Reprint from

ISSN 2220-5438

Moscow Journal of Combinatorics and Number Theory

URSS

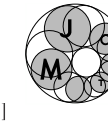
МФТИ

Яндекс

Volume 3 • Issue 3–4 2013

Moscow Journal of Combinatorics and Number Theory Volume 3 • Issue 3–4 2013 URSS

Moscow Journal
of Combinatorics
and Number Theory
2013, vol. 3, iss. 3–4,
pp. 189–239, [pp. 425–475]



Some new inequalities in additive combinatorics

Ilya D. Shkredov (Moscow)

Abstract: In the paper we find new inequalities involving the intersections $A \cap (A-x)$ of shifts of some subset A from an abelian group. We apply the inequalities to obtain new upper bounds for the additive energy of multiplicative subgroups and convex sets and also a series another results on the connection of the additive energy and so-called higher moments of convolutions. Besides we prove new theorems on multiplicative subgroups concerning lower bounds for its doubling constants, sharp lower bound for the cardinality of sumset of a multiplicative subgroup and its subprogression and another results.

Keywords: additive combinatorics, higher energies, multiplicative subgroups, structural theorems

AMS Subject classification: 11B13, 11B30, 11B50, 11T23

Received: 11.06.2013; **revised:** 03.09.2012

1. Introduction

There are two general ideas in additive combinatorics which are opposite to each other in some sense. The first one is the following. Let $\mathbf{G} = (\mathbf{G}, +)$ be a group and A be an arbitrary subset of $\mathbf{G}$. If we want to obtain an information about the additive structure of our set A then it is useful to consider "more smooth" and larger objects like sumsets $A+A$, $A-A$, $A+A+A$ and so on (see [26]). Finding good additive structure in sumsets can be used to get useful information about the original set A. The second idea is to consider smaller objects like $A \cap (A-x)$ and its generalizations to obtain some required properties of A again. The latter approach

is presented brightly in papers [5], [6] and once more time, recently, in [18]. In the article we concentrate on the last method and find new connections between the sets $A_x := A \cap (A - x)$ and the original set A.

The paper based on so-called eigenvalues method (see papers [22] and [21]) as well as Proposition 2. To obtain the proposition we develop the method from [19, 20, 24] choosing some weight optimally and use a simple fact that x belongs to $A - A_s$ iff s belongs to $A - A_x$. The eigenvalues method can be represented, very roughly speaking, as follows. The important role in additive combinatorics plays so-called the *additive energy* of a set A, that is the sum $\mathsf{E}(A) := \sum_x |A_x|^2$. We rewrite the sum as the action of a matrix

$$\mathsf{E}(A) = \sum_{x,y} (\chi_A \circ \chi_A)(x-y)\chi_A(x)\chi_A(y) = \langle \mathsf{T}\chi_A, \chi_A \rangle \,,$$

where χ_A is the characteristic function of A, by $\chi_A \circ \chi_A$ we denote the convolution of χ_A (see the definition in the section 2) and the square matrix T is $\mathsf{T}_{x,y} := (\chi_A \circ \chi_A)(x-y)$, $x, y \in A$. Studying the eigenvalues and the eigenfunctions of T, we obtain the information about the initial object $\mathsf{E}(A)$. Another idea here is an attempt to use "local" analysis on A in contrast to Fourier transformation method which is defined on the whole group. Our approach is especially useful in the situation when A coincide with a multiplicative subgroup of the finite field. The reason is that we know all eigenvalues as well as eigenfunctions in the case.

The simplest consequences of the results are unusual inequalities

$$\sum_x \frac{|A_x|^2}{|A \pm A_x|} \leqslant |A|^{-2} \sum_x |A_x|^3 \,, \qquad (1)$$

and

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

see Corollary 3 and Proposition 5, correspondingly. These formulas combining with another ingredient, so-called Katz—Koester inequality (see [11])

$$|(A+A) \cap (A+A-x)| \geqslant |A + (A \cap (A-x))| \qquad (3)$$

allow us to prove a series of applications (see sections 7, 8). Here we give just two of them.

First of all recall the previous results. In [7] (see also [12]) the following theorem was obtained.

THEOREM 1. *Let p be a prime number, and $\Gamma \subseteq (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ be a multiplicative subgroup, $|\Gamma| = O(p^{2/3})$. Then*

$$\mathsf{E}(\Gamma) = O(|\Gamma|^{5/2}).$$

Recall that a set $A = \{a_1, \dots, a_n\} \subseteq \mathbb{R}$ is called *convex* if $a_i - a_{i-1} < a_{i+1} - a_i$ for every $2 \leqslant i \leqslant n-1$. In paper [8] a result similar to Theorem 1 for convex sets was proved.

THEOREM 2. *Let $A \subseteq \mathbb{R}$ be a convex set. Then*

$$\mathsf{E}(A) = O(|A|^{5/2}).$$

It is known that statistical properties of multiplicative subgroups and convex sets are quite similar (see, e. g. section 3). In particular, both objects have very small characteristic E_3, that is the sum $\sum_x |A_x|^3$. The last situation exactly the case when our method works very well. Besides we exploit some additional irregularity properties of multiplicative subgroups and convex sets (see e. g. general Theorem 11 of section 8). Using our approach we prove that the constant $5/2$ in Theorems 1, 2 can be replaced by $5/2 - \varepsilon_0$, where $\varepsilon_0 > 0$ is an absolute constant. The question was asked to the author by Sergey Konyagin. Certainly, the result implies that $|\Gamma \pm \Gamma| \geqslant |\Gamma|^{3/2+\varepsilon_0}$ and $|A \pm A| \geqslant |A|^{3/2+\varepsilon_0}$ for any subgroup and a convex set, correspondingly. Nevertheless another methods from papers [14, 19, 20, 24] and also Corollary 29 of section 7 give better bounds for the doubling constant here. Further applications of inequalities (1), (2) can be found in sections 7, 8.

The paper is organized as follows. We start with definitions and notations used in the article. The instruments from section 4 concern to sumsets estimates, basically. Here we give our weighted version of Katz—Koester trick. In section 5 we use the obtained results to give a new lower bound for the size of sumsets of multiplicative subgroups and study basis properties of such sets. On the other hand the tools from the next section 6 will be applied to obtain new bounds for the additive energy. The main principle here is the following. Basically, an upper bound for $\mathsf{E}_3(A)$ does not imply something nontrivial concerning the additive energy (up to Hölder inequality, of course) but if we know a little bit more about irregularity of A then it

is possible to obtain a nontrivial upper bound for $\mathsf{E}(A)$. The rigorous statements are contained in sections 7 and 8. Besides inequalities (1), (2) and Katz—Koester trick we extensively use the methods from [21] in our proof.

The author is grateful to Sergey Konyagin, Misha Rudnev and Igor Shparlinski for useful discussions and, especially, Tomasz Schoen for very useful and fruitful explanations and discussions. Also I acknowledge Institute IITP RAS for providing me with excellent working conditions.

2. Definitions

Let $\mathbf{G}$ be an abelian group. If $\mathbf{G}$ is finite then denote by N the cardinality of $\mathbf{G}$. It is well–known [16] that the dual group $\widehat{\mathbf{G}}$ is isomorphic to $\mathbf{G}$ in the case. Let f be a function from $\mathbf{G}$ to $\mathbb{C}$. We denote the Fourier transform of f by $\widehat{f}$,

$$\widehat{f}(\xi) = \sum_{x\in\mathbf{G}} f(x)e(-\xi\cdot x)\,, \tag{4}$$

where $e(x) = e^{2\pi i x}$. We rely on the following basic identities

$$\sum_{x\in\mathbf{G}} |f(x)|^2 = \frac{1}{N}\sum_{\xi\in\widehat{\mathbf{G}}} \left|\widehat{f}(\xi)\right|^2. \tag{5}$$

$$\sum_{y\in\mathbf{G}} \left|\sum_{x\in\mathbf{G}} f(x)g(y-x)\right|^2 = \frac{1}{N}\sum_{\xi\in\widehat{\mathbf{G}}} \left|\widehat{f}(\xi)\right|^2\left|\widehat{g}(\xi)\right|^2. \tag{6}$$

and

$$f(x) = \frac{1}{N}\sum_{\xi\in\widehat{\mathbf{G}}} \widehat{f}(\xi)e(\xi\cdot x)\,. \tag{7}$$

If

$$(f*g)(x) := \sum_{y\in\mathbf{G}} f(y)g(x-y) \quad \text{and} \quad (f\circ g)(x) := \sum_{y\in\mathbf{G}} f(y)g(y+x)$$

then

$$\widehat{f*g} = \widehat{f}\widehat{g} \quad \text{and} \quad \widehat{f\circ g} = \widehat{f}^{\circ}\widehat{g} = \overline{\widehat{f}}\widehat{g}\,, \tag{8}$$

where for a function $f : \mathbf{G} \to \mathbb{C}$ we put $f^c(x) := f(-x)$. Clearly, $(f * g)(x) = (g * f)(x)$ and $(f \circ g)(x) = (g \circ f)(-x)$, $x \in \mathbf{G}$. The $k-$fold convolution, $k \in \mathbb{N}$ we denote by $*_k$, so $*_k := *(*_{k-1})$. It is unimportant but write for definiteness

$$(f \circ_k f)(x) := \sum_{y_1,\dots,y_k} f(y_1)\dots f(y_k) f(x + y_1 + \dots + y_k)\,.$$

We use in the paper the same letter to denote a set $S \subseteq \mathbf{G}$ and its characteristic function $S : \mathbf{G} \to \{0,1\}$. Write $\mathsf{E}(A,B)$ for *additive energy* of two sets $A, B \subseteq \mathbf{G}$ (see e. g. [26]), that is

$$\mathsf{E}(A,B) = \bigl|\{a_1 + b_1 = a_2 + b_2 \ : \ a_1, a_2 \in A,\ b_1, b_2 \in B\}\bigr|\,.$$

If $A = B$ we simply write $\mathsf{E}(A)$ instead of $\mathsf{E}(A,A)$. Clearly,

$$\mathsf{E}(A,B) = \sum_x (A * B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x)(B \circ B)(x)\,. \quad (9)$$

and by (6),

$$\mathsf{E}(A,B) = \frac{1}{N}\sum_{\xi} |\widehat{A}(\xi)|^2 |\widehat{B}(\xi)|^2\,. \quad (10)$$

Let

$$\mathsf{T}_k(A) := \bigl|\{a_1 + \dots + a_k = a'_1 + \dots + a'_k \ : \ a_1,\dots,a_k,a'_1,\dots,a'_k \in A\}\bigr|\,.$$

Let also

$$\sigma_k(A) := (A *_k A)(0) = \bigl|\{a_1 + \dots + a_k = 0 \ : \ a_1,\dots,a_k \in A\}\bigr|\,.$$

Notice that for a symmetric set A that is $A = -A$ one has $\sigma_2(A) = |A|$ and $\sigma_{2k}(A) = \mathsf{T}_k(A)$.

For a sequence $s = (s_1,\dots,s_{k-1})$ put $A^B_s = B \cap (A - s_1)\dots\cap(A - s_{k-1})$. If $B = A$ then write A_s for A^A_s. Let

$$\mathsf{E}_k(A) = \sum_{x \in \mathbf{G}} (A \circ A)(x)^k = \sum_{s_1,\dots,s_{k-1} \in \mathbf{G}} |A_s|^2 \quad (11)$$

and

$$\mathsf{E}_k(A,B) = \sum_{x\in\mathbf{G}}(A\circ A)(x)(B\circ B)(x)^{k-1} = \sum_{s_1,\dots,s_{k-1}\in\mathbf{G}} |B_s^A|^2 \qquad (12)$$

be the higher energies of A and B. The second formulas in (11), (12) can be considered as the definitions of $\mathsf{E}_k(A)$, $\mathsf{E}_k(A,B)$ for non integer k, $k \geqslant 1$.

Clearly,

$$\mathsf{E}_{k+1}(A,B) = \sum_x (A\circ A)(x)(B\circ B)(x)^k =$$

$$= \sum_{x_1,\dots,x_{k-1}} \Big(\sum_y A(y)B(y+x_1)\dots B(y+x_k)\Big)^2 = \mathsf{E}(\Delta_k(A), B^k), \quad (13)$$

where

$$\Delta(A) = \Delta_k(A) := \{(a,a,\dots,a)\in A^k\}\,.$$

We also put $\Delta(x) = \Delta(\{x\})$, $x\in\mathbf{G}$.

Quantities $\mathsf{E}_k(A,B)$ can be written in terms of generalized convolutions.

Definition 1. *Let $k\geqslant 2$ be a positive number, and $f_0,\dots,f_{k-1} : \mathbf{G}\to\mathbb{C}$ be functions. Write F for the vector $(f_0,\dots,f_{k-1})$ and x for vector $(x_1,\dots,x_{k-1})$. Denote by*

$$\mathcal{C}_k(f_0,\dots,f_{k-1})(x_1,\dots,x_{k-1})$$

the function

$$\mathcal{C}_k(F)(x) = \mathcal{C}_k(f_0,\dots,f_{k-1})(x_1,\dots,x_{k-1}) = \sum_z f_0(z)f_1(z+x_1)\dots f_{k-1}(z+x_{k-1})\,.$$

Thus, $\mathcal{C}_2(f_1,f_2)(x) = (f_1\circ f_2)(x)$. If $f_1=\dots=f_k=f$ then write $\mathcal{C}_k(f)(x_1,\dots,x_{k-1})$ for $\mathcal{C}_k(f_1,\dots,f_k)(x_1,\dots,x_{k-1})$.

In particular, $(\Delta_k(B)\circ A^k)(x_1,\dots,x_k) = \mathcal{C}_{k+1}(B,A,\dots,A)(x_1,\dots,x_k)$, $k\geqslant 1$.

For a positive integer n, we set $[n] = \{1,\dots,n\}$. All logarithms used in the paper are to base 2. By $\ll$ and $\gg$ we denote the usual Vinogradov's symbols. If p is a prime number then write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p^*$ for $(\mathbb{Z}/p\mathbb{Z})\setminus\{0\}$.

3. Preliminaries

Suppose that $l, k \geqslant 2$ be positive integers and $\mathbf{F} = (f_{ij})$, $i = 0, \dots, l-1$; $j = 0, \dots, k-1$ be a functional matrix, $f_{ij} : \mathbf{G} \to \mathbb{C}$. Let $R_0, \dots, R_{l-1}$ and $C_0, \dots, C_{k-1}$ be rows and columns of the matrix, correspondingly. The following commutative relation holds.

LEMMA 1. *For any positive integers $l, k \geqslant 2$, we have*

$$\mathcal{C}_l(\mathcal{C}_k(R_0), \dots, \mathcal{C}_k(R_{l-1})) = \mathcal{C}_k(\mathcal{C}_l(C_0), \dots, \mathcal{C}_l(C_{k-1}))\,. \qquad (14)$$

PROOF. Let $y^{(i)} = (y_{i1}, \dots, y_{i(k-1)})$, $i \in [l-1]$, and $y_{(j)} = (y_{1j}, \dots, y_{(l-1)j})$, $j \in [k-1]$. Put also $y_{0j} = 0$, $j = 0, \dots, k-1$, $y_{i0} = 0$, $i = 1, \dots, l-1$ and $x_0 = 0$. We have

$$\mathcal{C}_l(\mathcal{C}_k(R_0), \dots, \mathcal{C}_k(R_{l-1}))(y^{(1)}, \dots, y^{(l-1)}) =$$

$$= \sum_{x_1, \dots, x_{k-1}} \mathcal{C}_k(R_0)(x_1, \dots, x_{k-1})\mathcal{C}_k(R_1)(x_1 + y_{11}, \dots, x_{k-1} + y_{1(k-1)}) \dots$$

$$\dots \mathcal{C}_k(R_{l-1})(x_1 + y_{(l-1)1}, \dots, x_{k-1} + y_{(l-1)(k-1)}) =$$

$$= \sum_{x_0, \dots, x_{k-1}} \sum_{z_0, \dots, z_{l-1}} \prod_{i=0}^{l-1} \prod_{j=0}^{k-1} f_{ij}(x_j + y_{ij} + z_i)\,.$$

Changing the summation, we obtain

$$\mathcal{C}_l(\mathcal{C}_k(R_0), \dots, \mathcal{C}_k(R_{l-1}))(y^{(1)}, \dots, y^{(l-1)}) =$$

$$= \sum_{z_1, \dots, z_{l-1}} \mathcal{C}_l(C_0)(z_1, \dots, z_{l-1})\mathcal{C}_l(C_1)(z_1 + y_{11}, \dots, z_{l-1} + y_{(l-1)1}) \dots$$

$$\dots \mathcal{C}_l(C_{l-1})(z_1 + y_{1(k-1)}, \dots, z_{l-1} + y_{(l-1)(k-1)}) =$$

$$= \mathcal{C}_k(\mathcal{C}_l(C_0), \dots, \mathcal{C}_l(C_{k-1}))(y_{(1)}, \dots, y_{(k-1)})\,.$$

as required. □

COROLLARY 1. *For any functions the following holds*

$$\sum_{x_1, \dots, x_{l-1}} \mathcal{C}_l(f_0, \dots, f_{l-1})(x_1, \dots, x_{l-1})\, \mathcal{C}_l(g_0, \dots, g_{l-1})(x_1, \dots, x_{l-1}) =$$

$$= \sum_z (f_0 \circ g_0)(z) \dots (f_{l-1} \circ g_{l-1})(z) \quad \textbf{(scalar product),} \qquad (15)$$

moreover

$$\sum_{x_1,\dots,x_{l-1}} \mathcal{C}_l(f_0)(x_1,\dots,x_{l-1}) \dots \mathcal{C}_l(f_{k-1})(x_1,\dots,x_{l-1}) =$$

$$= \sum_{y_1,\dots,y_{k-1}} \mathcal{C}_k^l(f_0,\dots,f_{k-1})(y_1,\dots,y_{k-1}) \quad \textbf{(multi–scalar product),} \qquad (16)$$

and

$$\sum_{x_1,\dots,x_{l-1}} \mathcal{C}_l(f_0)(x_1,\dots,x_{l-1})\,(\mathcal{C}_l(f_1) \circ \dots \circ \mathcal{C}_l(f_{k-1}))(x_1,\dots,x_{l-1}) =$$

$$= \sum_z (f_0 \circ \dots \circ f_{k-1})^l(z) \quad (\sigma_k \quad \textbf{for} \quad \mathcal{C}_l)\,. \qquad (17)$$

Proof. Take $k = 2$ in (14). Thus $\mathbf{F}$ is a $l \times 2$ matrix in the case. We have

$$\mathcal{C}_l(f_0 \circ g_0,\dots,f_{l-1} \circ g_{l-1})(x_1,\dots,x_{l-1}) =$$
$$= (\mathcal{C}_l(f_0,\dots,f_{l-1}) \circ \mathcal{C}_l(g_0,\dots,g_{l-1}))(x_1,\dots,x_{l-1})\,.$$

Putting $x_j = 0$, $j \in [l-1]$, we obtain (15). Applying the last formula $(k-2)$ times and after that formula (15), we get (17). Finally, taking $\mathbf{F}_{ij} = f_j$, $i = 0,\dots,l-1$; $j = 0,\dots,k-1$ and putting all variables in (14) equal zero, we obtain (16). This completes the proof. □

We need in the Balog—Szemerédi—Gowers theorem in the symmetric form, see [26] section 2.5.

Theorem 3. *Let $A, B \subseteq \mathbf{G}$ be two sets, $K \geqslant 1$ and $\mathsf{E}(A,B) \geqslant |A|^{3/2}|B|^{3/2}/K$. Then there are $A' \subseteq A$, $B' \subseteq B$ such that*

$$|A'| \gg |A|/K\,, \quad |B'| \gg |B|/K\,,$$

and

$$|A' + B'| \ll K^7 |A|^{1/2}|B|^{1/2}\,.$$

Now let $\mathbf{G} = \mathbb{F}_p$, where p is a prime number and $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup. A set $Q \subseteq \mathbb{F}_p^*$ is called Γ-*invariant* if $Q\Gamma = Q$. In the situation the following lemma which is a consequence of Stepanov's approach [25] can be formulated (see, e. g. [24]).

LEMMA 2. *Let p be a prime number, $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, and $Q, Q_1, Q_2 \subseteq \mathbb{F}_p^*$ be any Γ-invariant sets such that $|Q||Q_1||Q_2| \ll |\Gamma|^5$, $|Q||Q_1||Q_2||\Gamma| \ll \ll p^3$, and $|(Q_1 \times Q_2) \cdot \Delta^{-1}(Q)| = |Q_1||Q_2||Q||\Gamma|^{-1}$. Then*

$$\sum_{x \in Q} (Q_1 \circ Q_2)(x) \ll |\Gamma|^{-1/3} (|Q||Q_1||Q_2|)^{2/3} . \tag{18}$$

Using Lemma 2, one can easily deduce upper bounds for moments of convolution of Γ (see, e. g. [19]).

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

$$\mathsf{E}(\Gamma) \ll |\Gamma|^{5/2} , \quad \mathsf{E}_3(\Gamma) \ll |\Gamma|^3 \log |\Gamma| , \tag{19}$$

and for all $l \geqslant 4$ the following holds

$$\mathsf{E}_l(\Gamma) = |\Gamma|^l + O(|\Gamma|^{\frac{2l+3}{3}}) . \tag{20}$$

Certainly, the condition $|\Gamma| \ll p^{2/3}$ in formula (20) can be relaxed.

The same method gives a generalization (see [12]).

THEOREM 4. *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| < \sqrt{p}$. Let also $d \geqslant 2$ be a positive integer. Then arranging values of $(\Gamma *_{d-1} \Gamma)(\xi)$ in decreasing order $(\Gamma *_{d-1} \Gamma)(\xi_1) \geqslant (\Gamma *_{d-1} \Gamma)(\xi_2) \geqslant \ldots$, where $\xi_j \neq 0$ belong to distinct cosets, we have*

$$(\Gamma *_{d-1} \Gamma)(\xi_j) \ll_d |\Gamma|^{d-2+3^{-1}(1+2^{2-d})} j^{-\frac{1}{3}} .$$

In particular

$$\mathsf{T}_d(\Gamma) \ll_d |\Gamma|^{2d-2+2^{1-d}} , \tag{21}$$

further

$$\sum_z (\Gamma \circ_{d-1} \Gamma)^3(z) \ll_d |\Gamma|^{3d-4+2^{2-d}} \cdot \log |\Gamma| , \tag{22}$$

and similar

$$\sum_z (\Gamma\circ\Gamma)(z)((\Gamma *_{d-1}\Gamma)\circ(\Gamma *_{d-1}\Gamma))^2(z) \ll_d |\Gamma|^{4d-2+3^{-1}(1+2^{3-2d})}\cdot\log|\Gamma|\,. \quad (23)$$

We need in a lemma about Fourier coefficients of an arbitrary Γ-invariant set (see e. g. [19]).

LEMMA 3. *Let $\Gamma\subseteq\mathbb{F}_p^*$ be a multiplicative subgroup, and Q be an Γ-invariant subset of $\mathbb{F}_p^*$. Then for any $\xi\neq 0$ the following holds*

$$|\widehat{Q}(\xi)|\leqslant\min\left\{\left(\frac{|Q|p}{|\Gamma|}\right)^{1/2}, \frac{|Q|^{3/4}p^{1/4}\mathsf{E}^{1/4}(\Gamma)}{|\Gamma|}, p^{1/8}\mathsf{E}^{1/8}(\Gamma)\mathsf{E}^{1/8}(Q)\left(\frac{|Q|}{|\Gamma|}\right)^{1/2}\right\}. \quad (24)$$

Recall that a set $A=\{a_1,\dots,a_n\}\subseteq\mathbb{R}$ is called *convex* if $a_i-a_{i-1}<a_{i+1}-a_i$ for every $2\leqslant i\leqslant n-1$. Convex sets have statistics similar to multiplicative subgroups, in some sense. We need in a lemma, see e. g. [20] or [14].

LEMMA 4. *Let A be a convex set, and B be an arbitrary set. Then*

$$\mathsf{E}_3(A)\ll|A|^3\log|A|\,,$$

and

$$\mathsf{E}(A,B)\ll|A||B|^{\frac{3}{2}}\,.$$

Now consider quantities $(A *_{k-1} A)(x)$. By a classical result of Andrews [1], we have for any x that

$$(A *_{k-1} A)(x)\ll_k |A|^{\frac{k(k-1)}{k+1}}\,.$$

The following result was proved in [8].

THEOREM 5. *Let A be a convex set, and $k\geqslant 2$ be an integer. Then arranging values of $(A *_{k-1} A)(x)$ in decreasing order $(A *_{k-1} A)(x_1)\geqslant(A *_{k-1} A)(x_2)\geqslant\dots$, we have*

$$(A *_{k-1} A)(x_j)\ll_k |A|^{k-\frac{4}{3}(1-2^{-k})}j^{-1/3}\,. \quad (25)$$

In particular

$$\sum_x (A\circ A)(x)((A*_{k-1}A)\circ(A*_{k-1}A))^2(x) \ll_k |A|^{4k-2+3^{-1}(1+2^{3-2k})}\cdot\log|A|\,. \quad (26)$$

As was realized by Li [14] (see also [21]) that subsets A of real numbers with small multiplicative doubling looks like convex sets. More precisely, the following lemma from [21] holds.

LEMMA 5. *Let $A, B\subseteq\mathbb{R}$ be finite sets and let $|AA| = M|A|$. Then arranging values of $(A\circ B)(x)$ in decreasing order $(A\circ B)(x_1)\geqslant(A\circ B)(x_2)\geqslant\ldots$, we have*

$$(A\circ B)(x_j)\ll(M\log M)^{2/3}|A|^{1/3}|B|^{2/3}j^{-1/3}\,.$$

In particular

$$\mathsf{E}(A,B)\ll M\log M|A||B|^{3/2}\,.$$

4. Weighted Katz—Koester transform

In the section we have deal with so-called Katz—Koester trick [11] based on inequality (3), which has recently found many applications, see [10, 14, 15, 17–21, 24]. Originally, estimate (3) was used by Katz and Koester to obtain the following result.

THEOREM 6. *Let $A\subseteq\mathbf{G}$ be a set such that $|A-A|\leqslant K|A|$. Then there exist two absolute constants $\epsilon, C>0$ and a set $A'\subseteq A-A$, $|A'|\gg|A|/K^C$ with $\mathsf{E}(A')\gg|A'|^3/K^{1-\epsilon}$.*

Of course, inequality (3), which is a consequence of the inclusion

$$A+A_s\subseteq(A+A)_s$$

can be derived from a more general *e–trick*, see e. g. [26], namely,

$$A\cup B+A\cap B\subseteq A+B,\qquad\forall\,A,B\subseteq\mathbf{G}\,.$$

A consequence of Katz—Koester trick is an useful inequality

$$|A|^6\leqslant\mathsf{E}_3(A)\sum_{x\in D}(D\circ D)(x)\,, \quad (27)$$

where $D = A-A$. One can show that estimate (27) implies Theorem 6, see e. g. [21]. In the section we, firstly, add some weight in inequality (27), and, secondly, prove a multidimensional generalization of the bound.

First of all let us recall Lemma 2.4 and Corollary 2.5 from [24]. We gather the results in the following proposition.

PROPOSITION 1. *Let $k \geqslant 2$, $m \in [k]$ be positive integers, and let $A_1, \dots, A_k, B$ be finite subsets of an abelian group. Then*

$$A_1 \times \dots \times A_k - \Delta_k(B) = \{(x_1, \dots, x_k) \ : \ B \cap (A_1 - x_1) \cap \dots \cap (A_k - x_k) \neq \varnothing\} \quad (28)$$

and

$$A_1 \times \dots \times A_k - \Delta_k(B) = \\ = \bigcup_{(x_1,\dots,x_m) \in A_1 \times \dots \times A_m - \Delta(B)} \{(x_1, \dots, x_m)\} \times \\ \times (A_{m+1} \times \dots \times A_k - \Delta_{k-m}(B \cap (A_1 - x_1) \cap \dots \cap (A_m - x_m)) \,. \quad (29)$$

Let $A, B \subseteq \mathbf{G}$ be sets, $x \in \mathbf{G}^k$, $s \in \mathbf{G}^l$. By the proposition, we have $x \in A^k - \Delta_k(A^B_s)$ iff $s \in A^l - \Delta_l(A^B_x)$ because of $x \in A^k - \Delta_k(A^B_s)$ iff $A^B_x \bigcap A^B_s \neq \varnothing$. Hence, we obtain the following formula

$$\sum_{s \in A^l - \Delta_l(B)} (A^k - \Delta_k(A^B_s))(x) = |A^l - \Delta_l(A^B_x)| \,. \quad (30)$$

In the case $k = l = 1$ we recover the trivial identities

$$(A - A_s)(x) = (A - A_x)(s) \quad \text{and} \quad \sum_s (A - A_s)(x) = |A - A_x| \,.$$

The next lemma is a very special case of Lemma 2.8 from [24].

LEMMA 6. *Let $A, B \subseteq \mathbf{G}$ be sets, and k, l be positive integers. Then*

$$\sum_{s \in \mathbf{G}^l} \mathsf{E}(A^k, \Delta(A^B_s)) = \mathsf{E}_{k+l+1}(B, A) \,.$$

Now we obtain the main proposition of the section.

PROPOSITION 2. *Let $A, B \subseteq \mathbf{G}$ be two sets, k, l be positive integers, and $q : \mathbf{G}^k \to \mathbb{C}$ be an arbitrary function. Then*

$$|A|^{2l} \left| \sum_{x \in \mathbf{G}^k} q(x)(A^k \circ \Delta_k(B))(x) \right|^2 \leqslant \mathsf{E}_{k+l+1}(B, A) \cdot \sum_{x \in \mathbf{G}^k} |A^l \pm \Delta_l(A_x^B)| |q(x)|^2 \,. \quad (31)$$

PROOF. We have

$$\sum_s \sum_x (A^k \circ \Delta(A_s^B))(x) q(x) = \sum_x q(x) \sum_s (A^k \circ \Delta(A_s^B))(x) =$$
$$= |A|^l \sum_x q(x)(A^k \circ \Delta(B))(x) \,. \quad (32)$$

Applying Cauchy—Schwartz twice, Lemma 6 and formula (30), we get

$$|A|^{2l} \left| \sum_x q(x)(A^k \circ \Delta(B))(x) \right|^2 \leqslant$$
$$\leqslant \left(\sum_s \left(\sum_x (A^k - \Delta(A_s^B))(x) |q(x)|^2 \right)^{1/2} \cdot \left(\sum_x (A^k \circ \Delta(A_s^B))^2(x) \right)^{1/2} \right)^2 \leqslant$$
$$\leqslant \sum_x |q(x)|^2 \sum_s (A^k - \Delta(A_s^B))(x) \cdot \sum_s \mathsf{E}(A^k, \Delta(A_s^B)) =$$
$$= \sum_x |q(x)|^2 |A^l - \Delta(A_x^B)| \cdot \mathsf{E}_{k+l+1}(B, A)$$

and formula (31) with minus follows. To get the remain formula with plus consider $A_s^* = A_s^*(B) := B \cap (s_1 - A) \cap \ldots \cap (s_l - A)$ instead of A_s^B. It is easy to see that formula (32) takes place for such sets. Besides as in Proposition 1, we have $x \in A^k - \Delta(A_s^*)$ iff $A_s^* \cap A - x_1 \cap \ldots \cap A - x_k \neq \varnothing$ and further iff $s \in A^l + \Delta(A_x^B)$. Thus, we obtain an analog of formula (30)

$$\sum_s (A^k - \Delta(A_s^*))(x) = |A^l + \Delta(A_x^B)| \,.$$

Finally,

$$\sum_s \mathsf{E}(A^k, \Delta(A_s^*)) = \sum_z (A\circ A)^k(x)(B\circ B)(x)(A\circ A)^l(-x) = \mathsf{E}_{k+l+1}(B,A)$$

and the result is proved. □

Let us derive simple consequences of the result above. Consider the case $A = B$. If we take $k = l = 1$ and $q(x) = (A - A)(x)$ then we obtain Corollary 3.2 from [19] as well as Lemma 2.3 from [24]. If we take $k = l = 1$ and $q(x) = (A\circ A)^{1/2}(x)$ then we get Lemma 2.5 from [14]. Let us derive further consequences.

COROLLARY 3. *Let $A, B \subseteq \mathbf{G}$ be two sets, and k, l be positive integers. Then*

$$|A|^{2l}\mathsf{E}^2_{k+1}(B,A) \leqslant \mathsf{E}_{k+l+1}(B,A)\cdot \sum_x |A^l \pm \Delta(A_x^B)|(A^k\circ \Delta_k(B))^2(x) \qquad (33)$$

and

$$|A|^{2l}\sum_x \frac{(A^k\circ\Delta_k(B))^2(x)}{|A^l \pm \Delta_l(A_x^B)|} \leqslant \mathsf{E}_{k+l+1}(B,A)\,. \qquad (34)$$

In particular

$$\sum_x \frac{|A_x|^2}{|A \pm A_x|} \leqslant \frac{\mathsf{E}_3(A)}{|A|^2}\,.$$

PROOF. Taking $q(x) = (A^k\circ\Delta(B))(x)$ and applying Corollary 1, we obtain the first formula. Choosing $q(x)$ optimally, that is

$$q(x) = \frac{(A^k\circ\Delta_k(B))(x)}{|A^l \pm \Delta_l(A_x^B)|}\,,$$

we get (34). □

Until the end of the section suppose, for simplicity, that $B = A$. Corollary 1 implies that $\sum_x (A^k\circ\Delta(A))^2(x) = \mathsf{E}_{k+1}(A)$. Combining the identity with formula (34), we obtain

Corollary 4.

$$\sum_{x\,:\,|A^l\pm\Delta_l(A_x)|\geqslant\frac{|A|^{2l}\mathsf{E}_{k+1}(A)}{2\mathsf{E}_{k+l+1}(A)}}(A^k\circ\Delta_k(A))^2(x)\geqslant 2^{-1}\mathsf{E}_{k+1}(A)\,. \qquad (35)$$

For example $(k=l=1)$

$$\sum_{x\,:\,|A\pm A_x|\geqslant 2^{-1}|A|^2\mathsf{E}(A)\mathsf{E}_3^{-1}(A)}|A_x|^2\geqslant 2^{-1}\mathsf{E}(A)\,.$$

Suppose that $\mathsf{E}_{k+l+1}(A)\ll|A|^{k+l+1}$. Using a trivial bound $|A^l\pm\Delta(A_x)|\leqslant$ $\leqslant|A|^l|A_x|$, we see that the lower bound for $|A_x|$, deriving from (35), namely, $|A_x|\geqslant 2^{-1}|A|^l\mathsf{E}_{k+1}(A)\mathsf{E}_{k+l+1}^{-1}(A)$ is potentially sharper then usual estimate $|A_x|\geqslant$ $\geqslant 2^{-1}\mathsf{E}_{k+1}(A)|A|^{-(k+1)}$, which follows from the identity $\sum\limits_x|A_x|^2=\mathsf{E}_{k+1}(A)$.

The same arguments give

Corollary 5.

$$\sum_{x\,:\,|A^l\pm\Delta_l(A_x)|\geqslant(A^k\circ\Delta_k(A))(x)\cdot\frac{|A|^{2l+k+1}}{2\mathsf{E}_{k+l+1}(A)}}(A^k\circ\Delta_k(A))(x)\geqslant 2^{-1}|A|^{k+1}\,. \qquad (36)$$

In the case $k=l=1$, we obtain

$$\sum_{x\,:\,|A\pm A_x|\geqslant|A_x|\cdot\frac{|A|^4}{2\mathsf{E}_3(A)}}|A_x|\geqslant 2^{-1}|A|^2\,.$$

Finally in the case $k=l=1$, let us obtain an useful corollary.

Corollary 6. *Let α, p be real numbers, $p>1$. Then*

$$\sum_x|A_x|^\alpha\leqslant\left(\frac{\mathsf{E}_3(A)}{|A|^2}\right)^{1/p}\cdot\left(\sum_x|A\pm A_x|^{\frac{1}{p-1}}|A_x|^{\frac{\alpha\ p-2}{p-1}}\right)^{(p-1)/p}\,. \qquad (37)$$

5. Applications of the weighted Katz—Koester trick

Our first application of the results of the previous section is an unusual upper bound for the additive energy of a multiplicative subgroup via its sumset. Theorems of such a sort was appeared in [21].

THEOREM 7. *Let p be a prime number, and $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| = O(p^{2/3})$ and*

$$\mathsf{E}(\Gamma) \leqslant \sqrt{p}|\Gamma|^{\frac{3}{2}} \log |\Gamma| . \qquad (38)$$

Then

$$\mathsf{E}(\Gamma) \ll |\Gamma|^{\frac{4}{3}}|\Gamma \pm \Gamma|^{\frac{2}{3}} \log |\Gamma| . \qquad (39)$$

PROOF. Let $Q = \Gamma \pm \Gamma$. We can assume that

$$|Q| = O\left(\frac{\mathsf{E}^{3/2}(\Gamma)}{|\Gamma|^2 \log^{3/2}|\Gamma|}\right) \qquad (40)$$

because otherwise inequality (39) is trivial. Applying formula (33) of Corollary 3 with $k = l = 1$ and using inequality

$$|\Gamma \pm \Gamma_x| \leqslant ((\Gamma \pm \Gamma) \circ ((\Gamma \pm \Gamma)))(x)$$

(see [11] or just Proposition 1), we obtain

$$|\Gamma|^2\mathsf{E}^2(\Gamma) \leqslant \mathsf{E}_3(\Gamma) \sum_x (Q \circ Q)(x)(\Gamma \circ \Gamma)^2(x) . \qquad (41)$$

If we prove that

$$\sum_{x \neq 0} (Q \circ Q)(x)(\Gamma \circ \Gamma)^2(x) \ll \frac{|Q|^{4/3}}{|\Gamma|^{2/3}}|\Gamma|^{7/3} \log |\Gamma| \ll |Q|^{4/3}|\Gamma|^{5/3} \log |\Gamma| \qquad (42)$$

then substituting the last formula into (41) and using the bound $\mathsf{E}_3(\Gamma) = O(|\Gamma|^3 \log|\Gamma|)$ from Corollary 2, we get formula (39). The term with $x = 0$ is $\mathsf{E}_3(\Gamma)|Q||\Gamma|^2$ and can be handed easily.

From (41) it follows that the summation is taken over nonzero x such that

$$(Q \circ Q)(x) \geqslant \frac{\mathsf{E}(\Gamma)|\Gamma|^2}{2\mathsf{E}_3(\Gamma)} := H .$$

Hence, it is sufficient to prove that

$$\sum_{x \neq 0 \,:\, (Q \circ Q)(x) \geqslant H} (Q \circ Q)(x)(\Gamma \circ \Gamma)^2(x) \ll |Q|^{4/3}|\Gamma|^{5/3} \log |\Gamma| . \qquad (43)$$

Let $(Q\circ Q)(\xi_1)\geqslant (Q\circ Q)(\xi_2)\geqslant\ldots$ and $(\Gamma\circ\Gamma)(\eta_1)\geqslant(\Gamma\circ\Gamma)(\eta_2)\geqslant\ldots$, where nonzero $\xi_1,\xi_2,\ldots$ and $\eta_1,\eta_2,\ldots$ belong to distinct cosets. Applying Lemma 2 once more, we get

$$(Q\circ Q)(\xi_j)\ll\frac{|Q|^{4/3}}{|\Gamma|^{2/3}}j^{-1/3}\,,\quad\text{and}\quad(\Gamma\circ\Gamma)(\eta_j)\ll|\Gamma|^{2/3}j^{-1/3}\,,\qquad(44)$$

provided that $j|\Gamma||Q|^2\ll|\Gamma|^5$ and $j|\Gamma||Q|^2|\Gamma|\ll p^3$. We have $j\ll|Q|^4/(|\Gamma|^2H^3)$. Using inequalities $\mathsf{E}(\Gamma)\ll|\Gamma|^{5/2}$, $\mathsf{E}_3(\Gamma)\ll|\Gamma|^3\log|\Gamma|$, formula (40) and assumption (38) it is easy to check that the last conditions are satisfied. Applying (44), we obtain (42). This completes the proof. □

For example if $|\Gamma|=O(p^{1/2})$ then assumption (38) holds. Using trivial lower bound for $\mathsf{E}(\Gamma)$, that is $\mathsf{E}(\Gamma)\geqslant|\Gamma|^4/|\Gamma+\Gamma|$, we obtain

Corollary 7. *Let $\Gamma\subseteq\mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma|\ll\sqrt{p}$. Then*

$$|\Gamma+\Gamma|\gg\frac{|\Gamma|^{8/5}}{\log^{3/5}|\Gamma|}\,.$$

As for the difference set it is known (see [24]) at the moment that $|\Gamma-\Gamma|\gg$ $\gg|\Gamma|^{5/3}\log^{-1/2}|\Gamma|$ for an arbitrary multiplicative subgroup Γ with $|\Gamma|\ll\sqrt{p}$. We will see soon that the condition $|\Gamma|\ll\sqrt{p}$ in Corollary 7 can be relaxed (see Theorem 8 below).

Corollary 8. *Let $\Gamma\subseteq\mathbb{F}_p^*$ be a multiplicative subgroup, $-1\in\Gamma$ such that $|\Gamma|\geqslant p^{\kappa}$, where $\kappa>33/68$. Then for all sufficiently large p we have $6\Gamma=\mathbb{F}_p$. If $\kappa>55/112$ then $\mathbb{F}_p^*\subseteq 6\Gamma$ without condition $-1\in\Gamma$.*

Proof. Put $S=\Gamma+\Gamma$, $n=|\Gamma|$, $m=|S|$, and $\rho=\max\limits_{\xi\neq0}|\widehat{\Gamma}(\xi)|$. By a well–known upper bound for Fourier coefficients of multiplicative subgroups (see e. g. Corollary 2.5 from [19] or Lemma 3) we have $\rho\leqslant p^{1/8}\mathsf{E}^{1/4}(\Gamma)$. If $\mathbb{F}_p^*\subseteq 6\Gamma$ then for some $\lambda\neq0$, we obtain

$$0=\sum_{\xi}\widehat{S}^2(\xi)\widehat{\Gamma}^2(\xi)\widehat{\lambda\Gamma}(\xi)=m^2n^3+\sum_{\xi\neq0}\widehat{S}^2(\xi)\widehat{\Gamma}^2(\xi)\widehat{\lambda\Gamma}(\xi)\,.$$

Therefore, by the estimate $\rho \leqslant p^{1/8}\mathsf{E}^{1/4}(\Gamma)$ and Parseval identity we get

$$n^3m^2 \leqslant \rho^3 mp \ll (p^{1/8}\mathsf{E}^{1/4})^3 mp\,. \qquad (45)$$

Now applying formula (39) and $m \gg n^{5/3}\log^{-1/2} n$ (see [24]), we obtain the required result. To obtain the same without condition $-1 \in \Gamma$ just use formula (45), combining with formula (39) and apply the lower bound for $\Gamma+\Gamma$ from Corollary 7. $\square$

Remark 5.1. The inclusion $\mathbb{F}_p^* \subseteq 6\Gamma$ was obtained in [21] under the assumption $\kappa > 99/203$. Even more stronger results than containing in Corollary 8 were obtained by A. Efremov using further development of our method (unpublished).

6. Eigenvalues of some operators

We make use of some operators, which were introduced in [22]. These operators have found some applications in additive combinatorics and number theory (see [22] and [21]).

Definition 2. *Let* $\mathbf{G}$ *be an abelian group, and* φ, ψ *be two complex functions on* $\mathbf{G}$. *By* $\mathrm{T}^{\varphi}_{\psi}$ *denote the following operator on the space of functions* $\mathbb{C}^{\mathbf{G}}$

$$(\mathrm{T}^{\varphi}_{\psi} f)(x) = \psi(x)(\widehat{\varphi^c} * f)(x)\,, \qquad (46)$$

where f *is an arbitrary complex function on* $\mathbf{G}$.

Suppose that $\mathbf{G}$ is a finite abelian group, and $A \subseteq \mathbf{G}$ is a set. Denote by $\overline{\mathrm{T}}^{\varphi}_{A}$ the restriction of operator T^{φ}_{A} onto the space of the functions with supports on A. Recall some simple properties of operators $\overline{\mathrm{T}}^{\varphi}_{A}$ which were obtained in [22]. First of all, it was proved, in particular, that operators T^{φ}_{A} and $\overline{\mathrm{T}}^{\varphi}_{A}$ have the same non–zero eigenvalues. Second of all, if φ is a real function then the operator $\overline{\mathrm{T}}^{\varphi}_{A}$ is symmetric (hermitian) and if φ is a nonnegative function then the operator is nonnegative definite. The action of $\overline{\mathrm{T}}^{\varphi}_{A}$ can be written as

$$\langle \overline{\mathrm{T}}^{\varphi}_{A} u, v\rangle = \sum_x (\widehat{\varphi^c} * u)(x)\overline{v}(x) = \sum_x \widehat{\varphi^c}(x)(u \circ \overline{v})(x) = \sum_x \varphi(x)\widehat{u}(x)\overline{\widehat{v}(x)}\,, \quad (47)$$

where u, v are arbitrary functions such that $\operatorname{supp} u, \operatorname{supp} v \subseteq A$. Further

$$\operatorname{tr}(\overline{\mathrm{T}}_A^{\varphi}) = |A|\widehat{\varphi}(0) = \sum_{j=1}^{|A|} \mu_j(\overline{\mathrm{T}}_A^{\varphi}) = \sum_{j=1}^{|\mathbf{G}|} \mu_j(\mathrm{T}_A^{\varphi})\,, \qquad (48)$$

where $\mu_j(\mathrm{T}_A^{\varphi})$ are eigenvalues of the operator T_A^{φ}. If φ is a real function then as was noted before $\overline{\mathrm{T}}_A^{\varphi}$ is a symmetric matrix. In particular, it is a normal matrix and we get

$$\operatorname{tr}(\overline{\mathrm{T}}_A^{\varphi}(\overline{\mathrm{T}}_A^{\varphi})^*) = \sum_z |\widehat{\varphi}(z)|^2 (A \circ A)(z) = \sum_z (\varphi \circ \varphi)(z)|\widehat{A}(z)|^2 =$$

$$= \sum_{j=1}^{|A|} \mu_j^2(\overline{\mathrm{T}}_A^{\varphi}) = \sum_{j=1}^{|\mathbf{G}|} \mu_j^2(\mathrm{T}_A^{\varphi})\,. \qquad (49)$$

We will deal with just nonnegative definite symmetric operators. In the case we arrange the eigenvalues in order of magnitude

$$\mu_0(\overline{\mathrm{T}}_A^{\varphi}) \geqslant \mu_1(\overline{\mathrm{T}}_A^{\varphi}) \geqslant \ldots \geqslant \mu_{|A|-1}(\overline{\mathrm{T}}_A^{\varphi})\,. \qquad (50)$$

Further properties of such operators can be found in [22]. The connection of such operators with higher energies $\mathrm{E}_k(A)$ is discussed in [21].

Now we consider the situation when A equals some multiplicative subgroup. It turns out that in this case we know all eigenvalues μ_j as well as all eigenfunctions.

Let p be a prime number, $q = p^s$ for some integer $s \geqslant 1$. Let $\mathbb{F}_q$ be the field with q elements, and let $\Gamma \subseteq \mathbb{F}_q$ be a multiplicative subgroup. We will write $\mathbb{F}_q^*$ for $\mathbb{F}_q \setminus \{0\}$. Denote by t the cardinality of Γ, and put $n = (q-1)/t$. Let also $\mathbf{g}$ be a primitive root, then $\Gamma = \{\mathbf{g}^{nl}\}_{l=0,1,\ldots,t-1}$. Let $\chi_\alpha(x)$, $\alpha \in [t]$ be the orthonormal family of multiplicative characters on Γ, that is

$$\chi_\alpha(x) = |\Gamma|^{-1/2} \cdot e\left(\frac{\alpha\, l}{t}\right)\,, \quad x = \mathbf{g}^{nl}\,, \quad 0 \leqslant l < t\,. \qquad (51)$$

In particular, $\chi_\alpha(x) = 0$ if $x \notin \Gamma$. Clearly, products of such functions form a basis on Cartesian products of Γ.

The following proposition was obtained, basically, in [21] (except formula (52)). We recall the proof for the sake of completeness.

PROPOSITION 3. *Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup. If ψ is an arbitrary Γ-invariant function then the functions $\chi_\alpha(x)$ are eigenfunctions of the operator $\overline{\mathrm{T}}_\Gamma^{\widehat{\psi}}$. Suppose, in addition, that $\widehat{\psi}(x) \geqslant 0$. Then for any functions $u : \mathbb{F}_q \to \mathbb{C}$ and $v : \mathbb{F}_q \to \mathbb{R}^+$ the following holds*

$$\sum_{x,y\in\Gamma} \psi(x-y)\mathcal{C}_3(v,\overline{u},u)(x,y) \geqslant |\Gamma|^{-2} \sum_x \psi(x)(\Gamma\circ\Gamma)(x) \cdot \sum_{x,y\in\Gamma} \mathcal{C}_3(v,\overline{u},u)(x,y)\,. \tag{52}$$

In particular, for any function u with support on Γ, we have

$$\sum_x \psi(x)(u\circ\overline{u})(x) \geqslant |\Gamma|^{-2} \sum_x \psi(x)(\Gamma\circ\Gamma)(x) \cdot \Big|\sum_{x\in\Gamma} u(x)\Big|^2\,. \tag{53}$$

PROOF. We have to show that

$$\mu f(x) = \Gamma(x)(\psi * f)(x)\,, \quad \mu \in \mathbb{C}$$

for $f(x) = \chi_\alpha(x)$. For every $\gamma \in \Gamma$, we obtain

$$(\psi * f)(\gamma x) = \sum_z f(z)\psi(\gamma x - z) = \sum_z f(\gamma z)\psi(\gamma x - \gamma z) = \tag{54}$$

$$= f(\gamma)\cdot \sum_z f(z)\psi(x-z) = f(\gamma)\cdot(\psi * f)(x) \tag{55}$$

as required.

Formula (53) follows from (52) if one take $v = \delta_0$. We give another independent proof. Because of $\widehat{\psi}(x) \geqslant 0$ the operator $\overline{\mathrm{T}}_\Gamma^{\widehat{\psi}}$ is symmetric and nonnegative definite. Thus all its eigenvalues are nonnegative. Put $\varphi = q^{-1}\widehat{\psi}$. If $u = \sum_\alpha c_\alpha \chi_\alpha$ then

$$\langle \overline{\mathrm{T}}_\Gamma^{\varphi} u, u\rangle = \sum_x \psi(x)(u\circ\overline{u})(x) = \sum_\alpha |c_\alpha|^2 \mu_\alpha(\overline{\mathrm{T}}_\Gamma^{\varphi}) \geqslant |\Gamma|^{-2}\langle u,\Gamma\rangle^2 \sum_x \psi(x)(\Gamma\circ\Gamma)(x)$$

and we obtain (53).

Finally, for any function $F : \Gamma\times\Gamma \to \mathbb{C}$, we have

$$F(x,y) = \sum_{\alpha,\beta} c_{\alpha,\beta}(F)\chi_\alpha(x)\chi_\beta(y)\,.$$

Thus

$$\sum_{x,y} F(x,y)\psi(x-y) = \sum_{\alpha} \mu_\alpha \cdot c_{-\alpha,\alpha}(F)$$

and we just need to check that $c_{-\alpha,\alpha}(F) \geqslant 0$ for $F(x,y) = \mathcal{C}_3(v,\overline{u},u)(x,y)$. By assumption $v \geqslant 0$. Hence by Corollary 1

$$c_{-\alpha,\alpha}(F) = \sum_{x,y} F(x,y)\overline{\chi_\alpha(x)}\chi_\alpha(y) = \sum_{z} v(z)\big|(\chi_\alpha \circ u)\big|^2(z) \geqslant 0 \qquad (56)$$

and the result follows. □

In particular, for any $k \geqslant 1$

$$\mathsf{E}_{k+1}(\Gamma) = \max_{f\,:\,\operatorname{supp} f \subseteq \Gamma,\, \|f\|_2^2 = |\Gamma|} \sum_x (\Gamma \circ \Gamma)^k(x)(f \circ f)(x)\,. \qquad (57)$$

Remark 6.1. It is not difficult to replace a multiplicative subgroup Γ in the previous proposition onto arbitrary coset (see [21]). Indeed, for every $\xi \in \mathbb{F}_q^*/\Gamma$ and $\alpha \in [|\Gamma|]$, let us define the functions $\chi_\alpha^\xi(x) := \chi_\alpha(\xi^{-1}x)$. Then, clearly, $\operatorname{supp}\chi_\alpha^\xi = \xi\cdot\Gamma$ and $\chi_\alpha^\xi(\gamma x) = \chi_\alpha(\gamma)\chi_\alpha^\xi(x)$ for all $\gamma \in \Gamma$. Using the argument from Proposition 3 it is easy to see that the functions χ_α^ξ are orthonormal eigenfunctions of the operator $\overline{\mathsf{T}}^{\widehat{\psi}}_{\xi\Gamma}$. Thus, we can replace Γ onto $\xi\Gamma$.

Proposition 3 has an interesting corollary about Fourier coefficients of functions with supports on Γ. In particular, it gives exact formula for exponential sums over multiplicative subgroups.

Corollary 9. *Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup. Suppose that u is a function with support on Γ. Then for any $\lambda \in \mathbb{F}_q$ the following holds*

$$|\widehat{u}(\lambda)|^2 = |\Gamma|^2 \cdot \min_h \frac{\sum\limits_x |\widehat{h}(x)|^2 |\widehat{u}(x+\lambda)|^2}{\sum\limits_x |\widehat{h}(x)|^2 |\widehat{\Gamma}(x)|^2}\,, \qquad (58)$$

and, in addition, for any $v : \mathbb{F}_q \to \mathbb{R}^+$, we have

$$\sum_{x,y\in\Gamma} \mathcal{C}_3(v,u,\overline{u})(x,y) = |\Gamma|^2 \cdot \min_h \mathsf{E}^{-1}(h,\Gamma) \cdot \sum_{x,y\in\Gamma} (h\circ\overline{h})(x-y)\mathcal{C}_3(v,u,\overline{u})(x,y)\,, \qquad (59)$$

where the minimum is taken over all nonzero Γ*-invariant functions.*

Proof. Taking $\psi = h \circ \overline{h}$ in formula (53) of Proposition 3 and using Fourier transform, we obtain that

$$|\sum_{z\in\Gamma} u(z)|^2 \leqslant |\Gamma|^2 \cdot \min_h \frac{\sum\limits_x |\widehat{h}(x)|^2 |\widehat{u}(x)|^2}{\sum\limits_x |\widehat{h}(x)|^2 |\widehat{\Gamma}(x)|^2} \qquad (60)$$

for any function u with support on Γ. Considering $h \equiv 1$ we make sure that formula (60) is actually equality. Now taking $u(x)e(-\lambda x)$ instead of $u(x)$, we have formula (58). Equality (59) is a consequence of (52) and can be obtained by similar arguments. This completes the proof. □

Let $g : \mathbb{F}_q \to \mathbb{C}$ be a Γ-invariant function. It is convenient to write $\mu_\alpha(g)$ for $\mu_\alpha(\mathrm{T}_\Gamma^{q-1}\overline{g})$. So, now the eigenvalues are indexed by $\alpha \in \mathbb{Z}/t\mathbb{Z}$ not in decreasing order as in (50). It is easy to see that $\overline{\mu_\alpha(g)} = \mu_\alpha(\overline{g}^c) = \mu_{-\alpha}(\overline{g})$. Multiplicative properties of the functions χ_α allow us to prove formula (61) below, which shows that the numbers $\mu_\alpha(\overline{g}h)$ and $\mu_\alpha(g)$, $\mu_\alpha(h)$ are connected.

Proposition 4. *Let* $g, h : \mathbb{F}_q \to \mathbb{C}$ *be two* Γ*-invariant functions. Then*

$$\mu_\alpha(\overline{g}h) = \frac{1}{|\Gamma|}\sum_\beta \overline{\mu}_\beta(g)\mu_{\alpha+\beta}(h) = (\mu(\overline{g}) * \mu(h))(\alpha)\,, \qquad (61)$$

and

$$\mu_\alpha(g) = |\Gamma|^{1/2}\sum_x g(x)\chi_\alpha(1-x)\,. \qquad (62)$$

Proof. We have

$$\frac{1}{|\Gamma|}\sum_\beta \overline{\mu}_\beta(g)\mu_{\alpha+\beta}(h) = \frac{1}{|\Gamma|}\sum_{x,y}\overline{g}(x)h(y)\sum_\beta(\overline{\chi}_\beta\circ\chi_\beta)(x)(\chi_{\alpha+\beta}\circ\overline{\chi}_{\alpha+\beta})(y) =$$

$$= \frac{1}{|\Gamma|}\sum_{x,y}\overline{g}(x)h(y)\sum_{z,w\in\Gamma}\sum_\beta \overline{\chi}_\beta(z)\chi_\beta(z+x)\chi_{\alpha+\beta}(w)\overline{\chi}_{\alpha+\beta}(w+y) =$$

$$= \frac{1}{|\Gamma|}\sum_{x,y}\overline{g}(x)h(y)\sum_{w\in\Gamma}\chi_\alpha(w)\overline{\chi}_\alpha(w+y)\varpi(x,y,w)\,,$$

where $\varpi(x,y,w)$ equals 1 iff $w, w+y \in \Gamma$ and, more importantly, $(z+x)/z = (w+y)/w$ for some z such that $z, z+x \in \Gamma$. It is easy to see that the last situation appears exactly when $xy^{-1} \in \Gamma$, provided by $y \neq 0$. Besides $y=0$ iff $x=0$. Thus by Γ-invariance of the function g

$$\frac{1}{|\Gamma|}\sum_{\beta}\overline{\mu}_{\beta}(g)\mu_{\alpha+\beta}(h) = \overline{g}(0)h(0) + \frac{1}{|\Gamma|}\sum_{x\neq 0,\, y\neq 0}\overline{g}(x)h(y)\Gamma(xy^{-1})(\chi_{\alpha}\circ\overline{\chi}_{\alpha})(y) =$$

$$= \overline{g}(0)h(0) + \sum_{y\neq 0}\overline{g}(y)h(y)(\chi_{\alpha}\circ\overline{\chi}_{\alpha})(y) = \sum_{y}\overline{g}(y)h(y)(\chi_{\alpha}\circ\overline{\chi}_{\alpha})(y) = \mu_{\alpha}(\overline{g}h)$$

and we obtain formula (61).

One can derive (62) from (61). Another way is to use formula (54) of Proposition 3. We propose one more variant. Consider $\mu_{\alpha}(g) = f(\alpha)$ as a function on α and compute the Fourier transform of f. Now write $e(x)$ for $e^{2\pi i x/|\Gamma|}$. We have for $\alpha \neq 0$

$$\widehat{f}(\alpha) = \sum_{\beta}\sum_{x} g(x)\sum_{z}\chi_{\beta}(z-x)\overline{\chi}_{\beta}(z)e(-\alpha\beta) = \sum_{x} g(x)\Gamma(x(1-\mathbf{g}^{n\alpha})^{-1}) =$$

$$= \sum_{x} g(x(1-\mathbf{g}^{n\alpha}))\Gamma(x) = |\Gamma| g(1-\mathbf{g}^{n\alpha})\,.$$

Besides the last formula holds in the case $\alpha = 0$ because we have general identity (48). Finally, using the inverse formula (7), we obtain

$$\mu_{\alpha}(g) = \sum_{\beta} g(1-\mathbf{g}^{n\beta})e(\alpha\beta) = |\Gamma|^{1/2}\sum_{x} g(1-x)\chi_{\alpha}(x) = |\Gamma|^{1/2}\sum_{x} g(x)\chi_{\alpha}(1-x)\,.$$

This completes the proof. □

In particular, taking $\alpha = 0$, $l = 2$ and $g = h$ in formula (61), we obtain formula (49) for operators $\overline{\mathrm{T}}^{\varphi}_{\Gamma}$, where $\varphi(x) = q^{-1}\widehat{g}$ and Γ is a multiplicative subgroup.

Corollary 10. *Let $g : \mathbb{F}_q \to \mathbb{R}$ be a Γ-invariant function. Put $\mu(\alpha) = \mu_{\alpha}(g)$. Then for all positive integers l, we have*

$$\mu_{\alpha}(g^l) = (\mu *_{l-1} \mu)(\alpha)\,, \tag{63}$$

and

$$g^l(x-y)=\sum_{\alpha}(\mu *_{l-1}\mu)(\alpha)\chi_\alpha(x)\overline{\chi_\alpha(y)}\,, \quad x,y\in\Gamma\,, \tag{64}$$

where $*$ *the normalized convolution over* $|\Gamma|$. *In particular, numbers* $\mathsf{E}(\Gamma,\chi_\alpha)$, $\alpha\in[|\Gamma|]$ *determine* $\mathsf{E}_l(\Gamma)$ *for all* $l\geqslant 2$.

Now consider for a moment the case of prime $q=p$.

Remark 6.2. Suppose that $g(x)=(\Gamma\circ\Gamma)(x)$ and $\mu_l(\alpha)=\mu_\alpha(g^l)$. By Corollary 2 and formulas (48), (49), we get for any $|\Gamma|\ll p^{2/3}$ and $l\geqslant 2$ that

$$\sum_{\alpha}(\mu_l(\alpha)-|\Gamma|^l)^2\ll|\Gamma|^{1+(2l+1)\cdot 2/3}=|\Gamma|^{4l/3+5/3}\,.$$

Thus, we have an asymptotic formula for all $l\geqslant 2$

$$\mu_l(\alpha)=\sum_x(\Gamma\circ\Gamma)^l(x)(\chi_\alpha\circ\chi_\alpha)(x)=|\Gamma|^l+O(|\Gamma|^{2l/3+5/6})\,,\quad \alpha\in[|\Gamma|]\,.$$

Using the arguments from the proof of Proposition 3, we obtain a general inequality.

Proposition 5. *Let* $A\subseteq\mathbf{G}$ *be a set, and* ψ *be a symmetric function such that* $\widehat{\psi}\geqslant 0$. *Then*

$$\sum_{x,y,z\in A}\psi(x-y)\overline{\psi(x-z)}\psi(y-z)\geqslant$$

$$\geqslant\max\left\{\frac{1}{|A|^3}\left(\sum_x\psi(x)(A\circ A)(x)\right)^3\,,\ |\psi^3(0)|\cdot|A|\,,\right.$$

$$\left.\frac{1}{|A|^{1/2}}\left(\sum_x|\psi^2(x)|(A\circ A)(x)\right)^{3/2}\right\}. \tag{65}$$

In particular, taking $\psi(x)=|A_x|$, *we get*

$$\sum_{x,y,z\in A}|A_{x-y}||A_{x-z}||A_{y-z}|\geqslant\left(\frac{\mathsf{E}(A)}{|A|}\right)^3\,, \tag{66}$$

PROOF. Put $u(x) = \psi^c(x) = \psi(x)$, $v(x) = A^c(x) \geqslant 0$. Let $\{f_\alpha\}_{\alpha\in A}$ be an orthonormal family of the eigenfunctions of the operator $\overline{\mathrm{T}}_A^{N^{-1}\widehat{\psi}}$ and $\{\mu_\alpha\}_{\alpha\in A}$ be the correspondent nonnegative eigenvalues. Then

$$\sigma := \sum_{x,y\in A} \psi(x-y)\mathcal{C}_3(v,\overline{u},u)(x,y) = \sum_{\alpha\in A} \mu_\alpha\ d_\alpha\ ,$$

where by Corollary 1

$$d_\alpha := \sum_{x,y} \mathcal{C}_3(v,\overline{u},u)(x,y)\overline{f_\alpha(x)}f_\alpha(y) = \sum_z v(z)|(f_\alpha\circ u)|^2(z) = \sum_{z\in A} |(\psi * f_\alpha)|^2(z)\ . \tag{67}$$

To get the last identities we have used the arguments from the proof of formula (56) and the fact that $\psi = \psi^c$. Further, because of f_α is the eigenfunctions of the operator $\overline{\mathrm{T}}_A^{N^{-1}\widehat{\psi}}$, we have

$$\mu_\alpha\ f_\alpha(x) = A(x)(\psi * f_\alpha)(x)\ .$$

Thus in view of $||f_\alpha||_2^2 = 1$, we obtain $d_\alpha = \mu_\alpha^2$. Note also a trivial lower bound for the largest eigenvalue μ_0, namely

$$\mu_0 \geqslant |A|^{-1}\langle \overline{\mathrm{T}}_A^{N^{-1}\widehat{\psi}} A, A\rangle = |A|^{-1}\sum_x \psi(x)(A\circ A)(x)\ .$$

Hence, applying the last inequality and the assumption $\psi = \psi^c$ once more, we get

$$\sigma = \sum_{x,y\in A} \psi(x-y)\mathcal{C}_3(v,\overline{\psi},\psi)(x,y) = \sum_{x,y,z\in A} \psi(x-y)\overline{\psi(x-z)}\psi(y-z) = \sum_{\alpha\in A}\mu_\alpha^3 \geqslant$$

$$\geqslant \mu_0^3 \geqslant \frac{1}{|A|^3}\left(\sum_x \psi(x)(A\circ A)(x)\right)^3$$

and the first inequality in (65) is proved. To get the second and the third ones, we use the obtained formula $\sigma = \sum\limits_{\alpha\in A}\mu_\alpha^3$, identities (48), (49), correspondingly, and Hölder inequality. This completes the proof. □

Another way to prove (65) is to write $\Psi(x,y)=\psi(x-y)A(x)A(y)$ as

$$\Psi(x,y)=\sum_{\alpha,\beta}c_{\alpha,\beta}\overline{f_\alpha(x)}f_\beta(y)$$

and note that all terms in the last sum except $\alpha=\beta$ vanish. Further, clearly, $c_{\alpha,\alpha}=\mu_\alpha$. Thus, substitution $\Psi(x,y)$ into (65) gives the result. In principle, this method gives further generalization of inequality (65) onto larger number of variables in the case of *multiplicative subgroups* because its eigenfunctions χ_α have multiplicative properties (see the proof of Proposition 4).

In the general situation we have just the following generalization, where each variable appears twice

$$\sum_{x_1,\dots,x_k\in A}\psi(x_1-x_2)\psi(x_2-x_3)\psi(x_3-x_4)\dots\psi(x_{k-1}-x_k)\psi(x_k-x_1)=$$

$$=\sum_{\alpha\in A}\mu_\alpha^k(\overline{\mathrm{T}}_A^{N^{-1}\widehat{\psi}})\geqslant\left(\frac{1}{|A|}\sum_x\psi(x)(A\circ A)(x)\right)^k\,, \quad (68)$$

where $k\geqslant 1$. Here ψ is a symmetric function and $\widehat{\psi}\geqslant 0$ ($k\geqslant 3$). For $k=1$, $k=2$ these are general identities (48), (49). If one use the singular–value decomposition lemma for $\mathcal{C}_{k+1}(\vec{x},y)$, $k\geqslant 3$ (see section 8 of [21]) then some functions ψ in (68) can be replaced by its moments. In the case of multiplicative subgroups one can replace ψ in (68) by *different* symmetric Γ-invariant functions with nonnegative Fourier transform.

Finally, note also that the condition $\widehat{\psi}\geqslant 0$ is vitally needed in the proposition above. Indeed if we consider a dense symmetric subset $Q\subseteq\mathbf{G}$ having no solutions of the equation $\alpha+\beta=\gamma$, $\alpha,\beta,\gamma\in Q$ and put $A=\mathbf{G}$, $\psi=Q$ then inequality (65) does not hold. The phenomenon that such sets must have (large) negative and positive Fourier coefficients was considered in [23], see section 5.

Let ψ be a nonnegative function on an abelian group Γ, and $A\subseteq\mathbf{G}$ be a set. Consider the operator $\overline{\mathrm{T}}_A^{N^{-1}\widehat{\psi}}$ and its orthonormal eigenfunctions $\{f_j\}_{j\in[|A|]}$. The condition $\psi\geqslant 0$ implies that $f_0\geqslant 0$, and $\mu_0\geqslant 0$. The next lemma shows that the function f_0 is close to $A(x)/|A|^{1/2}$ in some weak sense.

LEMMA 7. *Let $A \subseteq \mathbf{G}$ be a set, and ψ be a nonnegative function, μ_0 be the first eigenvalue of the operator $\overline{\mathrm{T}}_A^{N^{-1}\widehat{\psi}}$. Then*

$$|A| \geqslant \left(\sum_x f_0(x)\right)^2 \geqslant \max\left\{\frac{\mu_0}{||\psi||_\infty}, \frac{\mu_0^2}{||\psi||_2^2}\right\}, \tag{69}$$

and for the first eigenfunction of $\overline{\mathrm{T}}_A^{N^{-1}\widehat{\psi}}$, $||f_0||_2 = 1$ the following holds

$$||f_0||_\infty \leqslant \frac{||\psi||_2}{\mu_0}. \tag{70}$$

If $\widehat{\psi} \geqslant 0$ then

$$||f_0||_\infty \leqslant \frac{||\psi_1||_2}{\mu_0^{1/2}}, \tag{71}$$

where $\psi = \psi_1 \circ \overline{\psi}_1$.

PROOF. Let $\mu = \mu_0$, $f = f_0$, $g = \sum\limits_x f(x)$. We have

$$\mu f(x) = A(x)(\psi * f)(x). \tag{72}$$

Thus

$$\mu = \sum_x f(x)(\psi * f)(x) \tag{73}$$

and

$$\mu^2 = \sum_{x \in A} (\psi * f)^2(x). \tag{74}$$

Formula (72) implies that

$$\mu g = \sum_{x \in A} (\psi * f)(x).$$

Applying Cauchy—Schwarz and (74) (or just Cauchy—Schwarz), we obtain $g^2 \leqslant |A|$. Further, bound $g^2 \geqslant \mu ||\psi||_\infty^{-1}$ easily follows from (73). Using the formula once more, we get

$$\mu \leqslant \sum_x f(x) \cdot ||\psi||_2 ||f||_2 = ||\psi||_2 g$$

and we obtain (69). Returning to (72) and applying the same argument, we have (70). It remains to prove (71). Because of $\widehat{\psi} \geqslant 0$ there is ψ_1 such that $\psi = \psi_1 \circ \overline{\psi}_1$. Applying (72) and using Cauchy—Schwarz, we get for any $x \in A$

$$\mu|f(x)| \leqslant \sum_y (f * \overline{\psi}_1)(x+y)\psi_1(y) \leqslant ||\psi_1||_2 \cdot (\sum_y |(f * \overline{\psi}_1)(y)|^2)^{1/2} = ||\psi_1||_2 \cdot \mu^{1/2} ,$$

where formula (73) and the fact $\psi = \psi_1 \circ \overline{\psi}_1$ have been used. This completes the proof. □

We will use Lemma 7 in section 8.

7. Applications of the eigenvalues method to multiplicative subgroups

We begin with a new upper bound for the additive energy of a multiplicative subgroup. Our result is "unconditional", i. e. not depending on the size of a sumset, as opposed to Theorem 7. The method of the proof will be used in section 8.

THEOREM 8. *Let p be a prime number and $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| \ll p^{2/3}$. Then*

$$\mathsf{E}(\Gamma) \ll \min\{|\Gamma|^{\frac{32}{13}} \log^{\frac{41}{65}} |\Gamma|, |\Gamma|^3 p^{-\frac{1}{3}} \log |\Gamma| + p^{\frac{1}{26}} |\Gamma|^{\frac{31}{13}} \log^{\frac{8}{13}} |\Gamma|\} . \qquad (75)$$

PROOF. Let $|\Gamma| = t$, $\mathsf{E}_3(\Gamma) = \mathsf{E}_3$, $\mathsf{E}(\Gamma) = \mathsf{E} = t^3/K$, $K \gg t^{1/2}$. We need to find the lower bound for K.

Applying the first estimate of Theorem 4 and recalling the assumption $t \ll p^{2/3}$, we obtain

$$2^{-2}\mathsf{E} \leqslant \sum_{s\,:\, 2^{-1}|\Gamma|K^{-1} < (\Gamma\circ\Gamma)(s) \leqslant cK} (\Gamma \circ \Gamma)^2(s) , \qquad (76)$$

where $c > 0$ is an absolute constant. Put

$$S_j = \{s \in \Gamma - \Gamma \ :\ 2^{j-2}|\Gamma|K^{-1} < (\Gamma \circ \Gamma)(s) \leqslant 2^{j-1}|\Gamma|K^{-1}\} ,$$

where $j \in [l]$, $2^l \leqslant 2cK^2|\Gamma|^{-1} \ll K^2|\Gamma|^{-1} \leqslant t$. Thus by (76) the following holds

$$2^{-2}\mathsf{E} \leqslant \sum_{j=1}^{l} \sum_{s \in S_j} (\Gamma \circ \Gamma)^2(s) .$$

By the pigeonhole principle, we find $j \in [l]$ such that

$$2^{-2}l^{-1}\mathsf{E} \leqslant \sum_{s\in S_j}(\Gamma\circ\Gamma)^2(s) \leqslant |S_j|(2^{j-1}|\Gamma|K^{-1})^2\,. \qquad (77)$$

Put $S = S_j$, $\Delta = 2^{j-1}|\Gamma|K^{-1}$, and $g(x) = (\Gamma\circ\Gamma)(x)S(x)$. Let

$$\sigma_* = \sum_{x\in\Gamma}(\Gamma * g)^2(x)\,.$$

By the Cauchy—Schwartz inequality

$$\sigma_* \geqslant t^{-1}\left(\sum_{x\in\Gamma}(\Gamma * g)(x)\right)^2 \geqslant \frac{\mathsf{E}^2}{l^2t} = \frac{t^5}{l^2K^2}$$

(actually, in the case of multiplicative subgroups the first inequality is equality). Applying some modification of formula (52) of Proposition 3 with $\psi(x) = u(x) = (\Gamma\circ\Gamma)(x)$, $\psi^S(x) = \psi(x)S(x) = g(x)$, $v(x) = \Gamma(x)$ and the coset $(-\Gamma)$, we obtain

$$\sum_{x,y,z\in\Gamma}\psi(y-x)\psi^S(z-x)\psi^S(y-z) \geqslant \frac{\mathsf{E}}{t^2}\cdot\sigma_*\,.$$

In other words

$$\sum_{\alpha,\beta}\psi^S(\alpha)\psi^S(\beta)\psi(\alpha-\beta)\mathcal{C}_3(\Gamma)(\alpha,\beta) \geqslant \frac{\mathsf{E}}{t^2}\cdot\sigma_*\,. \qquad (78)$$

Clearly,

$$\sum_{\alpha\neq0,\beta\neq0,\alpha\neq\beta}\psi^S(\alpha)\psi^S(\beta)\psi(\alpha-\beta)\mathcal{C}_3(\Gamma)(\alpha,\beta) \geqslant 2^{-1}\frac{\mathsf{E}}{t^2}\cdot\sigma_* \qquad (79)$$

because if α, β or $\alpha-\beta$ equals zero then

$$t\mathsf{E}_3(\Gamma) \gg \frac{t^6}{l^2K^3}$$

which implies $K \gg t^{2/3}\log^{-1}t$ and the result follows. Further the summation in (79) can be taken over nonzero α such that

$$\psi(\alpha) \geqslant 2^{-4}\frac{\mathsf{E}}{t^2} := d \qquad (80)$$

because of for other α, we have

$$3d\sigma_* < 2^{-1}\frac{\mathsf{E}}{t^2}\cdot\sigma_*$$

with a contradiction. In the last formula we have used the fact that Γ is a subgroup. On the other hand consider a subset $Q = S_i$ of nonzero α from (80) such that

$$\sum_{\alpha\neq 0,\beta\neq 0,\alpha\neq\beta}\psi^S(\alpha)\psi^S(\beta)\psi^Q(\alpha-\beta)\mathcal{C}_3(\Gamma)(\alpha,\beta) =$$

$$= \sum_{x,y,z\in\Gamma}\psi^Q(y-x)\psi^S(z-x)\psi^S(y-z) \geqslant \frac{\mathsf{E}}{2lt^2}\cdot\sigma_*\,. \qquad (81)$$

The existence of Q follows from the pigeonhole principle. Put $q = 2^{i-1}tK^{-1}$. By one more application of the Cauchy—Schwartz inequality, we obtain

$$q\widetilde{\mathsf{E}} = q\sum_{\alpha\neq 0,\beta\neq 0,\alpha\neq\beta}(\psi^S)^2(\alpha)(\psi^S)^2(\beta)(\Gamma\circ\Gamma)(\alpha-\beta) \gg \frac{\mathsf{E}^2}{t^4}\cdot\sigma_*^2\mathsf{E}_3^{-1} \gg \frac{\mathsf{E}^6}{l^4t^6\mathsf{E}_3}\,. \qquad (82)$$

Our task is to estimate $\widetilde{\mathsf{E}}$. Firstly,

$$\widetilde{\mathsf{E}} \ll \Delta^4\mathsf{E}(S,\Gamma) \ll \Delta^4 t|S|^{3/2}\,, \qquad (83)$$

provided by

$$|S|^{3/2}t^2 \ll t^5 \quad \text{and} \quad |S|^{3/2}t^3 \ll p^3\,. \qquad (84)$$

Because of $|S| \ll t^2$ it is easy to check that the first condition takes place. The second condition is equivalent to $|S| \ll p^2t^{-2}$ and we will consider it later. Secondly,

$$\widetilde{\mathsf{E}} \ll q^2\Delta^3\sum_x(\Gamma\circ\Gamma)(x)(S\circ Q)(x) \ll$$

$$\ll q^2\Delta^3\mathsf{E}^{1/2}(S,\Gamma)\mathsf{E}^{1/2}(Q,\Gamma) \ll q^2\Delta^3 t|S|^{3/4}|Q|^{3/4}\,, \qquad (85)$$

provided by the additional condition $|Q|^{3/2}t^3 \ll p^3$ holds. Again, it is equivalent to $|Q| \ll p^2t^{-2}$ and we will consider it later. Now, combining (83), (85), we obtain

$$\Delta^3 t|S|^{3/4}\min\{q\Delta|S|^{3/4}, q^{-1/4}t^{9/4}\} \gg \Delta^3 t|S|^{3/4}\min\{q\Delta|S|^{3/4}, q^2|Q|^{3/4}\} \gg \frac{\mathsf{E}^6}{l^4t^6\mathsf{E}_3}\,,$$

where the inequalities $|Q| \ll t^3 q^{-3}$ and $t \ll p^{2/3}$ have been used. Optimizing over q ($q = t^{9/5}\Delta^{-4/5}|S|^{-3/5}$), we have

$$\Delta^{16/5} t^{14/5} |S|^{9/10} \gg \frac{\mathsf{E}^6}{l^4 t^6 \mathsf{E}_3} \,.$$

After some computations it gives us $\mathsf{E} \ll t^{32/13} \log^{41/65} t$ as required. It remains to consider the case $|S| \gg p^2 t^{-2}$ or $|Q| \gg p^2 t^{-2}$. We will do it later, before this we need in an appropriate upper bound for t.

Now let us obtain an upper bound for the additive energy for larger t, unconditionally. Returning to the beginning, we get

$$\frac{\mathsf{E}^6}{l^4 t^6} \ll \mathsf{E}_3 \Delta^4 q^2 \sum_x Q(x)(S \circ S)(x) \ll t^3 l \Delta^4 q^2 \sigma_Q(S) \,.$$

Using Fourier transform and the second inequality of Lemma 3, we obtain

$$\sigma_Q(S) \leqslant \frac{|S|^2 |Q|}{p} + |S| \frac{|Q|^{3/4} p^{1/4} \mathsf{E}^{1/4}}{t} \,. \tag{86}$$

If the first term in (86) dominates then using the inequalities $\Delta^2 |S| \leqslant \mathsf{E}$ and $q^2 |Q| \leqslant \mathsf{E}$, we obtain $\mathsf{E} \ll t^3 p^{-1/3} \log t$ and we are done in the case. Otherwise, applying a consequence of Theorem 4, namely

$$|Q| \ll \min\{\mathsf{E} q^{-2}, t^3 q^{-3}\} \,, \tag{87}$$

we have

$$\frac{\mathsf{E}^6}{l^4 t^6} \ll t^2 l \Delta^4 |S| p^{1/4} \min\{\mathsf{E} q^{1/2}, t^{9/4} \mathsf{E}^{1/4} q^{-1/4}\} \,.$$

Optimizing over q ($q = t^3 \mathsf{E}^{-1}$), we get

$$\frac{\mathsf{E}^5}{l^3 t^6} \ll t^2 l \Delta^2 p^{1/4} t^{3/2} \mathsf{E}^{1/2} \ll t^2 l (t^3 \mathsf{E}^{-1})^2 p^{1/4} t^{3/2} \mathsf{E}^{1/2} \,. \tag{88}$$

It gives us $\mathsf{E} \ll p^{1/26} t^{31/13} \log^{8/13} t$ and, hence, $\mathsf{E} \ll t^3 p^{-1/3} l$ provided by $t \gg p^{29/48} l^{-5/8}$. Note that $13/21 > 29/48$, so if $t \ll p^{29/48} l^{-5/8}$ then the first term in (75) dominates. Further, from the same formula (88), we have $\mathsf{E} \ll |\Gamma|^{32/13} \log^{41/65} |\Gamma|$ provided by $t \gg p^{1/2} l^{-1/5}$. It remains to consider the case

$t \ll p^{1/2}l^{-1/5}$ and check that $|S| \ll p^2t^{-2}$, $|Q| \ll p^2t^{-2}$ in the situation. The last inequalities follows from the fact $|S|, |Q| \ll t^2$ and our condition $t \ll p^{1/2}l^{-1/5}$. This completes the proof. $\square$

In principle, our method can be applied to estimate T_k but it works just for small k, $k = 2, 3$. For large k one can use more accurate arguments from [12] to improve these bounds. We do not make such calculations.

Note, finally, that inequality (75) gives bounds for $\mathsf{E}(\Gamma)$ which are better than Theorem 4 if $|\Gamma| \ll p^{2/3}\log^{-2} p$.

Now we formulate Corollary 39 from [21], which was obtained by eigenvalues method of section 6 also.

Corollary 11. *Let p be a prime number, $\Gamma_* \subseteq \mathbb{F}_q^*$ be a coset of a multiplicative subgroup Γ. If $Q^{(y)} \subseteq Q^k$, $y \in \Gamma'$ is an arbitrary family of sets, then*

$$\Big|\bigcup_{y\in\Gamma'}(Q^{(y)} \pm \Delta(y))\Big| \geqslant \frac{|\Gamma|}{|\Gamma'|\mathsf{E}_{k+1}(\Gamma_*, Q)} \cdot \Big(\sum_{y\in\Gamma'}|Q^{(y)}|\Big)^2 .$$

In particular for every set $A \subseteq \Gamma_*$, and every Γ-invariant set Q, we have

$$|Q + A| \geqslant |A| \cdot \frac{|\Gamma||Q|^2}{\mathsf{E}_2(\Gamma_*, Q)} . \qquad (89)$$

Corollary above combining with Theorem 8 say that multiplicative subgroups have strong expanding property.

Corollary 12. *Let p be a prime number, $\Gamma_* \subseteq \mathbb{F}_q^*$ be a coset of a multiplicative subgroup Γ, $|\Gamma| \ll p^{1/2}$. Then for any $A \subseteq \Gamma_*$, we have*

$$|A + \Gamma| \gg \frac{|A||\Gamma|^{7/13}}{\log^{41/65}|\Gamma|} .$$

Ordinary application of Cauchy—Schwarz gives $|A + \Gamma| \gg |A|^{1/2}|\Gamma|^{\kappa}$, $\kappa < 10/13$ for any set A and any multiplicative subgroup Γ, $|\Gamma| \ll p^{1/2}$.

Theorem 8 gives a direct application to the exponential sums over subgroups.

COROLLARY 13. *Let p be a prime number, Γ be a multiplicative subgroup, $|\Gamma| \ll p^{1/2}$. Then*

$$\max_{\xi\neq 0} |\widehat{\Gamma}(\xi)| \ll \min\{p^{1/8}|\Gamma|^{8/13}, p^{1/4}|\Gamma|^{19/52}\} \cdot \log^{41/260} |\Gamma| \,. \qquad (90)$$

PROOF. Let $\rho = \max\limits_{\xi\neq 0} |\widehat{\Gamma}(\xi)|$. Because of $\rho \leqslant p^{1/8}\mathsf{E}^{1/4}(\Gamma)$ and $\rho \leqslant p^{1/4}|\Gamma|^{-1/4}\mathsf{E}^{1/4}(\Gamma)$ (see e. g. Corollary 2.5 from [19] or Lemma 3), applying Theorem 8, we obtain (90). This completes the proof. □

For any function $f : \Gamma \to \mathbb{C}$ by $\mathsf{T}^{\times}_k(f)$ denote the quantity

$$\mathsf{T}^{\times}_k(f) = \sum_{x_1,\dots,x_k,x'_1,\dots,x'_k \,:\, x_1\dots x_k = x'_1\dots x'_k} f(x_1)\dots f(x_k)\overline{f(x'_1)}\dots\overline{f(x'_k)} \,.$$

$\mathsf{T}^{\times}_k(f)$ is a multiplicative analog of $\mathsf{T}_k(f)$ from section 2. Write also $\mathsf{E}^{\times}$ for $\mathsf{T}^{\times}_2$.

Using the eigenvalues method, we want to find some relations between $\mathsf{T}^{\times}_k(A)$ and another characteristics of an arbitrary subset A of a multiplicative subgroup. We need in a simple lemma.

LEMMA 8. *Let $\Gamma \subseteq \mathbb{F}^*_q$ be a multiplicative subgroup. Suppose that $f(x) = \sum\limits_{\alpha} c_\alpha \chi_\alpha(x)$ is an arbitrary function with support on Γ. Then*

$$\mathsf{T}^{\times}_k(f) = |\Gamma|^{k-1} \sum_{\alpha} |c_\alpha|^{2k} \,.$$

PROOF. By the multiplicative property of the functions $\chi_\alpha(x)$, we have

$$\sum_{\alpha} |c_\alpha|^{2k} = \sum_{\alpha} |\sum_{x} f(x)\chi_\alpha(x)|^{2k} =$$

$$= \sum_{\alpha} \sum_{x_1,\dots,x_k,x'_1,\dots,x'_k} f(x_1)\dots f(x_k)\overline{f(x'_1)}\dots$$

$$\dots\overline{f(x'_k)}\chi_\alpha(x_1)\dots\chi_\alpha(x_k)\overline{\chi_\alpha(x'_1)}\dots\overline{\chi_\alpha(x'_k)} = \frac{\mathsf{T}^{\times}_k(P)}{|\Gamma|^{k-1}}$$

as required. □

Corollary 14. *Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup, and $A \subseteq \Gamma$. Then $\mathsf{T}_k^\times(A) \geqslant \geqslant \dfrac{|A|^{2k}}{|\Gamma|}$.*

Now formulate a result on a relation between $\mathsf{T}_k^\times(A)$ and some another characteristics of an arbitrary subset A of a multiplicative subgroup.

Proposition 6. *Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup, and A be any subset of Γ. Then for an arbitrary integer $k \geqslant 2$, we have*

$$|A|^2 \leqslant |\Gamma|^2 (\mathsf{T}_k^\times(A))^{1/k} \cdot \min_h \left(\frac{||h||_1}{||h||_2}\right)^{2/k} \frac{\sum\limits_x |h(x)|^2}{\sum\limits_x (h \circ \overline{h})(x)(\Gamma \circ \Gamma)(x)}\,, \qquad (91)$$

where the minimum is taken over all nonzero Γ-invariant functions. In the case $k = 2$, we also have

$$|A| \leqslant |\Gamma|^{1/4} (\mathsf{E}^\times(A))^{1/4} \qquad (92)$$

and

$$\mathsf{E}_l(A, \Gamma) \leqslant |\Gamma|^{-1/2} \mathsf{E}_{2l-1}^{1/2}(\Gamma) (\mathsf{E}^\times(A))^{1/2} \qquad (93)$$

for any $l \geqslant 2$.

Proof. Take $g(x) = (h \circ \overline{h})(x)$. Then $\widehat{g} \geqslant 0$. Now proceed as in the proof of formula (53) from Proposition 3. Let $A = \sum\limits_\alpha c_\alpha \chi_\alpha$ and $\mu_\alpha = \mu_\alpha(\overline{\mathsf{T}}_\Gamma^{q^{-1}\widehat{g}})$. By Hölder, we have

$$\sum_x g(x)(A \circ A)(x) = \sum_\alpha |c_\alpha|^2 \mu_\alpha \leqslant \left(\sum_\alpha |c_\alpha|^{2k}\right)^{1/k} \left(\sum_\alpha \mu_\alpha^{\frac{k}{k-1}}\right)^{1-1/k}. \qquad (94)$$

Applying Lemma 8, we get

$$\sum_\alpha |c_\alpha|^{2k} = \frac{\mathsf{T}_k^\times(A)}{|\Gamma|^{k-1}}\,. \qquad (95)$$

On the other hand

$$\left(\sum_\alpha \mu_\alpha^{\frac{k}{k-1}}\right)^{1-1/k} \leqslant \mu_0^{1/k} \cdot (\sum_\alpha \mu_\alpha)^{1-1/k} \leqslant ||h||_1^{2/k} ||h||_2^{2-2/k} |\Gamma|^{1-1/k}\,, \qquad (96)$$

where a trivial estimate

$$\mu_0 = |\Gamma|^{-1} \sum_x g(x)(\Gamma \circ \Gamma)(x) \leqslant (\sum_x |h(x)|)^2$$

and a particular case of formula (48), namely,

$$\sum_\alpha \mu_\alpha = |\Gamma| g(0) = |\Gamma| ||h||_2^2$$

were used. Substituting (95) and (96) into (94), we get

$$\frac{|A|^2}{|\Gamma|^2} \sum_x g(x)(\Gamma \circ \Gamma)(x) = c_0^2 \mu_0 \leqslant \sum_x g(x)(A \circ A)(x) \leqslant$$

$$\leqslant ||h||_2^2 (\mathsf{T}_k^\times(A))^{1/k} \left(\frac{||h||_1}{||h||_2} \right)^{2/k} \qquad (97)$$

and (91) is proved.

To obtain (92), we just note that in the case $k = 2$ the sum $\sum_\alpha \mu_\alpha^2$ from (96) can be computed. Indeed by formula (49)

$$\sum_\alpha \mu_\alpha^2 = \sum_x |g(x)|^2 (\Gamma \circ \Gamma)(x) = \sum_x |(h \circ \overline{h})(x)|^2 (\Gamma \circ \Gamma)(x) \qquad (98)$$

and after using the same arguments as above, we have

$$|A|^2 \leqslant |\Gamma|^{3/2} (\mathsf{E}^\times(A))^{1/2} \cdot \min_h \frac{\left(\sum_x |(h \circ \overline{h})(x)|^2 (\Gamma \circ \Gamma)(x) \right)^{1/2}}{\sum_x (h \circ \overline{h})(x)(\Gamma \circ \Gamma)(x)} . \qquad (99)$$

Optimizing the last inequality over h (taking $h(x) \equiv 1$), we obtain (92). To get (93) take $g(x) = (\Gamma \circ \Gamma)^{l-1}(x)$, use formula (98) and repeat the arguments from (94), (98). After some computations, we have

$$\sum_x g(x)(A \circ A)(x) = \mathsf{E}_l(A, \Gamma) \leqslant |\Gamma|^{-1/2} \mathsf{E}_{2l-1}^{1/2}(\Gamma) (\mathsf{E}^\times(A))^{1/2}$$

as required. This completes the proof of the proposition. □

Note that formula (92) is just reformulation of Lemma 8. Formulas (91)–(93) give an explanation why Γ is a eigenfunction of operator $\mathsf{T}^{\widehat{g}}_{\Gamma}$. The thing is $\mathsf{T}^{\times}_{k}(\Gamma)$ is maximal over all subsets of a multiplicative subgroup.

Below we will deal with the field $\mathbb{F}_p$, where p is a prime number. There are plenty results about the quantity $\mathsf{T}^{\times}_{k}$ for arithmetic progressions in $\mathbb{F}_p$.

THEOREM 9. 1) *Let $P \subseteq \mathbb{F}_p^*$ be an arithmetic progression. Then* [4]

$$\mathsf{T}^{\times}_{2}(P) = \frac{|P|^4}{p} + O(|P|^{2+o(1)}) .$$

2) *If $|P| \ll p^{1/8}$ then* [3] *the number of solutions of the congruence*

$$xyz \equiv \lambda \pmod p , \quad \lambda \neq 0 , \quad x, y, z \in P$$

does not exceed $|P|^{o(1)}$ (uniformly over λ).
3) *If ν is a positive integer, $|P| \ll p^{c(\nu)}$, where $c(\nu) > 0$ is some constant depends on ν only. Then* [2] *the number of solutions of the congruence*

$$x_1 \dots x_\nu \equiv \lambda \pmod p , \quad \lambda \neq 0 , \quad x_1 \dots x_\nu \in P$$

is bounded by

$$\exp\left(c'(\nu)\frac{\log|P|}{\log\log|P|}\right) ,$$

where $c'(\nu) > 0$ depends on ν only.

COROLLARY 15. *Let $\Gamma \subseteq \mathbb{F}_q^*$ be a nontrivial multiplicative subgroup. Then for any progression $P \subseteq \Gamma$ the following holds*

$$|P| \ll |\Gamma|^{1/2+o(1)} , \qquad (100)$$

Suppose that $|\Gamma| \ll p^{2/3}$ and $l \geqslant 3$. Then

$$\mathsf{E}(P,\Gamma) \ll |P|^{1+o(1)}|\Gamma|\log^{1/2}|\Gamma| \quad \text{and} \quad \mathsf{E}_l(P,\Gamma) \ll |P|^{1+o(1)}|\Gamma|^{l-1} . \qquad (101)$$

PROOF. Suppose that $P \subseteq \Gamma$ is an arbitrary progression. By Theorem 9, we have

$$\mathsf{E}^{\times}(P) = \frac{|P|^4}{p} + O(|P|^{2+o(1)}) . \qquad (102)$$

If the first term is dominated then applying (92), we get

$$|P| \leqslant \frac{2^{1/4}|P|}{p^{1/4}}|\Gamma|^{1/4}$$

with contradiction. Thus the second term in (102) is dominated and using (92), we obtain (100). Applying Theorem 9 once again, formula (93) and Corollary 2, we get (101). This completes the proof. □

Clearly, the condition $|\Gamma| \ll p^{2/3}$ can be relaxed for large l. Obviously, inequality (101) is the best possible up to $|P|^{o(1)}$ factor.

Remark 7.1. The arguments from the proof of Proposition 6 give (we consider the simplest case $l = 2$) the following asymptotic formula

$$\mathsf{E}(P,\Gamma) = \sum_x (\Gamma \circ \Gamma)(x)(P \circ P)(x) = \frac{|P|^2\mathsf{E}(\Gamma)}{|\Gamma|^2} + \theta|P|^{1+o(1)}|\Gamma|^{-1/2}(\mathsf{E}^*_3(\Gamma))^{1/2}\,,$$

where $|\theta| \leqslant 1$ and $\mathsf{E}^*_3(\Gamma) = \sum\limits_{\alpha\neq 0}\mu^2_\alpha$. Here $P \subseteq \Gamma$ is an arithmetic progression. The asymptotic formula works just for large subgroups of size $p^{1-\delta}$, $\delta > 0$.

Remark 7.2. Certainly, inequality

$$|P+\Gamma| \gg |\Gamma||P|^{1-o(1)}\log^{-1/2}|\Gamma| \qquad (103)$$

follows from (101) by Cauchy—Schwartz and one can obtain analog of formula (103) for l larger than two, namely, $|\Gamma^{l-1}+\Delta_{l-1}(P)| \gg |P|^{1-o(1)}|\Gamma|^{l-1}$. Nevertheless in the case $l > 2$ a more exact and general bound was obtained in [21] (see Corollary 39, the case $k \geqslant 2$), namely,

$$|\Gamma^2+\Delta_2(A)| \gg |A||\Gamma|^2\log^{-1}|\Gamma| \quad \text{and} \quad |\Gamma^{l-1}+\Delta_{l-1}(A)| \gg |A||\Gamma|^{l-1}\,, \quad l > 3 \qquad (104)$$

for *any* $A \subseteq \Gamma$.

Finally, for the sake of completeness and because of it is difficult to find in the literature, we add a very simple result on progressions in small subgroups.

Proposition 7. *Let p be a prime number, $\delta \in (0,1)$ is a real number. Suppose that $\Gamma \subseteq \mathbb{F}^*_p$ is a multiplicative subgroup, $|\Gamma| = p^{1-\delta}$, and $P = \{a, 2a, \ldots, sa\} \subseteq \Gamma$,*

$a \neq 0$. *Then there is an absolute constant* $C > 0$ *such that for all* $p \geqslant p_0(\delta)$, *we have*

$$|P| \leqslant \exp(C\sqrt{\delta^{-1}\log(1/\delta)\log p})\,. \tag{105}$$

Moreover for any such arithmetic progression P, $\log|P| \gg \sqrt{\delta^{-1}\log(1/\delta)\log p}$ *the following holds*

$$|P \bigcap \Gamma| \leqslant |P|^{1-\delta/4}\,. \tag{106}$$

Proof. Suppose for a moment that $P = \{1, 2, \dots, s\} \subseteq \Gamma$. If

$$\log|P| \ll \sqrt{\delta^{-1}\log(1/\delta)\log p}$$

then it is nothing to prove. On the other hand we can take $s \geqslant 1$ as small as we want. Thus suppose that $\log s \sim \sqrt{\delta^{-1}\log(1/\delta)\log p}$.

Because of we take $p \geqslant p_0(\delta)$ sufficiently large we can choose minimal $k \geqslant 2$ such that $k \geqslant \log p/\log s$. One can quickly check that $k \ll \log s$. Using Dirichlet's method (see [9]) it is easy to prove

$$\mathsf{T}_k^{\times}(P) \leqslant |P|^k \left(\frac{C\log|P|}{k}\right)^{k(k-1)}\,, \tag{107}$$

where $C > 0$ is an absolute constant. By Corollary 14 and formula (107), we have

$$\frac{s^{2k}}{|\Gamma|} \leqslant \mathsf{T}_k^{\times}(P) \leqslant s^k \left(\frac{C\log s}{k}\right)^{k^2}\,.$$

In other words

$$\log s \leqslant k\log(Ck^{-1}\log s) + k^{-1}\log|\Gamma|\,.$$

Hence

$$\delta\log s \ll k\log(Ck^{-1}\log s) \ll \frac{\log p}{\log s}\cdot\log(C\log^2 s\cdot\log^{-1} p)\,.$$

Put $x = \log^2 s\cdot\log^{-1} p$. Then the last inequality can be rewritten as $x \ll \delta^{-1}\log Cx$. In other words $x \ll \delta^{-1}\log(1/\delta)$ and we have formula (105) because of our method equally works for progressions of the form $\{a, 2a, \dots, sa\}$ as well.

Thanks to Lemma 8 we can obtain estimate (106) using similar arguments as above. Indeed, let $A = P \cap \Gamma$, and suppose that $|A| \geqslant s^{1-\delta/4}$. Here P as before, $|P| = s$. Thus $\mathsf{T}_k^{\times}(A) \geqslant |A|^{2k}/|\Gamma|$ and we obtain

$$\log |A| \leqslant \frac{1}{2}\log s + \frac{\log s}{2\log p}\log|\Gamma| + \frac{\log p}{2\log s}\log\left(\frac{C\log^2 s}{\log p}\right) + \frac{\log^2 s}{\log^2 p}\log|\Gamma|\,.$$

Hence by $|A| \geqslant s^{1-\delta/4}$ and $|\Gamma| = p^{1-\delta}$, we have

$$\frac{\delta}{4}\log s \leqslant \frac{\log p}{2\log s}\log\left(\frac{C\log^2 s}{\log p}\right) + \frac{\log^2 s}{\log^2 p}\log|\Gamma| \ll \frac{\log p}{\log s}\log\left(\frac{C'\log^2 s}{\log p}\right)\,,$$

where $C' > 0$ is another absolute constant. In other words $x \ll \delta^{-1}\log C'x$ as above. This completes the proof. □

Thus, the statement above is nontrivial if $|\Gamma| \ll p/(\log p)^{C_1}$, where $C_1 > 0$ is a sufficiently large constant. Using Theorem 9 one can obtain a similar result for arithmetic progressions of general form.

Further results on arithmetic progressions in subgroups can be found in [2].

8. Applications of the eigenvalues method to general sets

Now we find applications of Proposition 5 to some further families of sets. Let us begin with the convex subsets of $\mathbb{R}$.

THEOREM 10. *Let $A \subseteq \mathbb{R}$ be a convex set. Then*

$$\mathsf{E}(A) \ll |A|^{\frac{89}{36}}\log^{1/2}|A|\,. \qquad (108)$$

PROOF. Let $\mathsf{E} = \mathsf{E}(A)$, $\mathsf{E}_3 = \mathsf{E}_3(A)$. In view of Lemma 4, as in the proof of Theorem 8, we have

$$\sum_{\alpha\neq 0,\beta\neq 0,\alpha\neq\beta\,:\,\psi(\alpha),\psi_1(\beta),\psi_1(\alpha-\beta)\gg d} \psi^2(\alpha)\psi_1^2(\beta)\psi_1^2(\alpha-\beta) \gg \frac{\mathsf{E}^6}{|A|^6\mathsf{E}_3}\,. \qquad (109)$$

where $\psi(x) = (A \circ A)(x)$, $\psi_1(x) = (A * A)(x)$ and $d = 2^{-3}\mathsf{E}^2|A|^{-3}\mathsf{E}_3^{-1/2}$. The last inequality implies an analog of (81), i. e.

$$d^6 \cdot \sum_{i,j,k=1}^{l} 2^{2i+2j+2k} \sum_{\alpha} S_i(\alpha)(S_j * S_k)(\alpha) \gg \frac{\mathsf{E}^6}{|A|^6\mathsf{E}_3}\,. \qquad (110)$$

One can suppose that the summation in the last formula is taken over $i \leqslant j \leqslant k$. Applying Lemma 4, we have

$$\begin{aligned}\sum_{\alpha} S_i(\alpha)(S_j * S_k)(\alpha) &\leqslant d^{-1}2^{-i}\sum_{\alpha}(A \circ A)(\alpha)(S_j * S_k)(\alpha) \leqslant \\ &\leqslant d^{-1}2^{-i}\mathsf{E}^{1/2}(S_j, A)\mathsf{E}^{1/2}(S_k, A) \ll \\ &\ll |A|d^{-1}2^{-i}|S_j|^{3/4}|S_k|^{3/4}\,. \qquad (111)\end{aligned}$$

By formula (25) of Theorem 5 with $k = 2$, we obtain $|S_i| \ll |A|^3/(d^3 2^{3i})$. Combining the last bound with (111) and (110), we get

$$\frac{\mathsf{E}^6}{|A|^6\mathsf{E}_3} \ll d^5|A| \cdot \sum_{i,j,k=1}^{l} 2^{i-j/4-k/4}|A|^{9/2}d^{-9/2} \ll d^{1/2}|A|^{11/2}2^{l/2}\log^2|A|\,. \qquad (112)$$

Finally, by Andrews' inequality $2^l \ll |A|^{2/3}d^{-1}$. Using Lemma 4 once more after some calculations we obtain the result. This completes the proof. □

Corollary 16. *Let $A \subseteq \mathbb{Z}$ be a convex set and*

$$P_A(\theta) = \sum_{a\in A} e^{2\pi i a\theta}\,.$$

Then

$$\int_0^{2\pi} |P_A(\theta)|^4\,d\theta \ll |A|^{\frac{89}{36}}\log^{1/2}|A|\,.$$

Remark 8.1. It can be appear that the argument from the proof of Theorem 10, namely, an application of an upper bound $(A * A)(x) \ll |A|^{2/3}$, $x \neq 0$ is quite rough. Nevertheless it is optimal modulo our current knowledge of convex sets. Indeed, let $i = j = k = l$ in formula (110). By Theorem 5, we just know that

$|S_i|, |S_j|, |S_k| \ll |A|$. Further to estimate the sum $\sum\limits_{\alpha} S_i(\alpha)(S_j * S_k)(\alpha)$ the only one can apply is estimate (111). Substituting all bounds in (110), we obtain exactly (108).

Using Theorem 5 instead of Theorem 4 and apply the arguments from the proof of Theorem 8 one can obtain new upper bounds for $\mathsf{T}_k(A)$ in the case of convex A. We do not make such calculations. As in the situation of multiplicative subgroups using the weighted Szemerédi—Trotter theorem would provide better bounds, probably.

Now we formulate a general result concerning the additive energy of sets with small multiplicative doubling.

THEOREM 11. *Let $A \subseteq \mathbb{R}$ be a set, and $\varepsilon \in [0,1)$ be a real number. Suppose that $|AA| = M|A|$, $M \geqslant 1$, and*

$$|\{x \neq 0 \ : \ (A \circ A)(x) \geqslant |A|^{1-\varepsilon}\}| \ll (M \log M)^{5/3}|A|^{(1/6)-(\varepsilon/4)} \log^{5/6} |A| \,, \quad (113)$$

where the sign $\circ$ means either $*$ or $\circ$. Then

$$\mathsf{E}(A) \ll M \log M |A|^{(5/2)-(\varepsilon/12)} \log^{1/2} |A| \,. \quad (114)$$

PROOF. By Lemma 5, we have $\mathsf{E}_3(A) \ll M^2 \log^2 M \cdot |A|^3 \log |A|$. Thus $\mathsf{E}_3(A)$ is small for small M and we can apply the arguments from the proofs of Theorems 8, 10. Using the second bound from Lemma 5, and a consequence of the first estimate, namely, $|S_i| \ll (M \log M)^2 |A|^3/(d^3 2^{3i})$, we obtain the required bound (114). We just need to check two inequalities. The first is that all three terms which appeared in the cases $\alpha = 0$, $\beta = 0$, and $\alpha - \beta = 0$ (see the arguments from formula (79)), namely

$$(M \log M)^{2/3}|A|^{7/3} \log^{1/3} |A|$$

are less than our upper bound (114). One can easily assure that this is the case. The second inequality is that the sum over nonzero x such that $(A \circ A)(x) \geqslant |A|^{1-\varepsilon}$ is small. Denote by S_ε the set from (113). If

$$\frac{\mathsf{E}^3(A)}{|A|^3} \ll \sum_{\alpha \in S_\varepsilon} \sum_{\beta} (A \circ A)(\alpha)(A \circ A)(\beta)(A \circ A)(\alpha - \beta) \mathcal{C}_3(A)(\alpha, \beta) \leqslant$$

$$\leqslant |A| \sum_{\alpha} \sum_{\beta} \sum_{z} S_\varepsilon(\alpha)(A\circ A)(\beta)(A\circ A)(\alpha-\beta)A(z)A(z+\beta) \leqslant$$

$$\leqslant |A| \sum_{\beta} (S_\varepsilon * (A\circ A))(\beta)(A\circ A)^2(\beta) \leqslant |A| \mathsf{E}_3^{2/3}(A) \left(\sum_{\beta} (S_\varepsilon * (A\circ A))^3(\beta) \right)^{1/3} \leqslant$$

$$\leqslant |A| (M^2 \log^2 M \cdot |A|^3 \log |A|)^{2/3} |S_\varepsilon| |A|^{4/3}$$

then (114) holds. This completes the proof. □

The result with $|A|^{5/2}$ instead of $|A|^{(5/2)-(\varepsilon/12)}$ was known before (see [21]).

Clearly, Theorem 11 implies Theorem 10, because for $\varepsilon = 1/3$ the set from (113) is empty by Andrews result. Note also that upper bound (113) is quite rough and just shows the main idea.

Apply Theorem 11 for a new family of sets A with small quantity $|A(A+1)|$. Such sets were considered in [10], where the following lemma was proved.

Lemma 9. *Let $A, B \subseteq \mathbb{R}$ be two sets, and $\tau \leqslant |A|, |B|$ be a parameter. Then*

$$|\{s \in AB \ : \ |A \cap sB^{-1}| \geqslant \tau\}| \ll \frac{|A(A+1)|^2 |B|^2}{|A| \tau^3} \,. \qquad (115)$$

Lemma above implies that for any $A \subseteq \mathbb{R}$ the following holds $\mathsf{E}^{\times}(A) \ll \ll |A(A+1)||A|^{3/2}$. We obtain better upper bound for $\mathsf{E}^{\times}(A)$ (see inequality (117) of Corollary 17 below). Also in [10] a series of interesting inequalities were obtained. Here we formulate just one result.

Theorem 12. *Let $A \subseteq \mathbb{R}$ be a set. Then*

$$\mathsf{E}^{\times}(A, A(A+1)) \,, \ \mathsf{E}^{\times}(A+1, A(A+1)) \ll |A(A+1)|^{5/2} \,.$$

We prove the following

Corollary 17. *Let $A \subseteq \mathbb{R}$ be a set, $a \in \mathbb{R}$ be a number, $|A(A+1)| = M|A|$, $M \geqslant 1$, and inequality (113) holds in multiplicative form. Then*

$$\mathsf{E}^{\times}(A, A+a) \ll M|A|^{(5/2)-(\varepsilon/12)} \log^{1/2} |A|. \qquad (116)$$

In particular

$$\mathsf{E}^{\times}(A) \ll M|A|^{(5/2)-(\varepsilon/12)} \log^{1/2} |A| \qquad (117)$$

Proof. Put $A' = A + a$ and $\psi(x) = |\{a_1, a_2 \in A \ : \ x = a_1 a_2^{-1}\}|$. Then as in (78), we have

$$\left(\frac{\mathsf{E}^{\times}(A', A)}{|A|}\right)^3 \leqslant \sum_{\alpha,\beta} \psi(\alpha)\psi(\beta)\psi(\alpha\beta^{-1})\mathcal{C}_3(A')(\alpha, \beta) \, .$$

Lemma 9 implies that $\mathsf{E}_3^{\times}(A') \ll M^2|A|^3 \log |A|$. After that apply the arguments from the proof of Theorem 11. □

Previous results of the section say, basically, that if $\mathsf{E}_3(A)$ is small and A has some additional properties such as condition (113) from Theorem 11 (which shows that A is "unstructured" in some sense) then we can say something nontrivial about the additive energy of A. Now we formulate (see Theorem 16) a variant of the principle using just smallness of $\mathsf{E}_3(A)$ to show that A has a structured subset. The first result of the type was proved in [21] (see Theorem 23).

Theorem 13. *Let A be a subset of an abelian group. Suppose that $|A - A| = K|A|$ and $\mathsf{E}_3(A) = M|A|^4/K^2$. Then there exists $A' \subseteq A$ such that $|A'| \gg |A|/M^{5/2}$ and*

$$|nA' - mA'| \ll M^{12(n+m)+5/2} K|A'|$$

for every $n, m \in \mathbb{N}$.

One can see that Theorem 13 has a strong condition, namely, the cardinality of the set $A - A$ is small. Theorem 14 below was proved in [21] (see Theorem 53, section 9) and do not assume any restrictions on doubling constants but require a stronger condition for the higher moment, namely, $\mathsf{E}_{3+\varepsilon}(A) = M|A|^{4+\varepsilon}/K^{2+\varepsilon}$, $\varepsilon \in (0, 1]$.

Theorem 14. *Let $A \subseteq \mathbf{G}$ be a set. Suppose that $\mathsf{E}(A) = |A|^3/K$ and $\mathsf{E}_{3+\varepsilon}(A) = M|A|^{4+\varepsilon}/K^{2+\varepsilon}$, where $\varepsilon \in (0, 1]$. Then there exists $A' \subseteq A$ such that $|A'| \gg M^{-\frac{3+6\varepsilon}{\varepsilon(1+\varepsilon)}}|A|$ and*

$$|nA' - mA'| \ll M^{6(n+m)\frac{3+4\varepsilon}{\varepsilon(1+\varepsilon)}} K|A'|$$

for every $n, m \in \mathbb{N}$.

Note that if $\varepsilon \to 0$ then the bounds in Theorem 14 becomes very bad. Finally we formulate Theorem 51 from [21], where the condition on the higher moment is relaxed but the obtained bound on the doubling constant is not so good.

THEOREM 15. *Let A be a subset of an abelian group. Suppose that $\mathsf{E}(A) = |A|^3/K$ and $\mathsf{E}_{2+\varepsilon}(A) = M|A|^{3+\varepsilon}/K^{1+\varepsilon}$. Then there exists $A' \subseteq A$ such that $|A'| \gg \gg |A|/(2M)^{1/\varepsilon}$ and*

$$|A' - A'| \ll 2^{\frac{6}{\varepsilon}} M^{\frac{6}{\varepsilon}} K^4 |A'| \,.$$

Let us formulate our result.

THEOREM 16. *Let $A \subseteq \mathbf{G}$ be a set, $\mathsf{E}(A) = |A|^3/K$, and $\mathsf{E}_3(A) = M|A|^4/K^2$. Suppose that $M \leqslant |A|/(6K)$. Then there is a real number r*

$$1 \leqslant r \leqslant \frac{1}{|A|} \max_{x \neq 0} (A \circ A)(x) \cdot KM^{1/2} \leqslant KM^{1/2} \,, \qquad (118)$$

and a set $A' \subseteq A$ such that

$$|A'| \gg M^{-23/2} r^{-2} \log^{-9} |A| \cdot |A| \,, \qquad (119)$$

and

$$|nA' - mA'| \ll (M^9 \log^6 |A|)^{7(n+m)} r^{-1} M^{1/2} K |A'| \qquad (120)$$

for every $n, m \in \mathbb{N}$.

PROOF. Let $\mathsf{E} = \mathsf{E}(A)$, $\mathsf{E}_3 = \mathsf{E}_3(A)$, $\psi = A \circ A$. Then as in (78), we have

$$\left(\frac{\mathsf{E}(A)}{|A|}\right)^3 \leqslant \sum_{\alpha,\beta} \psi(\alpha)\psi(\beta)\psi(\alpha-\beta)\mathcal{C}_3(A)(\alpha,\beta) \,.$$

Using the assumption $M \leqslant |A|/(6K)$, we get

$$2^{-1}\left(\frac{\mathsf{E}(A)}{|A|}\right)^3 \leqslant \sum_{\alpha\neq 0,\beta\neq 0,\alpha\neq\beta} \psi(\alpha)\psi(\beta)\psi(\alpha-\beta)\mathcal{C}_3(A)(\alpha,\beta) \,.$$

As before

$$\sum_{\alpha\neq 0,\beta\neq 0,\alpha\neq\beta \,:\, \psi(\alpha),\psi(\beta),\psi(\alpha-\beta)\gg d} \psi^2(\alpha)\psi^2(\beta)\psi^2(\alpha-\beta) \gg \frac{\mathsf{E}^6}{|A|^6 \mathsf{E}_3} \,, \qquad (121)$$

where $d = 2^{-3}\mathsf{E}^2|A|^{-3}\mathsf{E}_3^{-1/2}$. In terms of the sets S_i, we obtain a variant of formula (110), namely

$$d^4 \cdot \sum_{j,k=1}^{l} 2^{2j+2k} \sum_{\alpha} (A \circ A)^2(\alpha)(S_j * S_k)(\alpha) \gg \frac{\mathsf{E}^6}{|A|^6 \mathsf{E}_3} \,. \tag{122}$$

Trivially

$$|S_i|(d2^{i-1})^3 \leqslant \mathsf{E}_3 \,,$$

and whence

$$|S_i| \ll \mathsf{E}_3/(d^3 2^{3i}) \,. \tag{123}$$

Note also that $d2^i \leqslant \max\limits_{x \neq 0}(A \circ A)(x)$, $i \in [l]$ and hence

$$2^i \leqslant \frac{1}{|A|} \max_{x \neq 0}(A \circ A)(x) \cdot KM^{1/2} \leqslant KM^{1/2} \,.$$

Because of

$$\sum_{\alpha} (A \circ A)^2(\alpha)(S_j * S_k)(\alpha) \leqslant \mathsf{E}_3^{2/3} \left(\sum_{\alpha} (S_j * S_k)^3(\alpha) \right)^{1/3} \leqslant$$
$$\leqslant \mathsf{E}_3^{2/3} (|S_j||S_k|)^{1/6} \mathsf{E}^{1/3}(S_j, S_k) \tag{124}$$

then using (123), we can assume that the summation in (122) is taken over j, k such that

$$\mathsf{E}(S_j, S_k) \gg \frac{|S_j|^{3/2}|S_k|^{3/2}}{M^9 \log^6 |A|} := \mu |S_j|^{3/2}|S_k|^{3/2} \,. \tag{125}$$

Applying (123), (124) and a trivial upper bound for the additive energy, namely, $\mathsf{E}(S_j, S_k) \leqslant |S_j|^{3/2}|S_k|^{3/2}$, we obtain

$$d^4 \cdot \sum_{j,k=1}^{l} 2^{2j+2k} \sum_{\alpha} (A \circ A)^2(\alpha)(S_j * S_k)(\alpha) \ll d^4 \mathsf{E}_3^{2/3} \cdot \sum_{j,k=1}^{l} 2^{2j+2k} |S_j|^{2/3}|S_k|^{2/3} \ll$$

$$\ll d^2 \mathsf{E}_3^{4/3} \log^2 |A| \cdot \max_j 2^{2j} |S_j|^{2/3} \,.$$

Thus the summation in (122) is taken over $j \in [l]$ such that

$$2^j|S_j| \gg 2^{-2j}M^{-2}K\log^{-3}|A|\cdot|A|\,. \qquad (126)$$

By Balog—Szemerédi—Gowers Theorem 3 and estimate (125) there are $S' \subseteq S_j$, $S'' \subseteq S_k$ such that $|S'| \gg \mu|S_j|$, $|S''| \gg \mu|S_k|$ and $|S'+S''| \ll \mu^{-7}|S'|^{1/2}|S''|^{1/2}$. Suppose for definiteness that $|S''| \geqslant |S'|$. Then

$$|S'+S''| \ll \mu^{-7}|S''|\,.$$

Plünnecke—Ruzsa inequality (see e. g. [26]) yields

$$|nS'-mS'| \ll \mu^{-7(n+m)}|S'|\,, \qquad (127)$$

for every $n, m \in \mathbb{N}$. Using the definition of the set S_j and inequality (126), we find $x \in \mathbf{G}$ such that

$$|(A-x)\cap S'| \geqslant 2^{j-1}d|A|^{-1}|S'| \gg K^{-1}M^{-1/2}\mu 2^j|S_j| \gg M^{-23/2}2^{-2j}\log^{-9}|A|\cdot|A|\,. \qquad (128)$$

Put $A' = A\cap(S'+x)$. Using (127), (128) and the definition of d, we obtain for all $n, m \in \mathbb{N}$

$$|nA'-mA'| \leqslant |nS'-mS'| \ll \mu^{-7(n+m)}2^{-j}|A|d^{-1}|A'| \ll \mu^{-7(n+m)}2^{-j}KM^{1/2}|A'|$$

and the result follows with $r = 2^j$. □

Thus, for small r our result is better than Theorem 14 and Theorem 15 because we assume that just $\mathsf{E}_3(A)$ is small and we obtain better bound for the doubling constant of A', correspondingly. If r is large than lower bound (119) for cardinality of A' is not so good but upper bound (120) for the doubling constant becomes better than in Theorems 14, 15 as well as in Theorem 13.

Note, finally, that condition (118) can be certainly relaxed in spirit of assumption (113) from Theorem 11.

In the end of the section we give one more variant of the arguments, using eigenvalues method.

THEOREM 17. *Let* $A \subseteq \mathbf{G}$ *be a set,* $D \subseteq A - A$, $D = -D$, $\eta \in (0, 1]$ *be a real number,*

$$\sum_{x \in D} (A \circ A)(x) = \eta |A|^2 \,, \tag{129}$$

and $\mathsf{E}_3(A) = \eta^3 M |A|^6 / |D|^2$. *Then there is a set* $A' \subseteq A$ *such that*

$$|A'| \gg \frac{\eta^{16} |A|}{M^5} \,, \tag{130}$$

and

$$|nA' - mA'| \ll \left(\frac{\eta^{15}}{M^5} \right)^{-7(n+m)} \frac{|D|}{\eta |A|} \cdot |A'| \tag{131}$$

for every $n, m \in \mathbb{N}$.

PROOF. Let $\mathsf{E} = \mathsf{E}(A)$, $\psi = A \circ A$, σ be the sum from (129), and

$$D_* = \{ x \in D \ : \ (A \circ A)(x) \geqslant 2^{-1} \eta |A|^2 / |D| \} \,.$$

Clearly, $D_* = -D_*$. Put

$$\sigma_* = \sum_{x \in D_*} (A \circ A)(x) \geqslant 2^{-1} \sigma = 2^{-1} \eta |A|^2 \,. \tag{132}$$

Denote by $\{f_j\}_{j \in [|A|]}$ the orthonormal eigenfunctions of the symmetric operator $\overline{\mathrm{T}}_A^{N^{-1} \widehat{D_*}}$. Of course $f_0 \geqslant 0$. As in Proposition 5 and as in formula (78), we get

$$\sum_{\alpha, \beta} D_*(\alpha) D_*(\beta) (A \circ A)(\alpha - \beta) \mathcal{C}_3(A)(\alpha, \beta) =$$

$$= \sum_{x,y,z \in A} D_*(x - y) \overline{D_*(x - z)} (A \circ A)(y - z) =$$

$$= \sum_j |\mu_j(\overline{\mathrm{T}}_A^{N^{-1} \widehat{D_*}})|^2 \cdot \langle \overline{\mathrm{T}}_A^{N^{-1} \widehat{\psi}} f_j, f_j \rangle \,. \tag{133}$$

Because of $\widehat{\psi} \geqslant 0$, we obtain

$$\omega_j := \langle \overline{\mathrm{T}}_A^{N^{-1} \widehat{\psi}} f_j, f_j \rangle = \sum_x \psi(x) (f_j \circ \overline{f_j})(x) \geqslant 0, \qquad j \in [|A|] \,.$$

Trivially

$$\mu_0 := \mu_0(\overline{\mathrm{T}}_A^{N^{-1}\widehat{D_*}}) \geqslant |A|^{-1}\sigma_* \,. \tag{134}$$

Let us estimate ω_0. We have

$$\mu_0 f_0(x) = A(x)(D_* * f_0)(x) \,.$$

By Cauchy—Schwarz, we get

$$\mu_0^2 \left(\sum_x f_0(x)\right)^2 \leqslant |D_*| \sum_x (f_0 \circ A)^2(x) = |D_*|\omega_0 \,.$$

Using estimate (69) of Lemma 7 and the formula above, we obtain

$$\omega_0 \geqslant \frac{\mu_0^3}{|D_*|} \,. \tag{135}$$

Applying (134), (135), we get

$$\sum_{\alpha,\beta} D_*(\alpha)D_*(\beta)(A \circ A)(\alpha-\beta)\mathcal{C}_3(A)(\alpha,\beta) \gg \frac{\mu_0^5}{|D_*|} \gg \frac{\sigma_*^5}{|A|^5|D_*|} \,.$$

Using the upper bound for $\mathrm{E}_3(A)$ and estimate (132), we have

$$\sum_x (D_* \circ D_*)(x)(A \circ A)^2(x) \gg \frac{\eta^3\sigma_*^4}{M|A|^4} \,.$$

Applying the arguments from (124), we get

$$\mathrm{E}(D_*) \gg \frac{\eta^{15}|D|^3}{M^5} = \nu|D_*|^3 \,.$$

By Balog—Szemerédi—Gowers Theorem 3 there is $D' \subseteq D_*$, $|D'| \gg \nu|D_*|$ such that $|D'+D'| \ll \nu^{-7}|D'|$. Plünnecke—Ruzsa inequality (see e. g. [26]) yields

$$|nD' - mD'| \ll \nu^{-7(n+m)}|D'| \,, \tag{136}$$

for every $n, m \in \mathbb{N}$. Using the definition of the set D_* and the number ν, we find $x \in \mathbf{G}$ such that

$$|(A - x) \cap D'| \geqslant 2^{-1}\eta|A||D'|/|D| \geqslant 2^{-1}\eta|A|\nu|D_*|/|D| \gg \frac{\eta^{16}|A|}{M^5}\,. \qquad (137)$$

Put $A' = A \cap (D' + x)$. Using (136), (137), we obtain for all $n, m \in \mathbb{N}$

$$|nA' - mA'| \leqslant |nD' - mD'| \ll \nu^{-7(n+m)}|D'| \ll \nu^{-7(n+m)}\eta^{-1}|D||A|^{-1}|A'|$$

and the result follows. □

Taking $D = A - A$ in Theorem 17, we obtain Theorem 13 (with a little bit different constants). Thus the result above is a generalization of Theorem 13.

Acknowledgements

This work was supported by grant RFFI NN 11-01-00759, Russian Government project 11.G34.31.0053, Federal Program "Scientific and scientific–pedagogical staff of innovative Russia" 2009–2013, mol_a_ved grant 12-01-33080 and grant Leading Scientific Schools N 2519.2012.1.

Bibliography

1. ***G. E. Andrews,*** *A lower bound for the volume of strictly convex bodies with many boundary lattice points*, Trans. Amer. Math. Soc. **106** (1963), 270–279.
2. ***J. Bourgain, M. Z. Garaev, S. V. Konyagin, I. E. Shparlinski,*** *On the hidden shifted power problem*, arXiv:1110.0812v1 [cs.CC] 4 Oct 2011.
3. ***J. Cilleruelo, M. Garaev,*** *Concentration of points on two and three dimensional modular hyperbolas and applications*, Geom. and Func. Anal. **21** (2011), 892–904.
4. ***J. Cilleruelo, I. E. Shparlinski, A. Zumalacárregui,*** *Isomorphism classes of elliptic curves over a finite field in some thin families*, Math. Res. Letters **19** (2012), 335–343.
5. ***W. T. Gowers,*** *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. func. anal. **8** (1998), 529–551.
6. ***W. T. Gowers,*** *A new proof of Szemerédi's theorem*, Geom. func. anal. **11** (2001), 465–588.

7. **D. R. Heath-Brown, S. V. Konyagin,** *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Quart. J. Math. **51** (2000), 221–235.

8. **A. Iosevich, S. V. Konyagin, M. Rudnev, V. Ten,** *On combinatorial complexity of convex sequences*, Discrete Comput. Geom. **35** (2006), 143–158.

9. **H. Iwaniec, E. Kowalski,** *Analytic Number Theory*, AMS, Colloquium publ., v. 53.

10. **T. G. F. Jones, O. Roche-Newton,** *Improved bounds on the set $A(A+1)$*, arXiv:1205.3937v1 [math.CO].

11. **N. H. Katz, P. Koester,** *On additive doubling and energy*, SIAM J. Discrete Math. **24** (2010), 1684–1693.

12. **S. V. Konyagin,** *Estimates for trigonometric sums and for Gaussian sums*, IV International conference "Modern problems of number theory and its applications". Part 3 (2002), 86–114.

13. **S. Konyagin, I. Shparlinski,** *Character sums with exponential functions*, Cambridge University Press, Cambridge, 1999.

14. **L. Li,** *On a theorem of Schoen and Shkredov on sumsets of convex sets*, arXiv:1108.4382v1 [math.CO].

15. **L. Li, O. Roche-Newton,** *Convexity and a sum–product type estimate*, arXiv:1111.5159v1 [math.CO].

16. **W. Rudin,** *Fourier analysis on groups*, Wiley 1990 (reprint of the 1962 original).

17. **M. Rudnev, S. V. Konyagin,** *On new sum–product type estimates*, arXiv:1111.4977 [math.CO].

18. **T. Schoen,** *Near optimal bounds in Freiman's theorem*, Duke Math. Journal, to appear.

19. **T. Schoen, I. D. Shkredov,** *Additive properties of multiplicative subgroups of $\mathbb{F}_p$*, to appear in Quart. J. Math.

20. **T. Schoen, I. D. Shkredov,** *On sumsets of convex sets*, Comb. Probab. Comput. **20** (2011), 793–798.

21. **T. Schoen, I. D. Shkredov,** *Higher moments of convolutions*, J. of Number Theory, **133** (2013), 1693–1737.

22. **I. D. Shkredov,** *Some applications of W. Rudin's inequality to problems of combinatorial number theory*, Uniform Distribution Theory, **6**:2 (2011), 95–116.

23. **I. D. Shkredov,** *Fourier analysis in combinatorial number theory*, Uspekhi Mat. Nauk, v.5 **393**:3 (2010), 88–144; English transl. Russian Math. Surveys **65**:3 (2010), 513–567.

24. **I. D. Shkredov, I. V. V'ugin,** *On additive shifts of multiplicative subgroups*, Mat. Sbornik **203**:6 (2012), 81–100.

25. ***S. A. Stepanov,*** *On the number of points on hyperelliptic curve over prime finite field*, Izvestiya of Russian Academy of Sciences **33** (1969), 1171–1181.

26. ***T. Tao, V. Vu,*** *Additive combinatorics*, Cambridge University Press 2006.

I. D. Shkredov

Division of Algebra and Number Theory,
Steklov Mathematical Institute,
ul. Gubkina, 8, Moscow, Russia, 119991
and
Delone Laboratory of Discrete and Computational Geometry,
Yaroslavl State University,
Sovetskaya str. 14, Yaroslavl, Russia, 150000
and
IITP RAS,
Bolshoy Karetny per. 19, Moscow, Russia, 127994
ilya.shkredov@gmail.com