ for every x, this map is injective. □

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)
$A, B \subset (E,+)$ finite, $K \geqslant 1$. If $\#(A+B) \leqslant K\#A$, then $\exists X \subset E, \#X \leqslant K$, such that $B \subset A - A + X$.

Proof. Let $X \subset B$ be the maximal set such that $(x+A)_{x\in X}$ are pairwise disjoint. □

Remark 1.8 — Ruzsa Covering Lemma $\iff$ $B \subset A - A + \mathbb{O}\left(\frac{\#(A+B)}{\#A}\right)$.

Proposition 1.9 (Plünnecke-Ruzsa Inequality)
$A, B \subset E$ finite, $K \geqslant 1$. If $\#(A+B) \leqslant K\#A$, then $\forall k, l \geqslant 0$, we have

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

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

Lemma 1.10 (Petridis)
If $\#(A+B) \leqslant K\#A$, then $\exists A_0 \subset A$, such that for every $C \subset E$ finite,

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

Proof. Let $K_0 := \inf_{A' \subset A} \frac{\#(A'+B)}{\#A'} \leqslant K$ and $A_0 \subset A$ 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 $((C + A_0) \cap A_0) + B \subset (C + A_0 + B) \cap (A_0 + B)$. By assumption,

$$(C + A_0) \cap A_0 \subset A \implies \#((C + A_0) \cap A_0) + B \geqslant K_0\#((C + A_0) \cap A_0).$$

Hence by inductive assumption,

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

□

Proof of Plünnecke-Ruzsa Inequality 1.9. Applying lemma, we have

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

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

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

□

Question 1.11. 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 1.12

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 $\#(AA) \leqslant 3N + 1 \leqslant \#A$. 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 $\#(AA) \leqslant 3\#A$ but $\#(AAA) \geqslant N\#A$.

§2 Sum-product theorems

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

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

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

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

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

□

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

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

Lemma 2.4 (Ring Version of P-R)

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

Remark 2.5 — $\#(A+A) \leqslant K\#A$ and $\#(AA) \leqslant K\#A$ do not imply $\#(A+AA) \leqslant K^{O(1)}\#A$. For a counter example, we consider $A = \sqrt{-1}\mathbb{F}_p \subset \mathbb{F}_p[\sqrt{-1}]$ for some $p = 4k+3$ and $K = 1$, then $\#(A+AA) = p^2 = p\#A$.

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

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

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

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

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

Theorem 2.6 (Sum-Product Theorem in Fields)
Assume $\#(A+AA) \leqslant K\#A$, then

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

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

Remark 2.7 — If $E = \mathbb{R}$, then for every $A \subset \mathbb{R}$, $\#(A+AA) \geqslant (\#A)^{1+\frac{1}{10000}}$.

Lemma 2.8
For any $x \in E$, if $\#(A+xA) < (\#A)^2$, then $x \in \frac{A-A}{(A-A)\setminus\{0\}}$.

Proof of Theorem 2.6. Let $F = \frac{A-A}{(A-A)\setminus\{0\}}$. Then the sets $F+F, F-F, FF, F/F$ all come from A by at most $O(1)$ times of operations. It follows that $F+F, F-F, FF, F/F \subset R(A,K^{O(1)})$. For if $K^{O(1)} < \#A$, then $R(A,K^{O(1)}) \subset F$. We can verify that F is a field.

Precisely, consider $K = (\#A)^{\frac{1}{10000}}$, the lemma shows that $R(A,K^{9999}) \subset F$. By assumption, $\#(A+AA) \leqslant K\#A \leqslant K\#(AA)$, hence $1 \in R(A,K^3)$ by P-R. By "almost" ring structure, we have $A - A \subset R(A,K^{30})$ and $((A-A)\setminus\{0\})^{-1} \subset R(A,K^{30})$, hence $F \subset R(A,K^{300})$. Furthermore, $F+F, FF \subset R(A,K^{3000}) \subset F$. Hence F is a finite field.

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

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

where $u_x, v_x \in A - A$ are fixed elements to write $x = \frac{u_x}{v_x}$ for every x. The map is injective, hence $(\#F)(\#A-1) \leqslant (\#(AA-AA))^2 \leqslant K^4(\#A)^2$ by P-R.

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

$$(\#A)^4 = \sum_{x\in F}\#\left\{a,b,a',b' \in A : ax+b = a'x+b'\right\} \geqslant \sum_{x\in F}\frac{(\#A)^4}{\#(A+xA)} \geqslant \#F\frac{(\#A)^3}{K^{300}}.$$

Hence $\#F \leqslant K^{300}\#A$. $\square$

But the input condition in this Theorem is not as desired. Indeed, we want to show that if both $\#(AA)$ and $\#(A+A)$ are small, then $\#A$ is small. For interpreting this input to the case of previous theorem, we need a following lemma by Katz-Tao.

Lemma 2.9 (Katz-Tao Lemma)
Assume $\#(A+A) \leqslant K\#A, \#(AA) \leqslant K\#A$. Then $\exists A' \subset A$ such that

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

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

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

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

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

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

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

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

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

Let $d = a_1a_2 - a_3a_4$, then $dA \subset \bigcup_{x\in X} \left(b^2 \left(\sum_4 A - \sum_4 A\right) + x\right)$ where $\#X \lesssim 1$. Then $\exists x$ such that $\#\left(dA \cap \left(b^2\left(\sum_4 A - \sum_4 A\right) + x\right)\right) \gtrsim \#A$. 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 $\#F \leqslant \#(A-A)\#(\sum_8 A - \sum_8 A) \lesssim (\#A)^2$. On the other hand, $\#F \gtrsim \#A\#(A'A' - A'A')$ by the former deduction. Hence $\#(A'A' - A'A') \lesssim \#A$. $\square$

Corollary 2.10
If $\#(AA) \leqslant K\#A, \#(A+A) \leqslant K\#A$, 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 $\#F \ll K^{O(1)}\#A$.

Proof. Take such A' in lemma, we choose $a \in A' \setminus \{0\}$, let $B = a^{-1}A'$. Then $1 \in B$ and $B - BB \subset BB - BB$, hence $\#(B - BB) \leqslant K^{O(1)}\#B$. Then $\#(B + BB) \leqslant K^{O(1)}\#B$ by P-R and R-covering. Applying Theorem 2.6 to B, the corollary follows. $\square$

§3 More additive combinatorics

Let $(E,+)$ be an abelian group.

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

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

The trivial bound of energy is

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

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

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

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

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

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 $A = \{0,1,2,\cdots,N-1\}\cup\left\{N,2N,\cdots,N^2\right\}$, then $\#A = 2N$. We have $\#(A+A) \asymp N^2$ 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) $\mathscr{E}_+(A,B) \geqslant \frac{1}{K_1}(\#A)^{\frac{3}{2}}(\#B)^{\frac{3}{2}}$.

(ii) $\exists A' \subset A, B' \subset B$ with $\#A' \geqslant \frac{\#A}{K_2}, \#B' \geqslant \frac{\#B}{K_2}$, such that

$$\#(A'+B') \leqslant K_2(\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}}.$$

(iii) $\exists G \subset A\times B$ with $\#G \geqslant \frac{1}{K_3}\#A\#B$ such that

$$\#(A \overset{G}{+} B) \leqslant K_3(\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}},$$

where $A \overset{G}{+} B := \{a+b : (a,b)\in G\}$.

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

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

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

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

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

Theorem 3.5 (Multiplicative Balog-Szemerédi-Gowers)
For every group $(H,\cdot)$, $A, B \subset H$ finite sets. The following are equivalent, the parameter $K_i > 0$ differs from each other by at most a polynomial dependence:

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

(ii) $\exists A' \subset A, B' \subset B$ with $\#A' \geqslant \frac{\#A}{K_2}, \#B' \geqslant \frac{\#B}{K_2}$, such that

$$\#(A'B') \leqslant K_2(\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}}.$$

(iii) $\exists G \subset A \times B$ with $\#G \geqslant \frac{1}{K_3}\#A\#B$ such that

$$\#(A \overset{G}{\cdot} B) \leqslant K_3(\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}},$$

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, $G \subset A \times B$. Assume $\#G \geqslant \frac{1}{K}\#A\#B$. Then exists $A' \subset A, B' \subset B'$, $\#A' \gtrsim \#A, \#B' \gtrsim \#B$. And for every $a' \in A', b' \in B'$,

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

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

$$r_3(x) = \#\left\{(y_1,y_2,y_3) \in (A \overset{G}{\cdot} B)^3 : x = y_1y_2^{-1}y_3\right\} \gtrsim \#A\#B.$$

Then

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§4 A product theorem

Let $(G, \cdot)$ be a group, $A \subset G$ 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 $\#(AAA) \leqslant K\#A$, then $\#\prod_3(A \cup \{1\} \cup A^{-1}) \ll K^3 \#A$.
2. If $\#\prod_3(A \cup \{1\} \cup A^{-1}) \leqslant K\#A$, then for every $k \geqslant 3$,
$$\#\prod_k(A \cup \{1\} \cup A^{-1}) \ll K^{k-2}\#A.$$

Proof. 1. By Ruzsa-triangle,
$$\#(AAA^{-1}) \leqslant \frac{\#(AAA)\#(A^{-1}A^{-1})}{\#A^{-1}} \leqslant K^2\#A,$$
$$\#(AA^{-1}A) \leqslant \frac{\#(AA^{-1}A^{-1})\#(AA)}{\#A} \leqslant K^3\#A,$$
The result follow.

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

$\square$

Definition 4.3. A finite set $A \subset G$ is called a **K-approximate subgroup**, if

(i) $1 \in A, A^{-1} = A$,

(ii) $\exists X \subset G, \#X \leqslant K$, such that $AA \subset XA$.

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

Question 4.5. Does $\#(AAA) \leqslant K\#(AA)$ imply $\#\prod_k A \leqslant K^{O_k(1)}\#A$?

Theorem 4.6 (Helfgott)
$\forall \delta > 0, \exists \varepsilon > 0$, let $G = \mathrm{SL}(2, \mathbb{F}_p)$, where p is a prime number. Let $A \subset G, \langle A \rangle = G$, then

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

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

Theorem 4.7 (Equivalent formulation of Helfgott's Theorem)
If $A \subset G = \mathrm{SL}(2, \mathbb{F}_p)$ is a K-approximate subgroup, then

(i) either $\langle A \rangle \neq G$,

(ii) or $\#A \lesssim 1$,

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

Exercise 4.8. Prove two statements above are equivalent.

Remark 4.9 — $\mathrm{PSL}(2, \mathbb{F}_p)$ is a simple group for $p > 5$.

Remark 4.10 — Such result does not hold for abelian group.

Lemma 4.11 (Orbit-Stabalizer Formula)
$A \curvearrowright X$, then for every $x \in X$, we have

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

Remark 4.12 — If A is a subgroup, then identity holds.

Definition 4.13. $T \subset \mathrm{SL}(2, \overline{\mathbb{F}}_p)$ 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 4.14 (rich torus)
Assume A is a K-approximate subgroup, then $\exists T \subset \mathrm{SL}(2, \overline{\mathbb{F}}_p)$ a torus such that

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

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

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

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

hence there are some $b \in B$ such that $\#(C_G(b) \cap AA) \gtrsim \#B$. □

Definition 4.15. An affine variety over $\overline{\mathbb{F}}_p$ of **complexity** $\leqslant M$ is $V \subset \overline{\mathbb{F}}_p^n$,

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

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 4.16 (Escape from Subvarieties)
$\forall M > 0, \exists p_0 = p_0(M)$, such that for every $p > p_0$ prime, $G = \mathrm{SL}(2, \overline{\mathbb{F}}_p)$, $V \subset G$ a proper subvariety of complexity $\leqslant M$. $A \subset \mathrm{SL}(2, \mathbb{F}_p)$, 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 4.17 — $\mathrm{SL}(2, \mathbb{F}_p)$ is not Zariski dense in G, i.e., $\exists$ proper subvariety V such that $\mathrm{SL}(2, \mathbb{F}_p) \subset V$, hence we need an additional condition on complexity.

Definition 4.18. 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 4.19. **Krull dimension** of a subvariety V is defined as

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

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 $V \subset G$ 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, $\prod_m(A \cup \{1\}) \subset V$. Take $g_1, \cdots, g_s \in \prod_m(A \cup \{1\})$ such that

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

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

1. H is a subgroup, $A \subset H$.
2. $H \subset V$. 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 (Lang-Weil) theorem, we have

$$\#(H \cap \mathrm{SL}(2, \mathbb{F}_p)) \ll_M p^{\dim H} \ll_M p^{\dim V}.$$

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

Proof of Theorem 4.7. We separate the proof into following four steps.

I. $\exists T \subset G$ torus such that $\#(T \cap AA) \gtrsim \# \mathrm{tr}(A) - 2$.

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

III. T torus, finite $V \subset T$, then $\exists g \in \prod_{O(1)} A$ such that one of the following holds:

(1) $\#VVV \geqslant K'\#V$.

(2) $\#\operatorname{tr}(\prod_{20} Vg \prod_{20} Vg^{-1}) \geqslant K'\#V$.

(3) $\#V \lesssim 1$.

(4) $\#V \gtrsim p$.

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

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

$$\#V' \gtrsim \max\left\{\#\operatorname{tr}(\prod\nolimits_{20} Vg \prod\nolimits_{20} Vg^{-1}), \#VVV\right\}.$$

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

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

Hence, $\max\left\{\#\operatorname{tr}(\prod_{20} Vg \prod_{20} Vg^{-1}), \#VVV\right\} \lesssim (\#A)^{\frac{1}{3}}$. By III, take a suitable $K' = O(K^{O(1)})$, then there exists $g \in \prod_{O(1)} A$ such that $\#V \lesssim 1$ or $\#V \gtrsim p$. Which shows that $\#A \lesssim 1$ or $\#A \gtrsim p^3$. $\square$

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

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

Then

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

is a proper subvariety of $G \times G$ of complexity $O(1)$. By "escape"(4.16), there exists $g, h \in \prod_{O(1)}(A \cup \{1\})$ such that each fiber of $\Phi_{g,h}$ has $\# \leqslant 2$, hence $\#A \ll (\#\operatorname{tr}(\prod_{O(1)} A))^3$. $\square$

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"(4.16), 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 $\# \leqslant O(1)$. Therefore, $\#\phi_g(V^3) \gg (\#V)^3$. $\square$

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

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

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

Proposition 4.20
$\widehat{V}\subset\overline{\mathbb{F}}_p^{\times}, a_1,a_2\in\overline{\mathbb{F}}_p^{\times}$, assume $\widehat{V}$ is a K-approximate subgroup of $\overline{\mathbb{F}}_p$ and

$$\left\{a_1w(xy)+a_2w(xy^{-1}):x,y\in\prod_{20}\widehat{V}\right\}\leqslant K\#\widehat{V},$$

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

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, $\#(w(\prod_2\widehat{V})\overset{E}{+}w(\prod_2\widehat{V}))\lesssim\#\widehat{V}$. At the same time, $\#E\gg(\#\widehat{V})^2$, hence by B-S-G(3.4) and P-R, there exists $V'\subset\prod_2\widehat{V}, \#V'\gtrsim\#\widehat{V}$ such that

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

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

Exercise 4.21. Prove the general cases.

Remark 4.22 — Another view of this proposition is given by Eleke-Ronyai problem. Which shows that there exists $\varepsilon>0$, such that for every $f\in\mathbb{R}[x,y]$ or $f\in\mathbb{R}(x,y)$, then

(1) either $\forall A\subset\mathbb{R}$ finite, $\#A=N$, we have $\#f(A\times A)\gg N^{1+\varepsilon}$,

(2) or $\exists g,h,\phi:\mathbb{R}\to\mathbb{R}$ analytic such that $f(x,y)=\phi(g(x)+h(y))$.

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

Let $S\subset\mathrm{SL}(2,\mathbb{Z})$ 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 $\bmod p$. 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 $\chi_S=\frac{1}{\#S}\mathbb{1}_S$, define

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

then $T_p(\chi_S)\in\mathrm{End}(L^2(G_p))$. [Regard $L^2(G_p)$ as the family of density functions.]

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 $\langle S \rangle \subset \mathrm{SL}(2,\mathbb{Z})$ 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 $\bigoplus_p L_0^2(G_p)$ has no almost invariant vector).

Remark 5.4 — As a consequence of the exercise, let $S' \subset \langle S \rangle$ 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 $\mathrm{SL}(2,\mathbb{Z})$)
$\Gamma' \subset \mathrm{SL}(2,\mathbb{Z})$ 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, $\Gamma' \cap \Gamma(3) \subset \Gamma(3)$ 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. □

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

Remark 5.7 — This proposition allows us to reduce the statement of Theorem 5.2 to the case that S freely generates a non-abelian free group.

Theorem 5.8 (B-S-G weighted version)
Let μ,ν be two probability measures on G, $K\geqslant 2$, if

$$\|\mu*\nu\|\geqslant K^{-1}\|\mu\|^{\frac{1}{2}}\|\nu\|^{\frac{1}{2}},$$

then there exists an $O(K^{O(1)})$-approximate subgroup H, $a,b\in G$, such that

$$\#H\sim\|\mu\|^{-2}\sim\|\nu\|^{-2},\quad \mu(aH)\gtrsim 1,\nu(aH)\gtrsim 1.$$

Remark 5.9 — If $\mu=\frac{1}{\#A}\mathbb{1}_A$, then $\|\mu\|^2=\frac{1}{\#A}$. This shows that the exponent -2 is reasonable.

Remark 5.10 — $\|\mu\|^2\leqslant\|\mu\|_\infty\|\mu\|_1\leqslant 1$, and $\|\mu\|=1$ iff μ is Dirac. $\|\mu\|^2\geqslant\frac{1}{\#G}$, the equality holds iff $\mu=\chi_G$.

Remark 5.11 — $\|\mu*\nu\|\leqslant\|\mu\|_1\|\nu\|=\|\nu\|$, hence if $\|\mu\|^{\frac{1}{2}}\|\nu\|^{\frac{1}{2}}\lesssim\|\mu*\nu\|$, then $\|\mu\|\lesssim\|\nu\|$. Therefore, $\|\mu\|\sim\|\nu\|$.

Proof. Let $m=\frac{1}{16K^4}$, $M=4K^4$, let

$$A_0=\left\{x\in G: m\|\mu\|^2\leqslant\mu(x)\leqslant M\|\mu\|^2\right\},$$

$$A_-=\left\{x\in G:\mu(x)<m\|\mu\|^2\right\},\quad A_+=\left\{x\in G:\mu(x)>M\|\mu\|^2\right\}.$$

Consider $\mu_0=\mu\mathbb{1}_{A_0},\mu_-=\mu\mathbb{1}_{A_-},\mu_+=\mu\mathbb{1}_{A_+}$, then $\mu=\mu_0+\mu_-+\mu_+$. Similarly, write $\nu=\nu_0+\nu_-+\nu_+$. We have

$$\|\mu_-*\nu\|\leqslant\|\mu_-\|\leqslant m\|\mu\|\leqslant mK\|\mu\|^{\frac{1}{2}}\|\nu\|^{\frac{1}{2}},$$

$$\|\mu_+*\nu\|\leqslant\|\mu_+\|_1\|\nu\|\leqslant\frac{1}{M}\|\nu\|=\frac{K}{M}\|\mu\|^{\frac{1}{2}}\|\nu\|^{\frac{1}{2}}.$$

Hence

$$\|\mu_0*\nu_0\|\geqslant\frac{1}{2K}\|\mu\|^{\frac{1}{2}}\|\nu\|^{\frac{1}{2}}.$$

On the other hand,

$$\mu_0*\nu_0\sim\|\mu\|^2\|\nu\|^2\mathbb{1}_{A_0}*\mathbb{1}_{B_0},\quad\text{pointwise.}$$

Notice that $\#A_0\sim\|\mu\|^{-2}$, recall the additive energy, it shows that

$$\mathscr{E}_+(A_0,B_0)=\|\mathbb{1}_{A_0}*\mathbb{1}_{B_0}\|^2\gtrsim\|\mu\|^{-3}\|\nu\|^{-3}\gtrsim(\#A_0)^{\frac{3}{2}}(\#B_0)^{\frac{3}{2}}.$$

By B-S-G, $\exists A\subset A_0, B\subset B_0, \#A\gtrsim\#A_0,\#B\gtrsim\#B_0$ such that $\#(AB)\lesssim(\#A_0)^{\frac{1}{2}}(\#B_0)^{\frac{1}{2}}$. We have $\mu(A)=\mu_0(A)\gtrsim 1,\nu(B)\gtrsim 1$, it suffices to show the following lemma.

Lemma 5.12
Assume $\#AB\leqslant K(\#A)^{\frac{1}{2}}(\#B)^{\frac{1}{2}}$, then there exists $K^{O(1)}$-approximate subgroup H, $\exists a,b\in G$ such that

$$\#(A\cap aH)\gtrsim\#A,\quad\#(B\cap Hb)\gtrsim\#B.$$

Exercise 5.13. Assume $\#A\cdot A^{-1}\leqslant K\#A$. Then $\exists S\subset G$ symmetric such that

$$\#S\geqslant \frac{\#A}{2K}\quad\text{and}\quad \#\left(A\left(\prod_n S\right)A^{-1}\right)\leqslant 2^n K^{2n+1}\#A,\ \ \forall n\geqslant 0.$$

Show this statement by the following steps.

I. $\mathscr{E}(A,A^{-1})=\mathscr{E}(A^{-1},A)$.

II. Let $S=\left\{x\in G: r_{A^{-1}\cdot A}(x)\geqslant \frac{1}{2K}\#A\right\}$, show that $\#S\geqslant\frac{1}{2K}\#A$.

III. $\forall a,b\in A,\forall x_1,\cdots,x_n\in S$, bounded from below the number of ways to write $ax_1x_2\cdots x_nb^{-1}$ as $y_1y_2\cdots y_{n+1}$, where $y_j\in AA^{-1}$.

IV. Conclude.

Proof of Lemma assuming Exercise. By R-triangle, we have $\#AA^{-1}\lesssim\#A$. Take S as in the exercise, let $H=SS$. Then $\#(SSS)\lesssim\#A\lesssim\#S$, hence H is a $O(K^{O(1)})$-approximate subgroup. Besides $\#(AH)\lesssim\#H$, by R-covering, there holds $A\subset XHH\subset X'H$, where $\#X\lesssim 1,\#X'\lesssim 1$. Then theres is some $x\in X'$ such that $\#(A\cap xH)\gtrsim\#A$. $\square$

Proposition 5.14 (Bourgain-Gamburd expansion machine)

Γ group, $S\subset\Gamma$ finite, $S=S^{-1}$. Assume G is a finite quotient of Γ and $\pi:\Gamma\to G$ is the natural projection. Let $\chi_S=\frac{1}{\#S}\mathbb{1}_S$ and $\mu=\pi_*\chi_S$. Assume that

- (quasi-randomness) minimal degree of non-trivial irreducible linear representation of G over $\mathbb{C}$ is at least $(\#G)^\kappa$.
- (non-concentration in approximate subgroup)
  $\exists n_0\leqslant C\log\#G$, such that $\forall K$-approximate subgroup $H\subset G$,

$$\text{either}\quad \#H\geqslant\frac{1}{CK^C}\#G,\qquad\text{or}\quad \mu^{*2n_0}(H)\leqslant CK^C(\#G)^{-\kappa}.$$

Then $\mathrm{Spec}(T_0(\chi_S))\cap[1-c,1]=\varnothing$ for some $c=c(\kappa,C)>0$.

Lemma 5.15 (L^2-flattening)

Same assumption as above, $\forall\delta>0,\exists\varepsilon=\varepsilon(\delta,\kappa)>0$, let $\nu=\mu^{*n}$ where $n\geqslant n_0$. Assume $\|\nu\|^2\geqslant(\#G)^{-1+\delta}$, then $\|\nu*\nu\|\leqslant(\#G)^{-\varepsilon}\|\nu\|$.

Proof. Assume for a contradiction. Let $K=(\#G)^\varepsilon$, by B-S-G, there exists $H\subset G$ an $O(K^{O(1)})$-approximate subgroup such that $\#H\sim\|\nu\|^{-2}\leqslant(\#G)^{1-\delta}$ and $\nu(aH)\gtrsim 1$ for some $a\in G$. For every $x\in G$, we have

$$\mu^{*n_0}(xH)^2=\mu^{*n_0}(Hx^{-1})\mu^{*n_0}(xH)\leqslant\mu^{*2n_0}(HH).$$

Because HH is also an $O(K^{O(1)})$-approximate subgroup, by the assumption, at least one of the followings holds:

(1) $(\#G)^{1-\delta}\gtrsim\#(HH)\gtrsim\#G$.

(2) $\mu^{*2n_0}(HH)\lesssim(\#G)^{-\kappa}$, then $1\lesssim\nu(aH)\lesssim(\#G)^{-\frac{\kappa}{2}}$.

Take $\varepsilon = \varepsilon(\delta,\kappa)$ sufficiently small, both cases lead to a contradiction. $\square$

Proof of Proposition 5.14. Consequently, $\exists C_0 = C_0(\delta,\kappa)$ such that $\left\|\mu^{*C_0 n_0}\right\| \leqslant (\#G)^{-1+\delta}$. Let $n_1 = C_0 n_0$, let λ be an eigenvalue of $T_0(\chi_S)$, let m_λ be the multiplicity of λ. Consider $L^2(G)$ as the regular representation of G, then

$$L^2(G) = \bigoplus\nolimits_{\rho\in\widehat{G}} (\deg\rho)\rho.$$

Because $T(\chi_S) \in \mathbb{C}[\widehat{G}]$, hence it preserves each ρ, then $m_\lambda \geqslant \deg\rho \geqslant (\#G)^\kappa$.

On the other hand,

$$\operatorname{tr}(T(\chi_S)^{2n_1}) = \sum_{g\in G}\langle T(\chi_S)^{2n_1}\delta_g,\delta_g\rangle = \sum_{g\in G}\|T(\chi_S)^{n_1}\delta_g\|^2 = \#G\,\|\mu^{*n_1}\|^2 \leqslant (\#G)^\delta.$$

Hence $m_\lambda\lambda^{2n_1} \leqslant (\#G)^\delta$, take $\delta = \frac{\kappa}{2}$, then $\lambda^{2n_1} \leqslant (\#G)^{-\frac{\kappa}{2}}$. Therefore,

$$\log\lambda \leqslant -\frac{\kappa}{4}\frac{\log(\#G)}{C_0 n_0} \leqslant -\frac{\kappa}{4CC_0} \implies \lambda \leqslant 1-c.$$

$\square$

Quasi-randomness

Remark 5.16 — Gowers showed that if finite group G is κ-quasi-randomness, then Cayley graph of G for some generator sets is a quasi-random graph.

Theorem 5.17 (Frobenius)

Let $G = \mathrm{SL}(2,\mathbb{F}_p)$, let ρ be a non-trivial irreducible linear representation of G, then $\deg\rho \geqslant \frac{p-1}{2}$.

Proof. Let $(\rho,\mathcal{H})$ be a non-trivial linear representation of G. Consider $U = \left\{\begin{bmatrix}1 & * \\ & 1\end{bmatrix}\right\} \subset G$, then $U \cong \mathbb{F}_p$ is abelian. For $a\in\mathbb{F}_p$, let $\chi_a : \mathbb{F}_p \to \mathbb{C}, x \mapsto e(\frac{xa}{p})$. Then we have a decomposition

$$\mathcal{H} = \sum_{a\in\mathbb{F}_p}\mathcal{H}_a, \quad \mathcal{H}_a = \{\xi\in\mathcal{H} : \forall u\in U : \rho(u)\xi = \chi_a(u)\xi\}.$$

For $a_t = \begin{bmatrix}t & \\ & t^{-1}\end{bmatrix}, u\in U$, we have $a_t^{-1}ua_t = u^{-t^2}$. Then $\forall\xi\in\mathcal{H}_a, u\in U$,

$$\rho(u)\rho(a_t)\xi = \rho(a_t)\rho(a_t^{-1}ua_t)\xi = \rho(a_t)\chi_a(u)^{t^{-2}}\xi = \chi_{t^{-2}a}\rho(a_t)\xi.$$

Given $a\in\mathbb{F}_p$, the orbit $\left\{t^{-2}a : t\in\mathbb{F}_p^\times\right\}$ is either $\{0\}$ or have $\frac{p-1}{2}$ elements. Then $\dim\mathcal{H} \geqslant \frac{p-1}{2}$, otherwise $\mathcal{H} = \mathcal{H}_0$. In the second case, $U \in \ker\rho$, but $\ker\rho$ is a normal subgroup of G, hence ρ is trivial. $\square$

Non-concentration in approximate subgroup

Proposition 5.18

Let $S \subset \mathrm{SL}(2,\mathbb{Z})$ be a finite set, $S = S^{-1}$, freely generates a non-abelian free group. Then $\exists\kappa > 0, \exists C > 0$, such that for every prime p, there is some $n_0 \leqslant C\log p$, such that for every K-approximate subgroup $H \subset G_p$,

$$\text{either} \quad \#H \gtrsim \#G_p \asymp p^3, \quad \text{or} \quad \mu^{*2n_0}(H) \leqslant p^{-\kappa}.$$

Lemma 5.19 (Kesten)

Assume $\#S = 2k$, then $\exists c > 0$,

$$\max_{g\in\mathrm{SL}(2,\mathbb{Z})} \chi_S^{*2n}(g) = \chi_S^{*2n}(1) \leqslant \left(\frac{\sqrt{2k-1}}{k}\right)^n \leqslant e^{-cn}.$$

Exercise 5.20. Find a recursive relation and use generating function to prove the lemma.

Remark 5.21 — Let $B_n := \prod_n(\{1\}\cup S)$ be the ball of word metric. Then there is some $c > 0$, such that for every prime p and every $n \leqslant c\log p$, $\pi_p : B_n \mapsto G_p$ is injective. This is because the norms of elements in B_n are with at most exponential growth.

Proof of Proposition 5.18. Let H be a K-approximate subgroup of G_p, by Helfgott's Theorem (4.7), there are three cases:

(1) $\#H \lesssim 1$, then $\mu^{*n}(H) \leqslant e^{-cn}\#H \lesssim e^{-cn}$.

(2) $\#H \gtrsim \#G_p$.

(3) $\langle H\rangle \neq G_p$, we need a more technical theorem to deal with this case.

Theorem 5.22 (Dickson)

Let prime $p \geqslant 5$, assume $H \subset G_p$ and $\langle H\rangle \neq G_p$, then $\langle H\rangle$ is one of the followings:

(1) dihedral group $D_{2\frac{p\pm1}{2}}$ or its subgroup.

(2) Borel subgroup $\left\{\begin{bmatrix} * & * \\ & * \end{bmatrix}\right\} \subset G_p$.

(3) A_4, A_5, S_4.

Remark 5.23 — The third case in this theorem is similar with the case $\#H \lesssim 1$. For other two cases, we should notice that $\langle H\rangle$ is always a meta-abelian group, i.e.,

$$[[\langle H\rangle, \langle H\rangle], [\langle H\rangle, \langle H\rangle]] = \{1\}.$$

Continued Proof of Proposition 5.18. Take $n = \frac{c}{16}\log p$, we have

$$\mu^{*n}(H) \leqslant e^{-cn}\#(B_n \cap \pi_p^{-1}(H)).$$

Let $X = B_n \cap \pi_p^{-1}(H)$, we claim that $\#X \ll n^2$. Note that $[[X, X], [X, X]] \subset B_{16n}$, hence π_p is injective on it, which shows $[[X, X], [X, X]] = \{1\}$.

Let $z \in [X, X] \setminus \{1\}$, we have $[X, X] \in C(z)$. But S freely generates a non-abelian free group, we can show that

$$\#[X, X] \leqslant \#(C(z) \cap B_{4n}) \ll n.$$

Then there is $y \in X, b \in [X, X]$ such that

$$\#\{x \in X : [x, y] = b\} \gg \frac{\#X}{n}.$$

Take some x, then

$$\frac{\#X}{n} \ll \#(B_n \cap xC(y)) \ll n \implies \#X \ll n^2.$$

□

Combining above discussions, given $S \in \mathrm{SL}(2, \mathbb{Z})$, we can show that $(G_p, (\pi_p)_*\chi_S)$ satisfies the quasi-randomness condition and the non-concentration condition with parameters C, κ independent with p. By B-G expansion machine (5.14), $T_{p,0}(\chi_S)$ has a uniform spectral gap. This concludes the uniform expansion in $\mathrm{SL}(2, \mathbb{F}_p)$ (5.2). □

§6 Discretized sum-product theorems

The discretized settings: $A \subset \mathbb{R}$ bounded, $\delta > 0$.

Definition 6.1. The δ-covering number (metric entropy) of A is defined as

$$\mathcal{N}_\delta(A) := \min\left\{k \in \mathbb{N} : \exists x_1, x_2, \cdots, x_k, A \subset \bigcup_{i=1}^{n} B(x_i, \delta)\right\}.$$

Notation 6.2. $|A|$ denotes the Lebesgue measure of A. $A^{(\delta)} = A + B(0, \delta)$ be the δ-neighborhood of A.

Definition 6.3. A is called δ-separate if $\forall a \neq a' \in A, d(a, a') > \delta$.

We can also consider

$$\frac{|A^{(\delta)}|}{|B(0, \delta)|}, \quad \#\widetilde{A} \text{ where } \widetilde{A} \text{ is a maximal } \delta\text{-separated subset,}$$

$$\#\left\{k \in \mathbb{Z} : k\delta \in A^{(\delta)}\right\}, \quad \#\{k \in \mathbb{Z} : [k\delta, (k+1)\delta[\cap A = \varnothing\}.$$

Exercise 6.4. Show that all the quantities are big O of each other.

Remark 6.5 — How to understand $\mathcal{N}_\delta(A)$? We will always view δ as the size of a pixel or the resolution. Then think of $\mathcal{N}_\delta(A)$ as the number of pixels A needed at this resolution.

Some similar results hold:

1. (Ruzsa triangle) $\mathcal{N}_\delta(A - C)\mathcal{N}_\delta(B) \ll \mathcal{N}_\delta(A - B)\mathcal{N}_\delta(B - C)$.

2. (Ruzsa covering) If $\mathcal{N}_\delta(A+B) \leqslant K\mathcal{N}_\delta(A)$, then $B \subset A - A + \mathbb{O}(K) + B(0,\delta)$.
3. (Plünnecke-Ruzsa) If $\mathcal{N}_\delta(A+B) \leqslant K\mathcal{N}_\delta(A)$, then

$$\mathcal{N}_\delta\left(\sum_k B - \sum_l B\right) \ll_{k,l} K^{k+l}\mathcal{N}_\delta(A), \quad \forall k,l \in \mathbb{N}.$$

Definition 6.6. Let $\varphi : A \to \mathbb{R}$, the **$\varphi$-energy** of A at scale δ is

$$\mathscr{E}_\delta(\varphi, A) = \mathcal{N}_\delta\left((a,a') \in A \times A : |\varphi(a) - \varphi(a')| \leqslant \delta\right).$$

Remark 6.7 — We fix a norm on $\mathbb{R}^2$ to talk about $\mathcal{N}_\delta(B)$ with $B \subset \mathbb{R}^2$.

In particular, the additive energy between $A, B \subset \mathbb{R}$ at scale δ is

$$\mathscr{E}_\delta(+, A \times B), \quad \text{where } + : \mathbb{R} \times \mathbb{R} \to \mathbb{R}.$$

Theorem 6.8 (B-S-G)

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

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

(ii) $\exists G \subset A \times B$ such that

$$\mathcal{N}_\delta(G) \geqslant \frac{1}{K_2}\mathcal{N}_\delta(A)\mathcal{N}_\delta(B) \quad \text{and} \quad \mathcal{N}_\delta(A \overset{G}{+} B) \leqslant K_2\mathcal{N}_\delta(A)^{\frac{1}{2}}\mathcal{N}_\delta(B)^{\frac{1}{2}}.$$

(iii) $\exists A' \subset A, B' \subset B$ such that $\mathcal{N}_\delta(A') \geqslant \frac{1}{K_3}\mathcal{N}_\delta(A), \mathcal{N}_\delta(B') \geqslant \frac{1}{K_3}\mathcal{N}_\delta(B)$ and

$$\mathcal{N}_\delta(A' + B') \leqslant K_3\mathcal{N}_\delta(A)^{\frac{1}{2}}\mathcal{N}_\delta(B)^{\frac{1}{2}}.$$

Lemma 6.9

$\varphi : A \to \mathbb{R}$, then

$$\mathscr{E}_\delta(\varphi, A)\mathcal{N}_\delta(\varphi(A)) \gg \mathcal{N}_\delta(A)^2.$$

Sum-product estimate

Definition 6.10. Define $R_\delta(A,K) = \{x \in \mathbb{R} : \mathcal{N}_\delta(A + xA) \leqslant K\mathcal{N}_\delta(A)\}$.

Assume $A \subset B(0,1) \subset \mathbb{R}$, let $K, L \geqslant 1$, there are some properties:

1. $R_\delta(A,K)^{(K\delta)} \subset R_\delta(A, O(K^2))$.
2. $\forall s \geqslant 1$, $\langle R_\delta(A,K)\rangle_s \subset R_\delta(A, O_s(K^{O_s(1)}))$.
3. If $x \in R_\delta(A,K) \setminus B(0, L^{-1})$, then $x^{-1} \in R_\delta(A, KL)$.
4. If $\mathcal{N}_\delta(A+A) \leqslant K\mathcal{N}_\delta(A)$ and $\mathcal{N}_\delta(A + AA) \leqslant K\mathcal{N}_\delta(A)$, then

$$\mathcal{N}_\delta(\langle A\rangle_s) \ll_s K^{O_s(1)}\mathcal{N}_\delta(A), \quad \forall s \geqslant 1.$$

Remark 6.11 — $\mathcal{N}_\delta(AA)$ can be smaller than $\mathcal{N}_\delta(A)$. For example, let $A = B(0, \delta^{\frac{1}{2}})$, than $\mathcal{N}_\delta(A) \approx \delta^{-\frac{1}{2}}$ and $\mathcal{N}_\delta(AA) = 1$. That is, at scale δ, some points are somehow nilpotent.

Definition 6.12. The **Minkowski lower/upper dimension** are defined as

$$\underline{d}_M(A) = \liminf_{\delta \to 0^+} -\frac{\log \mathcal{N}_\delta(A)}{\log \delta}, \quad \overline{d}_M(A) = \limsup_{\delta \to 0^+} -\frac{\log \mathcal{N}_\delta(A)}{\log \delta}.$$

Theorem 6.13 (Bourgain Sum-Product Theorem)
$\forall \sigma \in (0,1), \exists \varepsilon = \varepsilon(\sigma) > 0$ such that for every $A \subset B(0,1) \subset \mathbb{R}, \delta > 0$ sufficiently small, assume that

- $\mathcal{N}_\delta(A) \leqslant \delta^{-\sigma-\varepsilon}$.
- (Frostman type non-concentration)

$$\forall \rho \geqslant \delta, \quad \max_{x \in \mathbb{R}} \mathcal{N}_\delta(A \cap B(x, \rho)) \leqslant \delta^{-\varepsilon} \rho^\sigma \mathcal{N}_\delta(A).$$

Then $\mathcal{N}_\delta(A + AA) \geqslant \delta^{-\varepsilon} \mathcal{N}_\delta(A)$.

Remark 6.14 — The conclusion does not hold without the non-concentration condition, for example, $A = B(0, \delta^{\frac{1}{2}})$.

Remark 6.15 — By a variant of Katz-Tao lemma (2.9), the conclusion can be replaced by $\max\{\mathcal{N}_\delta(A + A), \mathcal{N}_\delta(AA)\} \geqslant \delta^{-\varepsilon} \mathcal{N}_\delta(A)$.

Let us first explain the idea of proof. It is similar with the proof of sum-product theorem in a discrete case. Assume that $A + AA$ has no essential increasing. We construct the set $F = (A - A)/(A - A)$ and we can show that F is also not essential larger that A. Besides, F is similar with a field. In a discretized setting, we expect to show that $F^{(\delta)} = [0,1]$. Otherwise, for every $x \in [0,1] \setminus F^{(\delta)}$, we can show that $A + xA$ is large (recall Lemma 2.8). Precisely, $x \notin R_\delta(A, \delta^{-O(\varepsilon)})$. It follows that $R_\delta(A, \delta^{-O(\varepsilon)}) \subset F$. This will contradict with $F \subset R_\delta(A, \delta^{-O(\varepsilon)})$ and an almost ring structure.

Observation 6.16. For $A \subset \mathbb{R}, \delta < \delta'$, we have $\mathcal{N}_{\delta'}(A) \leqslant \mathcal{N}_\delta(A) \ll \frac{\delta'}{\delta} \mathcal{N}_{\delta'}(A)$.

Observation 6.17. For $A, B \subset \mathbb{R}, B \subset B(0, \rho)$, we have $\mathcal{N}_\delta(A + B) \geqslant \mathcal{N}_\rho(A) \mathcal{N}_\delta(B)$.

Proof. Let $\gamma = \gamma(\delta) > 0$ very small to be determined, let

$$F = \frac{A - A}{(A - A) \setminus B(0, \delta^\gamma)}.$$

Assume for a contradiction that

$$\mathcal{N}_\delta(A + AA) \leqslant \delta^{-\varepsilon} \mathcal{N}_\delta(A).$$

Let $\rho = \delta^{\frac{\varepsilon}{\sigma}}$, then $A \setminus B(0, \delta^{\frac{\varepsilon}{\sigma}}) \neq \varnothing$ by the non-concentration condition. Then

$$\mathcal{N}_\delta(AA) \geqslant \delta^{O(\frac{\varepsilon}{\sigma})}\mathcal{N}_\delta(A),$$

By the assumption and P-R, we have

$$\mathcal{N}_\delta(A+A) \leqslant \delta^{-O(\varepsilon+\frac{\varepsilon}{\sigma})}\mathcal{N}_\delta(A).$$

This shows that $\langle A\rangle_s \subset R_\delta(A, O_s(\delta^{O_s(\varepsilon)}))$ for every $s \geqslant 0$.

Claim Let $\delta_1 = \delta^{1-2\gamma}$, then either $F^{(2\delta_1)} \supset [0,1]$ or $\exists x \in F$, $\frac{x+1}{2} \notin F^{(\delta_1)}$ or $\frac{x}{2} \notin F^{(\delta_1)}$.
Proof of Claim. Assume $\forall x \in F, \frac{x+1}{2}, \frac{x}{2} \in F^{(\delta_1)}$. Then for every $x \in F^{(2\delta_1)}$, we have $\frac{x+1}{2}, \frac{x}{2} \in F^{(2\delta_1)}$. Because $0, 1 \in F \subset F^{(2\delta_1)}$, then $[0,1] \subset F^{(2\delta_1)}$.

Dense case: $F^{(2\delta_1)} \supset [0,1]$.
Then $\mathcal{N}_{\delta_1}(F) \gg \delta_1^{-1}$. Let $\widetilde{F} \subset F, \widetilde{A} \subset A \setminus B(0,\delta^\gamma)$ be maximal δ_1-separated sets. Consider

$$\widetilde{A} \times \widetilde{F} \to (AA-AA)\times(AA-AA), \quad (a,x) \mapsto (au_x, av_x), x = \frac{u_x}{v_x}.$$

We show that this map is injective and the image is $\frac{\delta}{C}$-separated. Assume $a'u_{x'} = au_x + O(\frac{\delta}{C}), a'v_{x'} = av_x + O(\frac{\delta}{C})$, then

$$|a|, |v_x| \geqslant \delta^\gamma \implies x' = \frac{au_{x'}}{av_{x'}} = \frac{au_x + O(\frac{\delta}{C})}{av_x + O(\frac{\delta}{C})} = \frac{u_x}{v_x} + O\left(\frac{\delta_1}{C}\right).$$

Choose C large enough, it implies that $|x - x'| \leqslant \delta_1$ and hence $x' = x$. By $\widetilde{A}$ is δ_1-separated, we have $a' = a$. Hence, by P-R,

$$\#\widetilde{A}\#\widetilde{F} \ll \mathcal{N}_\delta(AA-AA)^2 \leqslant \delta^{-O(\varepsilon)}\mathcal{N}_\delta(A)^2.$$

Because $\#\widetilde{F} \asymp \mathcal{N}_{\delta_1}(F) \asymp \delta_1^{-1} = \delta^{-1+2\gamma}$, and

$$\#\widetilde{A} \asymp \mathcal{N}_{\delta_1}(A \setminus B(0,\delta^\gamma)) \gg \delta^{-2\gamma}\mathcal{N}_\delta(A\setminus B(0,\delta^\gamma)) \gg \delta^{-2\gamma}(\mathcal{N}_\delta(A) - \delta^{-\varepsilon}\delta^{\gamma\sigma}\mathcal{N}_\delta(A)).$$

Choose γ small such that $\delta^{\gamma\sigma-\varepsilon} \leqslant \frac{1}{2}$, then

$$\mathcal{N}_\delta(A) \gg \delta^{-1+O(\gamma)+O(\varepsilon)}$$

contradict with $\mathcal{N}_\delta(A) \leqslant \delta^{-\varepsilon-\sigma}$ when γ, ε small enough.

Gap case: $\exists x \in F$, such that $\frac{x+1}{2} \notin F^{(\delta_1)}$ or $\frac{x}{2} \notin F^{(\delta_1)}$.
Write $\frac{x+1}{2}$ or $\frac{x}{2}$ as $\frac{u}{v}$, then $u, v \in A-A+A-A$ and $|v| \geqslant \delta^\gamma$. We know $u, v \in R_\delta(A, O(\delta^{-O(\varepsilon)}))$, by R-covering and P-R, we have $\mathcal{N}_\delta(A+uA+vA) \ll \delta^{-O(\varepsilon)}\mathcal{N}_\delta(A)$. We want to give a lower bound of $\mathcal{N}_\delta(uA+vA)$. Consider

$$\varphi : A \times A \to \mathbb{R}, \quad (a,b) \mapsto ua + vb,$$

it suffices to give an upper bound for $\mathscr{E}_\delta(\varphi, A\times A)$. For $a, b, c, d \in A$, if $|u(a-c)+v(b-d)| \leqslant \delta$, then

$$\left|\frac{u}{v} - \frac{d-b}{a-c}\right| \leqslant \frac{\delta}{|v||a-c|}.$$

Because $\frac{u}{v} \notin F^{(\delta_1)}$, $|v| \geqslant \delta^\gamma$, then $|a-c| \leqslant \delta^\gamma$. Now we estimate the choices of (a,b,c,d) :

- Choice for a : $\mathcal{N}_\delta(A)$ choices, choice for b : $\mathcal{N}_\delta(A)$ choices.
- Fix a, choice for c : $\mathcal{N}_\delta(A \cap B(a, \delta^\gamma)) \leqslant \delta^{-\varepsilon+\gamma\sigma}\mathcal{N}_\delta(A)$.
- Fix a, b, c, choice for d : $\mathcal{N}_\delta(A \cap B(-, \frac{\delta}{|v|})) \leqslant \delta^{-\varepsilon}(\frac{\delta}{|v|})^\sigma \mathcal{N}_\delta(A)$.

Then

$$\mathscr{E}_\delta(\varphi, A \times A) \leqslant \delta^{-O(\varepsilon)+\gamma\sigma+\sigma}|v|^{-\sigma}\mathcal{N}_\delta(A)^4 \implies \mathcal{N}_\delta(uA + vA) \geqslant |v|^\sigma \delta^{O(\varepsilon)-\gamma\sigma-\sigma}.$$

Because

$$\mathcal{N}_\delta(A) \leqslant \mathcal{N}_{2|v|}(A) \max_x \mathcal{N}_\delta(A \cap B(x, 2|v|)) \ll \delta^{-\varepsilon}|v|^\sigma \mathcal{N}_\delta(A)\mathcal{N}_{2|v|}(A),$$

we have $\mathcal{N}_{2|v|}(A) \gg \delta^\varepsilon |v|^{-\sigma}$. Notice that $(uA + vA) \subset B(0, 2|v|)$, then

$$\mathcal{N}_\delta(A + uA + vA) \gg \mathcal{N}_{2|v|}(A)\mathcal{N}_\delta(uA + vA) \gg |v|^{-\sigma}|v|^\sigma \delta^{O(\varepsilon)-\gamma\sigma-\sigma}.$$

But we know that $u, v \in (A - A + A - A) \subset R_\delta(A, \delta^{-O(\varepsilon)})$. Then

$$\mathcal{N}_\delta(A + uA + vA) \ll \delta^{-O(\varepsilon)}\mathcal{N}_\delta(A) \leqslant \delta^{-O(\varepsilon)-\sigma}.$$

Choose γ, ε small enough, a contradiction. (Choose γ small and ε much smaller than γ.) $\square$

Theorem 6.18 (Bourgain Sum-Product Theorem, another version)
$\forall \sigma \in (0, 1), \kappa > 0, \exists \varepsilon = \varepsilon(\sigma, \kappa) > 0$ such that for every $A \subset B(0, 1) \subset \mathbb{R}$ and $\delta > 0$ sufficiently small, assume that

- $\mathcal{N}_\delta(A) \leqslant \delta^{-\sigma-\varepsilon}$.
- $\forall \rho \geqslant \delta, \mathcal{N}_\rho(A) \geqslant \delta^\varepsilon \rho^{-\kappa}$.

Then $\mathcal{N}_\delta(A + AA) \geqslant \delta^{-\varepsilon}\mathcal{N}_\delta(A)$.

Proof. We prove a special case of $\kappa = \sigma$. Assume $\mathcal{N}_\delta(A + AA) \leqslant \delta^{-\varepsilon}\mathcal{N}_\delta(A)$, consider $\rho = \delta^{\frac{\varepsilon}{\sigma}}$, we can also have $A \setminus B(0, \rho) \neq \varnothing$. A same argument, we have $\mathcal{N}_\delta(A + A + AA) \leqslant \delta^{-O(\varepsilon)}\mathcal{N}_\delta(A)$. Hence

$$\delta^{-O(\varepsilon)}\mathcal{N}_\delta(A) \geqslant \mathcal{N}_\delta(A + A + AA) \geqslant \mathcal{N}_\delta(A + A) \geqslant \mathcal{N}_\rho(A) \max_{x \in \mathbb{R}} \mathcal{N}_\delta(A \cap B(x, \rho)),$$

then $\max_{x\in\mathbb{R}} \mathcal{N}_\delta(A \cap B(x, \rho)) \leqslant \delta^{-O(\varepsilon)}\rho^\sigma \mathcal{N}_\delta(A)$. It gives the condition in last version. $\square$

Remark 6.19 — An intuition is that, if $A + AA$ has no increasing, then A is like a fractal and A has a similar structure on each scale larger than δ.

§7 Projection theorem

Let $\mathbb{S}^1 = \{\theta \in \mathbb{R}^2 : \|\theta\| = 1\}$ be the unit circle in $\mathbb{R}^2$, for every $\theta \in \mathbb{S}^1$, let

$$\mathrm{proj}_\theta : \mathbb{R}^2 \to \mathbb{R} \cdot \theta$$

be the orthogonal projection.

Theorem 7.1 (Bourgain's Projection Theorem)

For every $\alpha \in (0,1), \kappa > 0$, there exists $\varepsilon = \varepsilon(\alpha,\kappa) > 0$, the following holds for $\delta > 0$ sufficiently small. Let $A \subset B_{\mathbb{R}^2}(0,1)$, assume

- $\mathcal{N}_\delta(A) \leqslant \delta^{-2\alpha}$.
- $\forall \rho \geqslant \delta, \forall x \in \mathbb{R}^2, \mathcal{N}_\delta(A \cap B(x,\rho)) \leqslant \delta^{-\varepsilon}\rho^{2\alpha}\mathcal{N}_\delta(A)$.

Write

$$\mathscr{E} = \left\{\theta \in \mathbb{S}^1 : \mathcal{N}_\delta(\mathrm{proj}_\theta A) \leqslant \delta^{-\alpha-\varepsilon}\right\},$$

then $\mathscr{E}$ does not support a probability measure μ satisfying

$$\mu(B_{\mathbb{S}^1}(\theta,\rho)) \leqslant \delta^{-\varepsilon}\rho^{\kappa}, \quad \forall \rho \geqslant \delta, \theta \in \mathbb{S}^1.$$

Remark 7.2 — $\mathscr{E}$ refers to an exception.

Example 7.3

Let $A = B(0,\delta^{\frac{1}{2}})$, then $\mathcal{N}_\delta(A) \asymp \delta^{-1}$. Notice that $\mathcal{N}_\delta(\mathrm{proj}_\theta A) \asymp \delta^{-\frac{1}{2}}$, hence $\mathscr{E} = \mathbb{S}^1$. This is a contradiction. The reason is that A does not satisfy the second condition (non concentration condition).

Example 7.4

$A = C \times C$, where C is a Cantor set. We can choose C let $\mathcal{N}_\delta(C - C) \asymp \mathcal{N}_\delta(C)$, then when θ near $0, \frac{\pi}{2}, \frac{\pi}{4}$, $\mathcal{N}_\delta(\mathrm{proj}_\theta A)$ is small. For more other θ's, $\mathcal{N}_\delta(\mathrm{proj}_\theta A)$ is large.

Idea Write $\theta = \theta_t = \frac{(1,t)}{\sqrt{1+t^2}}$, where $t \in [\frac{1}{2}, 2]$. Then

$$\mathrm{proj}_\theta(x,y) = \frac{\langle\theta,(x,y)\rangle}{\langle\theta,\theta\rangle}\theta = (x+ty)\frac{\theta}{\sqrt{1+t^2}}.$$

Consider a special case for $A = A_0 \times A_0$, then

$$\mathcal{N}_\delta(\mathrm{proj}_\theta A) \asymp \mathcal{N}_\delta(A_0 + tA_0).$$

Then $\mathscr{E}$ is almost the set $R_\delta(A_0, \delta^{-\varepsilon})$.

Theorem 7.5 (Bourgain Sum-Product Theorem, another version)

$\forall \alpha \in (0,1), \forall \kappa > 0, \exists \varepsilon = \varepsilon(\alpha,\kappa) > 0$, such that for every $A_0 \subset B(0,1) \subset \mathbb{R}$ and $\delta > 0$ sufficiently small, assume that

- $\mathcal{N}_\delta(A_0) \leqslant \delta^{-\alpha-\varepsilon}$.
- $\forall \rho \geqslant \delta, x \in \mathbb{R}, \mathcal{N}_\delta(A_0 \cap B(x,\rho)) \leqslant \delta^{-\varepsilon}\rho^{\kappa}\mathcal{N}_\delta(A_0)$.

Then for every $B_0 \subset \mathbb{R}$ such that $\forall \rho \geqslant \delta, \mathcal{N}_\rho(B_0) \geqslant \delta^{\varepsilon}\rho^{-\kappa}$, there exists $t \in B_0$, such that $\mathcal{N}_\delta(A_0 + tA_0) \geqslant \delta^{-\varepsilon}\mathcal{N}_\delta(A_0)$.

Remark 7.6 — The condition $\forall \rho \geqslant \delta, \mathcal{N}_\rho(B_0) \geqslant \delta^\varepsilon \rho^{-\kappa}$ is strictly weaker than the non concentration condition for B_0.

Lemma 7.7

$\kappa, \varepsilon > 0$, let μ be a probability measure on $\mathbb{R}$, $\operatorname{supp}\mu \subset B(0,1)$, satisfying

$$\mu(B(x,\rho)) \leqslant \delta^{-\varepsilon}\rho^\kappa, \quad \forall \rho \geqslant \delta, x \in \mathbb{R}.$$

Then $\exists B_0 \subset \operatorname{supp}\mu$ satisfying

$$\mathcal{N}_\delta(B_0 \cap B(x,\rho)) \leqslant \delta^{-O(\varepsilon)}\rho^\kappa \mathcal{N}_\delta(B_0), \quad \forall \rho \geqslant \delta, x \in \mathbb{R}.$$

Proof. Let

$$\mathcal{Q} := \{[k\delta, (k+1)\delta[: k \in \mathbb{Z}\},$$

for every $i \in \mathbb{N}$, define

$$\mathcal{Q}_i = \left\{Q \in \mathcal{Q} : 2^{-i-1} < \mu(Q) \leqslant 2^{-i}\right\}.$$

Observe that

$$\mu\left(\bigcup_{\substack{Q\in\mathcal{Q}_i,\\ i\geqslant 2|\log\delta|}} Q\right) \ll \delta^{-1}2^{-2|\log\delta|} \leqslant \delta < \frac{1}{2}.$$

Then $\exists i \in [0, 2|\log\delta|] \cap \mathbb{N}$, such that (for δ sufficiently small)

$$\mu\left(\bigcup_{Q\in\mathcal{Q}_i} Q\right) \geqslant \frac{1}{4|\log\delta|} \geqslant \delta^\varepsilon.$$

Fix this i, let $B_1 = \bigcup_{Q\in\mathcal{Q}_i} Q$ and $B_0 = B_1 \cap \operatorname{supp}\mu$. Then for every $\rho \geqslant \delta, x \in \mathbb{R}$,

$$\begin{aligned} \mathcal{N}_\delta(B_0 \cap B(x,\rho)) &\asymp \#\{Q \in \mathcal{Q}_i : Q \cap B(x,\rho) \neq \varnothing\} \\ &\ll \frac{\mu(B_0 \cap B(x,2\rho))}{\min_{Q\in\mathcal{Q}_i}\mu(Q)} \ll \frac{\delta^{-\varepsilon}\rho^\kappa}{\min_{Q\in\mathcal{Q}_i}\mu(Q)} \leqslant \delta^{-2\varepsilon}\rho^\kappa \#\mathcal{Q}_i \asymp \delta^{-2\varepsilon}\rho^\kappa\mathcal{N}_\delta(B_0). \end{aligned}$$

□

Lemma 7.7 + Theorem 7.5 $\implies$ the special case $A = A_0 \times A_0$ of Theorem 7.1.

Proof of General Case of Theorem 7.1. Assume for a contradiction that $\mathscr{E}$ supports such a probability measure μ. In particular, there exists $\theta_1, \theta_2 \in \mathscr{E}$ with $d(\theta_1,\theta_2) \geqslant \delta^{\frac{\varepsilon}{\kappa}} = \delta^{O(\varepsilon)}$. After a rotation and affine transformation of norm at most $\delta^{O(\varepsilon)}$, we can assume that x-axis and y-axis are both in $\mathscr{E}$. Let B, C be the projection of A to the x-axis and y-axis, respectively. For a $\theta_t = \frac{(1,t)}{\sqrt{1+t^2}} \in \mathscr{E}$, we have

$$\mathcal{N}_\delta(B \overset{A}{+} tC) \leqslant \delta^{-\alpha-\varepsilon},$$

here we abuse a notation $\overset{A}{+}$ to refer to $a = (b,c) \in A, b \in B, c \in C$. We have

$$\delta^{-2\alpha+O(\varepsilon)} \leqslant \mathcal{N}_\delta(A) \ll \mathcal{N}_\delta(B)\mathcal{N}_\delta(C),$$

hence $\mathcal{N}_\delta(B), \mathcal{N}_\delta(C) \geqslant \delta^{-\alpha+O(\varepsilon)}$. By B-S-G (6.8), there exists $B_t \subset B, C_t \subset C$ such that

$$\mathcal{N}_\delta(B_t) \geqslant \delta^{-\alpha+O(\varepsilon)}, \quad \mathcal{N}_\delta(C_t) \geqslant \delta^{-\alpha+O(\varepsilon)}, \quad \mathcal{N}_\delta(B_t + tC_t) \leqslant \delta^{-\alpha-O(\varepsilon)}.$$

If B_t, C_t are independent of t, then done. We need a following lemma.

Lemma 7.8 (popularity argument)
(X, λ) is a finite measure space, (T, ν) is a probability space, $K \geqslant 2$. If $\forall t \in T, X_t \subset X$ with $\lambda(X_t) \geqslant \frac{1}{K}\lambda(X)$. Then $\exists t_\star \in T$, such that

$$\nu\left\{t \in T : \lambda(X_{t_\star} \cap X_t) \geqslant \frac{1}{2K^2}\lambda(X)\right\} \geqslant \frac{1}{2K^2}.$$

Exercise 7.9. Prove the lemma. Hint: applying C-S to $x \mapsto \int \mathbb{1}_{X_t}(x)\mathrm{d}\nu(t)$.

Continued Proof of Theorem 7.1. Use lemma for $X = B^{(\delta)} \times C^{(\delta)}$, $\lambda = \mathrm{Leb}$. Let $X_t = B_t^{(\delta)} \times C_t^{(\delta)}$, let ν be the push forward of μ under $\theta_t \mapsto t$. Then $\exists t_\star \in \mathbb{R}, D \subset \mathbb{R}$ with $\nu(D) \geqslant \delta^{O(\varepsilon)}$ such that for every $t \in D$,

$$\mathcal{N}_\delta(B_t \cap B_\star) \geqslant \delta^{-\alpha+O(\varepsilon)}, \quad \mathcal{N}_\delta(C_t \cap C_\star) \geqslant \delta^{-\alpha+O(\varepsilon)},$$

where $B_\star = B_{t_\star}$ and $C_\star = C_{t_\star}$.

We use notation $E \approx F$ to refer to $\mathcal{N}_\delta(E-F) \ll \delta^{-O(\varepsilon)}\mathcal{N}_\delta(E)^{\frac{1}{2}}\mathcal{N}_\delta(F)^{\frac{1}{2}}$. Now, we do some Ruzsa calculus. We know $B_t \approx -tC_t$, hence $B_t \approx B_t$, and then $B_t \approx B_t \cap B_\star$. Moreover, for every $t \in D$, we have $B_\star \approx B_t \cap B_\star \approx B_t$ and $C_\star \approx C_t \cap C_\star \approx C_t$. Because $B_\star \approx -t_\star C_\star$, we have

$$B_\star \approx B_t \approx -tC_t \approx -tC_\star \approx \frac{t}{t_\star}B_\star, \quad \forall t \in D \subset [\frac{1}{2}, 2].$$

This will contradict with the Sum-Product Theorem (7.5) when ε is small. $\square$

Theorem 7.10 (Bourgain's Projection Theorem, adapted version)
For every $\alpha \in (0,1), \kappa > 0$, there exists $\varepsilon = \varepsilon(\alpha, \kappa) > 0$, the following holds for $\delta > 0$ sufficiently small. Let $A \subset B_{\mathbb{R}^2}(0,1)$, assume

- $\mathcal{N}_\delta(A) \leqslant \delta^{-2\alpha}$.
- $\forall \rho \geqslant \delta, \forall x \in \mathbb{R}^2, \mathcal{N}_\delta(A \cap B(x,\rho)) \leqslant \delta^{-\varepsilon}\rho^{2\alpha}\mathcal{N}_\delta(A)$.

Write

$$\mathscr{E} = \left\{\theta \in \mathbb{S}^1 : \exists A' \subset A, \mathcal{N}_\delta(A') \geqslant \delta^\varepsilon \mathcal{N}_\delta(A) \text{ and } \mathcal{N}_\delta(\mathrm{proj}_\theta A') \leqslant \delta^{-\alpha-\varepsilon}\right\},$$

then $\mathscr{E}$ does not support a probability measure μ satisfying

$$\mu(B_{\mathbb{S}^1}(\theta,\rho)) \leqslant \delta^{-\varepsilon}\rho^\kappa, \quad \forall \rho \geqslant \delta, \theta \in \mathbb{S}^1.$$

Corollary 7.11
$\forall \alpha \in (0,1), \exists \varepsilon = \varepsilon(\alpha) > 0$, let $A \subset \mathbb{R}^2$ be a Borel subset. If $\dim_H A = 2\alpha$, then

$$\dim_H\left(\left\{\theta \in \mathbb{S}^1 : \dim_H \mathrm{proj}_\theta A \leqslant \alpha + \varepsilon\right\}\right) = 0.$$

Remark 7.12 — To compare with Marstrand's Theorem: if $\alpha < \frac{1}{2}$, then

$$\mathrm{Leb}\left\{\theta \in \mathbb{S}^1 : \dim_H \mathrm{proj}_\theta A < 2\alpha\right\} = 0.$$

Recall Hausdorff dimension of A, $\dim_H A \leqslant \alpha$ if and only if $\forall \varepsilon > 0, \exists x_i \in \mathbb{R}^2, 0 < r_i < \varepsilon, i \in \mathbb{N}$, such that

$$A \subset \bigcup_{i \in \mathbb{N}} B(x_i, r_i), \quad \sum_{i=0}^{\infty} r_i^{\alpha+\varepsilon} < \varepsilon.$$

In other word, $\dim_H A = \inf\{\text{such } \alpha\}$.

Lemma 7.13 (Frostman Lemma)
If $A \subset \mathbb{R}^2, \dim_H A > \alpha$, then $\exists$ a finite nonzero Borel measure μ on $\mathbb{R}^2, \operatorname{supp} \mu \subset A$, and for every $\rho > 0, x \in \mathbb{R}^2$, $\mu(B(x, \rho)) < \rho^\alpha$.

Remark 7.14 — Such a measure is said to be α-Frostman (or α-Hölder?).

Proof of Corollary 7.11. Assume for a contradiction, let

$$\mathscr{E} = \left\{\theta \in \mathbb{S}^1 : \dim_H \mathrm{proj}_\theta A \leqslant \alpha + \varepsilon\right\},$$

assume $\dim_H \mathscr{E} > \kappa > 0$. By Frostman lemma, there exists μ on $\mathscr{E}$ which is κ-Frostman. There exists ν on A is $(2\alpha - \varepsilon)$-Frostman. For every $\theta \in \mathscr{E}$, we can cover $\mathrm{proj}_\theta A$ by $\bigcup_{i \in \mathbb{N}} B(x_i, r_i)$ with $r_i \leqslant \delta = 2^{k_0}$ and $\sum r_i^{\alpha+2\varepsilon} \leqslant \varepsilon$. WLOG, we can assume that $r_i = 2^{-k_i}$ where $k_i \in \mathbb{N}$, then

$$\mathrm{proj}_\theta A \subset \bigcup_{k \geqslant k_0} B_{\theta,k}, \quad \text{where } B_{\theta,k} := \bigcup_{x \in X_{\theta,k}} B(x, 2^{-k}).$$

We also have an estimate for every $k \geqslant k_0$, $\# X_{\theta,k} \leqslant 2^{k(\alpha+2\varepsilon)}$. Then

$$\nu(A)\mu(\mathscr{E}) = \int \nu\left(\bigcup_{k \geqslant k_0} \mathrm{proj}_\theta^{-1} B_{\theta,k}\right) \mathrm{d}\mu(\theta) \leqslant \int \sum_{k \geqslant k_0} \nu(\mathrm{proj}_\theta^{-1} B_{\theta,k}) \mathrm{d}\mu(\theta).$$

Let $A_{\theta,k} = \mathrm{proj}_\theta^{-1} B_{\theta,k}$, then $\exists k \geqslant k_0$, such that

$$\frac{1}{\nu(A)\mu(\mathscr{E})} \int \nu(A_{\theta,k}) \mathrm{d}\mu(\theta) \geqslant \frac{6}{\pi^2} \frac{1}{k} \gg |\log \delta|^{-2} \geqslant \delta^{-\varepsilon}.$$

Choose $\delta_0 = 2^{-k_0}$ sufficiently small, fix a such k, let $\delta = 2^{-k} \leqslant \delta_0$. We have $A_{\theta,k} \subset A$ and

$$\mathcal{N}_\delta(\mathrm{proj}_\theta A_{\theta,k}) \leqslant \# X_{\theta,k} \leqslant \delta^{-\alpha-2\varepsilon}.$$

Then $\exists D \subset \mathscr{E} \subset \mathbb{S}^1$ such that $\mu(D) \geqslant \delta^\varepsilon \mu(\mathscr{E})$ and $\forall \theta \in D$, $\nu(A_{\theta,k}) \geqslant \delta^\varepsilon \nu(A)$. We want to find $B \subset A$ such that

$$\mathcal{N}_\delta(A_{\theta,k} \cap B) \geqslant \delta^\varepsilon \mathcal{N}_\delta(B), \quad \mathcal{N}_\delta(B \cap B(x, \rho)) \leqslant \delta^{-O(\varepsilon)} \rho^{2\alpha} \mathcal{N}_\delta(B).$$

A similar argument in the proof of Lemma 7.7, we can find such a B and some $D' \subset D$, which contradicts with the Sum-Product theorem. $\square$

§8 Fourier decay of multiplicative convolution

Let μ be a Borel measure on $\mathbb{R}$, the Fourier transform of μ is

$$\widehat{\mu}(\xi) = \int e^{2\pi i \xi x} \mathrm{d}\mu(x), \quad \forall \xi \in \mathbb{R}.$$

Obviously, $|\widehat{\mu}(\xi)| \leqslant \mu(\mathbb{R})$. And $\widehat{\mu \boxplus \nu}(\xi) = \widehat{\mu}(\xi)\widehat{\nu}(\xi)$.

Theorem 8.1 (Bourgain)

For every $\kappa > 0$, there exists $\varepsilon = \varepsilon(\kappa) > 0, s = s(\kappa) \geqslant 1$. Let $\delta > 0$ sufficiently small and μ be a Borel probability measure on $\mathbb{R}$ with $\operatorname{supp} \mu \subset [-1, 1]$. Assume that

- $[\mathrm{NC}(\kappa, \varepsilon)] \quad \forall \rho \geqslant \delta, \max_{x \in \mathbb{R}} \mu(B(x, \rho)) \leqslant \delta^{-\varepsilon} \rho^{\kappa}$.

Then for every $\xi \in \mathbb{R}$ with $\delta^{-1+\varepsilon} \leqslant |\xi| \leqslant \delta^{-1-\varepsilon}$, we have

$$\left| \int e^{2\pi i \xi x_1 \cdots x_s} \mathrm{d}\mu(x_1) \cdots \mathrm{d}\mu(x_s) \right| \leqslant \delta^{\varepsilon}.$$

Or, $|\widehat{\mu^{*s}}(\xi)| \leqslant \delta^{\varepsilon}$, where μ^{*s} refers to the s-th multiplicative convolution of μ.

We first state another variant of sum-product theorem which includes a measure. It is a direct consequence of combining Theorem 7.5 and Lemma 7.7. And at the end of this section, we will show how to derive this version by Theorem 6.18.

Theorem 8.2

$\forall \sigma \in (0, 1), \kappa > 0, \exists \varepsilon = \varepsilon(\sigma, \kappa) > 0$ such that the following holds for all $\delta > 0$ small enough. Let $A \subset [-1, 1] \subset \mathbb{R}$ and μ be a probability measure on $[-1, 1]$. Assume that

- $\mathcal{N}_\delta(A) \leqslant \delta^{-\sigma-\varepsilon}$.
- $\forall \rho \geqslant \delta, \mathcal{N}_\rho(A) \geqslant \delta^{\varepsilon} \rho^{-\kappa}$.
- $\forall \rho \geqslant \delta, \max_{x \in \mathbb{R}} \mu(B(x, \rho)) \leqslant \delta^{-\varepsilon} \rho^{\kappa}$.

Then $\mu(R_\delta(A, \delta^{-\varepsilon})) \leqslant \delta^{\varepsilon}$.

Notation 8.3. • $P_\delta = \frac{1}{2\delta} \mathbb{1}_{B(0,\delta)}$, regard P_δ as a density of probability measure.

- For a probability measure μ, define

$$\mu_\delta(x) = (\mu \boxplus P_\delta)(x) = \int P_\delta(x - y) \mathrm{d}\mu(y) = \frac{1}{2\delta} \mu(B(x, \delta)).$$

  Also regard as a density function.

- $\|\mu\|_{2,\delta}^2 := \|\mu_\delta\|_2^2 = \int \mu_\delta(x)^2 \mathrm{d}x$.

Lemma 8.4 (L^2-flattening)

For every $\kappa > 0$, there exists $\varepsilon = \varepsilon(\kappa) > 0$. Let $\delta > 0$ sufficiently small and μ be a Borel probability measure on $\mathbb{R}$ with $\operatorname{supp}\mu \subset [-1, 1]$ satisfying $[\mathrm{NC}(\kappa, \varepsilon)]$. Assume that

$$\delta^{-\kappa+\varepsilon} \leqslant \|\mu\|_{2,\delta}^2 \leqslant \delta^{-1+\kappa-\varepsilon}.$$

Then

$$\|\mu * \mu \boxminus \mu * \mu\|_{2,\delta} \leqslant \delta^{\varepsilon} \|\mu\|_{2,\delta}.$$

Remark 8.5 — Condition $[\mathrm{NC}(\kappa, \varepsilon)]$ implies that $\|\mu\|_{2,\delta} \ll \delta^{-1+\kappa-\varepsilon}$.

Example 8.6

- Let $\mu = \delta_0$, the Dirac measure, then $\mu_\delta = P_\delta$ and $\|\mu\|_{2,\delta}^2 \asymp \delta^{-1}$.
- Let $\mu = \frac{1}{2}\mathbb{1}_{[-1,1]}$, then $\|\mu\|_{2,\delta} \asymp 1$.

Lemma 8.7

Assume μ has $[\mathrm{NC}(\kappa, \varepsilon)]$ and $\|\mu * \mu \boxminus \mu * \mu\|_{2,\delta} > \delta^{\varepsilon} \|\mu\|_{2,\delta}$. Then there exists $A \subset [-1, 1]$ with

$$\mathcal{N}_\delta(A) \leqslant \delta^{-1+O(\varepsilon)} \|\mu\|_{2,\delta}^{-2},$$

and an $a_0 \in \mathbb{R}$ with $|a_0| \geqslant \delta^{O(\varepsilon)}$ satisfying

- $\mu(-a_0 R_\delta(A, \delta^{-O(\varepsilon)})) \geqslant \delta^{O(\varepsilon)}$,
- $\forall \rho \geqslant \delta$, $\max_{x\in\mathbb{R}} \mathcal{N}_\delta(A \cap B(x, \rho)) \leqslant \delta^{-O(\varepsilon)} \rho^{\kappa} \mathcal{N}_\delta(A)$.

Applying Theorem 8.2 to $\widetilde{\mu}$ where $\widetilde{\mu}(E) = \mu(-a_0 E)$, Lemma 8.4 follows by this lemma.

Proof of Lemma 8.7. WLOG, $\delta = 2^{-k}$. We consider the dyadic partition

$$\mathcal{Q} = \left\{[j\delta, (j+1)\delta) : j \in [-2^k, 2^k - 1]\right\}.$$

Let

$$\mathcal{Q}_i = \left\{Q \in \mathcal{Q} : \mu(Q) \in [2^{-k+i-1}, 2^{-k+i}]\right\}, \quad \forall i \in \{1, \cdots, k\},$$
$$\mathcal{Q}_0 = \left\{Q \in \mathcal{Q} : \mu(Q) \leqslant 2^{-k}\right\}.$$

Write $A_i = \bigcup_{Q\in\mathcal{Q}_i} +B(0, \delta) \subset \mathbb{R}$. We can verify that

$$\mu_\delta \ll \sum_{i=0}^{k} 2^i \mathbb{1}_{A_i} \ll \mu_{3\delta} + \mathbb{1}_{[-1,1]}.$$

Besides, we have (leave as an exercise)

$$\|\mu * \mu \boxminus \mu * \mu \boxplus P_\delta\|_2 \asymp \|\mu * \mu_\delta \boxminus \mu * \mu_\delta\|_2.$$

By assumption, we have

$$\delta^{\varepsilon} \|\mu\|_{2,\delta} \leqslant \|\mu * \mu \boxminus \mu * \mu\|_{2,\delta} \asymp \|\mu * \mu_\delta \boxminus \mu * \mu_\delta\|_2$$
$$\ll \sum_{i,j=0}^{k} 2^{i+j} \left\|\mu * \mathbb{1}_{A_i} \boxminus \mu * \mathbb{1}_{A_j}\right\|_2 .$$

Note that $k = -\log\delta \leqslant \delta^{-\varepsilon}$, then there exists i, j such that

$$2^{i+j} \left\|\mu * \mathbb{1}_{A_i} \boxminus \mu * \mathbb{1}_{A_j}\right\|_2 \geqslant \delta^{O(\varepsilon)} \|\mu\|_{2,\delta} .$$

Fix this pair of i, j, we have

$$\mu * \mathbb{1}_{A_i} = \int \delta_a * \mathbb{1}_{A_i} \mathrm{d}\mu(a) = \int \frac{1}{|a|} \mathbb{1}_{aA_i} \mathrm{d}\mu(a).$$

By $[\mathrm{NC}(\kappa,\varepsilon)]$, we can assume that $\operatorname{supp}\mu \subset B(0,1) \setminus B(0,\delta^{O(\varepsilon)})$. Hence

$$2^{i+j} \iint \left\|\mathbb{1}_{aA_i} \boxminus \mathbb{1}_{bA_j}\right\| \mathrm{d}\mu(a)\mathrm{d}\mu(b) \geqslant \delta^{O(\varepsilon)} \|\mu\|_{2,\delta} .$$

Besides, for every a, b, we have

$$\left\|\mathbb{1}_{aA_i} \boxminus \mathbb{1}_{bA_j}\right\| \leqslant \|\mathbb{1}_{aA_i}\|_1 \|\mathbb{1}_{bA_j}\| = |aA_i| \cdot |bA_j|^{\frac{1}{2}}.$$

By definition of A_i, we have

$$2^i |A_i| \ll 1, \quad 2^i |A_i|^{\frac{1}{2}} \ll \|\mu_{3\delta}\|_2 \asymp \|\mu\|_{2,\delta} .$$

It shows that $2^{i+j} \left\|\mathbb{1}_{aA_i} \boxminus \mathbb{1}_{bA_j}\right\|$ is bounded above by $O(\|\mu\|_{2,\delta})$. By pigeonhole, there exists $a \in \operatorname{supp}\mu, B \subset \operatorname{supp}\mu$ with $\mu(B) \geqslant \delta^{O(\varepsilon)}$ such that

$$2^{i+j} \left\|\mathbb{1}_{aA_i} \boxminus \mathbb{1}_{bA_j}\right\| \geqslant \delta^{O(\varepsilon)} \|\mu\|_{2,\delta} , \quad \forall b \in B.$$

It follows that for every $b \in B$,

$$\left\|\mathbb{1}_{aA_i} \boxminus \mathbb{1}_{bA_j}\right\|_2^2 \geqslant \delta^{O(\varepsilon)} |aA_i|^{\frac{3}{2}} |bA_j|^{\frac{3}{2}}.$$

Apply B-S-G, popularity argument and Ruzsa calculus in last section. We can find $A \subset A_i, b_0 \in B$ and $B' \subset B$. Such that

- $\mu(B') \geqslant \delta^{O(\varepsilon)}$,
- $\mathcal{N}_\delta(A + b_0^{-1} bA) \leqslant \delta^{-O(\varepsilon)} \mathcal{N}_\delta(A)$, for every $b \in B'$.
- $\mathcal{N}_\delta(A) \geqslant \delta^{O(\varepsilon)} \frac{|A_i|}{\delta}$, hence $\mathcal{N}_\delta(A) = \delta^{-1+O(\varepsilon)} \|\mu\|_{2,\delta}^{-2}$.
- $\forall \rho \geqslant \delta$, we have

$$\mathcal{N}_\delta(A \cap B(x,\rho)) \ll \frac{|A_i \cap B(x,\rho)|}{\delta} \ll \frac{1}{2^i \delta} \mu_{3\delta}(B(x,\rho)) \leqslant \delta^{-O(\varepsilon)} \rho^{\kappa} \frac{|A_i|}{\delta}.$$

□

Lemma 8.8

For every $\kappa, \tau, \varepsilon > 0$. Let $\delta > 0$ sufficiently small and μ, ν be a Borel probability measures on $[-1,1]$. Assume that $\|\nu\|_{2,\delta}^2 \leqslant \delta^{-\tau}$ and μ has $[\mathrm{NC}(\kappa,\varepsilon)]$. Then for every $\xi \in \mathbb{R}$ with $\delta^{-1+\varepsilon} \leqslant |\xi| \leqslant \delta^{-1-\varepsilon}$, we have

$$|\widehat{\mu * \nu}(\xi)| \leqslant \delta^{\frac{\kappa-\tau}{4}-O(\varepsilon)}.$$

Proof. We have

$$\delta^{-\tau} \geqslant \|\nu\|_{2,\delta}^2 = \|\nu \boxplus P_\delta\|_2^2 = \int |\widehat{\nu}(\zeta)\widehat{P_\delta}(\zeta)|^2 \mathrm{d}\zeta \gg \int_{B(0,\frac{1}{10\delta})} |\widehat{\nu}(\zeta)|^2 \mathrm{d}\zeta.$$

Note that $\operatorname{supp}\nu \subset [-1,1]$ and ν is a probability measure, then $\widehat{\nu}$ is 10-Lipschitz (2π-Lipschitz). Let $R = \delta^{-1+\varepsilon}$ and $t \in (0,R)$, define

$$H_{R,t} = \{\zeta \in \mathbb{R} : |\zeta| < R, |\widehat{\nu}(\zeta)| > t\}.$$

Then $H_{R,t} + B(0,t/20) \subset H_{2R,t/2}$. Hence

$$|H_{R,t} + B(0,\frac{t}{20})| \ll t^{-2}\int_{B(0,2R)} |\widehat{\nu}(\zeta)|^2 \mathrm{d}\zeta \ll t^{-2}\delta^{-\tau}.$$

It follows that $\mathcal{N}_t(H_{R,t}) \ll t^{-3}\delta^{-\tau}$. For every ξ with $|\xi| \in [\delta^\varepsilon R, R]$, we have

$$\begin{aligned}\widehat{\mu * \nu}(\xi) &= \iint e^{2\pi i \xi x y}\mathrm{d}\mu(x)\mathrm{d}\nu(y) = \int \widehat{\nu}(\xi x)\mathrm{d}\mu(x)\\ &\leqslant t + \mu(\{x : \xi x \in H_{R,t}\}) = t + \mu(\xi^{-1}H_{R,t})\\ &\leqslant t + \mathcal{N}_t(H_{R,t})\max_{x\in\mathbb{R}} \mu(B(x,\xi^{-1}t)) \leqslant t + t^{-3}\delta^{-\tau}\delta^{\kappa-O(\varepsilon)}.\end{aligned}$$

Take $t = \delta^{\frac{\kappa-\tau}{4}}$, the conclusion follows. □

Proof of Theorem 8.1. Let $\tau = \kappa/2$. We apply Lemma 8.4 with $\kappa/2$ and get $\varepsilon_0 = \varepsilon(\kappa/2)$. Define

$$\mu_1 = \mu|_{\mathbb{R}\setminus B(0,\delta^{O(\varepsilon)})}, \qquad \mu_{k+1} = (\mu_k * \mu_k \boxminus \mu_k * \mu_k)|_{B(0,\delta^{O(\varepsilon)})}.$$

Then μ_k has $[\mathrm{NC}(\kappa, O_k(\varepsilon))]$ and either $\|\mu_k\|_{2,\delta} \leqslant \delta^{-\kappa/2}$ or $\|\mu_{k+1}\|_{2,\delta} \leqslant \delta^{\varepsilon_0}\|\mu_k\|_{2,\delta}$. Hence there is $s \leqslant \lceil \varepsilon_0^{-1} \rceil$ such that $\|\mu_s\|_{2,\delta} \leqslant \delta^{-\kappa/2}$. By the previous lemma, we have

$$|\widehat{\mu_s * \mu_s}(\xi)| \leqslant \delta^{\frac{\kappa}{8}-O(\varepsilon)} \leqslant \delta^{\frac{\kappa}{16}},$$

assuming ε small enough. It remains to show the relation between $\widehat{\mu^{*S}}(\xi)$ and $\widehat{\mu_s * \mu_s}(\xi)$.

Claim 8.9. Let η_1, η_2 be two probability measures on $\mathbb{R}$, then

$$|\widehat{\eta_1 * \eta_2}(\xi)|^2 \leqslant \widehat{\eta_1 * (\eta_2 \boxminus \eta_2)}(\xi) \in \mathbb{R}.$$

Write $\mu_s = \mu_{s-1} * \mu_{s-1} \boxminus \mu_{s-1} * \mu_{s-1}$, then

$$\widehat{\mu_s * \mu_s}(\xi) \geqslant |(\mu_s * \mu_{s-1} * \mu_{s-1})^\wedge(\xi)|^2 \geqslant |(\mu_{s-1} * \mu_{s-1} * \mu_{s-1} * \mu_{s-1})^\wedge(\xi)|^4.$$

By a variant of the claim above, we can show by induction that

$$\left|\widehat{\mu_{s-k}^{*2^k}}(\xi)\right|^{2^{2^k}} \leqslant \widehat{\mu_s * \mu_s}(\xi) \leqslant \delta^{\frac{\kappa}{16}}.$$

Take $k = s-1$, the conclusion follows. □

Now we turn back to the topic about different versions of sum product theorems. We will show a sketch of deriving Theorem 8.2 (indeed, we show Theorem 7.5) from Theorem 6.18. We need the following version as a transition.

Theorem 8.10

For every $\varepsilon_0 > 0, \kappa > 0$, there exists $\varepsilon = \varepsilon(\varepsilon_0, \kappa) > 0$ and $s = s(\varepsilon_0, \kappa) \geqslant 1$. Such that for every $A \subset [-1, 1]$ and $\delta > 0$ satisfying

$$\mathcal{N}_\rho(A) \geqslant \delta^\varepsilon \rho^{-\kappa}, \quad \forall \rho \geqslant \delta,$$

we have

$$\langle A \rangle_s + B(0, \delta) \supset B(0, \delta^{\varepsilon_0}).$$

Proof. Take $\sigma = 1 - \varepsilon_1$ and use Theorem 6.18 many times. Then there is $s \geqslant 1$ such that

$$\mathcal{N}_\delta(\langle A \rangle_s) \geqslant \delta^{-1+\varepsilon_1}.$$

We take ν to be the uniform measure on $\langle A \rangle_s + B(0, \delta)$, then $\|\nu\|_{2,\delta}^2 \ll \delta^{-\varepsilon_1}$. By Lemma 8.8, for every $\xi \in [\delta^{-1+\varepsilon}, \delta^{-1-\varepsilon}]$, we have

$$|\widehat{\nu * \nu}(\xi)| \leqslant \delta^{-O(\varepsilon)} |\xi|^{-\frac{\kappa - \varepsilon_1}{4}} \leqslant \delta^{-O(\varepsilon_1)} |\xi|^{-\frac{\kappa}{4}}.$$

Take $s' = \lceil 10\kappa^{-1} \rceil$, then

$$\widehat{(\nu * \nu)^{\boxplus s'}} \leqslant \delta^{-O(\varepsilon_1)} |\xi|^{-2}$$

for every $|\xi| \leqslant \delta^{-1+\varepsilon}$. Take ψ be a smooth function with $\operatorname{supp} \psi \subset [-1, 1]$ and $\widehat{\psi} \geqslant 0$. Let $\psi_\delta(x) = \delta^{-1}\psi(\delta^{-1}x)$ and $\widehat{\psi}_\delta(\xi) = \widehat{\psi}(\delta\xi)$. Take $\eta = (\nu * \nu)^{\boxplus s'} \boxplus \psi_\delta$, then $\widehat{\eta}(\xi) \leqslant \delta^{-O(\varepsilon_1)} |\xi|^{-2}$. Hence $\widetilde{\eta}$ is integrable and $(\operatorname{supp} \eta - \operatorname{supp} \eta)$ contains $B(0, \delta^{O(\varepsilon_1)})$. Precisely, we can estimate Fourier coefficient to show that $\operatorname{supp} \eta$ contains some $B(x, \delta^{O(\varepsilon_1)})$. $\square$

Proof of Theorem 7.5. We apply the above Theorem to ε_0, κ. If $B \subset R_\delta(A, \delta^{-\varepsilon})$, then $\langle B \rangle_s + B(0, \delta) \subset R_\delta(A, \delta^{-O(\varepsilon)})$. It follows that $B(0, \delta^{\varepsilon_0}) \subset R_\delta(A, \delta^{-O(\varepsilon)})$. Now we use a probability argument to show that this is not the case. Let t obeys the uniform distribution on $B(0, \delta^{\varepsilon_0})$, by Jensen's inequality,

$$\mathbb{E}[\mathcal{N}_\delta(A + tA)] \geqslant \frac{\mathcal{N}_\delta(A)^4}{\mathbb{E}[\mathscr{E}(\varphi_t, A \times A)]},$$

where $\varphi_t : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(x, y) \mapsto x + ty$. Fix a maximal δ-separated set $\widetilde{A} \subset A$, then

$$\mathbb{E}[\mathscr{E}(\varphi_t, A \times A)] \ll \sum_{x, x', y, y' \in \widetilde{A}} \mathbb{P}[t(y - y') \in (x - x') + B(0, \delta)].$$

Take $\rho = \delta^{\frac{1-\sigma}{1+\kappa}}$, for every $|y - y'| \geqslant \rho$, we have

$$\mathbb{P}[t(y - y') \in (x - x') + B(0, \delta)] \ll \delta^{-\varepsilon_0} \frac{\delta}{\rho}.$$

For the case of $|y - y'| \leqslant \rho$, by non-concentration,

$$\# \left\{ y, y' \in \widetilde{A} : |y - y'| \leqslant \rho \right\} \ll \delta^{-\varepsilon} \rho^\kappa \mathcal{N}_\delta(A)^2.$$

It follows that

$$\mathbb{E}[\mathscr{E}(\varphi_t, A \times A)] \ll \delta^{-\varepsilon_0} \frac{\delta}{\rho} \mathcal{N}_\delta(A)^4 + \delta^{-\varepsilon} \rho^\kappa \mathcal{N}_\delta(A)^3 \ll \delta^{-O(\varepsilon) - \varepsilon_0} \delta^{\frac{\kappa(1-\sigma)}{1+\kappa}} \mathcal{N}_\delta(A)^3.$$

For ε_0 small enough, there exists $t \in B(0, \delta^{\varepsilon_0})$ such that

$$\mathcal{N}_\delta(A + tA) \geqslant \delta^{-O(\varepsilon)} \delta^{-\frac{\kappa(1-\sigma)}{2(1+\kappa)}} \mathcal{N}_\delta(A),$$

a contradiction. $\square$

§9 Applications in homogeneous dynamics

Higher dimension setting

Let E be a semisimple algebra over $\mathbb{R}$. Recall Weddeburn's structure theorem, E is a direct sum of $\mathrm{Mat}(d,\mathbb{R}), \mathrm{Mat}(d,\mathbb{C})$ or $\mathrm{Mat}(d,\mathbb{H})$.

Theorem 9.1 (Saxcé-He)
Let E be a semisimple algebra over $\mathbb{R}$. $\forall\kappa>0, \exists\varepsilon>0$ and $k\in\mathbb{N}$, the following holds for $\delta>0$ sufficiently small. Let η be a probability measure on $B_E(0,1)$ satisfying

- $\forall\rho\geqslant\delta, \forall$ proper affine subspace $W\subset E, \eta(W+B(0,\rho))\leqslant\delta^{-\varepsilon}\rho^{\kappa}$.
- $\forall x\in E, \eta(\{y\in E : |\det(y-x)|\leqslant\delta^{\varepsilon}\})\leqslant\delta^{\kappa\varepsilon}$.

Then for any linear form $\xi\in E^*$ with $\|\xi\|\leqslant\delta^{-1}$, we have

$$|\widehat{\eta^{*k}}(\xi)|\leqslant\|\xi\|^{-\varepsilon}.$$

Fourier decay is a consequence of the following sum-product theorem in semisimple algebras.

Theorem 9.2 (Saxcé-He)
Let E be a semisimple algebra over $\mathbb{R}$. $\forall\kappa>0, \exists\varepsilon>0$ and $k\in\mathbb{N}$, the following holds for $\delta>0$ sufficiently small. Let $A\subset B_E(0,1)$ satisfying

- $\mathcal{N}_\delta(A)\leqslant\delta^{-\dim E+\kappa}$.
- $\forall\rho\geqslant\delta, \forall$ proper affine subspace $W\subset E, \mathcal{N}_\delta(A\cap(W+B(0,\rho)))\leqslant\delta^{-\varepsilon}\rho^{\kappa}\mathcal{N}_\delta(A)$.

Then
$$\mathcal{N}_\delta(A+A\cdot A)\geqslant\delta^{-\varepsilon}\mathcal{N}_\delta(A).$$

Random walk on a group

Let G be a group. Let μ be a measure on G. Let

$$g_1, g_2, \cdots, g_n, \cdots$$

be an i.i.d. sequence of random variables in G with law μ. The sequence $S_n := g_n\cdots g_2g_1, n\geqslant 1$ is a **random walk** on G. Then the law of S_n is μ^{*n}.

Now we consider G acting on a space X. Let x_0 be a random point in X, the initial point. We consider the sequence $x_n := S_nx_0 = g_n\cdots g_2g_1x_0, n\geqslant 1$. We call (x_n) a random walk on X. Let ν_0 denote the law of x_0, then the law of x_n is $\nu_n=\mu^{*n}*\nu_0$.

Question 9.3. Does (x_n) convergence in law?

We are interested in the action $\mathrm{GL}(d,\mathbb{Z})\curvearrowright\mathbb{T}^d$. Let μ be a probability measure on $\mathrm{GL}(d,\mathbb{Z})$. We assume that

- μ has a finite exponential moment: $\exists\alpha>0, \int_{\mathrm{GL}(d,\mathbb{Z})}\|g\|^{\alpha}\mathrm{d}\mu(g)<\infty$.
- the Zariski closure of $\Gamma=\langle\operatorname{supp}\mu\rangle$ is a semisimple algebraic group.

- the action $\Gamma \curvearrowright \mathbb{Q}^d$ is strongly irreducible: Γ does not preserves any finite union of nontrivial proper subspaces in $\mathbb{Q}^d$.
- the action $\Gamma \curvearrowright \mathbb{R}^d$ has no compact factor: there is no Γ-invariant subspace $W \subset \mathbb{R}^d$ such that the image $\Gamma \to \mathrm{GL}(W)$ is relatively compact.

The first version classifies orbit closures.

Theorem 9.4 (Orbit closures, Guivarc'h-Starkov)
Under the standing assumptions, for any $x \in \mathbb{T}^d$,

(1) either $x \in \mathbb{Q}^d/\mathbb{Z}^d$, then the orbit Γx is finite,

(2) or $\overline{\Gamma x} = \mathbb{T}^d$.

Remark 9.5 — This is sometimes known as **ID-property**: infinite orbits are dense.

Now we turn to the measure theoretic view.

Definition 9.6. A measure ν on $\mathbb{T}^d$ is called μ-stationary if $\nu = \mu * \nu$.

Theorem 9.7 (Classification of stationary measures, Benoist-Quint)
Under the standing assumptions, the only μ-stationary measure on $\mathbb{T}^d$ are convex combinations of

- uniform measures on finite orbits and
- the Haar measure $m_{\mathbb{T}^d}$.

Remark 9.8 — In particular, this result shows a stiffness: every μ-stationary measure is $\langle \operatorname{supp} \mu \rangle$-invariant.

Furthermore, there is a equidistribution result. The classification of orbit closures and that of stationary measures follows from this result.

Theorem 9.9 (Bourgain-Furman-Lindenstrauss-Mozes, Saxcé-He)
Under the standing assumptions, we have

(1) either $\mu^{*n} * \nu_0 \xrightarrow{w*} m_{\mathbb{T}^d}$,

(2) or $\nu_0(\mathbb{Q}^d/\mathbb{Z}^d) > 0$.

And a quantitative version,

Theorem 9.10 (Bourgain-Furman-Lindenstrauss-Mozes, Saxcé-He)
Under the standing assumptions. There exists $c > 0, C > 1$, the following holds for any $x_0 \in \mathbb{T}^d$. For every $n \geqslant 1$, $a_0 \in \mathbb{Z}^d \setminus \{0\}$ and $t \in (0, 1/2)$, if

$$|\widehat{\mu^{*n} * \delta_{x_0}(a_0)}| \geqslant t \quad \text{and} \quad n \geqslant C \log \frac{\|a_0\|}{t},$$

then there exists $q \in \mathbb{N}$ such that $q \leqslant \|a_0\|^C t^{-C}$ and

$$d(x_0, \frac{1}{q}\mathbb{Z}^d/\mathbb{Z}^d) \leqslant e^{-cn}.$$

Now we show the relations between these results and sum-product estimates. Assume that $\nu_n \not\rightharpoonup m_{\mathbb{T}^d}$, then there exists $t > 0, a_0 \in \mathbb{Z}^d \setminus \{0\}$ and an unbounded sequence of n,

$$|\widehat{\nu_n}(a_0)| \geqslant t.$$

We want to show that ν_0 has atoms at rational points.

Theorem 9.11 (Wiener's lemma)

$$\sum_{x \in \mathbb{T}^d} \nu_0(\{x\})^2 \asymp \lim_{N \to +\infty} \frac{1}{N^d} \sum_{a \in \mathbb{Z}^d \cap B(0,N)} |\widehat{\nu_0}(a)|^2.$$

So the idea is to show that ν_0 has a lot of large Fourier coefficients.
For $n, k \in \mathbb{N}$, let $\eta_{n,k}$ denote the push forward of $(\mu^{*n})^{\otimes 2k}$ by the map

$$\Phi_k : (g_1, \cdots, g_{2k}) \mapsto g_1 + \cdots + g_k - g_{k+1} - \cdots - g_{2k}.$$

Lemma 9.12 (Additive structure of Fourier coefficients)
If $|\widehat{\nu}_n(a_0)| \geqslant t$, then for every $k \in \mathbb{N}$, the set

$$A = \left\{g \in \mathrm{Mat}(d, \mathbb{Z}) : |\widehat{\nu_0}({}^t g a_0)| \geqslant t^{2k}/2\right\}$$

satisfies $\eta_{n,k}(A) \geqslant t^{2k}/2$.

Proof. By Hölder's inequality, $|\widehat{\nu}_n(a_0)|^{2k} \leqslant \int |\widehat{\nu_0}({}^t g a_0)| \mathrm{d}\eta_{n,k}(g)$. □

Recall that

$$\widehat{\eta_{n,k}(\xi)} = |\widehat{\mu^{*n}}(\xi)|^{2k}, \quad \forall \xi \in \mathrm{Mat}(d, \mathbb{R})^*.$$

We want to deduce that

$$\left\{{}^t g a_0 : g \in A\right\} \subset \left\{a \in \mathbb{Z}^d : |\widehat{\nu}_0(a)| \gg t^{O(k)}\right\}$$

is large from the fact that $\eta_{n,k}(A) \gg t^{O(k)}$ and the Fourier decay for μ^{*n}.

Proposition 9.13

Under the standing assumptions. There exists $C > 0, \sigma > \tau > 0$. If

$$|\widehat{\mu^{*n} * \nu_0}(a_0)| \geqslant t, \quad \text{for some } n \geqslant C|\log t|.$$

Then

$$\mathcal{N}_M(B(0,N) \cap \left\{a \in \mathbb{Z}^d : |\widehat{\nu}_0(a)| \gg t^C\right\}) \gg t^C \left(\frac{N}{M}\right)^d$$

where $N = e^{\sigma n} \|a_0\|$ and $M = e^{-\tau n} N$.