The eigenvalues method in Combinatorial Number Theory

I. D. Shkredov

Steklov Mathematical Institute

Let $\mathbf{G}$ be an abelian group, and $A \subseteq \mathbf{G}$ be a finite set.

Sets with small doubling

A is called a set with *small doubling* if

$$|A+A| \le K|A|\,.$$

Examples

$$A = P = \{a, a+d, \dots, a+d(k-1)\}\,,$$

$$A = P_1 + \dots + P_s \text{ (generalized arithmetic progression)},$$

$$\text{large subsets of } P_1 + \dots + P_s \, (P)\,.$$

Theorem (Freiman, 1973)

Let $A \subseteq \mathbb{Z}$, and $|A+A| \le K|A|$. Then there is $Q = P_1 + \cdots + P_d$ such that

$$A \subseteq Q$$

and

$$|Q| \le C|A|\,,$$

where d, C depend on K only.

Thus, A is a large subset of a generalized arithmetic progression.

Freiman, $\mathbb{F}_2^n$

Theorem (Freiman)

Let $A \subseteq \mathbb{F}_2^n$, and $|A+A| \le K|A|$. Then there is a subspace Q of dimension d such that

$$A \subseteq Q \quad \text{and} \quad |Q| \le C|A|\,,$$

where d, C depend on depend on K only
$(d(K) \sim 2K,\ C(K) \sim \exp(K))$.

Example

Let $A = \{e_1, \dots, e_s\}$, $|A+A| \sim |A|^2/2 \sim s^2$.
Thus $K \sim s$, and $C(K) \sim \exp(K)$.

Subsets

Instead of covering A let us find a structural *subset* of A.

Polynomial Freiman–Ruzsa Conjecture

Let $A \subseteq \mathbb{F}_2^n$, and $|A+A| \le K|A|$. Then there is a subspace Q such that

$$|A \cap Q| \ge |A|/C_1(K),$$

and

$$|Q| \le C_2(K)|A|,$$

where C_1, C_2 depends on K polynomially.

It is known (Sanders, 2012) for $C_1(K) \sim C_2(K) \sim \exp(\log^4(K))$.

Balog–Szemerédi–Gowers

Additive energy

Let $A, B \subseteq \mathbf{G}$ be sets. The (common) *additive energy* of A and B

$$\mathrm{E}(A,B) = \mathrm{E}_2(A,B) :=$$

$$|\{a_1 + b_1 = a_2 + b_2 \;:\; a_1, a_2 \in A,\; b_1, b_2 \in B\}|\,.$$

If $A = B$ then write $\mathrm{E}(A)$ for $\mathrm{E}(A,A)$.

Example, $\mathrm{E}(A)$ large

A is an arithmetic progression ($\mathbb{Z}$) or subspace ($\mathbb{F}_2^n$).

If $|A+A| \le K|A|$ then $\mathrm{E}(A) \ge |A|^3/K$.

Balog–Szemerédi–Gowers

Theorem (Balog–Szemerédi–Gowers)

Let $\mathbf{G}$ be an abelian group, and $A \subseteq \mathbf{G}$ be a finite set. Suppose that $\mathrm{E}(A) \geq |A|^3/K$. Then there is $A_* \subseteq A$ such that

$$|A_*| \geq |A|/C_1(K)\,,$$

and

$$|A_* + A_*| \leq C_2(K)|A_*|\,,$$

where C_1, C_2 depend on K polynomially.

So, firstly, we find a structural subset and, secondly, all bounds are polynomial.

So, $|A+A| \le K|A| \Rightarrow \mathrm{E}(A) \ge |A|^3/K$.
But $\mathrm{E}(A) \ge |A|^3/K \Rightarrow |A_* + A_*| \le C(K)|A_*|$ for some polynomially large A_*.

Can we have it for the whole A?

Example

$A \subseteq \mathbb{F}_2^n$,

$$A = Q \bigsqcup \Lambda\,,$$

where Q is a subspace, $|Q| \sim |A|^{1/3}$ and Λ is a basis ($|\Lambda| \sim |A|$).

$\mathrm{E}(Q) \sim \mathrm{E}(A)$ but $|A+A| \ge |\Lambda + \Lambda| \gg |A|^2$.

Example, again

$A \subseteq \mathbb{F}_2^n$,

$$A = Q \bigsqcup \Lambda \,,$$

where Q is a subspace, $|Q| \sim |A|^{1/3}$ and Λ is a basis ($|\Lambda| \sim |A|$).

$\mathrm{E}(Q) \sim \mathrm{E}(A)$ and, similarly, $\mathrm{E}(A, Q) \sim \mathrm{E}(A)$. Hence

$$\frac{\mathrm{E}(A, Q)}{|Q|} > \frac{\mathrm{E}(A, A)}{|A|} = \frac{\mathrm{E}(A)}{|A|} \,.$$

Convolutions

$$(g * h)(x) := \sum_y g(y)h(x-y)\,,$$

$$(g \circ h)(x) := \sum_y g(y)h(x+y)\,,$$

Consider the hermitian positively defined operator (matrix)

$$\mathrm{T}(x,y) = (A \circ A)(x-y)A(x)A(y)\,,$$

where $A(x)$ is the characteristic function of the set A, i.e. $A(x) = 1$, $x \in A$ and $A(x) = 0$ otherwise.

Recall

$$\mathrm{T}(x,y) = (A \circ A)(x-y)A(x)A(y)\,.$$

We have

$$\langle \mathrm{T}A, A\rangle = \sum_{x,y} (A\circ A)(x-y)A(x)A(y) = \|A\circ A\|_2^2 = \mathrm{E}(A)\,,$$

and, similarly,

$$\left\langle \mathrm{T}\frac{A(x)}{|A|^{1/2}}, \frac{A(x)}{|A|^{1/2}} \right\rangle = \frac{\mathrm{E}(A)}{|A|} < \left\langle \mathrm{T}\frac{Q(x)}{|Q|^{1/2}}, \frac{Q(x)}{|Q|^{1/2}} \right\rangle = \frac{\mathrm{E}(A,Q)}{|Q|}\,.$$

Thus, the action of T on (normalized) Q is larger then the action of T on (normalized) A.

Let

$$\mu_1 \geq \mu_2 \geq \dots \geq \mu_{|A|} > 0$$

be the spectrum of T and

$$f_1, f_2, \dots, f_{|A|}$$

the correspondent eigenfunctions.
By Courant–Fisher Theorem

$$\mu_1 = \max_{\|f\|_2=1} \langle \mathrm{T} f, f \rangle .$$

Thus, f_1 'sits' on Q not A !
Here $A = Q \bigsqcup \Lambda$.

Conjecture

The structured pieces of $A \subseteq \mathbf{G}$ are supports of the eigenfunctions of T.

Holds

- not for any A, A should be a 'popular difference set' :

$$A = \{x \ : \ (B \circ B)(x) \geq c|B|\}$$

for some B, $c = c(K) > 0$

- may be we need in some another 'weights'.

Operators

Let **G** be an abelian group, and $A \subseteq \mathbf{G}$ be a finite set. Take any real function g such that $g(-x) = g(x)$. Put

$$\mathrm{T}^g_A(x,y) = g(x-y)A(x)A(y)\,.$$

Let

$$\mu_1(\mathrm{T}^g_A) \ge \mu_1(\mathrm{T}^g_A) \ge \dots \ge \mu_{|A|}(\mathrm{T}^g_A)$$

be the spectrum of T^g_A and

$$f_1, f_2, \dots, f_{|A|}$$

the correspondent eigenfunctions.

$$\mathrm{T}_A^g(x,y) = g(x-y)A(x)A(y)\,.$$

Examples

- If $A = \mathbf{G}$, $g(x) = B(x)$, $B \subseteq \mathbf{G}$ then $\mathrm{T}_{\mathbf{G}}^B$ the adjacency matrix of Cayley graph defined by B.
- If $g(x) = B(x)$ and A is any then T_A^B is a submatrix of Cayley graph.
- Put $g(x) = (A \circ A)(x)$. Then $\mathrm{T} = \mathrm{T}_A^{A \circ A}$. Always

$$\mu_1(\mathrm{T}) \geq \frac{\mathrm{E}(A)}{|A|}\,.$$

Further examples

Let $\Gamma \subseteq \mathbb{F}_q^*$ be a subgroup, $q = p^s$, $|\Gamma|$ divides $q-1$, $n = \frac{q-1}{|\Gamma|}$, $\mathbf{g}$ be a primitive root. Then

$$\Gamma = \{1, \mathbf{g}^n, \mathbf{g}^{2n}, \dots, \mathbf{g}^{(t-1)n}\},$$

Consider the orthonormal family of multiplicative characters on Γ

$$\chi_\alpha(x) = |\Gamma|^{-1/2} \cdot \Gamma(x) e^{\frac{2\pi i \alpha l}{|\Gamma|}}, \quad x = \mathbf{g}^l, \quad 0 \le l < |\Gamma|.$$

Lemma

Let $\Gamma \subseteq \mathbb{F}_q^*$ be a subgroup, g be any real even Γ–invariant function

$$g(\gamma x) = g(x)\,, \qquad \gamma \in \Gamma\,.$$

Then χ_α, $\alpha = 0, 1, \dots, |\Gamma| - 1$ are eigenfunctions of T^g_Γ.

In particular

$$\mathrm{E}(\Gamma) = |\Gamma| \mu_1(\mathrm{T}^g_\Gamma)\,,$$

$$\mathrm{E}(\Gamma) = \max_{f \,:\, \|f\|_2 = |\Gamma|} \mathrm{E}(\Gamma, f)\,,$$

and

$$\mathrm{E}(\Gamma, A) \ge \mathrm{E}(\Gamma) \frac{|A|^2}{|\Gamma|^2}\,, \quad A \subseteq \Gamma\,.$$

$f : \mathbf{G} \to \mathbb{C}$ be a function, $\widehat{\mathbf{G}} = \{\xi\}$, $\xi : \mathbf{G} \to \mathbb{D}$ be the group of homomorphisms.

Fourier transform

$$\widehat{f}(\xi) := \sum_x f(x)\overline{\xi(x)}\,, \quad \xi \in \widehat{\mathbf{G}}\,.$$

Properties of T_A^g

We have

- $\mathrm{Spec}\,(\mathrm{T}_A^{\widehat{B}}) = \mathrm{Spec}\,(\mathrm{T}_{B^c}^{\widehat{A}}) = \mathrm{Spec}\,(\mathrm{T}_B^{\widehat{A^c}})$.
- $\mathrm{Spec}\,(\mathrm{T}_A^{\widehat{B}}(\mathrm{T}_A^{\widehat{B}})^*) = |\mathbf{G}| \cdot \mathrm{Spec}\,(\mathrm{T}_A^{|\widehat{B}|^2})$

Here $f^c(x) := f(-x)$ for any function $f : \mathbf{G} \to \mathbb{C}$.

Further properties

$$|A|g(0) = \sum_{j=1}^{|A|} \mu_j(\mathrm{T}_A^g)\,,$$

$$\sum_z |g(z)|^2 (A \circ A)(z) = \sum_{j=1}^{|A|} |\mu_j(\mathrm{T}_A^g)|^2\,.$$

Example

Let $\mathrm{T} = \mathrm{T}_A^{A \circ A}$. Then

$$\sum_{j=1}^{|A|} |\mu_j(\mathrm{T}_A^g)|^2 = \sum_z (A \circ A)^3(z) := \mathrm{E}_3(A)\,.$$

Structural E_2, E_3 result

Theorem (Shkredov, 2013)

Let $A \subseteq \mathbf{G}$ be a set, $\mathrm{E}(A) = |A|^3/K$, and $\mathrm{E}_3(A) = M|A|^4/K^2$. Then there is $A_* \subseteq A$ s.t.

$$|A_*| \ge M^{-C}|A|\,,$$

and for any n, m

$$|nA_* - mA_*| \le K \cdot M^{C(n+m)}|A_*|\,.$$

Let $Q \subseteq \mathbb{F}_2^n$ be a subspace, $A \subseteq Q$ be a random subset s.t. $|A| = |Q|/K \Rightarrow \mathrm{E}(A) \sim |A|^3/K$, $\mathrm{E}_3(A) \sim |A|^4/K^2 \Rightarrow M \sim 1$.

$$|A - A| \sim K|A| \sim |Q| \quad \text{as well as} \quad |nA - mA| \sim |Q|\,.$$

The additive energy of subgroups

Theorem (Konyagin, 2002)

Let $\Gamma \subseteq \mathbb{F}_p$ be a multiplicative subgroup, $|\Gamma| \ll p^{2/3}$. Then

$$\mathrm{E}(\Gamma) := |\{g_1 + g_2 = g_3 + g_4 \;:\; g_1, g_2, g_3, g_4 \in \Gamma\}| \ll |\Gamma|^{5/2} .$$

Theorem (Shkredov, 2012)

Let $\Gamma \subseteq \mathbb{F}_p$ be a multiplicative subgroup, $|\Gamma| \ll p^{3/5-}$. Then

$$\mathrm{E}(\Gamma) := |\{g_1 + g_2 = g_3 + g_4 \;:\; g_1, g_2, g_3, g_4 \in \Gamma\}|$$

$$\ll |\Gamma|^{\frac{22}{9}} \log^{\frac{2}{3}} |\Gamma| .$$

Why ?

Suppose that $\mathrm{E}(\Gamma) \sim |\Gamma|^{5/2} = |\Gamma|^3/K$, $K \sim |\Gamma|^{1/2}$.

Lemma

We have

$$\mathrm{E}_3(\Gamma) \ll |\Gamma|^3 \log |\Gamma| = \frac{M|\Gamma|^4}{K^2} \,,$$

where $M \sim \log |\Gamma|$.

Thus by our structural result Γ stabilized under addition but $k\Gamma = \mathbb{F}_p$ (more delicate arguments give the better bounds).

Thus, $\mathrm{E}(\Gamma) = |\Gamma|^{5/2-\varepsilon_0}$, $\varepsilon_0 > 0$.

Theorem (Shkredov, 2012)

Let $P \subseteq \Gamma$ be an arbitrary *progression*, and $|\Gamma| \ll p^{2/3}$. Then

$$|\Gamma + P| \geq c|\Gamma||P|^{1-o(1)}\,, \quad c > 0\,.$$

Further applications :

- new bounds for exponential sums over subgroups,
- variational formula for exponential sums over subgroups,
- multiplicative properties of eigenvalues and so on.

Convex sets

$A = \{a_1, ..., a_n\} \subseteq \mathbf{R}$ is called *convex* if

$$a_{i+1} - a_i > a_i - a_{i-1} \qquad \text{for all } i\,.$$

Example.

$$A = \{1^2, 2^2, \dots, n^2\}\,.$$

Theorem (Iosevich, Konyagin, Rudnev, Ten, 2006)

Let $A \subseteq \mathbb{R}$ be a convex set. Then

$$\mathrm{E}(A) \ll |A|^{5/2} .$$

Theorem (Shkredov, 2012–2013)

Let $A \subseteq \mathbb{R}$ be a convex set. Then

$$\mathrm{E}(A) \ll |A|^{\frac{32}{13}} \log^{\frac{71}{65}} |A| .$$

Proof : a formula for higher moments of eigenvalues and estimation of eigenvalues.

Further applications

New upper bounds for the additive energy for sets with

- small product set $|AA|$.
- small $|A(A+1)|$.

General principle :

higher moments of convolutions **+** (small) irregularity of $A \pm A$ give a non–trivial upper bound for the additive energy.

Doubling constants

If $\Gamma \subseteq \mathbb{F}_p$ is a random set, $|\Gamma| \le \sqrt{p}$ then

$$|\Gamma \pm \Gamma| \ge |\Gamma|^{2-\varepsilon}, \quad \varepsilon > 0.$$

Conjecture

Let $\Gamma \subseteq \mathbb{F}_p$ be a subgroup, $|\Gamma| \le \sqrt{p}$. Then

$$|\Gamma \pm \Gamma| \ge |\Gamma|^{2-\varepsilon}, \quad \varepsilon > 0.$$

Theorem (Garcia–Voloch, 1988)

Suppose that $|\Gamma| = O(p^{3/4})$. Then

$$|\Gamma \pm \Gamma| \ge c_1 |\Gamma|^{4/3}.$$

Theorem (Heath–Brown and Konyagin, 2000)

Suppose that $|\Gamma| = O(p^{2/3})$. Then

$$|\Gamma \pm \Gamma| \geq c_2 |\Gamma|^{3/2}.$$

Theorem (Shkredov–Vyugin, 2010)

Suppose that $|\Gamma| = O(p^{1/2})$. Then

$$|\Gamma - \Gamma| \geq c_3 \frac{|\Gamma|^{5/3}}{\log^{1/2} |\Gamma|}, \quad |\Gamma + \Gamma| \geq c_3 \frac{|\Gamma|^{8/5}}{\log^{3/5} |\Gamma|}$$

For subgroups $|\Gamma| > p^{1/2}$ there are better results (the same method) **Schoen–Shkredov, 2010**.

Convex sets

Recall that $A = \{a_1, ..., a_n\} \subseteq \mathbf{R}$ is called convex if

$$a_{i+1} - a_i > a_i - a_{i-1} \qquad \text{for all } i\,.$$

Conjecture (Elekes–Nathanson–Rusza, 1999)

Let $A \subseteq \mathbb{R}$ be a convex set. Then

$$|A+A| \gg |A|^{2-\varepsilon}\,,$$

Theorem (Elekes–Nathanson–Rusza, 1999)

Let $A \subseteq \mathbb{R}$ be a convex set. Then

$$|A+A| \gg |A|^{3/2} \,,$$

Theorem (Schoen–Shkredov, 2011)

Let $A \subseteq \mathbb{R}$ be a convex set. Then

$$|A-A| \gg |A|^{8/5-\varepsilon} \,,$$

and

$$|A+A| \gg |A|^{14/9-\varepsilon} \,.$$

Operators method.

Further applications

New lower bounds for the doubling constants for sets with

- small product set $|AA|$.
- small $|A(A+1)|$.
- mixed sets $|f(A)+B|$, f is a convex function.

An so on.

Heilbronn's exponential sums

Let p be a prime number.
Heilbronn's exponential sum is defined by

$$S(a) = \sum_{n=1}^{p} e^{2\pi i \cdot \frac{an^p}{p^2}} .$$

Fermat quotients defined as

$$q(n) = \frac{n^{p-1} - 1}{p}, \quad n \neq 0 \pmod{p} .$$

Theorem (Heath–Brown, Konyagin, 2000)

Let p be a prime, and $a \neq 0 \pmod p$. Then

$$|S(a)| \ll p^{\frac{7}{8}}.$$

Theorem (Shkredov, 2012–2013)

Let p be a prime, and $a \neq 0 \pmod p$. Then

$$|S(a)| \ll p^{\frac{31}{36}} \log^{\frac{1}{6}} p.$$

By l_p denote the smallest n such that $q(n) \neq 0 \pmod p$.

Theorem (Bourgain, Ford, Konyagin, Shparlinski, 2010)

One has

$$l_p \le (\log p)^{\frac{463}{252}+o(1)}$$

as $p \to \infty$.

Previously Lenstra (1979) : $l_p \ll (\log p)^{2+o(1)}$.

Theorem (Shkredov, 2012–2013)

One has

$$l_p \le (\log p)^{\frac{463}{252}-\varepsilon_0+o(1)}\,, \quad \varepsilon_0 > 0\,,$$

ε_0 is an absolute (small) constant.

Other applications are :

- discrepancy of Fermat quotients,
- new bound for the size of the image of $q(n)$,
- estimates for Ihara sum,
- better bounds for the sums

$$\sum_{n=1}^{k} \chi(q(n))\,, \quad \sum_{n=1}^{k} \chi(nq(n))\,.$$

- Surprising inequalities between $\mathrm{E}(A)$ and $\mathrm{E}_s(A)$, $s \in (1, 2]$.

A and A_x

Let $A \subseteq \mathbf{G}$ be a set. Put $A_x = A \cap (A - x)$.

Corollary (Shkredov, 2012)

$$\sum_x \frac{|A_x|^2}{|A \pm A_x|} \le |A|^{-2} \sum_x |A_x|^3 \,,$$

and

$$\sum_{x,y,z \in A} |A_{x-y}||A_{x-z}||A_{y-z}| \ge |A|^{-3} (\sum_x |A_x|^2)^3 \,.$$

Chang Theorem

Let $\mathbf{G}$ be an abelian group, and $A \subseteq \mathbf{G}$ be a finite set.

Dissociated sets

A set $\Lambda = \{\lambda_1, \dots, \lambda_d\} \subseteq \mathbf{G}$ is called *dissociated* if any equation of the form

$$\sum_{j=1}^{d} \varepsilon_j \lambda_j = 0 \,, \qquad \text{where} \qquad \varepsilon_j \in \{0, \pm 1\}$$

implies $\varepsilon_j = 0$ for all j.

Exm. $\mathbf{G} = \mathbb{F}_2^n$.

Proof of Chang Theorem via operators

Chang theorem

For any dissociated set Λ, any set $A \subseteq \mathbf{G}$, $|A| = \delta|\mathbf{G}|$ and an arbitrary function f, $\mathrm{supp}\, f \subseteq A$

$$\sum_{\xi \in \Lambda} |\widehat{f}(\xi)|^2 \le |A| \log(1/\delta) \cdot \|f\|_2^2 \,.$$

$$\sum_{x \in \Lambda} |\widehat{f}(x)|^2 = \langle \mathrm{T}^{\widehat{\Lambda}}_{A} f, f \rangle \le \mu_1(\mathrm{T}^{\widehat{\Lambda}}_{A}) \|f\|_2^2 = \mu_1(\mathrm{T}^{\widehat{A}}_{\Lambda}) \|f\|_2^2$$

Estimating $\mu_1(\mathrm{T}^{\widehat{A}}_\Lambda)$

$\operatorname{supp} w \subseteq \Lambda$, $k \sim \log(1/\delta)$.

$$\mu_1(\mathrm{T}^{\widehat{A}}_\Lambda) := \max_{\|w\|_2=1} \langle \mathrm{T}^{\widehat{A}}_\Lambda w, w \rangle = \sum_x |\widehat{w}(x)|^2 A(x)\,.$$

$$\mu_1^k(\mathrm{T}^{\widehat{A}}_\Lambda) \le \sum_x |\widehat{w}(x)|^{2k} \cdot |A|^{k-1}$$

$$\sum_x |\widehat{w}(x)|^{2k} = |\mathbf{G}| \sum_{x_1+\dots+x_k = x'_1+\dots+x'_k} w(x_1)\dots w(x_k)\overline{w(x'_1)}\dots\overline{w(x'_k)}$$

$$\le N C^k k! \|w\|_2^{2k} = N C^k k!\,.$$

Advantages of the approach

- Relaxation of dissociativity.

$$\sum_{\sum_j |\varepsilon_j| \ll \log(1/\delta)} \varepsilon_j \lambda_j = 0 \quad \text{instead of} \quad \sum_{j=1}^{|\Lambda|} \varepsilon_j \lambda_j = 0\,.$$

- Very weak dissociativity ($\sum_j |\varepsilon_j| \le C$)
- Other operators T_A^g. Higher moments

$$\sum_{\xi \in \Lambda} |\widehat{A}(\xi)|^l\,, \quad l > 2\,,$$

dual Chang theorems

$$\sum_{x \in \Lambda} (A_1 * A_2)^2(x) \ll |A_1||A_2| \log\left(\min\{|A_1|, |A_2|\}\right)\,.$$

Concluding remarks

- Studying the eigenvalues and the eigenfunctions of T, we obtain the information about the initial object $\mathrm{E}(A)$.

- Our approach tries to emulate Fourier analysis *onto* A not on the whole group $\mathbf{G}$.

Conjecture

The structured pieces of $A \subseteq \mathbf{G}$ are supports of the eigenfunctions of T.

Considered examples

In all examples above (multiplicative subgroups, convex sets and so on), we have

$$\mu_1 \gg \mu_2 \geq \mu_3 \geq \dots , \quad \mu_1 \text{ dominates } .$$

PFRC case

If our set A is a sumset $A = B - B$, $|A| = K|B|$ (or popular difference set) then

$$\mu_1 \sim \mu_2 \sim \dots \sim \mu_k \geq \mu_{k+1} \geq \dots , \quad k \sim K , \quad .$$

So, there many roughly equal eigenvalues.
The correspondent eigenfunctions lives on "disjoint" (sub)sets of $B - b$, $b \in B$.

Thank you for your attention!