Some new inequalities in additive combinatorics *

Shkredov I.D.

Annotation.

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.

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 $G = (G, +)$ be a group and $A$ be an arbitrary subset of $G$. 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 [16]. 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 $E(A) := \sum_x |A_x|^2$. We rewrite the sum as the action of a matrix

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

*This work was supported by grant RFFI NN 06-01-00383, 11-01-00759, Russian Government project 11.G34.31.0053, Federal Program "Scientific and scientific–pedagogical staff of innovative Russia" 2009–2013 and grant Leading Scientific Schools N 2519.2012.1.
where $\chi_A$ is the characteristic function of $A$, by $\chi_A \circ \chi_A$ we denote the convolution of $\chi_A$ (see the definition in the section 2) and the square matrix $T$ is $T_{x,y} := (\chi_A \circ \chi_A)(x - y)$, $x, y \in A$. Studying the eigenvalues and the eigenfunctions of $T$, we obtain the information about the initial object $E(A)$. 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

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

and

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

These formulas combining with another ingredient, so-called Katz–Koester inequality (see [11])

$$(A + A) \cap (A + A - x) \geq |A + (A \cap (A - x))| \quad (3)$$

allow us to prove a series of applications (see sections 6, 7). 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

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

Recall that a set $A \subseteq \mathbb{R}$ is called convex if it is the image of a convex map. In paper [3] a result similar to Theorem 1 for convex sets was proved.

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

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

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 49 of section 7). 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 $|\Gamma \pm \Gamma| \geq |\Gamma|^{3/2 + \varepsilon_0}$ and $|A \pm A| \geq |A|^{3/2 + \varepsilon_0}$ for any subgroup and a convex set, correspondingly. Nevertheless another
methods from papers [14, 19, 20, 24] and also Corollary 29 of section [6] give better bounds for the doubling constant here. Further applications of inequalities (1), (2) can be found in sections 6, 7.

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. On the other hand the tools from the next section 5 will be applied to obtain new bounds for the additive energy. The main principle here is the following. Basically, an upper bound for $E_3(A)$ 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 $E(A)$. The rigorous statements are contained in sections 6 and 7. 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 $G$ be an abelian group. If $G$ is finite then denote by $N$ the cardinality of $G$. It is well-known [16] that the dual group $\hat{G}$ is isomorphic to $G$ in the case. Let $f$ be a function from $G$ to $\mathbb{C}$. We denote the Fourier transform of $f$ by $\hat{f}$,

$$\hat{f}(\xi) = \sum_{x \in G} f(x)e(-\xi \cdot x),$$

(4)

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

$$\sum_{x \in G} |f(x)|^2 = \frac{1}{N} \sum_{\xi \in \hat{G}} |\hat{f}(\xi)|^2.$$  

(5)

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

(6)

and

$$f(x) = \frac{1}{N} \sum_{\xi \in \hat{G}} \hat{f}(\xi)e(\xi \cdot x).$$  

(7)

If

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

then

$$\widehat{f * g} = \hat{f} \hat{g} \quad \text{and} \quad \widehat{f \circ g} = \hat{f} \hat{g} = \hat{f} \hat{g},$$

(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

\[
(f \circ_k f)(x) := \sum_{y_1, \ldots, y_k} f(y_1) \cdots f(y_k) f(x + y_1 + \cdots + y_k).
\]

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 \(\mathcal{E}(A,B)\) for additive energy of two sets \(A, B \subseteq \mathbf{G}\) (see e.g. [26]), that is

\[
\mathcal{E}(A, B) = |\{a_1 + b_1 = a_2 + b_2 : a_1, a_2 \in A, b_1, b_2 \in B\}|.
\]

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

\[
\mathcal{E}(A,B) = \sum_x (A*B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x)(B \circ B)(x).
\]

and by \(\mathbf{[6]}\),

\[
\mathcal{E}(A,B) = \frac{1}{N} \sum_\xi |\widehat{A}(\xi)|^2 |\widehat{B}(\xi)|^2.
\]

Let \(\mathcal{T}_k(A) := |\{a_1 + \cdots + a_k = a'_1 + \cdots + a'_k : a_1, \ldots, a_k, a'_1, \ldots, a'_k \in A\}|\).

Let also \(\sigma_k(A) := (A *_k A)(0) = |\{a_1 + \cdots + a_k = 0 : a_1, \ldots, a_k \in A\}|\).

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

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

\[
\mathcal{E}_k(A) = \sum_{x \in \mathbf{G}} (A \circ A)(x)^k = \sum_{s_1, \ldots, s_{k-1} \in \mathbf{G}} |A_s|^2
\]

and

\[
\mathcal{E}_k(A,B) = \sum_{x \in \mathbf{G}} (A \circ A)(x)(B \circ B)(x)^{k-1} = \sum_{s_1, \ldots, s_{k-1} \in \mathbf{G}} |B_s^A|^2
\]

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

Clearly,

\[
\mathcal{E}_{k+1}(A,B) = \sum_x (A \circ A)(x)(B \circ B)(x)^k = \sum_{x_1, \ldots, x_{k-1}} \left( \sum_y A(y)B(y + x_1) \cdots B(y + x_k) \right)^2 = \mathcal{E}(\Delta_k(A), B^k),
\]

where

\[
\Delta(A) = \Delta_k(A) := \{(a, a, \ldots, a) \in A^k\}.
\]

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

Quantities \(\mathcal{E}_k(A,B)\) can be written in terms of generalized convolutions.
Definition 3 Let $k \geq 2$ be a positive number, and $f_0, \ldots, f_{k-1} : \mathbb{G} \to \mathbb{C}$ be functions. Write $F$ for the vector $(f_0, \ldots, f_{k-1})$ and $x$ for vector $(x_1, \ldots, x_{k-1})$. Denote by

\[ C_k(f_0, \ldots, f_{k-1})(x_1, \ldots, x_{k-1}) \]

the function

\[ C_k(F)(x) = C_k(f_0, \ldots, f_{k-1})(x_1, \ldots, x_{k-1}) = \sum_z f_0(z)f_1(z + x_1) \cdots f_{k-1}(z + x_{k-1}). \]

Thus, \( C_2(f_1, f_2)(x) = (f_1 \circ f_2)(x) \). If \( f_1 = \cdots = f_k = f \) then write \( C_k(f)(x_1, \ldots, x_{k-1}) \) for \( C_k(f_1, \ldots, f_k)(x_1, \ldots, x_{k-1}) \).

In particular, \( (\Delta_k(B) \circ A^k)(x_1, \ldots, x_k) = C_{k+1}(B, A, \ldots, A)(x_1, \ldots, x_k) \), \( k \geq 1 \).

For a positive integer \( n \), we set \( [n] = \{1, \ldots, n\} \). 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 \( l, k \geq 2 \) be positive integers and \( F = (f_{ij}) \), \( i = 0, \ldots, l-1; j = 0, \ldots, k-1 \) be a functional matrix, \( f_{ij} : \mathbb{G} \to \mathbb{C} \). Let \( R_0, \ldots, R_{l-1} \) and \( C_0, \ldots, C_{k-1} \) be rows and columns of the matrix, correspondingly. The following commutative relation holds.

Lemma 4 For any positive integers \( l, k \geq 2 \), we have

\[ C_l(C_k(R_0), \ldots, C_k(R_{l-1})) = C_k(C_l(R_0), \ldots, C_l(R_{k-1})). \tag{14} \]

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

\[ C_l(C_k(R_0), \ldots, C_k(R_{l-1}))(y^{(i)}, \ldots, y^{(l-1)}) = \]

\[ = \sum_{x_1, \ldots, x_{k-1}} C_k(R_0)(x_1, \ldots, x_{k-1})C_k(R_1)(x_1 + y_{11}, \ldots, x_{k-1} + y_{1(k-1)}) \]

\[ \cdots C_k(R_{l-1})(x_1 + y_{(l-1)1}, \ldots, x_{k-1} + y_{(l-1)(k-1)}) = \sum_{x_0, \ldots, x_{k-1}} \prod_{i=0}^{l-1} \prod_{j=0}^{k-1} f_{ij}(x_j + y_{ij} + z_i). \]

Changing the summation, we obtain

\[ C_k(C_l(R_0), \ldots, C_l(R_{l-1}))(y^{(i)}, \ldots, y^{(l-1)}) = \]

\[ = \sum_{z_1, \ldots, z_{l-1}} C_l(C_0)(z_1, \ldots, z_{l-1})C_l(C_1)(z_1 + y_{11}, \ldots, z_{l-1} + y_{(l-1)1}) \]

\[ \cdots C_l(C_{l-1})(z_1 + y_{1(l-1)}, \ldots, z_{l-1} + y_{(l-1)(k-1)}) = C_k(C_l(C_0), \ldots, C_l(C_{k-1}))(y_1, \ldots, y_{k-1}). \]

as required. \( \square \)
Corollary 5  For any functions the following holds
\[
\sum_{x_1,\ldots,x_{l-1}} C_l(f_0,\ldots,f_{l-1})(x_1,\ldots,x_{l-1}) C_l(g_0,\ldots,g_{l-1})(x_1,\ldots,x_{l-1}) = \\
= \sum_{z} (f_0 \circ g_0)(z) \ldots (f_{l-1} \circ g_{l-1})(z) \quad \text{(scalar product),} \tag{15}
\]
moreover
\[
\sum_{x_1,\ldots,x_{l-1}} C_l(f_0)(x_1,\ldots,x_{l-1}) \ldots C_l(f_{k-1})(x_1,\ldots,x_{l-1}) = \\
= \sum_{y_1,\ldots,y_{k-1}} C_k^l(f_0,\ldots,f_{k-1})(y_1,\ldots,y_{k-1}) \quad \text{(multi–scalar product),} \tag{16}
\]
and
\[
\sum_{x_1,\ldots,x_{l-1}} C_l(f_0)(x_1,\ldots,x_{l-1}) (C_l(f_1) \circ \cdots \circ C_l(f_{k-1}))(x_1,\ldots,x_{l-1}) = \\
= \sum_{z} (f_0 \circ \cdots \circ f_{k-1})(z) \quad (\sigma_k \; \text{for} \; C_l) \tag{17}
\]

Proof. Take \(k = 2\) in (13). Thus \(F\) is a \(l \times 2\) matrix in the case. We have
\[
C_l(f_0 \circ g_0,\ldots,f_{l-1} \circ g_{l-1})(x_1,\ldots,x_{l-1}) = (C_l(f_0,\ldots,f_{l-1}) \circ C_l(g_0,\ldots,g_{l-1}))(x_1,\ldots,x_{l-1}).
\]
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 \(F_{ij} = f_j, i = 0,\ldots,l-1; j = 0,\ldots,k-1\) and putting all variables in (13) equal zero, we obtain (16). This completes the proof. \(\square\)

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

Theorem 6  Let \(A, B \subseteq G\) be two sets, \(K \geq 1\) and \(E(A,B) \geq |A|^{3/2} |B|^{3/2} / K\). 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 \(G = \mathbb{F}_p\), where \(p\) is a prime number. In the situation the following lemma which is a consequence of Stepanov’s approach [25] can be formulated (see, e.g. [24]).

Lemma 7  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 \(\Gamma\)-invariant sets such that \(|Q||Q_1||Q_2| \ll |\Gamma|^5\) and \(|Q||Q_1||Q_2||\Gamma| \ll p^3\). 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 7, one can easily deduce upper bounds for moments of convolution of $\Gamma$ (see, e.g. [19]).

**Corollary 8** Let $p$ be a prime number and $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| \ll p^{2/3}$. Then
\[
E(\Gamma) \ll |\Gamma|^{5/2}, \quad E_3(\Gamma) \ll |\Gamma|^3 \log |\Gamma|,
\]
and for all $l \geq 4$ the following holds
\[
E_l(\Gamma) = |\Gamma|^l + O(|\Gamma|^{2^{l+3}}).
\] (20)

Certainly, the condition $|\Gamma| \ll p^{2/3}$ in formula (20) can be relaxed. The same method gives a generalization (see [12]).

**Theorem 9** Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| < \sqrt{p}$. Let also $d \geq 2$ be a positive integer. Then arranging $(\Gamma *_{d-1} \Gamma)(\xi_1) \geq (\Gamma *_{d-1} \Gamma)(\xi_2) \geq \ldots$, where $\xi_j \neq 0$ belong to distinct cosets, we have
\[
(\Gamma *_{d-1} \Gamma)(\xi_j) \ll_d |\Gamma|^{d-2+3^{-1}(1+2^{2-d})j^{-1/3}}.
\]

In particular
\[
T_d(\Gamma) \ll_d |\Gamma|^{2d-2+2^{-1-d}},
\] (21)

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

and similar
\[
\sum_z (\Gamma \circ \Gamma)(z)((\Gamma *_{d-1} \Gamma) \circ (\Gamma *_{d-1} \Gamma))^2(z) \ll_d |\Gamma|^{4d-2+3^{-1}(1+2^{3-2d})} \cdot \log |\Gamma|.
\] (23)

We need in a lemma about Fourier coefficients of an arbitrary $\Gamma$–invariant set (see e.g. [19]).

**Lemma 10** Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, and $Q$ be an $\Gamma$–invariant subset of $\mathbb{F}_p^*$, that is $Q\Gamma = Q$. Then for any $\xi \neq 0$ the following holds
\[
|\hat{Q}(\xi)| \leq \min \left\{ \left( \frac{|Q|}{|\Gamma|} \right)^{1/2}, \frac{|Q|^{3/4} p^{1/4} E^{1/4}(\Gamma)}{|\Gamma|}, p^{1/8} E^{1/8}(\Gamma) E^{1/8}(Q) \left( \frac{|Q|}{|\Gamma|} \right)^{1/2} \right\}.
\] (24)

Recall that a set $A = \{a_1, \ldots, a_n\} \subseteq \mathbb{R}$ is called convex if $a_i - a_{i-1} < a_{i+1} - a_i$ for every $2 \leq i \leq n - 1$. Convex sets have statistics similar to multiplicative subgroups, in some sense. We need in a lemma, see e.g. [20] or [14].
Lemma 11 Let $A$ be a convex set, and $B$ be an arbitrary set. Then

$$E_3(A) \ll |A|^3 \log |A|,$$

and

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

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

$$(A *_{k-1} A)(x) \ll_k |A|^\frac{k(k-1)}{2k-1}.$$

The following result was proved in [8].

Theorem 12 Let $A$ be a convex set, and $k \geq 2$ be an integer. Then arranging $(A *_{k-1} A)(x_1) \geq (A *_{k-1} A)(x_2) \geq \ldots$, we have

$$(A *_{k-1} A)(x_j) \ll_k |A|^\frac{k-\frac{j}{2}(1-2^{-k})}{j-1}.$$

In particular

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

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 13 Let $A, B \subseteq \mathbb{R}$ be finite sets and let $|A A| = M|A|$. Then arranging $(A \circ B)(x_1) \geq (A \circ B)(x_2) \geq \ldots$, we have

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

In particular

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

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, 18, 19, 20, 21, 24]. We collect all required tools in the section.

First of all let us recall Lemma 2.4 and Corollary 2.5 from [24]. We gather the results in the following proposition.
Proposition 14 Let $k \geq 2$, $m \in [k]$ be positive integers, and let $A_1, \ldots, A_k, B$ be finite subsets of an abelian group. Then

$$A_1 \times \ldots \times A_k - \Delta_k(B) = \{ (x_1, \ldots, x_k) : B \cap (A_1 - x_1) \cap \cdots \cap (A_k - x_k) \neq \emptyset \} \quad (27)$$

and

$$A_1 \times \ldots \times A_k - \Delta_k(B) = \bigcup_{(x_1, \ldots, x_m) \in A_1 \times \ldots \times A_m - \Delta(B)} \{(x_1, \ldots, x_m) \times (A_{m+1} \times \ldots \times A_k - \Delta_{k-m}(B \cap (A_1 - x_1) \cap \cdots \cap (A_m - x_m))) \}. \quad (28)$$

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

$$\sum_{s \in A^l - \Delta_l(B)} (A^k - \Delta_k(A^B_x))(x) = |A^l - \Delta_l(A^B_x)|. \quad (29)$$

In particular

$$(A - A_s)(x) = (A - A_x)(s) \quad \text{and} \quad \sum_s (A - A_s)(x) = |A - A_x|. \quad (30)$$

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

Lemma 15 Let $A, B \subseteq G$ be sets, and $k, l$ be positive integers. Then

$$\sum_{s \in G^l} E(A^k, \Delta(A^B_x)) = E_{k+l+1}(B, A). \quad (31)$$

Now we obtain the main proposition of the section.

Proposition 16 Let $A, B \subseteq G$ be two sets, $k, l$ be positive integers, and $q : G^k \to \mathbb{C}$ be an arbitrary function. Then

$$|A|^2 \left| \sum_{x \in G^k} q(x)(A^k \circ \Delta_k(B))(x) \right|^2 \leq E_{k+l+1}(B, A) \cdot \sum_{x \in G^k} |A^l \pm \Delta_l(A^B_x)||q(x)|^2. \quad (32)$$

Proof. We have

$$\sum_s \sum_x (A^k \circ \Delta(A^B_x))(x)q(x) = \sum_x q(x) \sum_s (A^k \circ \Delta(A^B_x))(x) = |A|^l \sum_x q(x)(A^k \circ \Delta(B))(x). \quad (33)$$

Applying Cauchy–Schwartz twice, Lemma 15 and formula 29, we get

$$|A|^2 \left| \sum_{x} q(x)(A^k \circ \Delta(B))(x) \right|^2 \leq$$
Corollary 17 Let $A, B \subseteq G$ be two sets, and $k, l$ be positive integers. Then

$$|A|^{2l}E_{k+l+1}(B, A) \leq E_{k+l+1}(B, A) \cdot \sum_x |A^l \pm \Delta(A_x^B)|\cdot|(A^k \circ \Delta_k(B))^2(x)| \quad (32)$$

and

$$|A|^{2l} \sum_x \frac{(A^k \circ \Delta_k(B))^2(x)}{|A^l \pm \Delta_l(A_x^B)|} \leq E_{k+l+1}(B, A). \quad (33)$$

Proof. Taking \( q(x) = (A^k \circ \Delta(B))(x) \) and applying Corollary 5 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 (33). \( \square \)

Until the end of the section suppose, for simplicity, that $B = A$. Corollary 5 implies that $\sum_x (A^k \circ \Delta(A))^2(x) = E_{k+1}(A)$. Combining the identity with formula (33), we obtain
Corollary 18

\[
\sum_{x : |A^l \pm \Delta l(A_x)| \geq |A|^{2E_{k+1}(A)} / \Delta_{k+l+1}(A)} (A^k \circ \Delta_k(A))^2(x) \geq 2^{-1} E_{k+1}(A). \tag{34}
\]

For example \((k = l = 1)\)

\[
\sum_{x : |A \pm A_x| \geq 2^{-1}|A|^2 E(A)E^{-1}(A)} |A_x|^2 \geq 2^{-1} E(A). \tag{35}
\]

Suppose that \(E_{k+l+1}(A) \ll |A|^{k+l+1}\). Using a trivial bound \(|A^l \pm \Delta(A_x)| \leq |A|^l |A_x|\), we see that the lower bound for \(|A_x|\), deriving from (34), namely, \(|A_x| \geq 2^{-1} |A|^{k+1} E_{k+1}(A) E^{-1}_{k+l+1}(A)\) is potentially sharper then usual estimate \(|A_x| \geq 2^{-1} E_{k+1}(A) |A|^{-(k+1)}\), which follows from the identity \(\sum_x |A_x|^2 = E_{k+1}(A)\).

The same arguments give

Corollary 19

\[
\sum_{x : |A^l \pm \Delta l(A_x)| \geq (A^k \circ \Delta_k(A))(x) / |A|^{2E_{k+1}(A)} / \Delta_{k+l+1}(A)} (A^k \circ \Delta_k(A))(x) \geq 2^{-1} |A|^{k+1}. \tag{35}
\]

In the case \(k = l = 1\), we obtain

\[
\sum_{x : |A \pm A_x| \geq |A_x| / |A|^4 E_3(A)} |A_x| \geq 2^{-1} |A|^2. \tag{35}
\]

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

Corollary 20 Let \(\alpha, p\) be real numbers, \(p > 1\). Then

\[
\sum_x |A_x|^\alpha \leq \left( E_3(A) / |A|^2 \right)^{1/p} \cdot \left( \sum_x |A \pm A_x|^{-1/p} |A_x|^{\alpha p - 2} / p \right)^{(p-1)/p}. \tag{36}
\]

5 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 21 Let \(G\) be an abelian group, and \(\varphi, \psi\) be two complex functions. By \(T_\psi^\varphi\) denote the following operator on the space of functions \(G^C\)

\[
(T_\psi^\varphi f)(x) = \psi(x)(\hat{\varphi} * f)(x), \tag{37}
\]

where \(f\) is an arbitrary complex function on \(G\).
Suppose that $G$ is a finite abelian group, and $A \subseteq G$ is a set. Denote by $T^\varphi_A$ the restriction of operator $T^\varphi_A$ onto the space of the functions with supports on $A$. Recall some simple properties of operators $T^\varphi_A$ which were obtained in [22]. First of all, it was proved, in particular, that operators $T^\varphi_A$ and $T^\varphi_A$ have the same non-zero eigenvalues. Second of all, if $\varphi$ is a real function then the operator $T^\varphi_A$ is symmetric (hermitian) and if $\varphi$ is a nonnegative function then the operator is nonnegative definite. The action of $T^\varphi_A$ can be written as
\[ \langle T^\varphi_A u, v \rangle = \sum_x (\varphi \ast u)(x)\overline{v(x)} = \sum_x \varphi(x)(u \circ \overline{v})(x) = \sum_x \varphi(x)u(x)\overline{v(x)}, \] (38)
where $u, v$ are arbitrary functions such that $\text{supp } u, \text{supp } v \subseteq A$. Further
\[ \text{tr}(T^\varphi_A) = |A|\varphi(0) = \sum_{j=1}^{|A|} \mu_j(T^\varphi_A) = \sum_{j=1}^{|G|} \mu_j(T^\varphi_A). \] (39)
If $\varphi$ is a real function then as was noted before $T^\varphi_A$ is a symmetric matrix. In particular, it is a normal matrix and we get
\[ \text{tr}(T^\varphi_A(T^\varphi_A)^*) = \sum_z |\hat{\varphi}(z)|^2(A \circ A)(z) = \sum_z (\varphi \circ \varphi)(z)|\hat{A}(z)|^2 = \sum_{j=1}^{|A|} \mu_j^2(T^\varphi_A) = \sum_{j=1}^{|G|} \mu_j^2(T^\varphi_A). \] (40)
We will deal with just nonnegative definite symmetric operators. In the case we arrange the eigenvalues in order of magnitude
\[ \mu_0(T^\varphi_A) \geq \mu_1(T^\varphi_A) \geq \cdots \geq \mu_{|A|-1}(T^\varphi_A). \]
Further properties of such operators can be found in [22]. The connection of such operators with higher energies $E_k(A)$ 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 $\mu_j$ as well as all eigenfunctions.

Let $p$ be a prime number, $q = p^s$ for some integer $s \geq 1$. 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 $\Gamma$, and put $n = (q-1)/t$. Let also $g$ be a primitive root, then $\Gamma = \{g^{nt}\}_{t=0,1,\ldots,t-1}$. Let $\chi_\alpha(x)$, $\alpha \in [t]$ be the orthonormal family of multiplicative characters on $\Gamma$, that is
\[ \chi_\alpha(x) = |\Gamma|^{-1/2} \cdot \Gamma(x)e\left(\frac{\alpha l}{t}\right), \quad x = g^{nt}, \quad 0 \leq l < t. \] (41)
Clearly, products of such functions form a basis on Cartesian products of $\Gamma$.

The following proposition was obtained, basically, in [21] (except formula (42)). We recall the proof for the sake of completeness.

**Proposition 22** Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup. If $\psi$ is an arbitrary $\Gamma$–invariant function then the functions $\chi_\alpha(x)$ are eigenfunctions of the operator $T^\psi_{\Gamma}$. Suppose, in addition, that $\psi(x) \geq 0$. Then for any functions $u : \mathbb{F}_q \to \mathbb{C}$ and $v : \mathbb{F}_q \to \mathbb{R}^+$ the following holds
\[ \sum_{x,y \in \Gamma} \psi(x-y)C_3(v, u)(x, y) \geq |\Gamma|^{-2} \sum_x \psi(x)(\Gamma \circ \Gamma)(x) \cdot \sum_{x,y \in \Gamma} C_3(v, u)(x, y). \] (42)
In particular, for any function $u$ with support on $\Gamma$, we have

$$\sum_x \psi(x)(u \circ \pi)(x) \geq |\Gamma|^{-2} \sum_x \psi(x)(\Gamma \circ \Gamma)(x) \cdot \left| \sum_{x \in \Gamma} u(x) \right|^2.$$  \hfill (43)

**Proof.** We have to show that

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

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

$$\psi \ast f)(\gamma x) = \sum_z f(z) \psi(\gamma x - z) = \sum_z f(\gamma z) \psi(\gamma x - \gamma z)$$

$$= f(\gamma) \cdot \sum_z f(z) \psi(x - z) = f(\gamma) \cdot (\psi \ast f)(x)$$  \hfill (45)

as required.

Formula (43) follows from (42) if one take $v = \delta_0$. We give another independent proof. Because of $\hat{\psi}(x) \geq 0$ the operator $T^\psi_\Gamma$ is symmetric and nonnegative definite. Thus all its eigenvalues are nonnegative. Put $\varphi = q^{-1}\psi$. If $u = \sum_\alpha c_\alpha \chi_\alpha$ then

$$\langle T^\varphi_\Gamma u, u \rangle = \sum_x \psi(x)(u \circ \pi)(x) = \sum_\alpha |c_\alpha|^2 \mu_\alpha(T^\varphi_\Gamma) \geq |\Gamma|^{-2} \langle u, \Gamma \rangle^2 \sum_x \psi(x)(\Gamma \circ \Gamma)(x)$$

and we obtain (43).

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 $c_{-\alpha, \alpha}(F) \geq 0$ for $F(x, y) = \mathcal{C}_3(v, \pi, u)(x, y)$. By assumption $v \geq 0$. Hence by Corollary 5

$$c_{-\alpha, \alpha}(F) = \sum_{x, y} F(x, y) \overline{\chi_\alpha(x)} \chi_\alpha(y) = \sum_z v(z) |(\chi_\alpha \circ u)(z)|^2(z) \geq 0$$  \hfill (46)

and the result follows. \qed

In particular, for any $k \geq 1$

$$E_{k+1}(\Gamma) = \max_{f : \text{supp } f \leq \Gamma, \|f\|_2 = |\Gamma|} \sum_x (\Gamma \circ \Gamma)^k(x)(f \circ f)(x).$$  \hfill (47)
Remark 23 It is not difficult to replace a multiplicative subgroup $\Gamma$ in the previous proposition onto arbitrary coset (see [21]). Indeed, for every $\xi \in \mathbb{F}_q^*/\Gamma$ and $\alpha \in \{1, \ldots, |\Gamma|\}$, let us define the functions $\chi_\alpha^\xi(x) := \chi_\alpha(\xi^{-1}x)$. Then, clearly, $\text{supp } \chi_\alpha^\xi = \text{supp } \chi_\alpha$ and $\chi_\alpha^\xi(\gamma x) = \chi_\alpha(\gamma)\chi_\alpha^\xi(x)$ for all $\gamma \in \Gamma$. Using the argument from Proposition 22 it is easy to see that the functions $\chi_\alpha^\xi$ are orthonormal eigenfunctions of the operator $T_{\xi \Gamma}^\alpha$. Thus, we can replace $\Gamma$ onto $\xi \Gamma$.

Proposition 22 has an interesting corollary about Fourier coefficients of functions with supports on $\Gamma$. In particular, it gives exact formula for exponential sums over multiplicative subgroups.

Corollary 24 Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup. Suppose that $u$ is a function with support on $\Gamma$. Then for any $\lambda \in \mathbb{F}_q$ the following holds

$$|\hat{u}(\lambda)|^2 = |\Gamma|^2 \cdot \min_h \frac{\sum_x |\hat{h}(x)|^2 \hat{u}(x + \lambda)^2}{\sum_x |\hat{h}(x)|^2 |\hat{\Gamma}(x)|^2},$$

(48)

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

$$\sum_{x,y \in \Gamma} C_3(v, u, \overline{\gamma})(x, y) = |\Gamma|^2 \cdot \min_h E^{-1}(h, \Gamma) \cdot \sum_{x,y \in \Gamma} (h \circ \overline{\gamma})(x - y)C_3(v, u, \overline{\gamma})(x, y),$$

(49)

where the minimum is taken over all nonzero $\Gamma$–invariant functions.

Proof. Taking $\psi = h \circ \overline{\gamma}$ in formula (43) of Proposition 22 and using Fourier transform, we obtain that

$$|\sum_{z \in \Gamma} u(z)|^2 \leq |\Gamma|^2 \cdot \min_h \frac{\sum_x |\hat{h}(x)|^2 |\hat{u}(x)|^2}{\sum_x |\hat{h}(x)|^2 |\hat{\Gamma}(x)|^2}$$

(50)

for any function $u$ with support on $\Gamma$. Considering $h \equiv 1$ we make sure that formula (50) is actually equality. Now taking $u(x)e(-\lambda x)$ instead of $u(x)$, we have formula (48). Equality (49) is a consequence of (50) and can be obtained by similar arguments. This completes the proof. $\square$

Let $g : \mathbb{F}_q \to \mathbb{C}$ be a $\Gamma$–invariant function. It is convenient to write $\mu_\alpha(g)$ for $\mu_\alpha(T_{\Gamma}^{-1}\overline{g})$. It is easy to see that $\overline{g} = \mu_\alpha(g) = \mu_{\alpha}(\overline{g}) = \mu_{-\alpha}(\overline{g})$. Multiplicative properties of the functions $\chi_\alpha$ allow us to prove formula (51) below, which shows that the numbers $\mu_\alpha(\overline{g}h)$ and $\mu_\alpha(g), \mu_\alpha(h)$ are connected.

Proposition 25 Let $g, h : \mathbb{F}_q \to \mathbb{C}$ be two $\Gamma$–invariant functions. Then

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

(51)

and

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

(52)
Proof. We have

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

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

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

where \(\varpi(x, y, w)\) equals 1 if \(w, w + y \in \Gamma\) 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 \(\Gamma\)-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 (51).

One can derive (52) from (51). Another way is to use formula (44) of Proposition 22. We propose one more variant. Consider \(\mu_\alpha(g) = f(\alpha)\) as a function on \(\alpha\) and compute the Fourier transform of \(f\). Now write \(e(x)\) for \(e^{2\pi i x/|\Gamma|}\). We have for \(\alpha \neq 0\)

\[
\hat{f}(\alpha) = \sum_{\beta} \sum_{x} g(x) \sum_{z} \chi_\beta(z - x) \overline{\chi}_\beta(z)e(-\alpha \beta) = \sum_{x} g(x) \Gamma(1 - g^{n\alpha})^{-1} =
\]

\[
= \sum_{x} g(x(1 - g^{n\alpha})) \Gamma(x) = |\Gamma|g(1 - g^{n\alpha}).
\]

Besides the last formula holds in the case \(\alpha = 0\) because we have general identity (39). Finally, using the inverse formula (11), we obtain

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

This completes the proof. □

In particular, taking \(\alpha = 0\), \(l = 2\) and \(g = h\) in formula (51), we obtain formula (40) for operators \(\overline{T}_\Gamma^2\), where \(\varphi(x) = q^{-1}g\) and \(\Gamma\) is a multiplicative subgroup.

**Corollary 26** Let \(g : \mathbb{F}_q \to \mathbb{R}\) be a \(\Gamma\)-invariant function. Put \(\mu(\alpha) = \mu_\alpha(g)\). Then for all positive integers \(l\), we have

\[
\mu_\alpha(g^l) = (\mu *_{l-1} \mu)(\alpha),
\]

and

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

where \(*\) the normalized convolution over \(|\Gamma|\). In particular, numbers \(E(\Gamma, \chi_\alpha), \alpha \in [|\Gamma|]\) determine \(E_l(\Gamma)\) for all \(l \geq 2\).
Now consider for a moment the case of prime \( q = p \).

**Remark 27** Suppose that \( g(x) = (\Gamma \circ \Gamma)(x) \) and \( \mu_1(\alpha) = \mu_\alpha(g^l) \). By Corollary 8 and formulas (39), (40), we get for any \( |\Gamma| \ll p^{2/3} \) and \( l \geq 2 \) that

\[
\sum_\alpha (\mu_\alpha(\alpha) - |\Gamma|^l)^2 \ll |\Gamma|^{1+(2l+1)2/3} = |\Gamma|^{4l/3+5/3}.
\]

Thus, we have an asymptotic formula for all \( l \geq 2 \)

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

Using the arguments from the proof of Proposition 22 we obtain a general inequality.

**Proposition 28** Let \( A \subseteq G \) be a set, and \( \psi \) be a symmetric function such that \( \hat{\psi} \geq 0 \). Then

\[
\sum_{x,y,z \in A} \psi(x - y)\overline{\psi(x - z)}\psi(y - z) \geq \\
\max \left\{ \frac{1}{|A|^3} \left( \sum_x \psi(x)(A \circ A)(x) \right)^3, \frac{|\psi^3(0)| \cdot |A|}{|A|^{1/2}}, \frac{1}{|A|^{1/2}} \left( \sum_x |\psi^2(x)(A \circ A)(x)\right)^{3/2} \right\}.
\]

**Proof.** Put \( u(x) = \psi^c(x) = \psi(x), \ v(x) = A^c(x) \geq 0 \). Let \( \{f_\alpha\}_{\alpha \in A} \) be an orthonormal family of the eigenfunctions of the operator \( T_A^{N-1}\hat{\psi} \) and \( \{\mu_\alpha\}_{\alpha \in A} \) be the correspondent nonnegative eigenvalues. Then

\[
\sigma := \sum_{x,y \in A} \psi(x - y)C_3(v, \overline{u}, u)(x, y) = \sum_{\alpha \in A} \mu_\alpha d_\alpha,
\]

where by Corollary 5

\[
d_\alpha := \sum_{x,y} C_3(v, \overline{u}, u)(x, y)f_\alpha(x)f_\alpha(y) = \sum_z v(z)(f_\alpha \circ u)^2(z) = \sum_{z \in A} |(\psi * f_\alpha)^2(z)|.
\]

To get the last identities we have used the arguments from the proof of formula (46) and the fact that \( \psi = \psi^c \). Further, because of \( f_\alpha \) is the eigenfunctions of the operator \( T_A^{N-1}\hat{\psi} \), we have

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

Thus in view of \( \|f_\alpha\|^2 = 1 \), we obtain \( d_\alpha = \mu_\alpha^2 \). Note also a trivial lower bound for the largest eigenvalue \( \mu_0 \), namely

\[
\mu_0 \geq |A|^{-1}\langle T_A^{N-1}\hat{\psi}, A \rangle = |A|^{-1} \sum_x \psi(x)(A \circ A)(x).
\]
Hence, applying the last inequality and the assumption \( \psi = \psi^c \) once more, we get
\[
\sigma = \sum_{x,y \in A} \psi(x - y)C_3(v, \overline{\psi}, \psi)(x, y) = \sum_{x,y,z \in A} \psi(x - y)\overline{\psi(x - z)}\psi(y - z) = \sum_{\alpha \in A} \mu_\alpha^3 \geq \mu_0^3 \geq \frac{1}{|A|^3} \left( \sum_x \psi(x)(A \circ A)(x) \right)^3
\]
and the first inequality in (55) is proved. To get the second and the third ones, we use the obtained formula \( \sigma = \sum_{\alpha \in A} \mu_\alpha^3 \), identities (39), (40), correspondingly, and Hölder inequality.

This completes the proof.

Another way to prove (55) is to write \( \Psi(x,y) = \psi(x - y)A(x)A(y) \) as
\[
\Psi(x,y) = \sum_{\alpha,\beta} c_{\alpha,\beta} f_\alpha(x)f_\beta(y)
\]
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 (55) gives the result. In principle, this method gives further generalization of inequality (55) onto larger number of variables in the case of multiplicative subgroups because its eigenfunctions \( \chi_\alpha \) have multiplicative properties (see the proof of Proposition 25).

In the general situation we have just the following generalization, where each variable appears twice
\[
\sum_{x_1,\ldots,x_k \in A} \psi(x_1 - x_2)\psi(x_2 - x_3)\psi(x_3 - x_4)\ldots\psi(x_{k-1} - x_k)\psi(x_k - x_1) = \sum_{\alpha \in A} \mu_\alpha^k (T_{N-1}^{A^k}\hat{\psi}) \geq \mu_0^k \geq \frac{1}{|A|^k} \left( \sum_x \psi(x)(A \circ A)(x) \right)^k,
\]  
where \( k \geq 1 \). Here \( \psi \) is a symmetric function and \( \hat{\psi} \geq 0 \) \( (k \geq 3). \) For \( k = 1, k = 2 \) these are general identities (59), (40). If one use the singular–value decomposition lemma for \( C_{k+1}(x,y) \), \( k \geq 3 \) (see section 8 of [21]) then some functions \( \psi \) in (57) can be replaced by its moments. In the case of multiplicative subgroups one can replace \( \psi \) in (57) by different symmetric \( \Gamma \)-invariant functions with nonnegative Fourier transform.

Finally, note also that the condition \( \hat{\psi} \geq 0 \) is vitally needed in the proposition above. Indeed if we consider a dense symmetric subset \( Q \subseteq G \) having no solutions of the equation \( \alpha + \beta = \gamma \), \( \alpha,\beta,\gamma \in Q \) and put \( A = G \), \( \psi = Q \) then inequality (55) does not hold. The phenomenon that such sets must have (large) negative and positive Fourier coefficients was considered in [23], see section 5.

Let \( \psi \) be a nonnegative function on an abelian group \( \Gamma \), and \( A \subseteq G \) be a set. Consider the operator \( T_{A}^{N-1}\hat{\psi} \) and its orthonormal eigenfunctions \( \{f_j\}_{j \in |A|}. \) The condition \( \psi \geq 0 \) implies that \( f_0 \geq 0 \), and \( \mu_0 \geq 0 \). The next lemma shows that the function \( f_0 \) is close to \( A(x)/|A|^{3/2} \) in some weak sense.
Lemma 29 Let \( A \subseteq G \) be a set, and \( \psi \) be a nonnegative function, \( \mu_0 \) be the first eigenvalue of the operator \( T_A^{N^{-1}} \). Then

\[
|A| \geq \left( \sum_x f_0(x) \right)^2 \geq \max \left\{ \frac{\mu_0}{\|\psi\|_\infty}, \frac{\mu_0^2}{\|\psi\|_2^2} \right\}, \tag{58}
\]

and for the first eigenfunction of \( T_A^{N^{-1}} \), \( \|f_0\|_2 = 1 \) the following holds

\[
\|f_0\|_\infty \leq \frac{\|\psi\|_2}{\mu_0}. \tag{59}
\]

If \( \hat{\psi} \geq 0 \) then

\[
\|f_0\|_\infty \leq \frac{\|\psi_1\|_2}{\mu_0^{1/2}}, \tag{60}
\]

where \( \psi = \psi_1 \circ \overline{\psi}_1 \).

Proof. Let \( \mu = \mu_0, f = f_0, g = \sum_x f(x) \). We have

\[
\mu f(x) = A(x)(\psi \ast f)(x). \tag{61}
\]

Thus

\[
\mu = \sum_x f(x)(\psi \ast f)(x) \tag{62}
\]

and

\[
\mu^2 = \sum_{x \in A} (\psi \ast f)^2(x). \tag{63}
\]

Formula (61) implies that

\[
\mu g = \sum_{x \in A} (\psi \ast f)(x). \] 

Applying Cauchy–Schwarz and (63) (or just Cauchy–Schwarz), we obtain \( g^2 \leq |A| \). Further, bound \( g^2 \geq \mu \|\psi\|_\infty^{-1} \) easily follows from (62). Using the formula once more, we get

\[
\mu \leq \sum_x f(x) \cdot \|\psi\|_2 \|f\|_2 = \|\psi\|_2 g
\]

and we obtain (58). Returning to (61) and applying the same argument, we have (59). It remains to prove (60). Because of \( \hat{\psi} \geq 0 \) there is \( \psi_1 \) such that \( \psi = \psi_1 \circ \overline{\psi}_1 \). Applying (61) and using Cauchy–Schwarz, we get for any \( x \in A \)

\[
\mu|f(x)| \leq \sum_y (f \ast \overline{\psi}_1)(x + y)\psi_1(y) \leq \|\psi_1\|_2 \cdot \left( \sum_y |(f \ast \overline{\psi}_1)(y)|^2 \right)^{1/2} = \|\psi_1\|_2 \cdot \mu^{1/2},
\]

where formula (62) and the fact \( \psi = \psi_1 \circ \overline{\psi}_1 \) have been used. This completes the proof.

We will use Lemma 29 in section 7.
6 Applications: multiplicative subgroups

We begin with an application of Corollary 17.

**Theorem 30** Let \( p \) be a prime number, and \( \Gamma \subseteq \mathbb{F}_p^* \) be a multiplicative subgroup, \( |\Gamma| = O(p^{2/3}) \) and

\[
E(\Gamma) \leq \sqrt{p}|\Gamma|^\frac{5}{2} \log |\Gamma|.
\]

Then

\[
E(\Gamma) \ll |\Gamma|^\frac{4}{3} |\Gamma \pm \Gamma|^\frac{5}{3} \log |\Gamma|.
\]

**Proof.** Let \( Q = \Gamma \pm \Gamma \). We can assume that

\[
|Q| = O\left(\frac{E^{3/2}(\Gamma)}{|\Gamma|^2 \log^{3/2} |\Gamma|}\right)
\]

because otherwise inequality (65) is trivial. Applying formula (32) of Corollary 17 with \( k = l = 1 \) and using inequality

\[
|\Gamma \pm \Gamma_x| \leq ((\Gamma \pm \Gamma) \circ ((\Gamma \pm \Gamma)))(x)
\]

(see [11] or just Proposition 14), we obtain

\[
|\Gamma|^2E^2(\Gamma) \leq E_3(\Gamma) \sum_x (Q \circ Q)(x)(\Gamma \circ \Gamma)^2(x).
\]

If we prove that

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

then substituting the last formula into (67) and using the bound \( E_3(\Gamma) = O(|\Gamma|^3 \log |\Gamma|) \) from Corollary 8 we get formula (65). The term with \( x = 0 \) is \( E_3(\Gamma)|Q||\Gamma|^2 \) and can be handled easily.

From (67) it follows that the summation is taken over nonzero \( x \) such that

\[
(Q \circ Q)(x) \geq \frac{E(\Gamma)|\Gamma|^2}{2E_3(\Gamma)} := H.
\]

Hence, it is sufficient to prove that

\[
\sum_{x \neq 0 : (Q \circ Q)(x) \geq H} (Q \circ Q)(x)(\Gamma \circ \Gamma)^2(x) \ll |Q|^{4/3} |\Gamma|^{5/3} \log |\Gamma|.
\]

Let \((Q \circ Q)(\xi_1) \geq (Q \circ Q)(\xi_2) \geq \ldots \) and \((\Gamma \circ \Gamma)(\eta_1) \geq (\Gamma \circ \Gamma)(\eta_2) \geq \ldots \), where nonzero \( \xi_1, \xi_2, \ldots \) and \( \eta_1, \eta_2, \ldots \) belong to distinct cosets. Applying Lemma 17 once more, we get

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

(70)
provided that \( j|\Gamma|Q^2 \ll |\Gamma|^5 \) and \( j|\Gamma||Q^2|\Gamma| \ll p^3 \). We have \( j \ll |Q|^{4/(|\Gamma|^2 H^3)} \). Using inequalities \( E(\Gamma) \ll |\Gamma|^{5/2}, E_3(\Gamma) \ll |\Gamma|^3 \log |\Gamma| \), formula (66) and assumption (64) it is easy to check that the last conditions are satisfied. Applying (70), we obtain (68). This completes the proof.

\[ \blacksquare \]

For example if \( |\Gamma| = O(p^{1/2}) \) then assumption (64) holds. Using trivial lower bound for \( E(\Gamma) \), that is \( E(\Gamma) \geq |\Gamma|^4/|\Gamma| + |\Gamma| \), we obtain

**Corollary 31** Let \( \Gamma \subseteq \mathbb{F}_p^* \) be a multiplicative subgroup, \( |\Gamma| \ll \sqrt{p} \). Then

\[ |\Gamma + \Gamma| \gg \frac{|\Gamma|^4 \log^{3/2} |\Gamma|}{|\Gamma|} \]

As for the difference set it is known (see [24]) at the moment that \( |\Gamma - \Gamma| \gg |\Gamma|^{5/2} \log^{-1/2} |\Gamma| \) for an arbitrary multiplicative subgroup \( \Gamma \) with \( |\Gamma| \ll \sqrt{p} \). We will see soon that the condition \( |\Gamma| \ll \sqrt{p} \) in Corollary 31 can be relaxed (see Theorem 34 below).

**Corollary 32** Let \( \Gamma \subseteq \mathbb{F}_p^* \) be a multiplicative subgroup, \(-1 \in \Gamma \) such that \( |\Gamma| \geq p^\kappa \), where \( \kappa > \frac{33}{68} \). Then for all sufficiently large \( p \) we have \( 6\Gamma = \mathbb{F}_p \). If \( \kappa > \frac{55}{112} \) then \( \mathbb{F}_p^* \subseteq 6\Gamma \) without condition \(-1 \in \Gamma \).

**Proof.** Put \( S = \Gamma + \Gamma, n = |\Gamma|, m = |S|, \) and \( \rho = \max_{\xi \neq 0} |\hat{\Gamma}(\xi)|. \) By a well-known upper bound for Fourier coefficients of multiplicative subgroups (see e.g. Corollary 2.5 from [19] or Lemma 10) we have \( \rho \leq p^{1/8}E^{1/4}(\Gamma). \) If \( \mathbb{F}_p^* \subseteq 6\Gamma \) then for some \( \lambda \neq 0, \) we obtain

\[ 0 = \sum_{\xi} \hat{S}^2(\xi)\hat{\Gamma}^2(\xi)\hat{\lambda}\hat{\Gamma}(\xi) = m^2n^3 + \sum_{\xi \neq 0} \hat{S}^2(\xi)\hat{\Gamma}^2(\xi)\hat{\lambda}\hat{\Gamma}(\xi). \]

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

\[ n^3m^2 \leq \rho^3mp \ll (p^{1/8}E^{1/4})^3mp. \tag{71} \]

Now applying formula (65) 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 (71), combining with formula (65) and apply the lower bound for \( \Gamma + \Gamma \) from Corollary 31. \( \blacksquare \)

**Remark 33** The inclusion \( \mathbb{F}_p^* \subseteq 6\Gamma \) was obtained in [24] under the assumption \( \kappa > \frac{99}{203} \). Even more stronger results than containing in Corollary 32 were obtained by A. Efremov using further development of our method (unpublished).

Now we obtain a result about the additive energy of multiplicative subgroups.
**Theorem 34** Let $p$ be a prime number and $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup. Then

$$E(\Gamma) \ll \max\{|\Gamma|^2 \log |\Gamma|, |\Gamma|^3 p^{-\frac{3}{4}} \log^4 |\Gamma|\}. \quad (72)$$

More precisely,

$$E(\Gamma) \ll |\Gamma|^\frac{3}{2} \log^\frac{5}{2} |\Gamma| \quad (73)$$

provided by $|\Gamma| \ll p^{\frac{3}{5}} \log^{-\frac{6}{5}} p$. Moreover, if $|\Gamma| < \sqrt{p}$, and $k \geq 2$ then we have

$$T_k(\Gamma) \ll_k |\Gamma|^{2k-\frac{17}{4} + \frac{13}{2} - 2k} \log^2 |\Gamma| . \quad (74)$$

**Proof.** Let $|\Gamma| = t$, $E_3(\Gamma) = E_3$, $E(\Gamma) = E = t^3/K$, $K \geq 1$, $T_t = T_t(\Gamma)$, $l \geq 2$. We need to find the lower bound for $K$ and the upper bound for $T_k$. Put

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

By Cauchy–Schwarz

$$\sigma_* \geq \frac{E^2}{t} = \frac{t^5}{K^2}$$

(actually in the case of multiplicative subgroups equality holds). Applying formula (42) of Proposition 22 with $\psi(x) = u(x) = (\Gamma \circ \Gamma)(x)$, $v(x) = \Gamma(x)$ and the coset $-\Gamma$, we obtain

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

In other words

$$\sum_{\alpha,\beta} \psi(\alpha)\psi(\beta)\psi(\alpha - \beta)C_3(\Gamma)(\alpha, \beta) \geq \frac{E}{t^2} \cdot \sigma_* . \quad (75)$$

Clearly,

$$\sum_{\alpha \neq 0, \beta \neq 0, \alpha \neq \beta} \psi(\alpha)\psi(\beta)\psi(\alpha - \beta)C_3(\Gamma)(\alpha, \beta) \geq 2^{-1} \frac{E}{t^2} \cdot \sigma_*$$

(76)

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

$$tE_3(\Gamma) \gg \frac{t^6}{K^5}$$

which implies $K \gg t^{2/3} \log^{-1/3} t$ and the result follows. Further the summation in (78) can be taken over nonzero $\alpha$ such that

$$\psi(\alpha) \geq 2^{-4} \frac{E}{t^2} := d$$

(77)

because of for other $\alpha$, we have

$$3d\sigma_* < 2^{-1} \frac{E}{t^2} \cdot \sigma_* .$$
with contradiction. In the last formula we have use the fact that $\Gamma$ is a subgroup. Thus suppose that formula
\[
\sum_{\alpha \neq 0, \beta \neq 0, \alpha \neq \beta} \psi(\alpha)\psi(\beta)\psi(\alpha - \beta)C_3(\Gamma) (\alpha, \beta) \geq 2^{-2} \frac{E}{t^2} \cdot \sigma_* \tag{78}
\]
takes place, where $d$ is defined by (77). By one more application of the Cauchy–Schwarz, we obtain
\[
\sum_{\alpha \neq 0, \beta \neq 0, \alpha \neq \beta} \psi^2(\alpha)\psi^2(\beta)\psi^2(\alpha - \beta) \gg \frac{E^2}{t^4} \cdot \sigma_*^2 E^{-1} \gg \frac{E^6}{t^6 E_3}. \tag{79}
\]
Put
\[S_i = \{ x \in \Gamma - \Gamma, x \neq 0 : 2^{i-1} d < \psi(x) \leq 2^i d \}, \quad i \in [l], \quad l \ll \log t.\]
Then
\[
d^6 \cdot \sum_{i,j,k=1}^l 2^{2i+2j+2k} \sum_{\alpha} S_i(\alpha)(S_j \ast S_k)(\alpha) \gg \frac{E^2}{t^4} \cdot \sigma_*^2 E^{-1}. \tag{80}
\]
To estimate the inner sum in (80) we use Lemma 7. Suppose that for all $i, j, k \in [l]$ the following two inequalities hold
\[
|S_i||S_j||S_k| \ll t^5 \tag{81}
\]
and
\[
|S_i||S_j||S_k|t \ll p^3. \tag{82}
\]
Then by Lemma 7
\[
d^6 t^{-1/3} \cdot \sum_{i,j,k=1}^l 2^{2i+2j+2k} (|S_i||S_j||S_k|)^{2/3} \gg \frac{E^2}{t^4} \cdot \sigma_*^2 E^{-1}. \tag{83}
\]
We can suppose that $K \ll t^{5/9} \log^{-2/3} t$ because otherwise the result is trivial. Note also a trivial upper bound for the size of any $S_i$, namely
\[
2^{i-1} d |S_i| \leq \sum_{x \neq 0} \psi(x) \leq t^2. \tag{83}
\]
or in other words
\[
|S_i| \ll 2^{-i} K t \ll K t. \tag{84}
\]
In particular
\[
t^3 |S_i| \ll t^4 K \ll t^4 t^{5/9} \log^{-2/3} t \ll p^3 \tag{84}
\]
because of $t \ll p^{27/41}$. In view of (81), a trivial inequality $|S_i|t^2 \ll t^5$, and Lemma 7 we obtain
\[
|S_i| \ll \frac{t^3}{23d^3}. \tag{85}
\]
A little bit worse bound

\[ |S_i| \ll \frac{t^3 \log t}{2^{n/3}} \]  

(86)

but for all \( t \ll p^{2/3} \) follows from the estimate of \( E_3 \), see Corollary 8. Substituting (85) into (80) gives us

\[ t^{6-1/3 \log^3 t} \gg \frac{E^2}{t^4} \cdot \sigma_3^2 E_3^{-1} \]

and after some calculations we obtain \( K \gg t^{5/9 \log^{-2/3} t} \). It is remain to check (81), (82).

Applying (83) and \( K \ll t^{5/9 \log^{-2/3} t} \), we have

\[ |S_i||S_j||S_k| \ll (Kt)^3 \cdot 2^{-(i+j+k)} \ll (Kt)^3 \ll t^{14/3 \log^{-2} t} \ll t^5 \]

(87)

and inequality (81) holds. Finally

\[ |S_i||S_j||S_k|t \ll t^{17/3 \log^{-2} t} \cdot 2^{-(i+j+k)} \ll t^{17/3 \log^{-2} t} \ll p^3 \]

(88)

provided by \( t \ll p^{\frac{9}{17}} \) and \( K \ll t^{5/9 \log^{-2/3} t} \).

Now let us prove the same for larger \( t \). Returning to (80), applying the first bound from estimate (24) of Lemma 10 and using Fourier transform, we obtain

\[ \sum_{\alpha} S_{i}(\alpha)(S_{j} \ast S_{k})(\alpha) \ll \max\{p^{-1}|S_i||S_j||S_k|, \sqrt{p/t(|S_i||S_j||S_k|)^{1/2}}\} \].

(89)

We have used the first formula of Lemma 10 it is the most effective in the choice of parameters. If the maximum from (89) is attained on the first term then by (80), and trivial inequality

\[ |S_j|d^22^{2j} \leq E, \]

(90)

we get

\[ E \ll \frac{t^3 \log^{4/3} t}{p^{1/3}}, \]

(91)

and if it is attained on the second term, we have by (90)

\[ 2^{i+j+k} \gg \frac{E^{3/2}t^{1/2}}{p^{1/2}E_3^{1/3} \log^{3} t}. \]

(92)

Simple computations show that having (91) we easily get (72) for \( t \ll p^{3/5 \log^{-6/5} t} \ll p^{21/47} \). Further by (90) we have an analog of (88)

\[ |S_i||S_j||S_k|t \ll \frac{E^3}{d^2}t^{2^{-2(i+j+k)}} \ll t^{17/3 \log^{-2} t} \ll p^3 \]

(93)

Thus substitution (92) into (93) gives \( t \ll p^{3/5 \log^{-6/5} t} \). This completes the proof of inequality (73). Bound (72) is obtained by accurate calculations using inequality (86) in the wide range \( t \ll p^{2/3} \) and estimate (91).
To get (74) take \( \psi(x) = ((\Gamma *_{k-1} \Gamma) \circ (\Gamma *_{k-1} \Gamma))(x) \) and use previous arguments. We have
\[
\sum_{\alpha, \beta} \psi(\alpha)\psi(\beta)\psi(\alpha - \beta)C_3(\Gamma)(\alpha, \beta) \geq t^{-3}T_{k+1}^3(\Gamma)
\]
and if \( \alpha, \beta \) or \( \alpha - \beta \) equals zero then by Theorem 9 we get
\[
t^{6k-4+3^{-1}(1+2^{3-2k})+2^1-k} \cdot \log t \gg_k T_k(\Gamma) \cdot \sum_x \psi^2(x)(\Gamma \circ \Gamma)(x) \gg t^{-3}T_{k+1}^3(\Gamma)
\]
and the result follows. As above
\[
\sum_{\alpha \neq 0, \beta \neq 0, \alpha \neq \beta} \psi^2(\alpha)\psi^2(\beta)\psi^2(\alpha - \beta) \gg t^{-6}T_{k+1}^6(\Gamma) : E_3^{-1},
\]
where
\[
d = \frac{T_{k+1}^3}{t^3T_{2k}E_3^{1/2}}.
\]
Consider the sets \( S_i \) similar way, we obtain by Theorem 9 that \( |S_i| \ll t^{6k-4+2^{3-2k}} / 2^{3i}d^3 \) and hence
\[
t^{12k-8+2^{3-2k}-1/3} \log^3 t \gg t^{-6}T_{k+1}^6(\Gamma) : E_3^{-1}, \tag{94}
\]
provided by inequalities (81), (82) hold. Inequality (84) implies that
\[
T_{k+1} \ll t^{2k+1/9+2^{3-2k}/3} \log^{2/3} t
\]
and we are done. Using Theorem 9 it is easy to check that (81) takes place. Hence, because of \( t < \sqrt{p} \) inequality (82) holds automatically. This completes the proof. \( \square \)

Thus, inequality (74) is better then Theorem 9 for \( k = 2 \) and for \( k = 3 \), namely, \( T_3(\Gamma) \ll t^{151/36} \log^{2/3} t \). Using more accurate arguments from [12] one can, certainly, improve our bounds for large \( k \). We do not make such calculations.

Note, finally, that inequality (73) gives bounds for \( E(\Gamma) \) which are better than Theorem 9 if \( |\Gamma| \ll p^{\frac{8}{3}} \log^{-\frac{8}{3}} p \).

Now we formulate Corollary 39 from [21], which was obtained by eigenvalues method of section 5 also.

**Corollary 35** Let \( p \) be a prime number, \( \Gamma_* \subseteq \mathbb{F}_q^* \) be a coset of a multiplicative subgroup \( \Gamma \). If \( Q(y) \subseteq \mathbb{F}_q^k, y \in \Gamma' \) is an arbitrary family of sets, then
\[
\left| \bigcup_{y \in \Gamma'} (Q(y) \pm \Delta(y)) \right| \geq \frac{|\Gamma|}{|\Gamma'|E_{k+1}(\Gamma_* , Q)} \cdot \left( \sum_{y \in \Gamma'} |Q(y)| \right)^2.
\]
In particular for every set \( A \subseteq \Gamma_* \), and every \( \Gamma \)-invariant set \( Q \), we have
\[
|Q + A| \geq |A| \cdot \frac{|\Gamma| |Q|^2}{E_2(\Gamma_* , Q)} \tag{95}
\]
Corollary above combining with Theorem 34 say that multiplicative subgroups have strong expanding property.

**Corollary 36** Let $p$ be a prime number, $\Gamma_* \subseteq \mathbb{F}_q^*$ be a coset of a multiplicative subgroup $\Gamma$, $|\Gamma| \ll p^{11/26}$. Then for any $A \subseteq \Gamma_*$, we have

$$|A + \Gamma| \gg \frac{|A||\Gamma|^{5/9}}{\log^{2/3} |\Gamma|}.$$ 

Ordinary application of Cauchy—Schwarz gives $|A + \Gamma| \gg |A|^{1/2}|\Gamma|^{7/9} \log^{-1/3} |\Gamma|$ for any set $A$ and any multiplicative subgroup $\Gamma$, $|\Gamma| \ll \sqrt{p}$.

Theorem 34 gives a direct application to the exponential sums over subgroups.

**Corollary 37** Let $p$ be a prime number, $\Gamma$ be a multiplicative subgroup, $|\Gamma| \ll p^{11/26}$. Then

$$\max_{\xi \neq 0} |\widehat{\Gamma}(\xi)| \ll \min\{p^{1/8}|\Gamma|^{11/18}, p^{1/4}|\Gamma|^{13/36}\} \cdot \log^{1/6} |\Gamma|.$$ 

(96)

**Proof.** Let $\rho = \max_{\xi \neq 0} |\widehat{\Gamma}(\xi)|$. Because of $\rho \leq p^{1/8}\mathcal{E}^{1/4}(\Gamma)$ and $\rho \leq p^{1/4}|\Gamma|^{-1/4}\mathcal{E}^{1/4}(\Gamma)$ (see e.g. Corollary 2.5 from [19] or Lemma [10]), applying Theorem 34, we obtain (96). This completes the proof.

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

$$T_k^\times(f) = \sum_{x_1, \ldots, x_k \neq x'_1, \ldots, x'_k : x_1 \cdots x_k = x'_1 \cdots x'_k} f(x_1) \cdots f(x_k) \overline{f(x'_1)} \cdots \overline{f(x'_k)}.$$ 

$T_k^\times(f)$ is a multiplicative analog of $T_k(f)$ from section 2. Write also $E^\times$ for $T_2^\times$.

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

**Lemma 38** Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup. Suppose that $f(x) = \sum_{\alpha} c_{\alpha} \chi_{\alpha}(x)$ is an arbitrary function with support on $\Gamma$. Then

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

**Proof.** By the multiplicative property of the functions $\chi_{\alpha}(x)$, we have

$$\sum_{\alpha} |c_{\alpha}|^{2k} = \sum_{\alpha} |\sum_x f(x) \chi_{\alpha}(x)|^{2k} = \sum_{\alpha} \sum_{x_1, \ldots, x_k, x'_1, \ldots, x'_k} f(x_1) \cdots f(x_k) \overline{f(x'_1)} \cdots \overline{f(x'_k)} \chi_{\alpha}(x_1) \cdots \chi_{\alpha}(x_k) \overline{\chi_{\alpha}(x'_1)} \cdots \overline{\chi_{\alpha}(x'_k)} = \frac{T_k^\times(P)}{|\Gamma|^{k-1}}$$ 
as required. 

\[\square\]
Corollary 39 Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup, and $A \subseteq \Gamma$. Then $T_k^\times(A) \geq \frac{|A|^{2k}}{|\Gamma|}$.

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

Proposition 40 Let $\Gamma \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup, and $A$ be any subset of $\Gamma$. Then for an arbitrary integer $k \geq 2$, we have

$$|A|^2 \leq |\Gamma|^2 (T_k^\times(A))^{1/k} \cdot \min_h \left(\frac{\|h\|_1}{\|h\|_2} \right)^{2/k} \frac{\sum_x |h(x)|^2}{\sum_x (h \circ h)(x)(\Gamma \circ \Gamma)(x)},$$

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

$$|A| \leq |\Gamma|^{1/4} (E^\times(A))^{1/4}$$

and

$$E_l(A, \Gamma) \leq |\Gamma|^{-l/2} E_{2l-1}(\Gamma)(E^\times(A))^{1/2}$$

for any $l \geq 2$.

Proof. Take $g(x) = (h \circ \overline{h})(x)$. Then $\hat{g} \geq 0$. Now proceed as in the proof of formula (43) from Proposition [22]. Let $A = \sum_\alpha c_\alpha \chi_\alpha$ and $\mu_\alpha = \mu_\alpha(T_{k-1}^\times \hat{g})$. By Hölder, we have

$$\sum_x g(x)(A \circ A)(x) = \sum_\alpha |c_\alpha|^2 \mu_\alpha \leq \left(\sum_\alpha |c_\alpha|^{2k}\right)^{1/k} \left(\sum_\alpha \mu_\alpha^{k-1}\right)^{1-1/k}. \tag{100}$$

Applying Lemma [38] we get

$$\sum_\alpha |c_\alpha|^{2k} = \frac{T_k^\times(A)}{|\Gamma|^{k-1}}. \tag{101}$$

On the other hand

$$\left(\sum_\alpha \mu_\alpha^{k-1}\right)^{1-1/k} \leq \mu_0^{1/k} \cdot \left(\sum_\alpha \mu_\alpha\right)^{1-1/k} \leq \|h\|_1^{2/k} \|h\|_2^{2-2/k} |\Gamma|^{1-1/k}, \tag{102}$$

where a trivial estimate

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

and a particular case of formula (39), namely,

$$\sum_\alpha \mu_\alpha = |\Gamma|g(0) = |\Gamma||\|h\|_2^2$$
were used. Substituting (101) and (102) into (100), we get
\[
\frac{|A|}{|\Gamma|}^2 \sum_x g(x)(\Gamma \circ \Gamma)(x) = c_0^2 \mu_0 \leq \sum_x g(x)(A \circ A)(x) \leq \|h\|_2^2 (\mathcal{T}_k^\times(A))^{1/k} \left( \frac{\|h\|_1}{\|h\|_2} \right)^{2/k}
\]
(103)
and (97) is proved.

To obtain (98), we just note that in the case \( k = 2 \) the sum \( \sum_\alpha \mu_\alpha^2 \) from (102) can be computed. Indeed by formula (40)
\[
\sum_\alpha \mu_\alpha^2 = \sum_x |g(x)|^2 (\Gamma \circ \Gamma)(x) = \sum_x |(h \circ \overline{h})(x)|^2 (\Gamma \circ \Gamma)(x)
\]
(104)
and after using the same arguments as above, we have
\[
|A| \leq |\Gamma|^{3/2} (\mathcal{E}^\times(A))^{1/2} \cdot \min_h \left( \sum_x |(h \circ \overline{h})(x)|^2 (\Gamma \circ \Gamma)(x) \right)^{1/2} \frac{1}{\sum_x (h \circ \overline{h})(x)(\Gamma \circ \Gamma)(x)}.
\]
(105)
Optimizing the last inequality over \( h \) (taking \( h(x) \equiv 1 \)), we obtain (98). To get (99) take \( g(x) = (\Gamma \circ \Gamma)^{l-1}(x) \), use formula (104) and repeat the arguments from (100), (104). After some computations, we have
\[
\sum_x g(x)(A \circ A)(x) = \mathcal{E}_l(A, \Gamma) \leq |\Gamma|^{-1/2} \mathcal{E}_{2l-1}^\times(\Gamma)(\mathcal{E}^\times(A))^{1/2}
\]
as required. This completes the proof of the proposition.

Note that formula (98) is just reformulation of Lemma 38. Formulas (97)–(99) give an explanation why \( \Gamma \) is a eigenfunction of operator \( \mathcal{T}_\Gamma^\times \Gamma \). The thing is \( \mathcal{T}_\Gamma^\times(\Gamma) \) 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 \( \mathcal{T}_k^\times(\Gamma) \) for arithmetic progressions in \( \mathbb{F}_p \).

**Theorem 41** 1) Let \( P \subseteq \mathbb{F}_p^* \) be an arithmetic progression. Then [4]
\[
\tau_2^\times(P) = \frac{|P|^4}{p} + O(|P|^{2+o(1)}).
\]
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 \( \lambda \)).
3) If \( \nu \) is a positive integer, \( |P| \ll p^{c(\nu)} \), where \( c(\nu) > 0 \) is some constant depends on \( \nu \) only. Then [2] the number of solutions of the congruence
\[
x_1 \ldots x_\nu \equiv \lambda \pmod{p}, \quad \lambda \neq 0, \quad x_1 \ldots x_\nu \in P
\]
is bounded by
\[
\exp \left( c'(\nu) \frac{\log |P|}{\log \log |P|} \right),
\]
where \( c'(\nu) > 0 \) depends on \( \nu \) only.
Corollary 42. Let $\Gamma \subseteq \mathbb{F}_q^*$ be a nontrivial multiplicative subgroup. Then for any progression $P \subseteq \Gamma$ the following holds
\[ |P| \ll |\Gamma|^{1/2+o(1)}, \] (106)
Suppose that $|\Gamma| \ll p^{2/3}$ and $l \geq 3$. Then
\[ E(P, \Gamma) \ll |P|^{1-o(1)}|\Gamma| \log^{1/2} |\Gamma| \quad \text{and} \quad E_l(P, \Gamma) \ll |P|^{1+o(1)}|\Gamma|^{l-1}. \] (107)

Proof. Suppose that $P \subseteq \Gamma$ is an arbitrary progression. By Theorem 41, we have
\[ E^\times(P) = \frac{|P|^4}{p} + O(|P|^{2+o(1)}). \] (108)
If the first term is dominated then applying (98), we get
\[ |P| \leq \frac{2^{1/4}|P|}{p^{1/4}} |\Gamma|^{1/4} \]
with contradiction. Thus the second term in (108) is dominated and using (98), we obtain (106).
Applying Theorem 41 once again, formula (99) and Corollary 8, we get (107). This completes the proof.

Clearly, the condition $|\Gamma| \ll p^{2/3}$ can be relaxed for large $l$. Obviously, inequality (107) is the best possible up to $|P|^{o(1)}$ factor.

Remark 43. The arguments from the proof of Proposition 40 give (we consider the simplest case $l = 2$) the following asymptotic formula
\[ E(P, \Gamma) = \sum_x (\Gamma \circ \Gamma)(x)(P \circ P)(x) = \frac{|P|^2 E(\Gamma)}{|\Gamma|^2} + \theta|P|^{1-o(1)}|\Gamma|^{-1/2}(E^*_3(\Gamma))^{1/2}, \]
where $|\theta| \leq 1$ and $E^*_3(\Gamma) = \sum_{\alpha \neq 0} \mu_\alpha^2$. Here $P \subseteq \Gamma$ is an arithmetic progression. The asymptotic formula works just for large subgroups of size $p^{1-\delta}$, $\delta > 0$.

Remark 44. Certainly, inequality
\[ |P + \Gamma| \gg |\Gamma||P|^{1-o(1)} \log^{-1/2} |\Gamma| \] (109)
follows from (107) by Cauchy–Schwartz and one can obtain analog of formula (109) 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 $k \geq 2$), namely,
\[ |\Gamma|^{l-1} + \Delta_{l-1}(A) \gg |A|^{1/2} \log^{-1/2} |\Gamma| \quad \text{and} \quad |\Gamma|^{l-1} + \Delta_{l-1}(A) \gg |A|^{1/2} |\Gamma|^{l-1}, \quad l > 3 \] (110)
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 45 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 \( p \geq p_0(\delta) \), we have
\[
|P| \leq \exp(C\sqrt{\delta^{-1}\log(1/\delta)\log p}).
\]
Moreover for any such arithmetic progression \( P \), \( \log|P| \gg \sqrt{\delta^{-1}\log(1/\delta)\log p} \) the following holds
\[
|P \cap \Gamma| \leq |P|^{1-\delta/4}.
\]

Proof. Suppose for a moment that \( P = \{1, 2, \ldots, s\} \subseteq \Gamma \). 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 \( s \geq 1 \) as small as we want. Thus suppose that \( \log s \sim \sqrt{\delta^{-1}\log(1/\delta)\log p} \).

Because of we take \( p \geq p_0(\delta) \) sufficiently large we can choose minimal \( k \geq 2 \) such that \( k \geq \log p/\log s \). One can quickly check that \( k \ll \log s \). Using Dirichlet’s method (see [9]) it is easy to prove
\[
T_k^\times(P) \leq |P|^k \left( \frac{C\log|P|}{k} \right)^{k(k-1)/2},
\]
where \( C > 0 \) is an absolute constant. By Corollary 39 and formula (113), we have
\[
\frac{s^{2k}}{|\Gamma|} \leq T_k^\times(P) \leq s^k \left( \frac{C\log s}{k} \right)^{k^2}.
\]
In other words
\[
\log s \leq k \log(Ck^{-1}\log s) + k^{-1} \log |\Gamma|.
\]
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 (114) because of our method equally works for progressions of the form \( \{a, 2a, \ldots, sa\} \) as well.

Thanks to Lemma 38 we can obtain estimate (112) using similar arguments as above. Indeed, let \( A = P \cap \Gamma \), and suppose that \( |A| \geq s^{1-\delta/4} \). Here \( P \) as before, \( |P| = s \). Thus \( T_k^\times(A) \geq |A|^{2k}/|\Gamma| \) and we obtain
\[
\log |A| \leq \frac{1}{2} \log s + \frac{\log s}{2\log p} \log |\Gamma| + \frac{\log p}{2\log s} \log \left( \frac{C\log^2 s}{\log p} \right) + \frac{\log^2 s}{\log^2 p} \log |\Gamma|.
\]
Hence by \( |A| \geq s^{1-\delta/4} \) and \( |\Gamma| = p^{1-\delta} \), we have
\[
\frac{\delta}{4} \log s \leq \frac{\log p}{2\log s} \log \left( \frac{C\log^2 s}{\log p} \right) + \frac{\log^2 s}{\log^2 p} \log |\Gamma| \ll \frac{\log p}{\log s} \log \left( \frac{C'\log^2 s}{\log p} \right),
\]
where \( C' > 0 \) is another absolute constant. In other words \( x \ll \delta^{-1}\log C'x \) as above. This completes the proof. \( \square \)
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 41 one can obtain a similar result for arithmetic progressions of general form.

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

7 Applications: general sets

Now we find applications of Proposition 28 to some further families of sets. Let us begin with the convex subsets of $\mathbb{R}$.

**Theorem 46** Let $A \subseteq \mathbb{R}$ be a convex set. Then

$$E(A) \ll |A|^\frac{89}{36} \log^\frac{1}{2} |A|.$$  \hfill (114)

**Proof.** Let $E = E(A)$, $E_3 = E_3(A)$. In view of Lemma 11, as in the proof of Theorem 34, we have

$$\sum_{\alpha \neq 0, \beta \neq 0, \alpha \neq \beta : \psi(\alpha), \psi(\beta), \psi(\alpha - \beta) \geq d} \psi^2(\alpha) \psi^2(\beta) \psi^2(\alpha - \beta) \gg \frac{E^6}{|A|^6 E_3}. \hfill (115)$$

where $\psi = (A \circ A)(x)$ and $d = 2^{-3}E^2 |A|^{-3} E_3^{-1/2}$. The last inequality implies an analog of (80), i.e.

$$d^6 \cdot \sum_{i,j,k=1}^l 2^{2i+2j+2k} \sum_\alpha S_i(\alpha)(S_j \ast S_k)(\alpha) \gg \frac{E^6}{|A|^6 E_3}. \hfill (116)$$

One can suppose that the summation in the last formula is taken over $i \leq j \leq k$. Applying Lemma 11 we have

$$\sum_\alpha S_i(\alpha)(S_j \ast S_k)(\alpha) \leq d^{-1}2^{-i} \sum_\alpha (A \circ A)(\alpha)(S_j \ast S_k)(\alpha) \leq d^{-1}2^{-i}E^{1/2}(S_j, A)E^{1/2}(S_k, A) \ll$$

$$\ll |A|d^{-1}2^{-i}|S_j|^{3/4}|S_k|^{3/4}. \hfill (117)$$

By formula (25) of Theorem 12 with $k = 2$, we obtain $|S_i| \ll |A|^3/(d^32^3)$. Combining the last bound with (117) and (116), we get

$$\frac{E^6}{|A|^6 E_3} \ll d^5 |A| \cdot \sum_{i,j,k=1}^l 2^{i-j-4-k/4} |A|^{9/2} d^{-9/2} \ll d^1/2 |A|^{11/2} 2^{l/2} \log^2 |A|. \hfill (118)$$

Finally, by Andrews’ inequality $2^l \ll |A|^{2/3}d^{-1}$. Using Lemma 11 once more after some calculations we obtain the result. This completes the proof. \hfill $\square$
Corollary 47 Let $A \subseteq \mathbb{Z}$ be a convex set and

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

Then

$$\int_0^{2\pi} |P_A(\theta)|^4 d\theta \ll |A|^{3\frac{5}{2}} \log \frac{1}{\varepsilon} |A|.$$ 

Remark 48 It can be appear that the argument from the proof of Theorem 46 namely, an application of an upper bound $(A \circ A)(x) \ll |A|^{2/3}$, $x \neq 0$ is quite rough. Nevertheless it is optimal modulo our current knowledge of convex sets. Indeed, let $i = j = k = l$ in formula (116). By Theorem 12 we just know that $|S_i|, |S_j|, |S_k| \ll |A|$. Further to estimate the sum $\sum a_i S_i(\alpha)(S_j * S_k)(\alpha)$ the only one can apply is estimate (117). Substituting all bounds in (116), we obtain exactly (114).

Using Theorem 12 instead of Theorem 9 and apply the arguments from the proof of Theorem 34 one can obtain new upper bounds for $T_k(A)$ 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 49 Let $A \subseteq \mathbb{R}$ be a set, and $\varepsilon \in [0, 1)$ be a real number. Suppose that $|AA| = M|A|$, $M \geq 1$, and

$$|\{ x \neq 0 : (A \circ A)(x) \geq |A|^{1-\varepsilon} \}| \ll (M \log M)^{\frac{3}{5}} |A|^{\frac{7}{10} - \frac{5}{7}} \log \frac{1}{\varepsilon} |A|.$$ 

Then

$$E(A) \ll M \log M |A|^{\frac{7}{10} - \frac{5}{7}} \log \frac{1}{\varepsilon} |A|.$$ 

Proof. By Lemma 13 we have $E_3(A) \ll M^2 \log^2 M \cdot |A|^3 \log |A|$. Thus $E_3(A)$ is small for small $M$ and we can apply the arguments from the proofs of Theorems 34 36. Using the second bound from Lemma 13 and a consequence of the first estimate, namely, $|S_i| \ll (M \log M)^2 |A|^3/(d^3 2^i)$, we obtain the required bound (120). 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 (78)), namely

$$(M \log M)^{\frac{3}{5}} |A|^{\frac{7}{10} \log \frac{1}{\varepsilon} |A|}$$

are less than our upper bound (120). One can easily assure that this is the case. The second inequality is that the sum over nonzero $x$ such that $(A \circ A)(x) \geq |A|^{1-\varepsilon}$ is small. Denote by $S_\varepsilon$ the set from (119). If

$$\frac{E^3(A)}{|A|^3} \ll \sum_{\alpha \in S_\varepsilon} \sum_{\beta} (A \circ A)(\alpha)(A \circ A)(\beta)(A \circ A)(\alpha - \beta) C_3(A)(\alpha, \beta) \leq$$
\[
\leq |A| \sum_{\alpha} \sum_{\beta} \sum_{z} S_{\epsilon}(\alpha)(A \circ A)(\beta)(A \circ A)(\alpha - \beta)A(z)A(z + \beta) \leq
\]

\[
\leq |A| \sum_{\beta} (S_{\epsilon} * (A \circ A))(\beta)(A \circ A)^2(\beta) \leq |A|E_{3/3}^2(A) \left( \sum_{\beta} (S_{\epsilon} * (A \circ A))^3(\beta) \right)^{1/3} \leq
\]

\[
\leq |A|(M^2 \log^2 M \cdot |A|^3 \log |A|)_{2/3} |S_{\epsilon}|A|^{4/3}
\]

then (120) holds. This completes the proof. \( \square \)

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

Clearly, Theorem 49 implies Theorem 46, because for \(\epsilon = 1/3\) the set from (119) is empty by Andrews result. Note also that upper bound (119) is quite rough and just shows the main idea.

Apply Theorem 49 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 50 Let \(A, B \subseteq \mathbb{R}\) be two sets, and \(\tau \leq |A|, |B|\) be a parameter. Then

\[
|\{s \in AB : |A \cap sB^{-1}| \geq \tau\}| \ll \frac{|A(A + 1)|^2|B|^2}{|A| \tau^3}.
\] (121)

Lemma above implies that for any \(A \subseteq \mathbb{R}\) the following holds \(E^\times(A) \ll |A(A + 1)||A|^{3/2}\). We obtain better upper bound for \(E^\times(A)\) (see inequality (123) of Corollary 52 below). Also in [10] a series of interesting inequalities were obtained. Here we formulate just one result.

Theorem 51 Let \(A \subseteq \mathbb{R}\) be a set. Then

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

We prove the following

Corollary 52 Let \(A \subseteq \mathbb{R}\) be a set, \(a \in \mathbb{R}\) be a number, \(|A(A + 1)| = M|A|, M \geq 1, \) and inequality (119) holds in multiplicative form. Then

\[
E^\times(A, A + a) \ll M|A|^\frac{5}{2 - \epsilon} \log^\frac{1}{2} |A|
\] (122)

In particular

\[
E^\times(A) \ll M|A|^\frac{5}{2 - \epsilon} \log^\frac{1}{2} |A|
\] (123)
Proof. Put \( A' = A + a \) and \( \psi(x) = |\{a_1, a_2 \in A : x = a_1 a_2^{-1}\}| \). Then as in (75), we have
\[
\left( \frac{E^x(A', A)}{|A|} \right)^3 \leq \sum_{\alpha, \beta} \psi(\alpha) \psi(\beta) \psi(\alpha^{-1}) C_3(A')(\alpha, \beta).
\]
Lemma 50 implies that \( E^3_\alpha(A') \ll M^2 |A|^3 \log |A| \). After that apply the arguments from the proof of Theorem 49. \( \square \)

Previous results of the section say, basically, that if \( E_3(A) \) is small and \( A \) has some additional properties such as condition (119) from Theorem 49 (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 56) a variant of the principle using just smallness of \( E_3(A) \) to show that \( A \) has a structured subset. The first result of the type was proved in [21] (see Theorem 23).

**Theorem 53** Let \( A \) be a subset of an abelian group. Suppose that \( |A - A| = K|A| \) and \( E_3(A) = M|A|^4/K^2 \). 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 53 has a strong condition, namely, the cardinality of the set \( A - A \) is small. Theorem 54 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, \( E_{3+\varepsilon}(A) = M|A|^{4+\varepsilon}/K^{2+\varepsilon} \), \( \varepsilon \in (0, 1] \).

**Theorem 54** Let \( A \subseteq G \) be a set. Suppose that \( E(A) = |A|^3/K \) and \( E_{3+\varepsilon}(A) = M|A|^{4+\varepsilon}/K^{2+\varepsilon} \), where \( \varepsilon \in (0, 1] \). Then there exists \( A' \subseteq A \) such that \( |A'| \gg M^{-\frac{4+6\varepsilon}{3+5\varepsilon}} |A| \) and
\[
|nA' - mA'| \ll M^{6(n+m)} \frac{2+4\varepsilon}{8+5\varepsilon} K |A'|
\]
for every \( n, m \in \mathbb{N} \).

Note that if \( \varepsilon \to 0 \) then the bounds in Theorem 54 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 55** Let \( A \) be a subset of an abelian group. Suppose that \( E(A) = |A|^3/K \) and \( E_{2+\varepsilon}(A) = M|A|^{3+\varepsilon}/K^{1+\varepsilon} \). Then there exists \( A' \subseteq A \) such that \( |A'| \gg |A|/(2M)^{1/\varepsilon} \) and
\[
|A' - A'| \ll 2^5 M^{5/2} K^4 |A'|
\]
Let us formulate our result.
Theorem 56 Let \( A \subseteq G \) be a set, \( E(A) = |A|^3/K \), and \( E_3(A) = M|A|^4/K^2 \). Suppose that \( M \leq |A|/(6K) \). Then there is a real number \( r \)

\[
1 \leq r \leq \frac{1}{|A|} \max_{x \neq 0} (A \circ A)(x) \cdot KM^{1/2} \leq KM^{1/2},
\]

(124)

and a set \( A' \subseteq A \) such that

\[
|A'| \gg M^{-23/2}r^{-2}\log^{-9}|A|\cdot |A|,
\]

(125)

and

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

(126)

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

Proof. Let \( E = E(A), E_3 = E_3(A), \psi = A \circ A \). Then as in (75), we have

\[
\left( \frac{E(A)}{|A|} \right)^3 \leq \sum_{\alpha, \beta} \psi(\alpha)\psi(\beta)\psi(\alpha - \beta)C_3(A)(\alpha, \beta).
\]

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

\[
2^{-1} \left( \frac{E(A)}{|A|} \right)^3 \leq \sum_{\alpha \neq 0, \beta \neq 0, \alpha \neq \beta} \psi(\alpha)\psi(\beta)\psi(\alpha - \beta)C_3(A)(\alpha, \beta).
\]

As before

\[
\sum_{\alpha \neq 0, \beta \neq 0, \alpha \neq \beta : \psi(\alpha), \psi(\beta), \psi(\alpha - \beta) \gg d} \psi^2(\alpha)\psi^2(\beta) \psi^2(\alpha - \beta) \gg \frac{E_3^6}{|A|^6E_3},
\]

(127)

where \( d = 2^{-3}E_3^2|A|^{-3}E_3^{-1/2} \). In terms of the sets \( S_i \), we obtain a variant of formula (80), namely

\[
d^4 \cdot \sum_{j,k=1}^l 2^{2j+2k} \sum_\alpha (A \circ A)^2(\alpha)(S_j \ast S_k)(\alpha) \gg \frac{E_3^6}{|A|^6E_3}.
\]

(128)

Trivially

\[
|S_1|(d2i-1)^3 \leq E_3,
\]

and hence

\[
|S_1| \ll E_3/(d^{3}2^{3i}).
\]

(129)

Note also that \( d2i \leq \max_{x \neq 0}(A \circ A)(x), i \in [l] \) and hence

\[
2^i \leq \frac{1}{|A|} \max_{x \neq 0}(A \circ A)(x) \cdot KM^{1/2} \leq KM^{1/2}.
\]

Because of

\[
\sum_\alpha (A \circ A)^2(\alpha)(S_j \ast S_k)(\alpha) \leq E_3^{2/3} \left( \sum_\alpha (S_j \ast S_k)^3(\alpha) \right)^{1/3} \leq E_3^{2/3}(\|S_j\|\|S_k\|)^{1/6}E^{1/3}(S_j, S_k)
\]

(130)
then using (129), we can assume that the summation in (128) is taken over \( j, k \) such that

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

(131)

Applying (129), (130) and a trivial upper bound for the additive energy, namely, \( E(S_j, S_k) \leq |S_j|^{3/2}|S_k|^{3/2} \), we obtain

\[
d^4 \cdot \sum_{j, k=1}^l 2^{j+2k} \sum_{\alpha} (A \circ A)^2(\alpha)(S_j \ast S_k)(\alpha) \ll d^4 E_3^{2/3} \cdot \sum_{j, k=1}^l 2^{j+2k}|S_j|^{2/3}|S_k|^{2/3} \ll
\]

\[
\ll d^8 E_3^{4/3} \log^2 |A| \cdot \max_j 2^{2j}|S_j|^{2/3}.
\]

Thus the summation in (128) is taken over \( j \in [l] \) such that

\[
2^j |S_j| \gg 2^{-2j} M^{-2} K \log^{-3} |A| \cdot |A|.
\]

(132)

By Balog–Szemerédi–Gowers Theorem 6 and estimate (131) 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 \( |S''| \geq |S'| \). Then

\[
|S' + S''| \ll \mu^{-7} |S''|.
\]

Plünnecke–Ruzsa inequality (see e.g. [25]) yields

\[
|nS' - mS'| \ll \mu^{-7(n+m)} |S'|,
\]

(133)

for every \( n, m \in \mathbb{N} \). Using the definition of the set \( S_j \) and inequality (132), we find \( x \in G \) such that

\[
|(A - x) \cap S'| \geq 2^{j-1} d |A|^{-1} |S'| \gg K^{-1} M^{-1/2} \mu 2^j |S_j| \gg M^{-23/2} 2^{-2j} \log^{-9} |A| \cdot |A|.
\]

(134)

Put \( A' = A \cap (S' + x) \). Using (133), (134) and the definition of \( d \), we obtain for all \( n, m \in \mathbb{N} \)

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

and the result follows with \( r = 2^j \).

Thus, for small \( r \) our result is better than Theorem 54 and Theorem 55 because we assume that just \( E_3(A) \) is small and we obtain better bound for the doubling constant of \( A' \), correspondingly. If \( r \) is large than lower bound (125) for cardinality of \( A' \) is not so good but upper bound (126) for the doubling constant becomes better than in Theorems 54, 55 as well as in Theorem 53.

Note, finally, that condition (124) can be certainly relaxed in spirit of assumption (119) from Theorem 49.

In the end of the section we give one more variant of the arguments, using eigenvalues method.
**Theorem 57** Let $A \subseteq G$ be a set, $D \subseteq A - A$, $D = -D$, $\eta \in (0, 1]$ be a real number,

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

and $E_3(A) = \eta^3 M |A|^6 / |D|^2$. Then there is a set $A' \subseteq A$ such that

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

and

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

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

**Proof.** Let $E = E(A)$, $\psi = A \circ A$, $\sigma$ be the sum from (135), and

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

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

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

Denote by $\{f_j\}_{j \in [|A|]}$ the orthonormal eigenfunctions of the symmetric operator $T_A^{N-1} \hat{D}_r$. Of course $f_0 \geq 0$. As in Proposition 28 and as in formula (75), we get

$$
\sum_{\alpha, \beta} D_*(\alpha)D_*(\beta)(A \circ A)(\alpha - \beta)C_3(A)(\alpha, \beta) = \sum_{x,y,z \in A} D_*(x-y)D_*(x-z)(A \circ A)(y-z) =
$$

$$
= \sum_j |\mu_j(T_A^{N-1} \hat{D}_r)|^2 \cdot \langle T_A^{N-1} \hat{D}_r f_j, f_j \rangle.
$$

Because of $\hat{\psi} \geq 0$, we obtain

$$
\omega_j := \langle T_A^{N-1} \hat{\psi} f_j, f_j \rangle = \sum_x \psi(x)(f_j \circ f_j)(x) \geq 0, \quad j \in [|A|].
$$

Trivially

$$
\mu_0 := \mu_0(T_A^{N-1} \hat{D}_r) \geq |A|^{-1} \sigma_*.
$$

Let us estimate $\omega_0$. We have

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

By Cauchy–Schwarz, we get

$$
\mu_0^2 \left( \sum_x f_0(x) \right)^2 \leq |D_*| \sum_x (f_0 \circ A)^2(x) = |D_*| \omega_0.
$$
Using estimate (58) of Lemma 29 and the formula above, we obtain
\[ \omega_0 \geq \frac{\mu_0^3}{|D_0|}. \] (141)

Applying (140), (141), we get
\[ \sum_{\alpha, \beta} D_\star(\alpha)D_\star(\beta)(A \circ A)(\alpha - \beta)C_3(A)(\alpha, \beta) \gg \frac{\mu_0^5}{|D_0|} \gg \frac{\sigma_5}{|A|^5|D_\star|}. \]

Using the upper bound for \( E_3(A) \) and estimate (138), we have
\[ \sum_x (D_\star \circ D_\star)(x)(A \circ A)^2(x) \gg \frac{\eta^3 \sigma_4^4}{M|A|^4}. \]

Applying the arguments from (130), we get
\[ E(D_\star) \gg \frac{\eta^{15}|D|^3}{M^5} = \nu|D_\star|^3. \]

By Balog–Szemerédi–Gowers Theorem 6 there is \( D' \subseteq D_\star, |D'| \gg \nu|D_\star| \) such that \( |D' + D'| \ll \nu^{-7}|D'| \). Plünnecke–Ruzsa inequality (see e.g. 26) yields
\[ |nD' - mD'| \ll \nu^{-7(n+m)}|D'|, \] (142)

for every \( n, m \in \mathbb{N} \). Using the definition of the set \( D_\star \) and the number \( \nu \), we find \( x \in G \) such that
\[ |(A - x) \cap D'| \geq 2^{-1}\eta|A||D'|/|D| \geq 2^{-1}\eta|A|\nu|D_\star|/|D| \gg \frac{\eta^{16}|A|}{M^5}. \] (143)

Put \( A' = A \cap (D' + x) \). Using (142), (143), we obtain for all \( n, m \in \mathbb{N} \)
\[ |nA' - mA'| \leq |nD' - mD'| \ll \nu^{-7(n+m)}|D'| \ll \nu^{-7(n+m)}\eta^{-1}|D||A|^{-1}|A'| \]
and the result follows. \( \square \)

Taking \( D = A - A \) in Theorem 57, we obtain Theorem 53 (with a little bit different constants). Thus the result above is a generalization of Theorem 53.

References

[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, \textit{Isomorphism classes of elliptic curves over a finite field in some thin families}, Math. Res. Letters \textbf{19} (2012), 335–343.

[5] W. T. Gowers \textit{A new proof of Szemerédi's theorem for arithmetic progressions of length four}, Geom. func. anal. \textbf{8} (1998) 529–551.

[6] W. T. Gowers \textit{A new proof of Szemerédi's theorem}, Geom. func. anal. \textbf{11} (2001) 465–588.

[7] D. R. Heath–Brown, S. V. Konyagin \textit{New bounds for Gauss sums derived from \textit{kth} powers, and for Heilbronn's exponential sum}, Quart. J. Math. \textbf{51} (2000), 221–235.

[8] A. Iosevich, S. V. Konyagin, M. Rudnev, V. Ten, \textit{On combinatorial complexity of convex sequences}, Discrete Comput. Geom. \textbf{35} (2006), 143–158.

[9] H. Iwaniec, E. Kowalski, \textit{Analytic Number Theory}, AMS, Colloquium publ., v. 53.

[10] T. G. F. Jones, O. Roche–Newton, \textit{Improved bounds on the set} $A(A + 1)$, \texttt{arXiv:1205.3937v1 [math.CO]}.

[11] N. H. Katz, P. Koester, \textit{On additive doubling and energy}, SIAM J. Discrete Math. \textbf{24} (2010), 1684–1693.

[12] S. V. Konyagin, \textit{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, \textit{Character sums with exponential functions}, Cambridge University Press, Cambridge, 1999.

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

[15] L. Li, O. Roche–Newton, \textit{Convexity and a sum–product type estimate}, \texttt{arXiv:1111.5159v1 [math.CO]}.

[16] W. Rudin, \textit{Fourier analysis on groups}, Wiley 1990 (reprint of the 1962 original).

[17] M. Rudnev, S. V. Konyagin \textit{On new sum–product type estimates}, \texttt{arXiv:1111.4977v1 [math.CO]}.

[18] T. Schoen, \textit{Near optimal bounds in Freiman's theorem}, Duke Math. Journal, to appear.

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

[20] T. Schoen, I. D. Shkredov, \textit{On sumsets of convex sets}, Comb. Probab. Comput. \textbf{20} (2011), 793–798.

[21] T. Schoen, I. D. Shkredov, \textit{Higher moments of convolutions}, \texttt{arXiv:1110.2986v1 [math.CO]} 13 Oct 2011.
[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.

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