

Jean Bourgain
Institute for Advanced Study
Princeton, NJ 08540

ADDITIVE COMBINATORICS

SUM-PRODUCT PHENOMENA

Applications to:

- Exponential sums
- Expanders and spectral gaps
- Invariant measures
- Pseudo-randomness

SUM-PRODUCT THEOREM

IN $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Theorem. (BKT, BGK).

For all $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset \mathbb{F}_p$ and $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| > c|A|^{1+\delta}$$

Proof based on **Plunnecke–Ruzsa** theory of set addition

Extensions to:

Arbitrary finite fields \mathbb{F}_{p^r}

$\mathbb{Z}/q\mathbb{Z}$

O/I ($O =$ integers in numberfield)

GAUSS SUMS IN PRIME FIELDS

Theorem. (BK).

For all $\varepsilon > 0$, there is $\delta > 0$ such that if $H < \mathbb{F}_p^$ and $|H| > p^\varepsilon$, then*

$$\max_{(a,p)=1} \left| \sum_{x \in H} e_p(ax) \right| < C \cdot p^{-\delta} \cdot |H|$$

$$e_p(x) = e^{\frac{2\pi i}{p}x}$$

Earlier results up to $\varepsilon > \frac{1}{4}$ based on Stepanov's method

Conjecture. (MVW)

$$H < \mathbb{F}_p^*, \quad \frac{|H|}{\log p} \rightarrow \infty$$

$\Rightarrow H$ equidistributed

Limitation of sum-product method

$$\log |H| > C \frac{\log p}{\log \log p}$$

GAUSS SUMS IN $\mathbb{Z}/q\mathbb{Z}$

Theorem. (B)

For all $\varepsilon > 0$, there is $\delta > 0$ such that if $H < (\mathbb{Z}/q\mathbb{Z})^$ and $|H| > q^\varepsilon$, then*

$$\max_{(a,q)=1} \left| \sum_{x \in H} e_q(ax) \right| < Cq^{-\delta} |H|$$

Estimate is uniform in q .

WEIL'S INEQUALITY

Theorem. (W)

Let $f(x) \in \mathbb{F}_p[x]$ be of degree $d \geq 1$.

Then

$$\left| \sum_{1 \leq x \leq p} e_p(f(x)) \right| \leq (d-1)\sqrt{p}$$

Problem. Obtain nontrivial estimates

for $d > \sqrt{p}$

MORDELL POLYNOMIALS

Theorem. (B)

$$f(x) = \sum_{i=1}^r a_i x^{k_i} \in \mathbb{Z}[X]$$

$$(a_i, p) = 1$$

$$(k_i, p-1) < p^{1-\varepsilon} \quad (1 \leq i \leq r)$$

$$(k_i - k_j, p-1) < p^{1-\varepsilon} \quad (1 \leq i \neq j \leq r)$$

then

$$\left| \sum_{x=1}^p e_p(f(x)) \right| < Cp^{1-\delta}$$

where $\delta = \delta(r, \varepsilon) > 0$

VERSION FOR INCOMPLETE SUMS

Theorem. Let $\theta_1, \dots, \theta_r \in \mathbb{F}_p^*$ satisfy

$$\text{ORD}(\theta_i) > p^\varepsilon \quad (1 \leq i \leq r)$$

$$\text{ORD}(\theta_i \theta_j^{-1}) > p^\varepsilon \quad (1 \leq i \neq j \leq r)$$

Let $t > p^\varepsilon$. Then

$$\max_{a_i \in \mathbb{F}_p^*} \left| \sum_{s=1}^t e_p \left(\sum_{i=1}^r a_i \theta_i^s \right) \right| < C p^{-\delta} t$$

where $\delta = \delta(r, \varepsilon) > 0$

APPLICATIONS TO PSEUDO-RANDOMNESS AND CRYPTOGRAPHY

- Distribution of **Diffie-Hellman** triples

$$\{\theta^x, \theta^y, \theta^{xy}\}$$

- Joint distribution of **RSA** sequences

$$u_{n+1} = u_n^e$$

($e = 2$: **Blum-Blum-Shub** generator)

SCALAR SUM-PRODUCT THEOREMS



PRODUCT THEOREMS IN MATRIX SPACE

Theorem. (HELFGOTT)

$$G = SL_2(p) \text{ or } SL_3(p)$$

Assume $A \in G$ generates G and

$$|A| < |G|^{1-\varepsilon}$$

Then

$$|A.A.A| > |A|^{1+\delta}$$

EXPANSION OF CAYLEY GRAPHS

Theorem. (BG)

Let $S_p = \{g_1, g_1^{-1}, \dots, g_k, g_k^{-1}\}$ be a symmetric generating set for $SL_2(p)$, such that

$$\text{girth}(\mathcal{G}(SL_2(p), S_p)) > \tau \log p$$

Then the expansion coefficient of $\mathcal{G}(SL_2(p), S_p)$ admits a uniform lower bound $c(\tau) > 0$

Problem. Remove large girth assumption

(Relevant work by **E. Breuillard**)

\mathcal{G} = GRAPH ON VERTEX SET V

Definition.

$$c(\mathcal{G}) = \inf \left\{ \frac{|\partial X|}{|X|} \text{ where } |X| < \frac{1}{2}|V| \right\}$$

(Expansion coefficient of \mathcal{G})

LUBOTZKY–WEISS CONJECTURE

Let S be a finite subset of $SL_d(\mathbb{Z})$ generating a Zariski dense subgroup of SL_d . Then there is $q_0 \in \mathbb{Z}$ such that the family of Cayley Graphs

$$\mathcal{G}(SL_d(\mathbb{Z}/q\mathbb{Z}), \pi_q(S))$$

with

$$q \in \mathbb{Z}_+, (q, q_0) = 1$$

forms a family of expanders

Also motivated by the work of

B-Gamburd-Sarnak on prime sieving

CONNECTEDNESS OF THE GRAPH
ROLE OF STRONG APPROXIMATION
PROPERTY

Theorem. Let G be a Zariski dense subgroup of $SL_d(\mathbb{Z})$. There is $q_0 \in \mathbb{Z}$ such that $\pi_q(G) = SL_d(\mathbb{Z}/q\mathbb{Z})$ if $(q, q_0) = 1$

π_q : reduction mod q

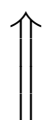
Matthews, Vaserstein, Weisfeiler,
Pink

KNOWN RESULTS

- $SL_2(p)$ **(B-G)**
- $SL_2(q)$ (q square free) **(B-G-S)**
- $SL_2(p^n)$ **(B-G)**
- $SL_d(p^n)$ (p fixed prime) **(B-G)**
 (d arbitrary)
- $SL_3(p)$

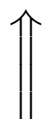
GENERAL OUTLINE OF PROOFS

Expansion Property



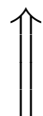
Spectral multiplicity argument
(**Sarnak–Xue**)

Measure Convolution on $SL(q)$



Non-commutative B-S-G theorem
(**Tao**)

Product Theorems in $SL(q)$



Scalar Sum-Product Theorems

$\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}, O/I$

**PRIME SIEVING IN ORBITS OF
LINEAR GROUPS
USING EXPANSION PROPERTIES
(B-G-S)**

$$\Lambda \subset SL_2(\mathbb{Z})$$

Λ nonelementary

$$\delta(\Lambda) > 0 \quad (\text{arbitrary})$$

Sieving in balls defined using either
word-metric or Archimedean metric

$$\begin{cases} \delta(\Lambda) > \frac{1}{2} & (\text{Lax} - \text{Phillips}) \\ \delta(\Lambda) \leq \frac{1}{2} & (\text{Lalley} - \text{Dolgopiat} - \text{Naud}) \end{cases}$$

Definition.

$r(z) =$ number of prime factors of
 $z \in \mathbb{Z} \setminus \{0\}$

Theorem. (BGS)

There is $C(\Lambda) \in \mathbb{Z}_+$ such that for $M \rightarrow \infty$

$$|\{g = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in B_M; r(\prod g_{ij}) < C(\Lambda)\}|$$
$$\sim \frac{|B_M|}{(\log M)^4}$$

$$B_M = \{g \in \Lambda; \left(\sum g_{ij}^2\right)^{1/2} \leq M\}$$

Theorem. (BGS)

Let $f \in \mathbb{Q}[x_1, x_2, x_3, x_4]$ taking integer values on Λ and not a multiple of

$$g(x_1, x_2, x_3, x_4) = x_1x_4 - x_2x_3 - 1$$

There is $r = r(\Lambda) \in \mathbb{Z}_+$ s.t.

$\{x \in \Lambda \mid f(x) \text{ has at most } r \text{ prime factors}\}$

is Zariski dense in SL_2

EXPLICIT APPLICATIONS

Example. Appolonian packings

Appolonian packing corresponding to:

Quadruple $(-6, 11, 14, 23)$

DESCARTE FORM

$$F(x_1, x_2, x_3, x_4) =$$

$$2(x_1^2 + x_2^2 + x_3^2 + x_4^2) - (x_1 + x_2 + x_3 + x_4)^2$$

O_F = Orthogonal group

$$A = \langle S_1, S_2, S_3, S_4 \rangle$$

= Apollonian packing group

$$S_1 = \begin{bmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$S_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$S_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$S_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{bmatrix}$$

CONJECTURE (BGS)

($SL_2(\mathbb{Z})$ analogue of Dirichlet's Theorem)

Λ non-elementary subgroup of $SL_2(\mathbb{Z})$

$b \in \mathbb{Z}^2$ primitive vector

$$\mathcal{O} = \{gb \mid g \in \Lambda\}$$

$$\pi(\mathcal{O}) = \{x \in \mathcal{O} \mid x_1, x_2 \text{ are prime}\}$$

Then

$\pi(\mathcal{O})$ is Zariski dense in \mathbb{A}^2

if no local obstruction:

For every $q \geq 2$, there is $x \in \mathcal{O}$ such that

$$x_1 x_2 \in (\mathbb{Z}/q\mathbb{Z})^*$$

SU(2)

Theorem. (B-G) *Let $k \geq 2$ and g_1, \dots, g_k algebraic elements in $G = SU(2)$ generating a free group*

Consider the Hecke operator

$$T : L^2(G) \rightarrow L^2(G) : Tf(x) = \sum_{j=1}^k (f(g_j x) + f(g_j^{-1} x))$$

Then there is a spectral gap

$$\lambda_1(T) < 2k - \gamma$$

where $\gamma = \gamma(g_1, \dots, g_k) > 0$ may

*be controlled by a noncommutative
diophantine property*

APPLICATIONS

- Banach-Ruziewicz problem
- Quantum-computation
(Solovay-Kitaev algorithm)
- Orientations in Conway-Radin
Quaquaversal tiling

THE QUAQUAVERSAL TILING

DISCRETIZED RING THEOREM

Definition. $A \subset \mathbb{R}, \varepsilon > 0$

$N(A, \varepsilon)$ = minimum number of ε -intervals covering A

Theorem. *Given $0 < \delta_1, \delta_2 < 1$, there is $\delta_3 > 0$ such that if $A \subset [1, 2]$ satisfies (ε small)*

$$(i) N(A, \varepsilon) < \left(\frac{1}{\varepsilon}\right)^{1-\delta_1}$$

$$(ii) N(A, \varepsilon_1) > \left(\frac{1}{\varepsilon_1}\right)^{\delta_2} \text{ if } \varepsilon < \varepsilon_1 < 1$$

Then

$$N(A + A, \varepsilon) + N(A.A, \varepsilon) > \left(\frac{1}{\varepsilon}\right)^{\delta_3} N(A, \varepsilon)$$

ACTIONS OF NON-ABELIAN GROUPS ON TORI (BFLM)

Margulis

Furstenberg

Guivarch

Theorem. (BFLM)

$$S = \{g_1, \dots, g_k\} \subset SL_d(\mathbb{Z})$$

$\langle S \rangle$ Zariski dense in SL_d

$$\nu = \frac{1}{|S|} \sum_{g \in S} \delta_g$$

$\xi \in \mathbb{T}^d$ irrational

Then for $\nu^{(\infty)}$ -almost every sequence (x_1, x_2, \dots)
the sequences

$$x_r x_{r-1} \dots x_1 \xi \text{ and } x_1 x_2 \dots x_r \xi \quad (r \rightarrow \infty)$$

are equidistributed in \mathbb{T}^d

Corollary. *Let μ be a probability measure on \mathbb{T}^d which is ν -stationary, i.e.*

$$\mu = \mu * \nu = \sum_g \nu(g) g_* [\mu]$$

then μ is a combination of Haar measure and atomic measure supported by rational points and μ is $\langle \nu \rangle$ -invariant

Remark. $\langle \nu \rangle = SL_d(\mathbb{Z})$: Furstenberg's stiffness problem

Corollary. (Starkov, Muchnik, Guivarch)

Let $K \subset \mathbb{T}^d$ be $\langle \nu \rangle$ -invariant compact then K is finite or $K = \mathbb{T}^d$.

QUANTITATIVE EQUIDISTRIBUTION STATEMENT

Theorem. (BFLM)

There are constants $c > 0$ and $C < \infty$ such that if $\xi \in \mathbb{T}^d \setminus \{0\}$ and $b \in \mathbb{Z}^d \setminus \{0\}$, $\|b\| < e^{cn}$. Then either

$$(*) = \left| \sum_g \nu^{(n)}(g) e^{2\pi i \langle b, g\xi \rangle} \right| < e^{-cn}$$

or

$$\left\| \xi - \frac{a}{q} \right\| < e^{-cn}$$

$$q < e^{\frac{1}{4}cn}$$

and

$$(*) < \frac{|b|^C}{q^c}$$

