Journal of Number Theory 133 (2013) 1693–1737

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Higher moments of convolutions

Tomasz Schoen [a,1], Ilya D. Shkredov [b,c,d,*,2]

[a] Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Umultowska 87, 61-614 Poznań, Poland
[b] Division of Algebra and Number Theory, Steklov Mathematical Institute, ul. Gubkina, 8, Moscow 119991, Russia
[c] Delone Laboratory of Discrete and Computational Geometry, Yaroslavl State University, Sovetskaya str. 14, Yaroslavl 150000, Russia
[d] IITP RAS, Bolshoy Karetny per. 19, Moscow 127994, Russia

ARTICLE INFO

Article history:
Received 8 February 2012
Accepted 30 October 2012
Available online 23 December 2012
Communicated by David Goss

Keywords:
Additive combinatorics
Generalizations of the additive energy

ABSTRACT

We study higher moments of convolutions of the characteristic function of a set, which generalize a classical notion of the additive energy. Such quantities appear in many problems of additive combinatorics as well as in number theory. In our investigation we use different approaches including basic combinatorics, Fourier analysis and eigenvalues method to establish basic properties of higher energies. We provide also a sequence of applications of higher energies additive combinatorics.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbf{G}$ be an abelian group, and $A \subseteq \mathbf{G}$ be an arbitrary finite set. The *additive energy* of the set A is defined by

$$\mathsf{E}_2(A) = \big|\{a_1 - a_2 = a_3 - a_4 \colon a_1, a_2, a_3, a_4 \in A\}\big|.$$

This quantity plays an important role in many problems of additive combinatorics as well as in number theory (see e.g. [36]). In the article we study, basically, the following generalization of the additive energy

$$\mathsf{E}_k(A) = \big|\{a_1 - a_2 = a_3 - a_4 = \cdots = a_{2k-1} - a_{2k} \colon a_1, \ldots, a_{2k} \in A\}\big|, \quad k \geqslant 2.$$

* Corresponding author at: Division of Algebra and Number Theory, Steklov Mathematical Institute, ul. Gubkina, 8, Moscow 119991, Russia.
E-mail addresses: schoen@amu.edu.pl (T. Schoen), ilya.shkredov@gmail.com (I.D. Shkredov).

[1] The author is supported by MNSW grant N N201 543538.
[2] This work was supported by grant RFFI NN 06-01-00383, 11-01-00759, Russian Government project 11.G34.31.0053 and grant Leading Scientific Schools N 2519.2012.1.

0022-314X/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jnt.2012.10.010

Geometrically, $\mathsf{E}_k(A)$ is the number of k-tuples of Cartesian product A^k, which belong to the same line from the system of lines of the form $y = x + c$, $c \in A - A$. An analog of $\mathsf{E}_3(A)$ for general systems of lines and points has applications in combinatorial geometry and in sum-product problems (see [36, Chapter 8]). $\mathsf{E}_k(A)$ can be also expressed as the kth moment of the convolution of the characteristic function of the set A (see [32]).

Higher energies have already found some applications (see [27,28,32]). Here we collect further properties and applications of $\mathsf{E}_k(A)$. To prove them we use different approaches including basic combinatorics, Fourier analysis and eigenvalues method.

The paper is organized as follows. We start with definitions and notations used in the paper. In the next section we consider some basic properties of higher energies. We prove, in particular, that the smallness of energy E_k implies a non-trivial upper bound for the cardinality of the set of large Fourier coefficients and vice versa. These sets play an important role in every problem of additive combinatorics where Fourier analysis is used (see [36]).

Quantities $\mathsf{E}_k(A)$ can be expressed in terms of higher convolutions of the set A (see [32]). We continue to study supports of these convolutions in Section 3. We establish a generalization of Ruzsa's triangle inequality, which allows us to introduce a hierarchy of bases of abelian groups (that is sets B with $B \pm B = \mathbf{G}$) and prove some its properties.

In Section 5 we show that the knowledge of energies E_k allows to refine Croot–Sisask almost periodicity lemma (see [8]). Further, we prove in Section 6, that for any A with $|A - A| = K|A|$ and $\mathsf{E}_3(A) = M|A|^4/K^2$, for a relatively small M, there is a large subset $A' \subseteq A$ such that A' has almost no growth under addition. To show this result, we use a technique introduced in [27], where among other things Katz–Koester transform [15] is applied. Series of results contained in Sections 5–9 can be considered as statements on structure of sets with small $\mathsf{E}_3(A)$ (results on structure of sets with small proportion of two another generalizations of the additive energy can be found in [5,6]).

In Section 7 we prove some results related to sum-product problem in $\mathbb{R}$. Solymosi [34] showed an upper bound for multiplicative energy in terms of the size of the sumset $A + A$. Improving a theorem of Li [19], we prove an upper estimate of $\mathsf{E}_k(A)$ in terms of $|A \cdot A|$. Our approach is based on the Szemerédi–Trotter theorem and develops some ideas introduced in [28] and [19].

In the next section we use so-called eigenvalue method to study $\mathsf{E}_k(A)$. Using this approach, we show that the magnification ratio of a set A (see [36] and also [20]) is closely related with the behavior of $\mathsf{E}_k(A)$. Actually, it turns out that the method allows to prove lower bounds for the cardinality of restricted sumsets $A \overset{G}{+} B$, where G is a subgraph of the complete bipartite graph with bipartition A, B (see Theorem 43). As an application, we obtain some results concerning sumsets of sets with small E_k (another application will be also given in Section 9). The results are particularly powerful in the case of multiplicative subgroups of the field $\mathbb{F}_q$.

In Section 9 we prove two versions of the well-known Balog, Szemerédi and Gowers [2,4,10]. Assuming $\mathsf{E}_2(A) = |A|^3/K$ and $\mathsf{E}_3(A) \leqslant M|A|^4/K^2$ we obtain an improvement of the Balog–Szemerédi–Gowers theorem, and with the assumptions $\mathsf{E}_2(A) = |A|^3/K$ and $\mathsf{E}_4(A) \leqslant M|A|^5/K^3$ we show an optimal version of the Balog–Szemerédi–Gowers theorem.

Finally, in the last section we prove some results, which connect higher energies and higher moments of the Fourier transform of A.

2. Notation

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 [21] 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 $\widehat{f}$,

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

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

$$\sum_{x\in\mathbf{G}}\bigl|f(x)\bigr|^2=\frac{1}{N}\sum_{\xi\in\widehat{\mathbf{G}}}\bigl|\widehat{f}(\xi)\bigr|^2, \tag{2}$$

$$\sum_{y\in\mathbf{G}}\Bigl|\sum_{x\in\mathbf{G}}f(x)g(y-x)\Bigr|^2=\frac{1}{N}\sum_{\xi\in\widehat{\mathbf{G}}}\bigl|\widehat{f}(\xi)\bigr|^2\bigl|\widehat{g}(\xi)\bigr|^2. \tag{3}$$

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

$$\widehat{f*g}=\widehat{f}\,\widehat{g}\quad\text{and}\quad\widehat{f\circ g}=\overline{\widehat{f}}\,\widehat{g}. \tag{4}$$

For a function $f:\mathbf{G}\to\mathbb{C}$ put $f^c(x):=f(-x)$. Clearly, $(f*g)(x)=(g*f)(x)$, $x\in\mathbf{G}$. The k-fold convolution, $k\in\mathbb{N}$ we denote by $*_k$, so $*_k:=*(*_{k-1})$.

Write $\mathsf{E}(A,B)$ for *additive energy* of two sets $A,B\subseteq\mathbf{G}$ (see e.g. [36]), that is

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

We use in the paper the same letter to denote a set $S\subseteq\mathbf{G}$ and its characteristic function $S:\mathbf{G}\to\{0,1\}$.

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

$$\mathsf{E}(A,B)=\sum_x(A*B)(x)^2=\sum_x(A\circ B)(x)^2=\sum_x(A\circ A)(x)(B\circ B)(x), \tag{5}$$

and by (3),

$$\mathsf{E}(A,B)=\frac{1}{N}\sum_{\xi}\bigl|\widehat{A}(\xi)\bigr|^2\bigl|\widehat{B}(\xi)\bigr|^2. \tag{6}$$

Let

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

Generally, for every function $f:\mathbf{G}\to\mathbb{C}$ set $\mathsf{T}_k(f)=\sum_x|(f*_{k-1}f)(x)|^2$. Clearly, $\mathsf{T}_k(A)=\frac{1}{N}\sum_\xi|\widehat{A}(\xi)|^{2k}$. Let also

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

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 $A_s=A\cap(A-s_1)\cap\dots\cap(A-s_{k-1})$. Let

$$\mathsf{E}_k(A)=\sum_{x\in\mathbf{G}}(A\circ A)(x)^k=\sum_{s_1,\dots,s_{k-1}\in\mathbf{G}}|A_s|^2 \tag{7}$$

and

$$\mathsf{E}_k(A,B)=\sum_{x\in\mathbf{G}}(A\circ A)(x)(B\circ B)(x)^{k-1}. \qquad (8)$$

Similarly, we write $\mathsf{E}_k(f,g)$ for any complex functions f and g. Putting $\mathsf{E}_1(A)=|A|^2$.

We shall write $\sum_x$ and $\sum_\xi$ instead of $\sum_{x\in\mathbf{G}}$ and $\sum_{\xi\in\widehat{\mathbf{G}}}$ for simplicity.

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.

3. Basic properties of higher energies

Here we collect basic properties of $\mathsf{E}_k(A)$, where A is a finite subset of an abelian group $\mathbf{G}$. If $|A-A|=K|A|$ then

$$\mathsf{E}_k(A)\geqslant\frac{|A|^{k+1}}{K^{k-1}}.$$

The first very useful property of higher energy was proved in [27] and [32]. The next lemma is a special case of Lemma 2.8 from [32].

Lemma 1. *Let A be a subset of an abelian group. Then for every $k,l\in\mathbb{N}$*

$$\sum_{\substack{s,t:\\ \|s\|=k-1,\ \|t\|=l-1}}\mathsf{E}(A_s,A_t)=\mathsf{E}_{k+l}(A),$$

where $\|x\|$ denote the number of components of vector x.

Lemma 2. *Let A be a subset of an abelian group. Then for every $\alpha\in\mathbb{R}$*

$$\sum_{\|s\|=1}\mathsf{E}_{1+\alpha}(A_s,A)=\mathsf{E}_{2+\alpha}(A).$$

Lemma 3. *Let A be a subset of an abelian group. Then for every $k\in\mathbb{N}$, we have*

$$|A|^{2k}\leqslant\mathsf{E}_k(A)\cdot\sigma_k(A-A),\qquad |A|^{4k}\leqslant\mathsf{E}_{2k}(A)\cdot\mathsf{T}_k(A+A), \qquad (9)$$

and

$$|A|^{2k+4}\leqslant\mathsf{E}_{k+2}(A)\cdot\mathsf{E}_k(A-A),\qquad |A|^{2k+4}\leqslant\mathsf{E}_{k+2}(A)\cdot\mathsf{E}_k(A+A). \qquad (10)$$

Proof. Let us prove the first inequality from (9). The formula is trivial for $k=1$, so suppose that $k\geqslant 2$. Consider the map

$$\varphi: A^k\to(A-A)^k$$

defined by

$$\varphi(a_1,\dots,a_k)=(a_1-a_2,a_2-a_3,\dots,a_{k-1}-a_k,a_k-a_1)=(x_1,\dots,x_k).$$

Clearly, $x_1+\dots+x_k=0$. Thus $\sigma_k(A-A)\geqslant|\mathbf{Im}(\varphi)|$. By the Cauchy–Schwarz inequality

$$\begin{aligned}|A|^{2k}&\leqslant\big|\mathbf{Im}(\varphi)\big|\cdot\big|\big\{z,w\in A^k\colon\ \varphi(z)=\varphi(w)\big\}\big|\\&\leqslant\sigma_k(A-A)\cdot\big|\big\{z,w\in A^k\colon\ \varphi(z)=\varphi(w)\big\}\big|.\end{aligned}$$

To finish the proof it is enough to observe that

$$\big|\big\{z,w\in A^k\colon\ \varphi(z)=\varphi(w)\big\}\big|=\mathsf{E}_k(A).$$

To obtain the second inequality from (9), consider

$$\varphi'(a_1,\dots,a_{2k})=(a_1+a_2,a_2+a_3,\dots,a_{2k-1}+a_{2k},a_{2k}+a_1)=(x_1,\dots,x_{2k}),$$

instead of φ. Because of $x_1-x_2+x_3-x_4+\dots+x_{2k-1}-x_{2k}=0$ and

$$\big|\big\{z,w\in A^k\colon\ \varphi'(z)=\varphi'(w)\big\}\big|=\mathsf{E}_k(A),$$

we can use the previous arguments.

To obtain the first inequality in (10) consider the map

$$\psi:A^{k+2}\to(A-A)^{2k}$$

defined by

$$\psi(b_1,b_2,a_1,\dots,a_k)=(b_1-a_1,b_2-a_1,\dots,b_1-a_k,b_2-a_k)=(x_1,y_1,\dots,x_k,y_k)$$

and similar with pluses. It is easy to check that

$$\big|\big\{z,w\in A^{k+2}\colon\ \psi(z)=\psi(w)\big\}\big|=\mathsf{E}_{k+2}(A)$$

and $\mathsf{E}_k(A-A)\geqslant|\mathbf{Im}(\psi)|$ because of

$$x_1-y_1=\dots=x_k-y_k.$$

Thus, we obtain (10) by the arguments above. □

It turns out that $\mathsf{E}_k(A)$ is also closely related with higher dimensional sumsets. Observe that

$$\begin{aligned}\mathsf{E}_{k+1}(A,B)&=\sum_x(A\circ A)(x)(B\circ B)(x)^k\\&=\sum_{x_1,\dots,x_{k-1}}\Big(\sum_y A(y)B(y+x_1)\dots B(y+x_k)\Big)^2=\mathsf{E}\big(\Delta(A),B^k\big)\end{aligned}\tag{11}$$

and

$$\sum_{x\in X}(A\circ B)(x)^k=\sum_{x\in X}\big|\big\{(a_1,b_1),\dots,(a_k,b_k)\in A\times B\colon\ b_1-a_1=\dots=b_k-a_k=x\big\}\big|$$
$$=\sum_{y\in A^k}\big(\Delta(X)\circ B^k\big)(y),$$

where

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

We also put $\Delta(x)=\Delta(\{x\})$, $x\in\mathbf{G}$. The formula above gives a motivation to study the sumsets $A^k-\Delta(A)$, where $A^k,\Delta(A)\subseteq\mathbf{G}^k$. Another motivation to study such sets was discussed in [32]. It turns out that these sets appear naturally as supports of higher convolutions of the set A.

Clearly

$$A^k-\Delta(A)=\bigcup_{a\in A}(A-a)^k\quad\text{and}\quad A^k+\Delta(A)=\bigcup_{a\in A}(A+a)^k.$$

By the Cauchy–Schwarz inequality we have

$$\big|A^k-\Delta(A)\big|\geqslant\frac{|A|^{2k+2}}{\mathsf{E}(A^k,\Delta(A))}=\frac{|A|^{2k+2}}{\mathsf{E}_{k+1}(A)}.\tag{12}$$

Trivially for every $A_1,\dots,A_k\subseteq\mathbf{G}$

$$\big|A_1\times\dots\times A_{k-1}-\Delta(A_k)\big|\leqslant\min\left(\prod_{i=1}^{k}|A_i|,\prod_{j=1}^{k-1}|A_j-A_k|\right).\tag{13}$$

Now assume that $\mathbf{G}$ is a finite abelian group and $A\subseteq\mathbf{G}$. For any $\alpha\in(0,1]$ put

$$R_\alpha=R_\alpha(A)=\big\{r\in\widehat{\mathbf{G}}\colon\ \big|\widehat{A}(r)\big|\geqslant\alpha|A|\big\}.$$

Thus, $R_\alpha(A)$ is the set of large Fourier coefficients of the set A. We show that the size and the structure of R_α are highly related to $\mathsf{E}_k(A)$. We make use of the following lemma, which was proved in [29,30].

Lemma 4. *Let $\alpha\in(0,1]$ be a real number. Let also A be a subset of a finite abelian group $\mathbf{G}$, $|A|=\delta N$, and let $\Lambda\subseteq R_\alpha\setminus\{0\}$. Then*

$$\mathsf{T}_k(\Lambda)\geqslant\delta\alpha^{2k}|\Lambda|^{2k}.$$

Theorem 5. *Let $\alpha\in(0,1]$ be a real number. Suppose that A is a subset of an abelian group $\mathbf{G}$ of order N and $|A|=\delta N$. Suppose that $\mathsf{E}_k(A)=\kappa_k|A|^{k+1}$. Then*

$$|R_\alpha|\leqslant\alpha^{-3}\delta^{-1}\big(\kappa_{2k}-\delta^{2k-1}\big)^{1/2k},\tag{14}$$

and

$$\max_{r\neq0}\big|\widehat{A}(r)\big|\geqslant k^{-1/2}\big(\kappa_k-\delta^{k-1}\big)^{1/2}|A|.\tag{15}$$

Moreover, $\kappa_k \geqslant \kappa_{k-1}^{\frac{k-1}{k-2}} \geqslant \delta\kappa_{k-1}$, *and*

$$\max_{r\neq 0}\bigl|\widehat{A}(r)\bigr| \geqslant (\kappa_k - \delta\kappa_{k-1})^{1/2}|A|. \tag{16}$$

Proof. By the Fourier inversion formula

$$\begin{aligned}\mathsf{E}_{2k}(A) &= \sum_t (A\circ A)(t)^{2k} = \sum_t \biggl(N^{-1}\sum_r \bigl|\widehat{A}(r)\bigr|^2 e(tr)\biggr)^{2k}\\ &= N^{1-2k}\sum_{\sum r_i=0}\bigl|\widehat{A}(r_1)\bigr|^2\ldots\bigl|\widehat{A}(r_{2k})\bigr|^2.\end{aligned} \tag{17}$$

Lemma 4 implies that

$$\kappa_{2k}|A|^{2k+1} \geqslant \delta^{2k-1}|A|^{2k+1} + N^{1-2k}\delta\alpha^{2k}|R_\alpha|^{2k}\bigl(\alpha|A|\bigr)^{4k},$$

which gives the first inequality.

Next, notice that

$$\begin{aligned}\kappa_k|A|^{k+1} &\leqslant \delta^{k-1}|A|^{k+1} + k\max_{r\neq 0}\bigl|\widehat{A}(r)\bigr|^2 N^{1-k}\biggl(\sum_r\bigl|\widehat{A}(r)\bigr|^2\biggr)^{k-1}\\ &= \delta^{k-1}|A|^{k+1} + k\max_{r\neq 0}\bigl|\widehat{A}(r)\bigr|^2|A|^{k-1},\end{aligned}$$

and we have proved (15).

Finally, let us show (16). The Hölder inequality gives $\kappa_k \geqslant \kappa_{k-1}^{\frac{k-1}{k-2}}$, so that $\kappa_k \geqslant \delta\kappa_{k-1}$. For $k \geqslant 2$ put $\varphi(x) = (A\circ A)^{k-1}(x)$. Again, by the inverse formula

$$\mathsf{E}_k(A) = \kappa_k|A|^{k+1} = \frac{1}{N}\sum_r\bigl|\widehat{A}(x)\bigr|^2\widehat{\varphi}(x) \leqslant \kappa_{k-1}\delta|A|^{k+1} + \max_{r\neq 0}\bigl|\widehat{A}(r)\bigr|^2|A|^{k-1}$$

and the assertion follows. □

Clearly, the inequality (14) is better than trivial bound $|R_\alpha| \leqslant \alpha^{-2}\delta^{-1}$, provided that

$$\alpha > \bigl(\kappa_{2k} - \delta^{2k-1}\bigr)^{1/2k}.$$

Next, we show that $A \pm A$ contains long arithmetic progressions and even more general configurations. The first part of the proof of the corollary below uses an idea of Vsevolod Lev the second part is rather similar to the method introduced in [9].

Corollary 6. *Let* $A \subseteq \mathbf{G}$ *be a set,* $|A| = \delta N$. *Let also* $k \gg \log N/\log(1/\delta)$ *and* $c_1,\ldots,c_k$ *are any numbers not all equals zero. Then* $A \pm A$ *contains a configuration of the form* $x + c_1 d,\ldots,x + c_k d$ *with* $d \neq 0$.

Proof. We find a tuple $x+c_1d,\ldots,x+c_kd$ in $A-A$ because the case $A+A$ follows from the additional observation that there is $s \in \mathbf{G}$ such that $|A\cap(s-A)| \geqslant \delta^2 N$ and $A\cap(s-A) - A\cap(s-A) \subseteq A+A-s$. Let $\vec{1} = (1,\ldots,1)$, $\vec{c} = (c_1,\ldots,c_k)$, and $\vec{u} = (u_1,\ldots,u_k)$. Assume the contrary and apply analog of formula (17), we get

$$|A|^{k+1} \geqslant \mathsf{E}_k(A) = \sum_{x,d} (A\circ A)(x+c_1d)\dots(A\circ A)(x+c_kd)$$
$$= \frac{1}{N^{k-2}} \sum_{\langle \vec{u},\vec{1}\rangle = \langle \vec{u},\vec{c}\rangle = 0} \left|\widehat{A}(u_1)\right|^2 \dots \left|\widehat{A}(u_k)\right|^2 \geqslant \delta^{2k} N^{k+2}$$

and the result follows.

Now we give a non-abelian variant of the proof in the case $A-A$. Suppose that $|A^k| > N^{k-1}$. Then the sets $A^k + (dc_1,\dots,dc_k)$, $d \in \mathbf{G}$ cannot be disjoint. It means that for some different d', d'' we have $(A^k + (d'c_1,\dots,d'c_k)) \cap (A^k + (d''c_1,\dots,d''c_k)) \neq \emptyset$. In other words $((d'-d'')c_1,\dots,(d'-d'')c_k) \in (A-A)^k$. Thus, $|A^k| \leqslant N^{k-1}$ and the result follows. □

4. Ruzsa's triangle inequality and bases of higher depth

Next results provide basic relations between sizes of higher dimensional sumsets. The following theorem generalizes the well-known Ruzsa's triangle inequality [22,23].

Theorem 7. *Let $k \geqslant 1$ be a positive integer, and let $A_1,\dots,A_k, B$ be finite subsets of an abelian group $\mathbf{G}$. Further, let $W, Y \subseteq \mathbf{G}^k$, and $X, Z \subseteq \mathbf{G}$. Then*

$$|W\times X|\left|Y - \Delta(Z)\right| \leqslant \left|Y\times W\times Z - \Delta(X)\right|, \tag{18}$$
$$\left|A_1\times\dots\times A_k - \Delta(B)\right| \leqslant \left|A_1\times\dots\times A_m - \Delta(A_{m+1})\right|\left|A_{m+1}\times\dots\times A_k - \Delta(B)\right| \tag{19}$$

for any $m \in [k]$. Furthermore, we have

$$\left|Y\times Z - \Delta(X)\right| = \left|Y\times X - \Delta(Z)\right|. \tag{20}$$

Proof. To show the first inequality we apply Ruzsa's argument. For every $\mathbf{a} \in Y - \Delta(Z)$ choose the smallest element (in any linear order of Z) $z \in Z$ such that $\mathbf{a} = (y_1 - z,\dots,y_k - z)$ for some $(y_1,\dots,y_k) \in Y$. Next, observe that the function

$$(\mathbf{a},\mathbf{w},x) \mapsto (y_1 - x,\dots,y_k - x, z - x, w_1 - x,\dots,w_k - x),$$

where $\mathbf{w} = (w_1,\dots,w_k) \in W$ from $(Y-\Delta(Z))\times W\times X$ to $Y\times W\times Z - \Delta(X)$ is injective.

To obtain the second inequality consider the following matrix

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & -1 \\ 0 & 1 & 0 & \dots & 0 & -1 \\ 0 & 0 & 1 & \dots & 0 & -1 \\ \dots & \dots & \dots & \dots & \dots & \\ 0 & \dots & 0 & 0 & 1 & -1 \end{pmatrix}.$$

Clearly, $A_1\times\dots\times A_k - \Delta(B) = \mathbf{Im}(\mathbf{M}|_{A_1\times\dots\times A_k\times B})$. Further, non-degenerate transformations of lines does not change the cardinality of the image. Thus, subtracting the $(m+1)$th line, we obtain vectors of the form

$$(a_1 - a_{m+1},\dots,a_m - a_{m+1}, a_{m+1} - b,\dots,a_k - b),$$

which belong to $(A_1\times\dots\times A_m - \Delta(A_{m+1}))\times(A_{m+1}\times\dots\times A_k - \Delta(B))$.

To obtain (20) it is sufficient to show that

$$\big|Y\times Z-\Delta(X)\big|\leqslant\big|Y\times X-\Delta(Z)\big|.$$

But the map

$$(y_1-x,\dots,y_k-x,z-x)\mapsto(y_1-z,\dots,y_k-z,x-z),$$

where $(y_1,\dots,y_k)\in Y$, $x\in X$, $z\in Z$ is an injection. This completes the proof. □

Remark 8. The proof of the theorem above gives another way to obtain formula (9) of Lemma 3. Indeed for any $k\geqslant 2$ by (12) the following holds

$$|A|^{2k}\leqslant \mathsf{E}_k(A)\cdot\big|A^{k-1}-\Delta(A)\big|$$

and we just need to estimate $|A^{k-1}-\Delta(A)|$ in terms of the set $D:=A-A$. Such bounds were obtained in [32] (see Lemma 2.6) but here we use another arguments. The cardinality of the set $A^{k-1}-\Delta(A)$ equals the number of tuples

$$(a_1-a_2,a_2-a_3,\dots,a_{k-1}-a_k)=(x_1,\dots,x_{k-1})\in D^{k-1},$$

where $a_j\in A$, $j\in[k]$. Thus

$$\begin{aligned}\big|A^{k-1}-\Delta(A)\big|&\leqslant\sum_{x_1,\dots,x_{k-1}}\prod_{j=1}^{k-1}\prod_{l=0}^{k-1-j}D(x_j+x_{j+1}+\dots+x_{j+l})\\&\leqslant\sum_{x_1,\dots,x_{k-1}}D(x_1)\dots D(x_{k-1})D(x_1+\dots+x_{k-1})=\sigma_k(D)\end{aligned}$$

and the result follows.

As an immediate consequence of (18), (19) we get

$$\big|A^k-\Delta(A)\big||A|\leqslant\big|A^{k+1}+\Delta(A)\big|, \tag{21}$$

and

$$\big|A^k+\Delta(A)\big||A|\leqslant\big|A^k-\Delta(A)\big||A+A|.$$

In view of (12) we can formulate the following.

Corollary 9. *Let A and B be finite subsets of an abelian group. Then*

$$|A+B|\geqslant\frac{|A|^2|B|^{1/k}}{\mathsf{E}_k(A)^{1/k}}.$$

Let us also remark that the proof of Theorem 7 prompts to consider different matrices not necessary the matrix $\mathbf{M}$. The type of matrices we used appears naturally in studying E_k.

There is another way to prove estimate (19) in spirit of Lemma 2.4 and Corollary 2.5 from [32]. We recall this result.

Proposition 10. *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*

$$A_1 \times \dots \times A_k - \Delta(B) = \big\{(x_1, \dots, x_k)\colon\ B \cap (A_1 - x_1) \cap \dots \cap (A_k - x_k) \neq \emptyset\big\} \tag{22}$$

and

$$A_1 \times \dots \times A_k - \Delta(B) = \bigcup_{(x_1,\dots,x_m) \in A_1 \times \dots \times A_m - \Delta(B)} \big\{(x_1, \dots, x_m)\big\} \times \big(A_{m+1} \times \dots \times A_k - \Delta\big(B \cap (A_1 - x_1) \cap \dots \cap (A_m - x_m)\big)\big). \tag{23}$$

From (22) one can deduce another characterization of the set $A^k - \Delta(B)$

$$A^k - \Delta(B) = \big\{X \subseteq \mathbf{G}\colon\ |X| = k,\ B \nsubseteq \big((\mathbf{G} \setminus A) - X\big)\big\}.$$

Here we used X to denote a multiset and a corresponding sequence created from X. Using the characterization it is easy to prove, that if A is a subset of finite abelian group $\mathbf{G}$ then there is X, $|X| \sim \frac{N}{|A|} \cdot \log N$ such that $A + X = \mathbf{G}$. Indeed, let $A^c = \mathbf{G} \setminus A$, and $k \sim \frac{N}{|A|} \cdot \log N$. Consider

$$\big|\big(A^c\big)^k - \Delta\big(A^c\big)\big| \leqslant \big|A^c\big|^{k+1} = N^{k+1}\big(1 - |A|/N\big)^{k+1} < N^k.$$

Thus, there is a multiset X, $|X| = k$ such that $A^c \subseteq A - X$. Whence the set $-X \cup \{0\}$ has the required property.

Let $D_k(A)$, $S_k(A)$ stand for the cardinalities of $A^k - \Delta(A)$, $A^k + \Delta(A)$, respectively. Next result describes dependencies between $D_k(A)$, $S_k(A)$ for different k.

Proposition 11. *Let $n, m \geqslant 1$ be positive integers, and $A \subseteq \mathbf{G}$ be a finite set. Then*

$$D_n(A)|A|^m \leqslant D_{n+m}(A) \leqslant D_n(A)D_m(A), \tag{24}$$

and

$$S_n(A)|A|^m \leqslant S_{n+m}(A) \leqslant S_n(A) \cdot \min\big\{S_m(A), D_m(A)\big\}. \tag{25}$$

Finally, for $m \geqslant 2$, we have

$$D_n(A)|A|^m \leqslant S_{n+m}(A), \tag{26}$$

and for $m = 1$, $n \geqslant 2$, we get

$$D_{n-1}(A)|A|^2 \leqslant S_{n+1}(A). \tag{27}$$

Proof. The first inequality of (24) follows from (18). The second one is a consequence of (19) or Proposition 10. The first inequality of (25) follows from (18) and (20). To establish the second inequality of (25) we use Proposition 10. We have

$$S_{n+m}(A) = \sum_{(x_1,\dots,x_m) \in A^m + \Delta(A)} \big|A^n + \Delta\big(A \cap (x_1 - A) \cap \dots \cap (x_m - A)\big)\big|. \tag{28}$$

Trivially,

$$\bigl|A^n + \Delta\bigl(A\cap(x_1-A)\cap\dots\cap(x_m-A)\bigr)\bigr| \leqslant \min\bigl\{S_n(A), D_n(A)\bigr\}.$$

It remains to prove (26), (27). By (18) we have $|A^{n+1} - \Delta(B)| \geqslant D_n(A)|B|$ for every set B. Thus, using (28) once again, we get

$$S_{n+m}(A) \geqslant D_n(A)\cdot \sum_{(x_1,\dots,x_{m-1})\in A^{m-1}+\Delta(A)} \bigl|A\cap(x_1-A)\cap\dots\cap(x_{m-1}-A)\bigr| = D_n(A)|A|^m,$$

provided that $m\geqslant 2$. Similarly, if $m=1$, $n\geqslant 2$ then

$$S_{n+1}(A) \geqslant D_{n-1}(A)\cdot \sum_{x\in A+A} \bigl|A\cap(x-A)\bigr| = D_{n-1}(A)|A|^2.$$

This completes the proof. □

Remark 12. It is easy to see that all inequalities in Proposition 11 are sharp up to constant factors. For example, if $n,m\geqslant 2$ then one can consider A to be a multiplicative subgroup of $\mathbb{F}_p$ or a convex subset of $\mathbb{R}$. In this case $D_k, S_k \sim |A|^{k+1}$, for $k\geqslant 3$ and $|A|^3 \gg D_2,\ S_2 \gg |A|^3/\log|A|$ (see [27,28,32]) and the lower bounds of Proposition 11 attained for large n. If m, n are arbitrary then let A be an arithmetic progression in $\mathbb{Z}$ or a subspace of $\mathbb{Z}_p^n$. We know by (13) that $|A|^k \leqslant D_k \leqslant |A-A|^k$, $|A|^k \leqslant S_k \leqslant |A+A|^k$ hence all bounds in Proposition 11 are sharp. Nevertheless, if $A\subseteq\mathbb{Z}$, we have always $D_k, S_k \geqslant (k+1)|A|^k - O_k(|A|^{k-1})$, which is a consequence of the trivial inequality $|P+Q|\geqslant |P|+|Q|-1$, where $P,Q\subseteq\mathbb{Z}$ are arbitrary sets.

Proposition 11 allows us to introduce a hierarchy of basis of abelian groups, i.e. of sets B such that $B\pm B = \mathbf{G}$. For simplicity, if B is a basis let us write $B\oplus_k B$ and $B\ominus_k B$ for $B^k+\Delta(B)$ and $B^k-\Delta(B)$, respectively.

Definition 13. Let $k\geqslant 1$ be a positive integer. A subset B of an abelian group $\mathbf{G}$ is called *basis of depth k* if $B\ominus_k B = \mathbf{G}^k$.

It follows from Theorem 7 that if B is a basis of depth k of finite abelian group $\mathbf{G}$, then for every set $A\subseteq\mathbf{G}$

$$|B+A| \geqslant |A|^{\frac{1}{k+1}}|\mathbf{G}|^{\frac{k}{k+1}}. \tag{29}$$

An analogous inequality for sum bases will be given in Section 8.

Inequality (29) is trivial if $|B|\geqslant |A|^{\frac{1}{k+1}}|\mathbf{G}|^{\frac{k}{k+1}}$. In this situation one can use (24) of Proposition 11, which for any $m\geqslant k$ gives the following

$$|B+A| \geqslant |B|^{\frac{m-k}{m+1}}|A|^{\frac{1}{m+1}}|\mathbf{G}|^{\frac{k}{m+1}}. \tag{30}$$

Taking any one-element A in formula (29) we obtain, in particular, that $|B|\geqslant |\mathbf{G}|^{\frac{k}{k+1}}$ for any basis of depth k. It is easy to see, using Proposition 10 that every set with B, $|B|>(1-1/(k+1))|\mathbf{G}|$ is a basis of depth k and this inequality is sharp. If $S_1,\dots,S_k$ are any sets such that $S_1+\dots+S_k=\mathbf{G}$ then the set $\bigcup_{j=1}^k(\sum_{i\neq j}(S_i-S_i))$ is a basis of depth k (see Corollary 16 below, the construction can be found in [18]). Let us give another example. Using Weil's bounds for exponential sums we show that quadratic residuals in $\mathbb{Z}/p\mathbb{Z}$, for a prime p, is a basis of depth $(\frac{1}{2}+o(1))\log p$. Clearly, the bound is the best possible up to constants for subsets of $\mathbb{Z}/p\mathbb{Z}$ of the cardinality less than $p/2$.

Proposition 14. *Let p be a prime number, and let R be the set of quadratic residuals. Then R is the bases of depth k, where $k2^k < \sqrt{p}$.*

Proof. Clearly,

$$R(x) = \frac{1}{2}\left(1 + \left(\frac{x}{p}\right)\right),$$

where $\left(\frac{x}{p}\right)$ is the Legendre symbol. Put $\alpha_0 = 0$. For all distinct non-zero $\alpha_1, \dots, \alpha_k$, we have

$$\big|R \cap (R-\alpha_1) \cap \dots \cap (R-\alpha_k)\big| = \frac{1}{2^k}\sum_x \prod_{j=0}^{k}\left(1 + \left(\frac{x+\alpha_j}{p}\right)\right) \geqslant \frac{1}{2^k}\left(p - \sqrt{p}\cdot \sum_{j=2}^{k} jC_k^j\right)$$
$$\geqslant \frac{1}{2^k}\big(p - \sqrt{p}\cdot k2^k\big) > 0.$$

We used the well-known Weil bound for exponential sums with multiplicative characters (see e.g. [14]). By (22) in Proposition 10 we see that $R \ominus_k R = \mathbb{Z}_p^k$. □

Another consequence of Proposition 14 is that quadratic non-residuals Q (and, hence, quadratic residuals) have no completion of size smaller then $(\frac{1}{2} + o(1))\log p$, that is a set X such that $X + Q = \mathbb{Z}/p\mathbb{Z}$.

The next proposition is due to N.G. Moshchevitin.

Proposition 15. *Let k_1, k_2 be positive integers, and $X_1, \dots, X_{k_1}, Y$, $Z_1, \dots, Z_{k_2}, W$ be finite subsets of an abelian group. Then we have a bound*

$$\big|X_1 \times \dots \times X_{k_1} - \Delta(Y)\big|\big|Z_1 \times \dots \times Z_{k_2} - \Delta(W)\big|$$
$$\leqslant \big|(X_1 - W) \times \dots \times (X_{k_1} - W) \times (Y - Z_1) \times \dots \times (Y - Z_{k_2}) - \Delta(Y - W)\big|.$$

Proof. It is enough to observe that the map

$$(x_1 - y, \dots, x_{k_1} - y, z_1 - w, \dots, z_{k_2} - w)$$
$$\mapsto \big(x_1 - w - (y-w), \dots, x_{k_1} - w - (y-w), y - z_1 - (y-w), \dots, y - z_{k_2} - (y-w)\big)$$

where $x_j \in X_j$, $j \in [k_1]$, $y \in Y$, $z_j \in Z_j$, $j \in [k_2]$, $w \in W$ is injective. □

In particular, the difference and the sum of two bases of depths k_1 and k_2 is a basis of depth $k_1 + k_2$. Let us also formulate a simple identity, which is a consequence of Theorem 7.

Corollary 16. *Let $k \geqslant 2$ be a positive integer, and let $A_1, \dots, A_k$ be a subset of a finite abelian group $\mathbf{G}$. Then*

$$\big|A_1 \times \dots \times A_k - \Delta(\mathbf{G})\big| = |\mathbf{G}|\big|A_1 \times \dots \times A_{k-1} - \Delta(A_k)\big|. \tag{31}$$

Thus, B is a basis of depth k iff B is $(k+1)$-universal set (see [1]), i.e. a set that is for any $x_1, \dots, x_{k+1} \in \mathbf{G}$ there is $z \in \mathbf{G}$ such that $z + x_1, \dots, z + x_{k+1} \in B$. A series of very interesting examples of universal sets can be found in [18].

Finally, we also formulate an interesting consequence of the inequality (25).

Corollary 17. *Let $k > m \geqslant 1$ be integers and let $B \subseteq \mathbf{G}$ be a set such that $B \oplus_k B = \mathbf{G}^k$. Then B is a basis of depth m, that is $B \ominus_m B = \mathbf{G}^m$.*

An inverse theorem to Corollary 17 is related to a known problem: does there exist an integer n such that if $A - A = \mathbf{G}$ then $nA = \mathbf{G}$? It was answer in the negative in [12]. However, it is easy to see that such a constant exists provided A is a basis of sufficiently high depth.

Proposition 18. *Let B be a basis of depth k of a finite abelian group $\mathbf{G}$ of density δ. Then $nB = \mathbf{G}$ for every*

$$n \geqslant 3 + \frac{2}{\log(k+1)} \log\left(\frac{\log(1/\delta)}{\log((k+1)/2)}\right).$$

Proof. We will use an elementary fact that if $X, Y \subseteq G$ then there exists x such that

$$\big|(X+x) \cap Y\big| \leqslant |X||Y|/N. \tag{32}$$

Now prove that for every set $A \subseteq \mathbf{G}$ we have $|A+B| \geqslant \min((k+1)|A|/2, N/2)$. Indeed, applying iteratively (32), there exists a set S of size k such that $|A+S| \geqslant \min((k+1)|A|/2, N/2)$. Since $B \ominus_k B = \mathbf{G}^k$ it follows that there is $a \in B$ such that $S + a \subseteq B$, so that $|B+A| \geqslant \min((k+1)|A|/2, N/2)$. Therefore, for every $s \geqslant 1$

$$|sB| > \min\big(\big((k+1)/2\big)^s |B|, N/2\big). \tag{33}$$

On the other hand, using (29) iteratively, we get

$$|lB| \geqslant \delta^{\frac{1}{(k+1)^l}} N \tag{34}$$

for all positive integers l. Combining, (33), (34) and optimizing over s, l, we have for

$$t > \frac{1}{\ln(k+1)} + \frac{\log\ln(k+1)}{\log(k+1)} + \frac{1}{\log(k+1)} \log\left(\frac{\log(1/\delta)}{\log((k+1)/2)}\right)$$

that $2tA = \mathbf{G}$. $\square$

5. Croot–Sisask lemma

Croot and Sisask [8] proved the following remarkable result, which found many deep applications, see [24,25]. We formulate their result in a simple form.

Theorem 19 *(Croot–Sisask). Let A, B be subsets of a group and $k \in \mathbb{N}$. Suppose that $|A - A| \leqslant K|A|$. Then there exists $T \subseteq A$ such that $|T| \geqslant |A|/(2K)^k$ and*

$$\big\|(A * B)(x) - (A * B)(x+t)\big\|_2^2 \leqslant 8|A|^2|B|/k$$

for every $t \in T$.

We prove that if the energy $\mathsf{E}_k(A)$ is not much larger than $|A|^{k+1}/K^{k-1}$ then one can substantially improve the lower bound on size of the set of almost-periods T (provided that $\mathbf{G}$ is abelian).

Theorem 20. *Let A, B be subsets of an abelian group and $k \in \mathbb{N}$. Suppose that $|A-A| \leqslant K|A|$ and $\mathsf{E}_{2k+2}(A) = M|A|^{2k+3}/K^{2k+1}$. Then there exists $T \subseteq A-A$ such that $|T| \geqslant K|A|/(16M)$ and*

$$\big\|(A*B)(x) - (A*B)(x+t)\big\|_2^2 \leqslant 32|A|^2|B|/k$$

for every t belonging to a shift of T.

Proof. We choose uniformly at random a k-element sequence $X = (x_1, \dots, x_k)$, $x_i \in A$. As in the proof of the Croot–Sisask theorem we say that X *approximates* A if

$$\big\|(\mu_X * B)(x) - (A*B)(x)\big\|_2^2 \leqslant 2|A|^2|B|/k,$$

where $\mu_X(x) = X(x)\cdot|A|/k$ (by X we mean the characteristic function of the set $\{x_1, \dots, x_k\}$). Following Croot–Sisask argument we have

$$\mathbb{P}(X \text{ approximates } A) \geqslant 1/2. \tag{35}$$

For $s \in A^k - \Delta(A)$ let A'_s be the set of all $a \in A$ such that $s + \Delta(a) \subseteq A^k$ and $s + \Delta(a)$ approximates A. Then

$$\big\|(\mu_{\Delta(a)+s} * B)(x) - (A*B)(x)\big\|_2^2 \leqslant 2|A|^2|B|/k$$

for every s and $a \in A'_s$. Therefore, by the triangle inequality we have

$$\big\|(A*B)(x) - (A*B)(x+a)\big\|_2^2 \leqslant 8|A|^2|B|/k \tag{36}$$

for every a belonging to a shift of A'_s. By the Cauchy–Schwarz inequality

$$\big|A'_s\big|\big|A'_t\big| \leqslant \mathsf{E}\big(A'_s, A'_t\big)^{1/2}\big|A'_s - A'_t\big|^{1/2}.$$

Again using the Cauchy–Schwarz inequality and Lemma 1 we get

$$\Big(\sum_{s,t\in A^k-\Delta(A)} \big|A'_s\big|\big|A'_t\big|\Big)^2 \leqslant \mathsf{E}_{2k+2}(A) \sum_{s,t\in A^k-\Delta(A)} \big|A'_s - A'_t\big|.$$

By (35)

$$\sum_{s\in A^k-\Delta(A)} \big|A'_s\big| \geqslant (1/2)|A|^{k+1},$$

so that

$$(1/16)K^{2k+1}M^{-1}|A|^{2k+1} \leqslant \sum_{s,t\in A^k-\Delta(A)} \big|A'_s - A'_t\big| \leqslant \big|A^k - \Delta(A)\big|^2 \max\big|A'_s - A'_t\big|.$$

Thus, there exist s_0 and t_0 such that $|A'_{s_0} - A'_{t_0}| \geqslant K|A|/(16M)$. To finish the proof it is enough to use (36) for s_0 and t_0 and apply the triangle inequality. The assertion is satisfied for a shift of $A'_{s_0} - A'_{t_0}$. □

6. Small higher energies and the structure of sets

The aim of this section is to prove that small $\mathsf{E}_3(A)$ implies the existence of a large very structured subset of A. We make use of the following lemma (see [28]).

Lemma 21. *Let A be a subset of an abelian group, $P_* \subseteq A-A$ and $\sum_{s\in P_*}|A_s| = \eta|A|^2$, $\eta \in (0,1]$. Then*

$$\sum_{s\in P_*}|A \pm A_s| \geqslant \eta^2|A|^6\mathsf{E}_3^{-1}(A).$$

The next lemma is the well-known Balog–Szemerédi–Gowers theorem.

Lemma 22. *Let A and B be finite sets of an abelian group, and $|A| \geqslant |B|$. If $\mathsf{E}(A,B) = \alpha|A|^3$, then there exist sets $A' \subseteq A$ and $B' \subseteq B$ such that $|A'|, |B'| \gg \alpha|A|$ and*

$$\big|A'+B'\big| \ll \alpha^{-5}|A|.$$

For a set A denote by $P = P(A)$ the set of all elements in $A-A$ that have at least $|A|^2/(2|A-A|)$ representations.

Theorem 23. *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*

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

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

Proof. Put $D = A-A$ and let $P = P(A)$. Clearly, $M \geqslant 1$. Then

$$\sum_{s\in P}(A\circ A)(s) \geqslant \frac{1}{2}|A|^2 \quad \text{and} \quad \sum_{s\in P}(A\circ A)(s)^3 \geqslant \frac{1}{2}\mathsf{E}_3(A).$$

By the Hölder inequality

$$|A|^2 \ll \mathsf{E}_3(A)^{1/3}|P|^{2/3},$$

so that $|P| \gg |D|/M^{1/2}$.

By the Katz–Koester transform (see [15]), we have $A - A_s \subseteq D \cap (D+s)$. Using the Cauchy–Schwarz inequality and Lemma 21, we obtain

$$\mathsf{E}(D,P) = \sum_{s,s'\in P}\big|(D+s)\cap\big(D+s'\big)\big| \geqslant |D|^{-1}\Big(\sum_{s\in P}\big|D\cap(D+s)\big|\Big)^2 \tag{37}$$

$$\geqslant |D|^{-1}\Big(\sum_{s\in P}|A-A_s|\Big)^2 \gg |D|^3/M^2. \tag{38}$$

Hence by Lemma 22 there are sets $D' \subseteq D$, $P' \subseteq P$ such that $|D'| \gg M^{-2}|D|$, $|P'| \gg M^{-2}|P|$ and

$$\big|D'+P'\big| \ll M^{12}\big|D'\big|.$$

The Plünnecke–Ruzsa inequality (see e.g. [36]) yields

$$\big|nP' - mP'\big| \ll M^{12(n+m)}\big|D'\big| \ll M^{12(n+m)+5/2}\big|P'\big|, \tag{39}$$

for every $n, m \in \mathbb{N}$. By pigeonhole principle there is x such that

$$\big|(A-x)\cap P'\big| \gg \big|P'\big|/(2K) \gg |A|/M^{5/2}.$$

Put $A' = A \cap (P' - x)$. Thus, by (39) and the previous inequality, we get

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

for every $n, m \in \mathbb{N}$. □

Observe that if A' is a set given by Theorem 23 then

$$\frac{M|A|^4}{K^2} = \mathsf{E}_3(A) \geqslant \mathsf{E}_3\big(A'\big) \geqslant \frac{|A'|^6}{|A'-A'|^2},$$

hence

$$\big|A'-A'\big| \gg M^{-O(1)}K\big|A'\big|.$$

Therefore, by Theorem 23, we obtain

$$\big|\big(A'-A'\big)+\big(A'-A'\big)\big| \leqslant M^{O(1)}\big|A'-A'\big|.$$

Applying the Sanders theorem [24] for $A'-A'$, we obtain that $A'-A'$ is contained in a generalized arithmetic progression of dimension $M^{O(1)}$ and size $Ke^{M^{O(1)}}|A'|$. In particular, $4A'-4A'$ contains an arithmetic progressions of length $|A'|^{(\log M)^{-O(1)}}$.

Recall that a subset $\Lambda = \{\lambda_1, \dots, \lambda_t\}$ of a finite abelian group $\mathbf{G}$ is called *dissociated* if $\sum_{j=1}^t \varepsilon_j\lambda_j = 0$, where $\varepsilon_j \in \{0, -1, 1\}$ implies $\varepsilon_j = 0$, $j \in [t]$. For a set $Q \subseteq \mathbf{G}$ let $\dim(Q)$ denote the size of the largest dissociated subset of Q.

In [33] the following result was proved.

Theorem 24. *Let $\mathbf{G}$ be a finite abelian group, $A, B \subseteq \mathbf{G}$ be two sets, and $c \in (0, 1]$. Suppose $\mathsf{E}(A, B) \geqslant c|A||B|^2$; then there exists a set $B_1 \subseteq B$ such that $\dim(B_1) \ll c^{-1}\log|A|$ and*

$$\mathsf{E}(A, B_1) \geqslant 2^{-5}\mathsf{E}(A, B). \tag{40}$$

In particular, $|B_1| \geqslant 2^{-3}c^{1/2}|B|$. If $B = A$ then $\mathsf{E}(B_1) \geqslant 2^{-10}\mathsf{E}(A)$ and, consequently, $|B_1| \geqslant 2^{-4}c^{1/3}|A|$.

We supplement Theorem 23 with the following statement.

Corollary 25. *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 $|A_*| \gg |A|/M$ and*

$$\dim(A_*) \ll M^2\big(\log|A| + \log K\big).$$

Proof. By (37), we have

$$\mathsf{E}(D,P) \gg \frac{K^3|A|^3}{M^2}$$

and by Theorem 24 there exists $P_* \subseteq P$ with $\dim(P_*) \ll M^2(\log|A| + \log K)$ such that

$$|P_*|^2|D| \geqslant \mathsf{E}(D,P_*) \gg \frac{K^3|A|^3}{M^2}.$$

Thus $|P_*| \gg K|A|/M$. Again for some x we have $|A\cap(P_*-x)| \gg |P_*|/K \gg |A|/M$, so that the assertion follows for $A_* = A\cap(P_*-x)$. $\square$

7. Bounding energies in terms of $|AA|$

Let $A \subseteq \mathbb{R}$ and let $AA = \{ab\colon\ a,b\in A\}$ and $A/A = \{a/b\colon\ a,b\in A,\ \ b\neq 0\}$. Denote by $\mathsf{E}^{\times}_k(A)$ the multiplicative energy of order k. Solymosi [34] using ingenious argument proved that

$$\mathsf{E}^{\times}(A) \ll |A+A|^2\log|A|$$

for every set of real numbers A.

In this section we prove some sum-product type estimates. Our basic tool is the following Lemma 27, which is a generalization of Lemma 2.6 in [28] and an improvement of Lemma 4.1 in [19]. We will make use of the Szemerédi–Trotter theorem [35]. We call a set $\mathcal{L}$ of continuous plane curve a *pseudo-line system* if any two members of $\mathcal{L}$ share at most one point in common.

Theorem 26. *(See [35].) Let $\mathcal{P}$ be a set of points and let $\mathcal{L}$ be a pseudo-line system. Then*

$$\mathcal{I}(\mathcal{P},\mathcal{L}) = \big|\big\{(p,l)\in\mathcal{P}\times\mathcal{L}\colon\ p\in l\big\}\big| \ll |\mathcal{P}|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{P}| + |\mathcal{L}|.$$

Lemma 27. *Let A, B, C be subsets of reals and let f be a strictly convex function. Suppose that $|A+B| \leqslant M|B|$. Then*

$$\big|\big\{x\in f(A)+C\colon\ \big(f(A)*C\big)(x) \geqslant \tau\big\}\big| \ll (M\log M)^2\frac{|B||C|^2}{\tau^3}.$$

Proof. Obviously, it is enough to prove the assertion for $1 \ll \tau \leqslant \min\{|A|,|C|\}$. For real numbers α,β put $l_{\alpha,\beta} = \{(q,f(q))\colon\ q\in A\} + (\alpha,\beta)$. We consider the pseudo-line system $\mathcal{L} = \{l_{\alpha,\beta}\colon\ \alpha\in B,\ \ \beta\in C\}$, and the set of points $\mathcal{P} = (A+B)\times(f(A)+C)$. Let $\mathcal{P}_\tau$ be the set of points of $\mathcal{P}$ belonging to at least τ curves from $\mathcal{L}$. Clearly, $|\mathcal{L}| = |B||C|$ and $\mathcal{I}(\mathcal{P}_\tau,\mathcal{L}) \geqslant \tau|\mathcal{P}_\tau|$.

By Szemerédi–Trotter's theorem we have

$$\tau|\mathcal{P}_\tau| \ll \big(|\mathcal{P}_\tau||B||C|\big)^{2/3} + |B||C| + |\mathcal{P}_\tau|, \tag{41}$$

so that $|\mathcal{P}_\tau| \ll |B|^2|C|^2/\tau^3$.

Now suppose that $(f(A)*C)(x) \geqslant \tau$. Let X be the set of all $a\in A$ such that there exists $c\in C$ with $f(a)+c = x$. Clearly $|X| = (f(A)*C)(x)$ and

$$\sum_{s\in X+B}(X*B)(s) = |X||B|,$$

so that there is $0 \leqslant i = i(x) \leqslant \log M$ such that

$$\sum_{2^{i-1}\tau/M \leqslant (X*B)(s) \leqslant 2^i\tau/M} (X*B)(s) \geqslant \frac{\tau|B|}{2\log(2M)}.$$

Hence each x with $(f(A)*C)(x) \geqslant \tau$ gives at least $M|B|/2^{i(x)+1}\log(2M)$ points $p \in \mathcal{P}_{\tau 2^{i(x)-1}/M}$ having the same ordinate. Furthermore, for at least $|\{x:\ (f(A)*C)(x) \geqslant \tau\}|/\log(2M)$ elements x we have the same choice for $i(x) = i_0$. Thus, we have

$$\frac{M|B|}{2^{i_0}\log M}\,\frac{|\{x:\ (f(A)*C)(x) \geqslant \tau\}|}{\log M} \ll |\mathcal{P}_{2^{i_0-1}\tau/M}|.$$

In view of

$$|\mathcal{P}_{2^{i_0-1}\tau/M}| \ll M^3|B|^2|C|^2/2^{3i_0}\tau^3,$$

we infer that

$$\big|\big\{x:\ \big(f(A)*C\big)(x) \geqslant \tau\big\}\big| \ll (M\log M)^2\,\frac{|B||C|^2}{\tau^3}. \qquad \square$$

Order elements $s \in A-A$ such that $(A\circ A)(s_1) \geqslant (A\circ A)(s_2) \geqslant \dots \geqslant (A\circ A)(s_t)$, $t = |A-A|$. Taking in Lemma 27, $A = B := \log A$ (if necessary we consider A_+ or $(-A_-)$), $C := A$ and $f = \exp$, we obtain the following bound.

Corollary 28. *Suppose that $A \subseteq \mathbb{R}$ and $|AA| \leqslant M|A|$. Then for every $r \geqslant 1$ we have*

$$(A\circ A)(s_r) \ll (M\log M)^{2/3}|A|/r^{1/3}.$$

Thus, we have

$$\mathsf{E}(A) \ll |AA||A|^{3/2}\log|A|$$

and

$$\mathsf{E}_k(A) \ll |AA|^{2k/3}|A|^{k/3}\big(\log|A|\big)^{O(k)}$$

for every $k \geqslant 3$. One can improve the above bounds for a dense subset of A provided that $\mathsf{E}^{\times}_3(A)$ is small.

Corollary 29. *Suppose that $A \subseteq \mathbb{R}$ and $\mathsf{E}^{\times}_3(A) \leqslant M|A|^6/|A/A|^2$. Then there exists a set $A' \subseteq A$ such that $|A'| \geqslant |A|/M^{O(1)}$ and*

$$\mathsf{E}\big(A'\big) \ll M^{O(1)}|AA|^{1/2}|A|^2,$$

and $\mathsf{E}_k(A') \ll M^{O(k)}|AA|^{k/3}|A|^{2k/3}(\log|A|)^{O(k)}$ for every $k \geqslant 3$.

Proof. By Theorem 23 there is a set $A' \subseteq A$ such that $|A'| \geqslant |A|/M^{O(1)}$ and $|A'A'A'| \leqslant M^{O(1)}|A/A|$. Furthermore,

$$M^{O(1)}\frac{|A|^4}{|A/A|} \geqslant \mathsf{E}^{\times}(A) \geqslant \mathsf{E}^{\times}(A') \geqslant \frac{|A'|^4}{|A'A'|},$$

so that $|A'A'| \geqslant |A/A|/M^{O(1)}$ and $|A'A'A'| \leqslant M^{O(1)}|A'A'|$. We apply Lemma 27 with $A = \log A'$ (if necessary we consider A'_+ or $(-A'_-)$), $B = \log A'A'$, $C = A$, $f = \exp$. Thus

$$\big|\{x:\ (A' * A')(x) \geqslant \tau\}\big| \ll (M\log M)^{O(1)}\frac{|A'A'||A|^2}{\tau^3},$$

and the assertion follows. □

In [34] Solymosi proved the inequality $|kA||AA|^{2(k-1)} \gg_k |A|^{2k-1/k}$, $k \geqslant 2$, which is useful if $|AA|$ is small. We improve this estimate applying Lemma 27.

Corollary 30. *Suppose that $X \subseteq \mathbb{R}$ then*

$$|kX|\big(|XX|\log|X|\big)^{2-2^{-k+2}} \gg_k |X|^{4-3\cdot 2^{-k+1}}.$$

Proof. We use induction on $k \geqslant 2$. For $k = 2$ the assertion follows from Corollary 28. Suppose that $k > 2$. We apply Lemma 27 with $A = B = \log X$ and $C = (k-1)X$ and $f = \exp$ (if necessary we consider X_+ or $(-X_-)$). Put

$$H = \frac{\mathsf{E}(X,(k-1)X)}{2|X||(k-1)X|},$$

then

$$\mathsf{E}\big(X,(k-1)X\big) \ll \sum_{j\geqslant 1} H^2 2^{2j}\frac{|XX|^2|(k-1)X|^2\log^2|X|}{|X|H^3 2^{3j}} \ll \frac{|XX|^2|(k-1)X|^2\log^2|X|}{|X|H},$$

so that

$$\mathsf{E}\big(X,(k-1)X\big) \ll |XX|\big|(k-1)X\big|^{3/2}\log|X|.$$

Therefore

$$|kX| \gg \frac{|X|^2|(k-1)X|^{1/2}}{|XX|\log|X|} \gg_k \frac{|X|^{4-3\cdot 2^{-k+1}}}{(|XX|\log|X|)^{2-2^{-k+2}}}$$

and the proof is completed. □

We finish this section with some remarks concerning a sum-product kind result of Balog [3]. He proved that for every finite sets A, B, C, D of reals we have

$$|AC + A||BC + B| \gg |A||B||C|$$

and

$$|AC + AD||BC + BD| \gg |B/A||C||D|,$$

so, in particular, $|AA + A| \gg |A|^{3/2}$ and $|AA + AA| \gg |A||A/A|^{1/2}$. However, carefully following his argument one can see that actually he obtained stronger inequalities

$$\big|(A \times B) \cdot \Delta(C) + A \times B\big| \gg |A||B||C|$$

and

$$\big|(A \times B) \cdot \Delta(C) + (A \times B) \cdot \Delta(D)\big| \gg |B/A||C||D|.$$

Assume for simplicity that $A = B = C$ and put $A_q^\times = A \cap Aq^{-1}$.

Theorem 31. *Let $A \subseteq \mathbb{R}$ be a finite set and suppose that $\mathsf{E}_3^\times(A) = M|A|^6/|A/A|^2$. Then*

$$|AA + A| \gg |A||A/A|^{1/2}M^{-1/2}$$

and

$$|AA + AA| \gg |A/A|^{3/2}M^{-1}.$$

Proof. We will closely follow Balog's proof, so we only sketch the argument. Let l_i be the line $y = q_i x$. Thus, $(x, y) \in l_i \cap A^2$ if and only if $x \in A_q^\times$. Let $q_1, \dots, q_n \in A/A$ be such that $q_1 < q_2 < \dots < q_n$ and $|A_{q_i}^\times| \geqslant |A|^2/2|A/A|$, so that $\sum_i |A_{q_i}^\times| \geqslant \frac{1}{2}|A|^2$. We multiply all points of A^2 lying on the line l_i by $\Delta(A)$, so we obtain $|AA_{q_i}^\times|$ points still belonging to the line l_i and then we consider sumset of the resulting set with $l_{i+1} \cap A^2$. Clearly, we obtain $|AA_{q_i}^\times||A_{q_{i+1}}^\times|$ points from the set $(AA + A)^2$ lying between the lines l_i and l_{i+1}. Therefore, we have

$$|AA + A|^2 \geqslant \sum_{i=1}^{n-1} \big|A_{q_i}^\times\big|\big|AA_{q_{i+1}}^\times\big| \gg \frac{|A|^2}{|A/A|} \sum_{i=1}^{n-1} \big|AA_{q_{i+1}}^\times\big|,$$

and by Lemma 21

$$|AA + A|^2 \gg \frac{|A|^8}{|A/A|\mathsf{E}_3^\times(A)}.$$

To prove the second assertion let $q_1, \dots, q_n \in A/A$ be such that $q_1 < q_2 < \dots < q_n$ and $|AA_{q_i}^\times| \geqslant |A/A|/2M$. We multiply all points of $l_i \cap A^2$ and $l_{i+1} \cap A^2$ by $\Delta(A)$ and the we consider their sumset. We obtain $|AA_{q_{i+1}}^\times||AA_{q_i}^\times|$ points that belong to $(AA + AA)^2$. By Lemma 21 we have

$$\sum_q \big|AA_q^\times\big| \geqslant \frac{|A|^6}{\mathsf{E}_3^\times(A)} = \frac{|A/A|^2}{M}$$

so that $n \gg |A/A|/M$. Therefore, it follows that

$$|AA+AA|^2 \geqslant \sum_j \bigl|AA^{\times}_{q_j}\bigr|\bigl|AA^{\times}_{q_{j+1}}\bigr| \gg \frac{|A/A|^3}{M^2},$$

which completes the proof. □

Remark 32. By Proposition 10, we have

$$\sum_{q\in A/A} \bigl|AA^{\times}_q\bigr| = \bigl|(A\times A)\cdot\Delta^*(A)\bigr|,$$

where $\Delta^*(A) = \{(a,a^{-1}):\ a\in A\}$. Thus by the averaging argument, one gets

$$\sum_{q\in A/A:\ |AA^{\times}_q|\geqslant 2^{-1}|(A\times A)\cdot\Delta^*(A)|/|A/A|} \bigl|AA^{\times}_q\bigr| \geqslant 2^{-1}\bigl|(A\times A)\cdot\Delta^*(A)\bigr|. \tag{42}$$

The proof of Theorem 31 and formula (42) give another inequality on, namely

$$|AA+AA| \gg \frac{|(A\times A)\cdot\Delta^*(A)|}{|A/A|^{1/2}}.$$

We also formulate another consequence of Solymosi's bound for multiplicative energy.

Corollary 33. *Let $A\subseteq\mathbb{R}$ be a finite set and suppose that $\mathsf{E}_3(A) = M|A|^6/|A-A|^2$. Then*

$$\bigl|A(A+A)\bigr| \gg \frac{|A|^2}{M^{O(1)}\log|A|}.$$

Proof. By Theorem 23 there is a set $A'\subseteq A$ such that $|A'|\gg|A|/M^{O(1)}$ and $|4A'|\ll M^{O(1)}|A-A|$. Moreover, observe that

$$\frac{|A'|^4}{|A'+A'|} \leqslant \mathsf{E}\bigl(A'\bigr) \leqslant \mathsf{E}(A) \leqslant \frac{M^{1/2}|A|^4}{|A-A|},$$

so that $|A'+A'|\geqslant|A-A|/M^{O(1)}$ and $|4A'|\ll M^{O(1)}|A'+A'|$. The required estimate follows now from a general version of Solymosi's result

$$\mathsf{E}^{\times}\bigl(A',A'+A'\bigr) \leqslant \bigl|A'+A'\bigr|\bigl|4A'\bigr|\log|A|$$

and the trivial estimate $\mathsf{E}^{\times}(A',A'+A')\gg|A'|^2|A'+A'|^2/|A'(A'+A')|$. □

8. Higher energies, eigenvalues and the magnification ratios

Let $A,B\subseteq\mathbf{G}$ be two finite sets. The magnification ratio $R_B[A]$ of the pair (A,B) (see e.g. [36]) is defined by

$$R_B[A] = \min_{\emptyset\neq Z\subseteq A} \frac{|B+Z|}{|Z|}. \tag{43}$$

We simply write $R[A]$ for $R_A[A]$. Petridis [20] obtained an amazingly short proof of the following fundamental theorem.

Theorem 34. *Let $A \subseteq \mathbf{G}$ be a finite set, and n, m be positive integers. Then*

$$|nA - mA| \leqslant R^{n+m}[A] \cdot |A|.$$

Another beautiful result (which implies Theorem 34) was proven also by Petridis [20].

Theorem 35. *For any A, B, C, we have*

$$|B + C + X| \leqslant R_B[A] \cdot |C + X|,$$

where $X \subseteq A$ and $|B + X| = R_B[A]|X|$.

For a set $B \subseteq \mathbf{G}^k$ define

$$R_B[A] = \min_{\emptyset \neq Z \subseteq A} \frac{|B + \Delta(Z)|}{|Z|}.$$

In the next two results we assume that $X \subseteq A$ is such that $|B + \Delta(X)| = R_B[A]|X|$. It is easy to see that Petridis argument can be adopted to higher dimensional sumsets, giving a generalization of Theorem 35.

Theorem 36. *Let $A \subseteq \mathbf{G}$ and $B \subseteq \mathbf{G}^k$. Then for any $C \subseteq \mathbf{G}$, we have*

$$\big|B + \Delta(C + X)\big| \leqslant R_B[A] \cdot |C + X|.$$

A consequence of Theorem 36, we obtain a generalization of the sum version of the triangle inequality (see, e.g. [7]).

Corollary 37. *Let k be a positive integer, $A, C \subseteq \mathbf{G}$ and $B \subseteq \mathbf{G}^k$ be finite sets. Then*

$$|A|\big|B + \Delta(C)\big| \leqslant \big|B + \Delta(A)\big||A + C|.$$

Proof. Using Theorem 36, we have

$$\big|B + \Delta(C)\big| \leqslant \big|B + \Delta(C + X)\big| \leqslant R_B[A] \cdot |C + X| \leqslant \frac{|B + \Delta(A)|}{|A|}|A + C|$$

and the result follows. □

Thus, we have the following sum-bases analog of inequality (29).

Corollary 38. *Let k be a positive integer, and $B \oplus_k B = \mathbf{G}^k$. Then for any set $A \subseteq \mathbf{G}$, we have*

$$|B + A| \geqslant |A|^{\frac{1}{k+1}}|\mathbf{G}|^{\frac{k}{k+1}}.$$

For an integer $k \geqslant 1$ define

$$R_B^{(k)}[A] = \min_{\emptyset \neq Z \subseteq A} \frac{|B^k + \Delta(Z)|}{|Z|}, \tag{44}$$

where $A, B \subseteq \mathbf{G}$. So, $R_B^{(1)}[A] = R_B[A]$. The aim of this section is to obtain *lower* bounds for $R_B^{(k)}[A]$ in terms of the energies $\mathsf{E}_{2k+1}(A, B)$. We make use of the singular-value decomposition lemma (see e.g. [11]).

Lemma 39. *Let n, m be two positive integers, $n \leqslant m$, and let X, Y be sets of cardinalities n and m, respectively. Let also $\mathbf{M} = \mathbf{M}(x, y)$, $x \in X$, $y \in Y$, be $n \times m$ real matrix. Then there are functions $u_j : X \to \mathbb{R}$, $v_j : Y \to \mathbb{R}$, and nonnegative numbers λ_j such that*

$$\mathbf{M}(x, y) = \sum_{j=1}^{n} \lambda_j u_j(x) v_j(y), \tag{45}$$

where (u_j), $j \in [n]$, and (v_j), $j \in [n]$ form two orthonormal sequences, and

$$\lambda_1 = \max_{w \neq 0} \frac{\|\mathbf{M}w\|_2}{\|w\|_2}, \quad \lambda_2 = \max_{w \neq 0,\, w \perp u_1} \frac{\|\mathbf{M}w\|_2}{\|w\|_2}, \quad \ldots, \quad \lambda_n = \max_{w \neq 0,\, w \perp u_1, \ldots, w \perp u_{n-1}} \frac{\|\mathbf{M}w\|_2}{\|w\|_2}. \tag{46}$$

Next corollary collects further properties of singular values λ_j and vectors u_i, v_j, which we shall use in the course of the proof of the main result.

Corollary 40. *With the notation of the previous lemma, we have*:

- $\mathbf{M}u_j = \lambda_j v_j$, $j \in [n]$.
- *The numbers λ_j^2 and the vectors u_j are all eigenvalues and eigenvectors of the matrix $\mathbf{M}^*\mathbf{M}$.*
- *The numbers λ_j^2 and the vectors v_j form n eigenvalues and eigenvectors of the matrix $\mathbf{M}\mathbf{M}^*$. Another $(m - n)$ eigenvalues of $\mathbf{M}\mathbf{M}^*$ equal zero.*
- *We have $\sum_{j=1}^{n} \lambda_j^2 = \sum_{x,y} \mathbf{M}^2(x, y)$, and*

$$\sum_{j=1}^{n} \lambda_j^4 = \sum_{x,x'} \left| \sum_{y} \mathbf{M}(x, y)\mathbf{M}\big(x', y\big) \right|^2. \tag{47}$$

Proof. The first and the last properties follow directly from Lemma 39. To obtain the second and the third statements let us note that

$$\big(\mathbf{M}^*\mathbf{M}\big)(x, y) = \sum_{j=1}^{n} \lambda_j^2 u_j(x) u_j(y)$$

and similarly for $\mathbf{M}\mathbf{M}^*$. Thus, by the first formula of the fourth statement, all another eigenvalues of nonnegative definite matrix $\mathbf{M}\mathbf{M}^*$ equal zero. □

The quantity (47) is called the *rectangular norm* of $\mathbf{M}$. We denote it by $\|\mathbf{M}\|_\square^4$. Further properties of λ_j, u_i, v_j can be found in [11].

Let $k \geqslant 1$ be a positive integer, $A, B \subseteq \mathbf{G}$ be finite sets, and put $X = B^k - \Delta(A)$, $Y = A$. Clearly, $|X| \geqslant |Y|$. Define the matrix

$$\mathbf{M}(x, y) = \mathbf{M}_k^{A,B}(x, y) = A(y)B(y + x_1) \ldots B(y + x_k),$$

where $x = (x_1, \ldots, x_k) \in X$, $y \in Y$. If $y \in Y$ is fixed then $x = (x_1, \ldots, x_k)$ runs over $B^k - \Delta(y)$, i.e. over the set of cardinality $|B|^k$. If $x = (x_1, \ldots, x_k) \in X$ is fixed then y belongs to the set $A \cap (B - x_1) \cap \cdots \cap$

$(B - x_k)$. Denote by $\lambda_j = \lambda_j(A, B, k)$, $j \in [|A|]$ the singular values of the matrix $\mathbf{M}$. By Corollary 40, we have

$$\sum_{j=1}^{|A|} \lambda_j^2 = |A||B|^k, \tag{48}$$

and

$$\sum_{j=1}^{|A|} \lambda_j^4 = \mathsf{E}_{2k+1}(A, B) \tag{49}$$

because of

$$\|\mathbf{M}\|_\square^4 = \sum_{y,y'} A(y)A(y') \sum_{x_1,\dots,x_k} \sum_{x'_1,\dots,x'_k} B(y+x_1)\dots B(y+x_k)\cdot B(y+x'_1)\dots B(y+x'_k)$$
$$\times B(y'+x_1)\dots B(y'+x_k)\cdot B(y'+x'_1)\dots B(y'+x'_k) = \mathsf{E}_{2k+1}(A, B).$$

We make use of some operators, which were introduced in [31].

Definition 41. Let φ, ψ be two complex functions. By T^φ_ψ denote the following operator on the space of functions $\mathbf{G}^\mathbb{C}$

$$\left(\mathrm{T}^\varphi_\psi f\right)(x) = \psi(x)\left(\widehat{\varphi^c} * f\right)(x), \tag{50}$$

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

Let $E \subseteq \mathbf{G}$ be a set. Denote by $\bar{\mathrm{T}}^\varphi_E$ the restriction of operator T^φ_E onto the space of the functions with supports on E. It was shown in [31], in particular, that operators T^φ_E and $\bar{\mathrm{T}}^\varphi_E$ have the same non-zero eigenvalues. If φ is a real function then the operator $\bar{\mathrm{T}}^\varphi_E$ is symmetric. If φ is a nonnegative function then the operator is nonnegative definite. The action of $\bar{\mathrm{T}}^\varphi_E$ can be written as

$$\left\langle \bar{\mathrm{T}}^\varphi_E u, v\right\rangle = \sum_x \left(\widehat{\varphi^c} * u\right)(x)\bar{v}(x) = \sum_x \varphi(x)\widehat{u}(x)\overline{\widehat{v}(x)}, \tag{51}$$

where u, v are arbitrary functions such that $\operatorname{supp} u, \operatorname{supp} v \subseteq E$. Further properties of such operators can be found in [31].

Using Lemma 39 and the definitions above we can give another characterization of singular values λ_j. We express this in the next proposition.

Proposition 42. *We have*

$$\lambda_1^2 = \max_{\|w\|_2=1,\ \operatorname{supp} w\subseteq A} \sum_s (w\circ w)(s)(B\circ B)(s)^k,$$

$$\lambda_2^2 = \max_{\substack{\|w\|_2=1,\ \operatorname{supp} w\subseteq A,\\ w\perp w_1}} \sum_s (w\circ w)(s)(B\circ B)(s)^k,$$

$$\dots$$

$$\lambda_{|A|}^2 = \max_{\substack{\|w\|_2=1,\ \operatorname{supp} w\subseteq A,\\ w\perp w_1,\dots,w\perp w_{|A|-1}}} \sum_s (w\circ w)(s)(B\circ B)(s)^k, \tag{52}$$

where $w_1,\dots,w_{|A|}$ are eigenvectors of $\mathbf{M}^*\mathbf{M}$. In particular, $\lambda_j^2(A,B,k)=\lambda_j^2(\pm A,\pm B,k)$, $j\in[|A|]$. Furthermore, if $\mathbf{G}$ is a finite group, then λ_j^2 coincide with eigenvalues of the operator $\bar{\mathrm{T}}_A^{\varphi}$ with $\varphi(x)=\frac{1}{|\mathbf{G}|}((B\circ B)^k)\widehat{\ }(x)$.

Proof. For $x=(x_1,\dots,x_k)\in B^k$ and an arbitrary function w, $\operatorname{supp} w\subseteq A$, we have

$$\begin{aligned}\|\mathbf{M}w\|_2^2 &= \sum_{x_1,\dots,x_k}\left|\sum_y \mathbf{M}(x,y)w(y)\right|^2\\ &= \sum_{x_1,\dots,x_k}\sum_{y,y'} w(y)w(y')B(y+x_1)\dots B(y+x_k)\cdot B(y'+x_1)\dots B(y'+x_k)\\ &= \sum_s (w\circ w)(s)(B\circ B)(s)^k,\end{aligned}$$

which gives (52). Further, by the obtained formula and the fact $(C^c\circ C^c)(x)^k=(C\circ C)(x)^k$ for any set $C\subseteq\mathbf{G}$, we get $\lambda_j^2(A,B,k)=\lambda_j^2(\pm A,\pm B,k)$, $j\in[|A|]$. Finally, the last assertion easily follows from (51). □

Thus, taking $w(x)=A(x)/|A|^{1/2}$, we obtain

$$\lambda_1^2 \geqslant \frac{\mathsf{E}_{k+1}(A,B)}{|A|}. \tag{53}$$

Note also the function φ above satisfies $\varphi^c(x)=\varphi(x)$ and the following holds $((B\circ B)^k)^c(x)=(B\circ B)^k(x)$.

We are in position to prove a lower bound for $R_B^{(k)}[A]$ and even for more general quantities (see estimate (56)) in terms of the energies $\mathsf{E}_{2k+1}(A,B)$.

Theorem 43. *Let $A,B\subseteq\mathbf{G}$ be sets, and $k\geqslant 1$ be a positive integer. Then*

$$R_B^{(k)}[A] \geqslant \frac{|B|^{2k}}{\lambda_1^2(A,B,k)}, \tag{54}$$

and

$$R_B^{(k)}[A] \geqslant \frac{|B|^{2k}}{\mathsf{E}_{2k+1}^{1/2}(A,B)}. \tag{55}$$

Moreover, suppose that $A_1\subseteq A$ is a set and $B^{(y)}\subseteq B^k$, $y\in A_1$ is an arbitrary family of sets. Then

$$\left|\bigcup_{y\in A_1}\left(B^{(y)}\pm\Delta(y)\right)\right| \geqslant \frac{(\sum_{y\in A_1}|B^{(y)}|)^2}{\mathsf{E}_{k+1}(A,B)}. \tag{56}$$

Proof. By the definition of the matrix $\mathbf{M}$, we see that for every nonempty $Z \subseteq A$ we have

$$\sigma := \langle \mathbf{M}Z, B^k - \Delta(Z)\rangle = \sum_{x,y} \mathbf{M}(x,y)Z(y)\big(B^k - \Delta(Z)\big)(x) = |Z||B|^k. \tag{57}$$

Using the extremal property of λ_1, we get

$$\sigma \leqslant \lambda_1 |Z|^{1/2} \big|B^k - \Delta(Z)\big|^{1/2}.$$

Thus

$$\frac{|B|^{2k}}{\lambda_1^2} \leqslant \frac{|B^k - \Delta(X)|}{|X|} = R_B^{(k)}[-A],$$

where $X \subseteq A$ is a set that achieves the minimum in (44). By Proposition 42, $\lambda_j^2(A,B,k) = \lambda_j^2(\pm A, \pm B, k)$, for all $j \in [|A|]$, which implies (54). Finally, (55) follows from (49).

To prove (56) it is enough to notice that by (11)

$$\left|\bigcup_{y\in A_1} \big(B^{(y)} \pm \Delta(y)\big)\right| \geqslant \frac{(\sum_{y\in A_1} |B^{(y)}|)^2}{\mathsf{E}(\Delta(A), B^k)} = \frac{(\sum_{y\in A_1} |B^{(y)}|)^2}{\mathsf{E}_{k+1}(A,B)}.$$

This completes the proof. □

Observe that from (55) it follows that for every $A_1, A_2 \subseteq A$ we have

$$|A_1 \pm A_2| \geqslant \frac{|A_2|^{2/k}|A_1|^2}{\mathsf{E}_{k+1}^{1/k}(A_1,A_2)} \geqslant \frac{|A_2|^{2/k}|A_1|^2}{\mathsf{E}_{k+1}^{1/k}(A)},$$

for every $k \geqslant 1$.

The theorem above implies some results for sets with small higher energy. For example, multiplicative subgroups $\mathbb{Z}/p\mathbb{Z}$, convex subsets of $\mathbb{R}$ (i.e. sets $A = \{a_1, \dots, a_n\}_<$ such that $a_i - a_{i-1} < a_{i+1} - a_i$ for every $2 \leqslant i \leqslant n-1$). Another examples are provided by subsets of $\mathbb{R}$ with small product sets (see Section 7). We consider here just the case of multiplicative subgroups.

Corollary 44. *Let p be a prime number. Suppose that Γ is a multiplicative subgroup of $\mathbb{Z}/p\mathbb{Z}$ with $|\Gamma| = O(p^{2/3})$. Then for every set $\Gamma' \subseteq \Gamma$, we have*

$$\big|\Gamma + \Gamma'\big| \gg \big|\Gamma'\big| \cdot \left(\frac{|\Gamma|}{\log|\Gamma|}\right)^{1/2}. \tag{58}$$

Furthermore, for every $k \geqslant 2$, we get

$$R_\Gamma^{(k)}[\Gamma] \gg |\Gamma|^{k-1/2}.$$

Proof. Indeed, by Lemma 3.3 in [27], we have $\mathsf{E}_3(\Gamma) = O(|\Gamma|^3 \log|\Gamma|)$, and $\mathsf{E}_l(\Gamma) = O(|\Gamma|^l)$, for $l \geqslant 4$. Now the assertion follows directly from (55). □

We show that the bounds in Corollary 44 can be improved for multiplicative subgroups. It turns out that in this case we know all singular values λ_j^2 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. Denote by t the cardinality of Γ, and put $n = (q-1)/t$. Let also g be a primitive root, then $\Gamma = \{g^{nl}\}_{l=0,1,\dots,t-1}$. Let $\chi_\alpha(x)$, $\alpha \in [t]$ be the orthogonal family of multiplicative characters on Γ, that is

$$\chi_\alpha(x) = \Gamma(x) e\left(\frac{\alpha l}{t}\right), \quad x = g^{nl},\ 0 \leqslant l < t.$$

Proposition 45. *Let $\Gamma \subseteq \mathbb{F}_q$ be a multiplicative subgroup, and let φ be a Γ-invariant function. Then the functions $\chi_\alpha(x)$ are eigenfunctions of the operator $\bar{\mathrm{T}}^{\varphi}_{\Gamma}$. If φ has nonnegative Fourier transform then $\mathsf{E}_{k+1}(\Gamma, \widehat{\varphi^c})/(|\Gamma|q)$ is the maximal eigenvalue corresponding with the eigenfunction $\Gamma(x)$. Furthermore, for any Γ-invariant function ψ, $\psi(x) = \psi(-x)$, $\widehat{\psi}(x) \geqslant 0$ and an arbitrary real function u with support on Γ, we have*

$$\sum_x \psi(x)(u \circ u)(x) \geqslant |\Gamma|^{-2} \left|\sum_{x\in\Gamma} u(x)\right|^2 \cdot \sum_x \psi(x)(\Gamma \circ \Gamma)(x). \tag{59}$$

Proof. We have to show that

$$\mu f(x) = \Gamma(x)\big(\widehat{\varphi^c} * f\big)(x), \quad \mu \in \mathbb{R}$$

for $f(x) = \chi_\alpha(x)$. By the assumption $\varphi(x)$ is a Γ-invariant function, whence so is $\widehat{\varphi^c}$. Thus, for every $\gamma \in \Gamma$, we have

$$\begin{aligned}\big(\widehat{\varphi^c} * f\big)(\gamma) &= \sum_z f(z)\widehat{\varphi^c}(\gamma - z) = \sum_z f(\gamma z)\widehat{\varphi^c}(\gamma - \gamma z)\\ &= f(\gamma)\cdot \sum_z f(z)\widehat{\varphi^c}(1-z) = f(\gamma)\cdot\big(\widehat{\varphi^c} * f\big)(1).\end{aligned}$$

Further, for every $\alpha \in [|\Gamma|]$, $\mathsf{E}_{k+1}(\Gamma, \widehat{\varphi^c}) \geqslant \mathsf{E}_{k+1}(\chi_\alpha, \widehat{\varphi^c})$.

Next, we prove (59). Let φ be such that $\psi = \widehat{\varphi^c}$. Since $\psi(x) = \psi(-x)$, it follows that φ is a real function and, consequently, the operator $\bar{\mathrm{T}}^{\varphi}_{\Gamma}$ is symmetric. By assumption $\widehat{\psi}(x) \geqslant 0$, so $\bar{\mathrm{T}}^{\varphi}_{\Gamma}$ is nonnegative definite and all its eigenvalues $\mu_\alpha(\bar{\mathrm{T}}^{\varphi}_{\Gamma})$ are nonnegative. If $u = \sum_\alpha c_\alpha \chi_\alpha$ then

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

and the result follows. □

In particular, we have equality in (53) for multiplicative subgroups. Note also that an analog of the proposition above holds for an arbitrary tiling not necessary for tiling by cosets.

Corollary 46. *Let $\Gamma_* \subseteq \mathbb{F}_q$ be a coset of a multiplicative subgroup Γ. Then for every set $\Gamma' \subseteq \Gamma_*$, and every Γ-invariant set Q, we have*

$$\big|Q + \Gamma'\big| \geqslant \big|\Gamma'\big| \cdot \frac{|\Gamma||Q|^2}{\mathsf{E}_2(\Gamma_*, Q)}. \tag{60}$$

If $Q^{(y)} \subseteq Q^k$, $y \in \Gamma'$, is an arbitrary family of sets, then

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

Furthermore, for each $k \geqslant 2$, we have

$$R^{(k)}_Q[\Gamma_*] \geqslant \frac{|\Gamma||Q|^{2k}}{\mathsf{E}_{k+1}(\Gamma_*, Q)}. \tag{61}$$

Proof. For every $\xi \in \mathbb{F}_q^*/\Gamma$ and $\alpha \in [|\Gamma|]$, let us define the functions $\chi^{\xi}_{\alpha}(x) := \chi_\alpha(\xi^{-1}x)$. Then, clearly $\operatorname{supp}\chi^{\xi}_{\alpha} = \xi\cdot\Gamma$ and $\chi^{\xi}_{\alpha}(\gamma x) = \chi_\alpha(\gamma)\chi^{\xi}_{\alpha}(x)$ for all $\gamma \in \Gamma$. Using the argument from Proposition 45 it is easy to see that the functions χ^{ξ}_{α} are orthogonal eigenfunctions of the operator $\bar{\mathsf{T}}^{\varphi}_{\Gamma_*}$. This completes the proof. □

It is easy to see that in the case $\mathbb{F}_q = \mathbb{Z}/p\mathbb{Z}$, p is a prime number, $|\Gamma| = O(p^{2/3})$ the bound (61) is best possible up to a constant factor. In particular, it gives asymptotic formulas for the sizes of the sets $\Gamma^k \pm \Delta(\Gamma)$, $k \geqslant 3$.

To apply the inequality (59) of Proposition 45 we need a lemma (see, e.g. [32] or [16,17]).

Lemma 47. *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 $|Q||Q_1||Q_2| \ll |\Gamma|^5$ and $|Q||Q_1||Q_2||\Gamma| \ll p^3$. Then*

$$\sum_{x\in Q}(Q_1 \circ Q_2)(x) \ll |\Gamma|^{-1/3}\left(|Q||Q_1||Q_2|\right)^{2/3}. \tag{62}$$

Using Lemma 47, one can easily deduce bounds for moments of convolution of Γ, e.g. (see [27]) that $\mathsf{E}(\Gamma) = O(|\Gamma|^{5/2})$ and $\mathsf{E}_3(\Gamma) = O(|\Gamma|^3\log|\Gamma|)$, provided that $|\Gamma| = O(p^{2/3})$.

Corollary 48. *Let p be a prime number, and $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| = O(p^{1/2})$. Then*

$$\mathsf{E}(\Gamma) \ll |\Gamma|^{\frac{23}{12}}|\Gamma \pm \Gamma|^{\frac{1}{3}}\log^{\frac{1}{2}}|\Gamma|, \tag{63}$$

and

$$\mathsf{E}(\Gamma) \ll |\Gamma|^{\frac{31}{18}}|\Gamma \pm \Gamma|^{\frac{4}{9}}\log^{\frac{1}{2}}|\Gamma|. \tag{64}$$

Proof. We have $\mathsf{E}(\Gamma) = O(|\Gamma|^{5/2})$. One can assume that

$$|\Gamma \pm \Gamma| = O\left(\frac{\mathsf{E}^3(\Gamma)}{|\Gamma|^{23/4}\log^{1/2}|\Gamma|}\right) = O\left(\frac{|\Gamma|^{7/4}}{\log^{1/2}|\Gamma|}\right) \tag{65}$$

because otherwise inequality (63) is trivial. To obtain (63), we use a formula from [19] (see Lemma 2.5)

$$\left(\sum_x(\Gamma\circ\Gamma)^{3/2}(x)\right)^2|\Gamma|^2 \leqslant \mathsf{E}_3(\Gamma)\cdot\mathsf{E}(\Gamma, \Gamma\pm\Gamma).$$

Further, by the assumption $|\Gamma| = O(p^{3/4})$ and Lemma 47, we have (see also the proof of Theorem 1.1 from [19])

$$\mathsf{E}^3(\Gamma) \ll |\Gamma|^3 \cdot \Big(\sum_x (\Gamma \circ \Gamma)^{3/2}(x) \Big)^2 .$$

Combining the last two formulas, we obtain

$$\mathsf{E}^3(\Gamma) \ll |\Gamma| \mathsf{E}_3(\Gamma) \cdot \mathsf{E}(\Gamma, \Gamma \pm \Gamma). \tag{66}$$

We show that for every Γ-invariant set Q we have

$$\sum_x (Q \circ Q)(x)(\Gamma \circ \Gamma)^2(x) \geqslant |\Gamma|^{-2} \mathsf{E}(\Gamma) \cdot \mathsf{E}(\Gamma, Q). \tag{67}$$

By (59) of Proposition 45 with $\psi(x) = (Q \circ Q)(x)$ and $u(x) = \Gamma_s(x) = (\Gamma \cap (\Gamma - s))(x)$, we get

$$\sum_x (Q \circ Q)(x)(\Gamma_s \circ \Gamma_s)(x) \geqslant \frac{|\Gamma_s|^2}{|\Gamma|^2} \mathsf{E}(Q, \Gamma). \tag{68}$$

Summing over $s \in \Gamma - \Gamma$, we obtain (67). Inserting (67) in (66), we infer that

$$\mathsf{E}^4(\Gamma) \ll |\Gamma|^3 \mathsf{E}_3(\Gamma) \cdot \sum_x (Q \circ Q)(x)(\Gamma \circ \Gamma)^2(x),$$

where $Q = \Gamma \pm \Gamma$. By the assumption $|\Gamma| = O(p^{1/2})$. Let us prove that

$$\sum_x (Q \circ Q)(x)(\Gamma \circ \Gamma)^2(x) \ll \frac{|Q|^{4/3}}{|\Gamma|^{2/3}} |\Gamma|^{7/3} \log|\Gamma| \ll |Q|^{4/3} |\Gamma|^{5/3} \log|\Gamma|. \tag{69}$$

From (67) and (66) it follows that the summation in the (69) can be taken over x such that

$$(Q \circ Q)(x) \geqslant \frac{\mathsf{E}(\Gamma, Q)}{2|\Gamma|^2} \gg \frac{\mathsf{E}^3(\Gamma)}{|\Gamma|^3 \mathsf{E}_3(\Gamma)} := H. \tag{70}$$

Hence, it is sufficient to prove that

$$\sum_{x:\ (Q \circ Q)(x) \geqslant H} (Q \circ Q)(x)(\Gamma \circ \Gamma)^2(x) \ll |Q|^{4/3} |\Gamma|^{5/3} \log|\Gamma|. \tag{71}$$

Let $(Q \circ Q)(\xi_1) \geqslant (Q \circ Q)(\xi_2) \geqslant \dots$ and $(\Gamma \circ \Gamma)(\eta_1) \geqslant (\Gamma \circ \Gamma)(\eta_2) \geqslant \dots$, where $\xi_1, \xi_2, \dots$ and $\eta_1, \eta_2, \dots$ belong to distinct cosets. Applying Lemma 47 once more, we get

$$(Q \circ Q)(\xi_j) \ll \frac{|Q|^{4/3}}{|\Gamma|^{2/3}} j^{-1/3} \quad \text{and} \quad (\Gamma \circ \Gamma)(\eta_j) \ll |\Gamma|^{2/3} j^{-1/3}, \tag{72}$$

provided that $j|\Gamma||Q|^2 \ll |\Gamma|^5$ and $j|\Gamma||Q|^2|\Gamma| \ll p^3$. We have $j \ll |Q|^4/(|\Gamma|^2 H^3)$, $\mathsf{E}_3(\Gamma) = O(|\Gamma|^3 \log|\Gamma|)$ and $|\Gamma| = O(p^{1/2})$, thus, the last conditions are satisfied. Applying (72), we obtain (69). Using the fact $\mathsf{E}_3(\Gamma) = O(|\Gamma|^3 \log|\Gamma|)$, and the formula (69), we get

$$\mathsf{E}^4(\Gamma) \ll |\Gamma|^6 \log|\Gamma| \cdot |Q|^{4/3}|\Gamma|^{5/3}\log|\Gamma|$$

and (63) is proved.

To show (64), we just put $u(x) = (\Gamma \cap (Q-s))(x)$ in (68) instead of $u(x) = \Gamma_s(x)$. We have

$$\sum_x (Q\circ Q)^2(x)(\Gamma\circ\Gamma)(x) \geqslant |\Gamma|^{-2}\cdot \mathsf{E}^2(\Gamma, Q), \tag{73}$$

where $Q = \Gamma \pm \Gamma$. Applying (66), we get

$$\sum_x (Q\circ Q)^2(x)(\Gamma\circ\Gamma)(x)\cdot|\Gamma|^4\mathsf{E}_3^2(\Gamma) \geqslant \mathsf{E}^6(\Gamma). \tag{74}$$

As before, we need an analog of the estimate (69)

$$\sum_x (Q\circ Q)^2(x)(\Gamma\circ\Gamma)(x) \ll |Q|^{8/3}|\Gamma|^{1/3}\log|\Gamma|. \tag{75}$$

Again, using the inequality (73) and the definition of H (70), it is sufficient to prove that

$$\sum_{x:\ (Q\circ Q)(x)\geqslant H} (Q\circ Q)^2(x)(\Gamma\circ\Gamma)(x) \ll |Q|^{8/3}|\Gamma|^{1/3}\log|\Gamma|.$$

One can assume that an analog of (65) holds

$$|Q| = O\left(\frac{\mathsf{E}^{9/4}(\Gamma)}{|\Gamma|^{31/8}\log^{1/2}|\Gamma|}\right) = O\left(\frac{|\Gamma|^{7/4}}{\log^{1/2}|\Gamma|}\right) \tag{76}$$

because otherwise the inequality (64) is trivial. Using previous arguments, the bound (76) and applying Lemma 47, and inequalities $|\Gamma| \ll p^{1/2}$, $\mathsf{E}_3(\Gamma) \ll |\Gamma|^3\log|\Gamma|$, we get the required estimate. Inserting (75) in (74), and using $\mathsf{E}_3(\Gamma) \ll |\Gamma|^3\log|\Gamma|$ once again, we obtain (64). □

In particular, if $\mathsf{E}(\Gamma) \gg |\Gamma|^{5/2}$ then $|\Gamma \pm \Gamma| \gg |\Gamma|^{\frac{7}{4}-\epsilon}$, for any $\epsilon > 0$. At the moment it is known (see [32]), unconditionally, that $|\Gamma - \Gamma| \gg |\Gamma|^{\frac{5}{3}-\epsilon}$, for an arbitrary $\epsilon > 0$ and any multiplicative subgroup Γ with $|\Gamma| = O(p^{1/2})$. Note also that the condition $|\Gamma| = O(p^{1/2})$ in the previous result can be slightly relaxed.

Corollary 49. *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup such that $-1 \in \Gamma$, $|\Gamma| \geqslant p^\kappa$, where $\kappa > \frac{99}{203}$. Then for all sufficiently large p we have $\mathbb{F}_p^* \subseteq 6\Gamma$.*

Proof. Put $S = \Gamma + \Gamma$, $n = |\Gamma|$, $m = |S|$, and $\rho = \max_{\xi\neq 0}|\widehat{\Gamma}(\xi)|$. By a well-known upper bound for Fourier coefficients of multiplicative subgroups (see e.g. Corollary 2.5 from [27]) we have $\rho \leqslant p^{1/8}\mathsf{E}^{1/4}(\Gamma)$. If $\mathbb{F}_p^* \nsubseteq 6\Gamma$ then for some $\lambda \neq 0$, we obtain

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

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

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

Now applying formula (64) and $m \gg n^{5/3}\log^{-1/2} n$ (see [32]), we obtain the required result. □

The inclusion $\mathbb{F}_p^* \subseteq 6\Gamma$ was obtained in [32] under the assumption $\kappa > \frac{33}{67}$.

9. Two versions of the Balog–Szemerédi–Gowers theorem

We show here two versions of the Balog–Szemerédi–Gowers theorem (see Lemma 22) in the case when $\mathsf{E}_k(A)$ is not much bigger than the trivial lower bound in terms of additive energy i.e. $\mathsf{E}(A)^{k-1}/|A|^{2k-4}$. The first result (Theorem 52) provides an improvement on the size of a "structured" subset A' of A and the size of $A' - A'$, as well, assuming that $\mathsf{E}_{2+\varepsilon}(A)$ is "small". Our method essentially follows, with some modifications, the Gowers proof [10]. Our second theorem (Theorem 54) gives a near optimal estimate on $|A' - A'|$, again for a very large $A' \subseteq A$, however we have to assume that $\mathsf{E}_{3+\varepsilon}(A)$ is small. To prove Theorem 54 we develop the idea used in the proof of Theorem 23. At the end of this section we establish some results concerning sumsets and energies of multiplicative subgroups and convex sets.

We will need two lemmas. The first one is a version of Gowers Lemma 7.4 [10], see also Lemma 1.9 in [26].

Lemma 50. *Let I and S be sets with $|I| = n$ and $|S| = m$. Suppose that $S_i \subseteq S$, $i \in I$, is a family of sets such that*

$$\sum_{i,j\in I} |S_i \cap S_j| \geqslant \delta^2 mn^2,$$

where $0 \leqslant \delta \leqslant 1$. Let $\eta > 0$. Then there is $J \subseteq I$, $|J| \geqslant \delta n/\sqrt{2}$ such that

$$\left|\left\{(i,j) \in J \times J\colon\ |S_i \cap S_j| \geqslant \eta\delta^2 n/2\right\}\right| \geqslant (1-\eta)|J|^2. \tag{77}$$

Proof. We have

$$\delta^2 mn^2 \leqslant \sum_{i,j\in I} |S_i \cap S_j| = \sum_{\alpha} \sum_{i,j\in I} S_i(\alpha) S_j(\alpha). \tag{78}$$

For $\alpha \in S$, we put $K_\alpha = \{i \in I\colon\ \alpha \in S_i\}$. Clearly $K_\alpha(i) = S_i(\alpha)$, so we can rewrite (78) as

$$\delta^2 mn^2 \leqslant \sum_{\alpha} |K_\alpha|^2.$$

Let

$$Y = \left\{(i,j) \in I \times I\colon\ |S_i \cap S_j| < \eta\delta^2 m/2\right\},$$

then

$$\sum_{\alpha\in S} |K_\alpha \times K_\alpha \cap Y| = \sum_{(i,j)\in Y} |S_i \cap S_j| < \eta\delta^2 mn^2/2,$$

so that

$$\sum_{\alpha\in S} |K_\alpha|^2 - \eta^{-1} \sum_{\alpha\in S} |K_\alpha \times K_\alpha \cap Y| > \delta^2 mn^2/2.$$

Thus, there exists $\alpha \in S$ such that $|K_\alpha| \geqslant \delta n/\sqrt{2}$ and $|K_\alpha \times K_\alpha \cap Y| < \eta |K_\alpha|^2$. It is enough to observe that the assertion holds with $J = K_\alpha$. $\square$

Corollary 51. *With the assumption of Lemma 50 there is a set $J' \subseteq J$ of size at least $2^{-5}\delta n$ such that for every $i, j \in J'$ there are at least $2^{-2}\delta n$ elements $k \in I$ with*

$$|S_i \cap S_k| \geqslant 2^{-4}\delta^2 m, \qquad |S_j \cap S_k| \geqslant 2^{-4}\delta^2 m.$$

Proof. Applying the previous lemma with $\eta = 1/8$, we obtain a set J satisfying (77). Let V be the set of all pairs $(i, j) \in J \times J$ such that $|S_i \cap S_j| \geqslant 2^{-1}\eta\delta^2 m = 2^{-4}\delta^2 m$. Then we have

$$\sum_{(i,j)\in J\times J} V(i,j) \geqslant (1-\eta)|J|^2 = \frac{7}{8}|J|^2.$$

Put $J' = \{i \in J\colon \sum_j V(i,j) \geqslant \frac{3}{4}|J|\}$. Clearly

$$\sum_{i\in J'}\sum_{j\in J} V(i,j) \geqslant \frac{1}{16}|J|^2,$$

whence $|J'| \geqslant 2^{-4}|J| > 2^{-5}\delta n$. Furthermore, observe that if $i, j \in J'$, then

$$\sum_k V(i,k)V(j,k) \geqslant |J|/2,$$

as required. $\square$

Now we are ready to prove the first main result of this section.

Theorem 52. *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 $|A'| \gg |A|/(2M)^{1/\varepsilon}$ and*

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

Proof. Observe that

$$\frac{|A|^3}{K} = \mathsf{E}(A) = \sum_a A(a) \sum_b A(b)(A\circ A)(a-b).$$

For $a \in A$, we set

$$S_a = \big\{b \in A\colon (A\circ A)(a-b) \geqslant |A|/(2K)\big\},$$

hence

$$\sum_a A(a) \sum_b S_a(b)(A\circ A)(a-b) \geqslant \frac{|A|^3}{2K}.$$

By the Hölder inequality we have

$$\sum_a A(a)\sum_b S_a(b)(A\circ A)(a-b) \leqslant \sum_a A(a)\Big(\sum_b S_a(b)\Big)^{\frac{\varepsilon}{1+\varepsilon}}\Big(\sum_b S_a(b)(A\circ A)(a-b)^{1+\varepsilon}\Big)^{\frac{1}{1+\varepsilon}}$$
$$\leqslant \Big(\sum_a |S_a|\Big)^{\frac{\varepsilon}{1+\varepsilon}}\Big(\sum_a A(a)\sum_b A(b)(A\circ A)(a-b)^{1+\varepsilon}\Big)^{\frac{1}{1+\varepsilon}}$$
$$\leqslant \Big(\sum_a |S_a|\Big)^{\frac{\varepsilon}{1+\varepsilon}} \mathsf{E}_{2+\varepsilon}(A)^{\frac{1}{1+\varepsilon}}, \qquad (79)$$

so that

$$\sum_a |S_a| \geqslant \frac{|A|^2}{2^{\frac{1+\varepsilon}{\varepsilon}} M^{\frac{1}{\varepsilon}}} \qquad (80)$$

and

$$\sum_{a,a'\in A} |S_a \cap S_{a'}| \geqslant \frac{|A|^3}{2^{\frac{2+2\varepsilon}{\varepsilon}} M^{\frac{2}{\varepsilon}}}.$$

We apply Corollary 51 with $I = S = A$, $n = m = |A|$, and the family $\{S_a\}$, $a \in A$. Set $\delta = 2^{-\frac{1+\varepsilon}{\varepsilon}} M^{-\frac{1}{\varepsilon}}$. By Corollary 51 there exists a set $A' \subseteq A$, $|A'| \geqslant 2^{-5}\delta n \gg |A|/2^{\frac{1}{\varepsilon}} M^{\frac{1}{\varepsilon}}$ such that for every $x, y \in A'$ there are at least $2^{-2}\delta n \gg |A|/2^{\frac{1}{\varepsilon}} M^{\frac{1}{\varepsilon}}$ elements $z \in A$ with

$$|S_x \cap S_z|, |S_y \cap S_z| \geqslant 2^{-4}\delta^2 m.$$

For each $b \in S_x \cap S_z$ we have $(A\circ A)(x-b), (A\circ A)(z-b) \geqslant |A|/(2K)$. Similarly, for each $b \in S_y \cap S_z$ we have $(A\circ A)(y-b), (A\circ A)(z-b) \geqslant |A|/(2K)$. Therefore,

$$\big((A\circ A)\circ(A\circ A)\big)(x-z) \geqslant \sum_b (A\circ A)(x-b)(A\circ A)(z-b) \geqslant 2^{-4}\delta^2 m\frac{|A|^2}{4K^2} \gg \frac{|A|^3}{2^{\frac{2}{\varepsilon}} M^{\frac{2}{\varepsilon}} K^2}$$

and the same holds for $y - z$. Thus, there are $\gg |A|^7/(2^{\frac{5}{\varepsilon}} M^{\frac{5}{\varepsilon}} K^4)$ ways to write $x - y$ in the form $a_1 - a_2 + a_3 - a_4 + a_5 - a_6 + a_7 - a_8$, $a_i \in A$. Hence

$$\big|A' - A'\big|\frac{|A|^7}{2^{\frac{5}{\varepsilon}} M^{\frac{5}{\varepsilon}} K^4} \ll |A|^8$$

and the assertion follows. □

Corollary 53. *Let A be a subset of an abelian group. Suppose that $\mathsf{E}(A) = |A|^3/K$ and $\mathsf{E}_3(A) = M|A|^4/K^2$. Then there exists $A' \subseteq A$ such that $|A'| \gg |A|/M$ and*

$$\big|A' - A'\big| \ll M^6 K^4 \big|A'\big|.$$

Now, using a different approach, we prove the following almost optimal version of Balog–Szemerédi–Gowers theorem, provided that $\mathsf{E}_{3+\varepsilon}(A)$, $\varepsilon > 0$, is small.

Theorem 54. *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*

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

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

Proof. Let P be the set of popular differences with at least $|A|/2K$ representations. Similarly, as in the proof of Theorem 23 we have

$$\sum_{s\in P}(A\circ A)(s)^2 \geqslant \frac{1}{2}\mathsf{E}(A) \geqslant \frac{|A|^3}{2K}$$

and

$$\frac{|A|^3}{K} \ll \mathsf{E}_{3+\varepsilon}(A)^{\frac{2}{3+\varepsilon}}|P|^{\frac{1+\varepsilon}{3+\varepsilon}},$$

so $|P| \gg K|A|/M^{2/(1+\varepsilon)}$. Furthermore, by the Hölder inequality

$$\sum_{s\in P}(A\circ A)(s) \gg \frac{\mathsf{E}(A)^{\frac{2+\varepsilon}{1+\varepsilon}}}{\mathsf{E}_{3+\varepsilon}(A)^{\frac{1}{1+\varepsilon}}} \gg M^{-\frac{1}{1+\varepsilon}}|A|^2. \tag{81}$$

As in Theorem 52, put $S_a = A \cap (a - P)$, $a \in A$ i.e. S_a is the set of all $b \in A$ such that $a - b \in P$. We show that P has huge additive energy. To do this we apply a generalization of Katz–Koester transform. Observe that for every $s \in A - A$ we have

$$\bigcup_{a\in A_s}\big(a - (S_a \cap S_{a-s})\big) \subseteq P \cap (P + s).$$

From the Cauchy–Schwarz inequality it follows that

$$(P\circ P)(s) \geqslant \left|\bigcup_{a\in A_s}\big(a - (S_a \cap S_{a-s})\big)\right| \geqslant \frac{(\sum_{a\in A_s}|S_a \cap S_{a-s}|)^2}{\mathsf{E}(A_s, A)}. \tag{82}$$

By (81), we have

$$\sum_{s\in P}(A\circ A)(s) = \sum_{a\in A}|S_a| := \gamma|A|^2 \gg \max\big(M^{-\frac{1}{1+\varepsilon}}, K^{-1}|A|^{-1}|P|\big)|A|^2, \tag{83}$$

so that

$$\sum_{a,a'\in A}|S_a \cap S_{a'}| = \sum_s\sum_{a\in A_s}|S_a \cap S_{a-s}| \gg \gamma^2|A|^3.$$

Let $p > 1$ and $q > 1$, then by the Hölder inequality and Lemma 2

$$\gamma^2|A|^3 \ll \Big(\sum_s \frac{(\sum_{a\in A_s}|S_a\cap S_{a-s}|)^q}{\mathsf{E}(A_s,A)^{q/2}}\Big)^{\frac{1}{q}}\Big(\sum_s \mathsf{E}(A_s,A)^{\frac{q}{2(q-1)}}\Big)^{\frac{q-1}{q}}$$

$$\ll \mathsf{E}_{\frac{q}{2}}(P)^{\frac{1}{q}}\Big(\sum_s |A_s|^{\frac{(p-1)q}{(q-1)p}}\mathsf{E}_{1+p}(A_s,A)^{\frac{q}{2p(q-1)}}\Big)^{\frac{q-1}{q}}$$

$$\leqslant \mathsf{E}_{\frac{q}{2}}(P)^{\frac{1}{q}}\Big(\sum_s |A_s|^{\frac{2(p-1)q}{2p(q-1)-q}}\Big)^{\frac{2p(q-1)-q}{2pq}}\mathsf{E}_{2+p}(A)^{\frac{1}{2p}}$$

$$= \mathsf{E}_{\frac{q}{2}}(P)^{\frac{1}{q}}\mathsf{E}_{\frac{2(p-1)q}{2p(q-1)-q}}(A)^{\frac{2p(q-1)-q}{2pq}}\mathsf{E}_{2+p}(A)^{\frac{1}{2p}}.$$

In particular, taking $p=1+\varepsilon$, $q=2p$, we get

$$\gamma^2|A|^3 \ll \mathsf{E}_{1+\varepsilon}(P)^{\frac{1}{2+2\varepsilon}}|A|^{\frac{2\varepsilon}{1+\varepsilon}}\mathsf{E}_{3+\varepsilon}(A)^{\frac{1}{2+2\varepsilon}},$$

hence

$$\mathsf{E}_{1+\varepsilon}(P) \gg \big(\gamma^2|A|^{3-\frac{2\varepsilon}{1+\varepsilon}}\big)^{2+2\varepsilon}\mathsf{E}_{3+\varepsilon}(A)^{-1}.$$

In view of the inequality $K|A|/M^{\frac{2}{1+\varepsilon}} \ll |P| \leqslant 2K|A|$ and the definition of γ, we infer that

$$\mathsf{E}(P) \geqslant |P|^{2-\frac{2}{\varepsilon}}\mathsf{E}_{1+\varepsilon}(P)^{\frac{1}{\varepsilon}} \tag{84}$$

$$\gg |P|^{2-\frac{2}{\varepsilon}}\gamma^{4+\frac{4}{\varepsilon}}|A|^{\frac{6}{\varepsilon}+2}\mathsf{E}_{3+\varepsilon}(A)^{-\frac{1}{\varepsilon}} \tag{85}$$

$$= \frac{\gamma^4K|A|}{|P|}\Big(\frac{\gamma^4K^2|A|^2}{M|P|^2}\Big)^{\frac{1}{\varepsilon}}|P|^3 \tag{86}$$

$$\gg M^{-\beta}|P|^3, \tag{87}$$

where $\beta=\frac{3+4\varepsilon}{\varepsilon(1+\varepsilon)}$. Note that the first inequality in the formula above follows certainly from Hölder for $\varepsilon\in(0,1)$ but it is also takes place for $\varepsilon=1$.

Now we proceed as in the proof of Theorem 23. By the Balog–Szemerédi–Gowers Theorem 22 there exists a set $P'\subseteq P$ such that $|P'|\gg M^{-\beta}|P|$, and

$$\big|P'+P'\big| \ll M^{6\beta}\big|P'\big|,$$

so that by the Plünnecke–Ruzsa inequality

$$\big|nP'-mP'\big| \ll M^{6(n+m)\beta}\big|P'\big|.$$

By the pigeonhole principle, we find x such that

$$\big|(A-x)\cap P'\big| \gg \big|P'\big|/K \gg |A|/M^{\beta+\frac{2}{1+\varepsilon}}.$$

Setting $A'=A\cap(P'+x)$, the assertion follows. □

Remark 55. In the proof of the theorem above we need the assumption that the energy $\mathsf{E}_4(A)$ is small. However, for some sets, for instance multiplicative subgroups, one can apply the inequality $\mathsf{E}_3(A_s, A) \leqslant \frac{|A_s|}{|A|}\mathsf{E}_3(A)$ (see Proposition 45) to obtain the same result.

Corollary 56. *Suppose that* $\mathsf{E}(A) = |A|^3/K$ *and* $\mathsf{E}_4(A) = M|A|^5/K^3$. *Then there exists* $A' \subseteq A$ *such that* $|A'| \gg M^{-9/2}|A|$ *and*

$$\big|nA' - mA'\big| \ll M^{21(n+m)}K\big|A'\big|$$

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

Remark 57. Observe that Corollary 56 can be proved by arguments used in the proof of Lemma 3. Indeed, let $\mathcal{G}$ be the popularity graph on A i.e. for $a, b \in A$, $\{a, b\}$ is an edge in $\mathcal{G}$ if and only if $(A \circ A)(a - b) \geqslant |A|/(2K)$. By (83)

$$\big|E(\mathcal{G})\big| = \sum_{x\in P}(A \circ A)(x) := \gamma|A|^2 \gg \max\big(M^{-1/2}, K^{-1}|A|^{-1}|P|\big)|A|^2.$$

Let $\mathcal{C}$ be the family of 4-tuples $(a_1, a_2, a_3, a_4) \in V(\mathcal{G})$ such that $\{a_1, a_2\}, \{a_2, a_3\}, \{a_3, a_4\}, \{a_4, a_1\} \in E(\mathcal{G})$. Then we have

$$|\mathcal{C}| \geqslant \gamma^4|A|^4.$$

Let us consider a map $\psi : \mathcal{C} \to P^4$ defined in the following way. If $C = (a_1, a_2, a_3, a_4) \in \mathcal{C}$ then

$$\psi(C) = (a_1 - a_2, a_2 - a_3, a_3 - a_4, a_4 - a_1).$$

Arguing as in Lemma 3, we get

$$\mathsf{E}(P) \geqslant \frac{|\mathcal{C}|^2}{\mathsf{E}_4(A)} \gg \gamma^8 M^{-1}K^3|A|^3.$$

The rest of the proof remains the same.

As an applications of ideas that appeared Lemma 3 and Theorem 54, we also prove some estimates on the size and the additive energy of multiplicative subgroups of $\mathbb{F}_p$ and convex sets.

Corollary 58. *Let* A *be a convex set. Then*

$$|A - A||A|^{\frac{285}{8}} \gg \mathsf{E}(A)^{15}\log^{-\frac{15}{2}}|A|. \tag{88}$$

Further, let p *be a prime number,* Γ *be a multiplicative subgroup,* $|\Gamma| \ll \sqrt{p}$. *Then*

$$|\Gamma - \Gamma||\Gamma|^{33} \gg \mathsf{E}(\Gamma)^{14}\log^{-\frac{15}{2}}|\Gamma|. \tag{89}$$

Proof. Let $D = A - A$, $\mathsf{E}(A) = |A|^3/K$. Let also P be the set of popular differences with at least $|A|/2K$ representations. As before

$$\sum_{a\in A}|S_a| \geqslant \frac{\mathsf{E}(A)^2}{4\mathsf{E}_3(A)} \gg |A|^3K^{-2}\log^{-1}|A|,$$

and hence

$$\sum_{a,a'\in A}|S_a\cap S_{a'}|=\sum_{s\in D}\sum_{a\in A_s}|S_a\cap S_{a-s}|\gg |A|^5K^{-4}\log^{-2}|A|.$$

Further, by (82), we have

$$|A|^{10}K^{-8}\log^{-4}|A|\ll\Big(\sum_{s\in D}\sum_{a\in A_s}|S_a\cap S_{a-s}|\Big)^2\ll\Big(\sum_{s\in D}|P_s|^{1/2}\cdot \mathsf{E}(A_s,A)^{1/2}\Big)^2 \tag{90}$$

$$\ll \mathsf{E}_3(A)\sum_{s\in D}(P\circ P)(s). \tag{91}$$

Whence

$$\sum_{s\in D}(A\circ A\circ A\circ A)(s)\gg\Big(\frac{|A|}{K}\Big)^2\sum_{s\in D}(P\circ P)(s)\gg |A|^9K^{-10}\log^{-5}|A|.$$

By Theorem 1 from [13], we get

$$|A|^{4-4/3+1/12}|D|^{2/3}\gg |A|^9K^{-10}\log^{-5}|A|,$$

so

$$|D|K^{15}\gg |A|^{\frac{75}{8}}\log^{-\frac{15}{2}}|A|$$

and finally,

$$|D||A|^{\frac{285}{8}}\gg \mathsf{E}(A)^{15}\log^{-\frac{15}{2}}|A|.$$

To get (89) return to (90) and obtain

$$|\Gamma|^7K^{-8}\log^{-5}|\Gamma|\ll\sum_{s\in D}(P\circ P)(s).$$

We can suppose that $|P|^2|D|\ll (K|\Gamma|)^2|D|\ll|\Gamma|^5$, because otherwise $|D|\gg|\Gamma|^3K^{-2}$ and (89) holds. Thus, $|P|^2|D||\Gamma|\ll|\Gamma|^6\ll p^3$ by the assumption $|\Gamma|\ll\sqrt{p}$. Applying Lemma 47, we have

$$|\Gamma|^7K^{-8}\log^{-5}|\Gamma|\ll\frac{(K|\Gamma|)^{4/3}|D|^{2/3}}{|\Gamma|^{1/3}}.$$

In other words

$$|\Gamma|^9\ll|D|K^{14}\log^{\frac{15}{2}}|\Gamma|\ll|D||\Gamma|^{42}\mathsf{E}^{-14}(\Gamma)\log^{\frac{15}{2}}|\Gamma|$$

and we obtain (89). This completes the proof. □

In particular, if $\mathsf{E}(A)\sim|A|^{\frac{5}{2}}$ then $|A-A|\gg|A|^{\frac{15}{8}}\log^{-\frac{15}{2}}|A|$ for any convex set. Similarly, if $\mathsf{E}(\Gamma)\sim|\Gamma|^{\frac{5}{2}}$ then $|\Gamma-\Gamma|\gg|\Gamma|^2\log^{-\frac{15}{2}}|\Gamma|$ for an arbitrary multiplicative subgroup Γ, $|\Gamma|\ll\sqrt{p}$.

Corollary 58 easily implies that $|A-A| \gg |A|^{\frac{3}{2}+\epsilon}$, $\epsilon > 0$ for any convex set or multiplicative subgroup of size $O(\sqrt{p})$.

10. Relations between $\mathsf{E}_k(A)$ and $\mathsf{T}_l(A)$

Notice that from Corollary 56 one can deduce that there exists a constant $C > 0$ such that if $\mathsf{E}(A) = |A|^3/K$ and $\mathsf{E}_4(A) = M|A|^5/K^3$ then

$$\mathsf{T}_l(A) \geqslant \frac{|A|^{2l-1}}{K(CM)^{Cl}}.$$

Theorem 54 gives similar bound provided by $\mathsf{E}_{3+\varepsilon}(A) = M|A|^{4+\varepsilon}/K^{2+\varepsilon}$. The proof of Theorem 52 bring up the following question. Does there exist a set A such that $\mathsf{E}(A) = |A|^3/K$, $\mathsf{E}_3(A) = M_1|A|^4/K^2$, and $\mathsf{T}_l(A) = M_2|A|^{2l-1}/K^{l-1}$, $l \geqslant 3$ with M_1, M_2 relatively small simultaneously? Note that if $\mathsf{E}(A) = |A|^3/K$ then the estimates $\mathsf{E}_3(A) \geqslant |A|^4/K^2$, $\mathsf{T}_l(A) \geqslant |A|^{2l-1}/K^{l-1}$ easily follows from the Cauchy–Schwarz inequality. Interesting, that the answer is negative, provided that the assumption on the additive energy we replace by $|A-A| = K|A|$. It can be deduced from Theorem 23, but we describe a more direct approach providing a slightly better lower bounds. Similar arguments were used in [28].

Proposition 59. *Let $A \subseteq \mathbf{G}$ be a set, and $l \geqslant 2$ be a positive integer. Then*

$$\left(\frac{|A|^8}{8\mathsf{E}_3(A)}\right)^l \leqslant \mathsf{T}_l(A)|A-A|^{2l+1}, \tag{92}$$

$$\left(\frac{|A|^9}{8\mathsf{E}_3(A)}\right)^l \leqslant \mathsf{T}_l(A)|A+A|^{3l+1}, \tag{93}$$

and

$$\left(\frac{|A|^{20}}{32\mathsf{E}_3^3(A)}\right)^l \leqslant \mathsf{T}_l(A)|A+A|^{6l+1}. \tag{94}$$

Proof. Let $D = A-A$, $S = A+A$, $|D| = K|A|$, and $|S| = L|A|$. As before, we define $P = \{s \in D:\ |A_s| \geqslant |A|/(2K)\}$ and $P' = \{s \in D:\ |A_s| \geqslant |A|/(2L)\}$. Then

$$\sum_{x \in P} |A_s| \geqslant |A|^2/2$$

and

$$\sum_{s \in P'} |A_s|^2 \geqslant \frac{1}{2}\mathsf{E}(A).$$

By Lemma 21 and the Katz–Koester transform

$$\frac{|A|^6}{4\mathsf{E}_3(A)} \leqslant \sum_{s \in P} |A - A_s| \leqslant \sum_{s \in P} (D \circ D)(s).$$

Thus, by definition of the set P, we have

$$\frac{|A|^7}{8K\mathsf{E}_3(A)} \leqslant \sum_s (A\circ A)(s)(D\circ D)(s).$$

Using the Fourier inversion formula and the Hölder inequality, we infer that

$$\frac{|A|^7}{8K\mathsf{E}_3(A)} \leqslant \int\limits_{\xi} \bigl|\widehat{A}(\xi)\bigr|^2\bigl|\widehat{D}(\xi)\bigr|^2 \leqslant \Bigl(\int\limits_{\xi}\bigl|\widehat{A}(\xi)\bigr|^{2l}\Bigr)^{\frac{1}{l}}\Bigl(\int\limits_{\xi}\bigl|\widehat{D}(\xi)\bigr|^{\frac{2l}{(l-1)}}\Bigr)^{\frac{l-1}{l}},$$

so that

$$\left(\frac{|A|^7}{8K\mathsf{E}_3(A)}\right)^l \leqslant \mathsf{T}_l(A)\cdot|D|^{l+1}$$

for every $l\geqslant 2$ and (92) follows.

Next we prove (93). For every $1\leqslant j\leqslant t := \lfloor \log L+1\rfloor$ put

$$P'_j = \bigl\{s\in D\colon\ 2^{j-1}|A|/(2L) < |A_s| \leqslant 2^j|A|/(2L)\bigr\}.$$

Further, we have

$$\frac{|A|^3}{2L} \leqslant \sum_{s\in P'}|A_s|^2 \leqslant \frac{|A|}{2L}\sum_{j=1}^{t}2^j\sum_{s\in P'_j}|A_s| = \frac{|A|}{2L}\sum_{j=1}^{t}2^j\delta_j|A|^2, \tag{95}$$

where $\delta_j := \frac{1}{|A|^2}\sum_{s\in P'_j}|A_s|$. Whence

$$\sum_{j=1}^{t}2^j\delta_j \geqslant 1$$

and

$$\sum_{j=1}^{t}2^j\delta_j^2 \geqslant \frac{1}{2L}. \tag{96}$$

By Lemma 21 applied for arbitrary $j\in[t]$, we obtain

$$\delta_j^2|A|^6\mathsf{E}_3^{-1}(A) \leqslant \sum_{s\in P'_j}|A+A_s|.$$

By the definition of the sets P'_j and the Katz–Koester transform, we get

$$\delta_j^2|A|^6 2^{j-1}\frac{|A|}{2L\mathsf{E}_3(A)} \leqslant \sum_{s\in P'_j}(A\circ A)(s)(S\circ S)(s),$$

hence by (96)

$$\frac{|A|^7}{8L^2\mathsf{E}_3(A)} \leqslant \sum_s (A\circ A)(s)(S\circ S)(s).$$

Again using the Fourier inversion formula one has

$$\left(\frac{|A|^7}{8L^2\mathsf{E}_3(A)}\right)^l \leqslant \mathsf{T}_l(A)|S|^{l+1}$$

and the result follows.

It remains to show (94). By the first estimate from (95) and the Cauchy–Schwarz inequality, we obtain

$$\sum_{s\in P'} |A_s| \geqslant \frac{|A|^6}{4L^2\mathsf{E}_3(A)}.$$

Applying Lemma 21, we get

$$\frac{|A|^{14}}{16L^4\mathsf{E}_3^3(A)} \leqslant \sum_{s\in P'} |A+A_s|.$$

Using the same argument as before, we have

$$\frac{|A|^{15}}{32L^5\mathsf{E}_3^3(A)} \leqslant \sum_s (A\circ A)(s)(S\circ S)(s),$$

so that

$$\left(\frac{|A|^{15}}{32L^5\mathsf{E}_3^3(A)}\right)^l \leqslant \mathsf{T}_l(A)|S|^{l+1}$$

and the proposition is proved. □

Our next result describes the structure of the sets, whose energy $\mathsf{T}_l(A)$ is as small as possible in terms of $|A-A|$. It should be compared with the main theorem of [6], where a similar statement was obtained under weaker assumptions, namely $\mathsf{E}(A) = |A|^3/K$. Our assumption $|A-A| = K|A|$ is much stronger than $\mathsf{E}(A) = |A|^3/K$, but also our description of the structure of A is much more rigid.

Theorem 60. *Let A be a subset of an abelian group $\mathbf{G}$ such that $|A-A| = K|A|$ and $\mathsf{T}_3(A) \leqslant M|A|^5/K^2$. Then there exist sets $R \subseteq \mathbf{G}$ and $B \subseteq A$ such that $|R| \ll M^{3/2}|A|/|B|$, $|B| \gg |A|/KM$, $\mathsf{E}(B) \gg |B|^3/M^{9/2}$ and*

$$\big|A\cap(R+B)\big| \gg |A|/M^{3/2}.$$

Proof. Let $P = \{s\in A-A:\ (A\circ A)(s) \geqslant |A|/3K\}$ and define S_a as in Theorem 54. By the Hölder inequality we have

$$\mathsf{E}(A) = \sum_\xi \big|\widehat{A}(\xi)\big|^4 \leqslant \left(\sum_\xi \big|\widehat{A}(\xi)\big|^6\right)^{1/2}\left(\sum_\xi \big|\widehat{A}(\xi)\big|^2\right)^{1/2} = \mathsf{T}_3(A)^{1/2}|A|^{1/2} \leqslant \frac{M^{1/2}|A|^3}{K}.$$

Further, by $|A-A|=K|A|$,

$$\frac{2}{3}|A|^2 \leqslant \sum_{s\in P}(A\circ A)(s).$$

Observe that

$$\sum_s \sum_{a\in A_s} |S_a \cap S_{a-s}| = \sum_{x\in A}(A\circ P)(x)^2 \geqslant \frac{1}{|A|}\Big(\sum_{s\in P}(A\circ A)(s)\Big)^2 \geqslant \frac{4}{9}|A|^3,$$

and

$$\sum_{s\notin P}\sum_{a\in A_s}|S_a\cap S_{a-s}| \leqslant |A|\sum_{s\notin P}|A_s| \leqslant \frac{1}{3}|A|^2.$$

Hence

$$\sum_{s\in P}\sum_{a\in A_s}|S_a\cap S_{a-s}| \gg |A|^3.$$

By the Cauchy–Schwarz inequality and (82), we have

$$\begin{aligned}|A|^3 &\ll \Big(\sum_{s\in P}\frac{(\sum_{a\in A_s}|S_a\cap S_{a-s}|)^2}{\mathsf{E}(A_s,A)}\Big)^{1/2}\Big(\sum_s \mathsf{E}(A_s,A)\Big)^{1/2}\\ &\ll \Big(\sum_{s\in P}(P\circ P)(s)\Big)^{1/2}\mathsf{E}_3(A)^{1/2},\end{aligned}$$

so

$$\sum_{s\in P}(P\circ P)(s) \gg \frac{|A|^6}{\mathsf{E}_3(A)}. \tag{97}$$

On the other hand, we have

$$\Big(\frac{|A|}{K}\Big)^3\sum_{s\in P}(P\circ P)(s) \ll \mathsf{T}_3(A),$$

hence

$$\mathsf{E}_3(A) \geqslant c\frac{|A|^4}{KM} := \gamma|A|^4,$$

for some constant $c>0$.

Observe that

$$\sum_{|A_s|\leqslant \frac{1}{2}\gamma|A|}\mathsf{E}(A,A_s) \leqslant \sum_{|A_s|\leqslant\frac{1}{2}\gamma|A|}|A||A_s|^2 \leqslant \frac{1}{2}\mathsf{E}_3(A).$$

Put

$$\beta = \max_{|A_s|>\frac{1}{2}\gamma|A|} \frac{\mathsf{E}(A, A_s)}{|A||A_s|^2}.$$

Then, by Lemma 1, it follows that

$$\frac{1}{2}\mathsf{E}_3(A) \leqslant \sum_{|A_s|>\frac{1}{2}\gamma|A|} \mathsf{E}(A, A_s) \leqslant \beta|A| \sum_s |A_s|^2 = \beta|A|\mathsf{E}(A),$$

hence $\beta \gg M^{-3/2}$. Finally, there exists a set $B = A_s$ such that $|B| \gg |A|/KM$ and

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

By the Cauchy–Schwarz inequality

$$\mathsf{E}(B) \geqslant \frac{\mathsf{E}(A, B)^2}{\mathsf{E}(A)} \gg \frac{K|B|^4}{M^2|A|} \gg |B|^3/M^{9/2}.$$

Notice that

$$\mathsf{E}(A, B) = \sum_{a\in A,\, b\in B} \big|(a + B) \cap (b + A)\big|,$$

hence for some r, we have

$$\big|(r + B) \cap A\big| \geqslant \frac{\mathsf{E}(A, B)}{|A||B|} \gg |B|/M^{3/2}.$$

Moreover,

$$\mathsf{E}\big(A', B\big) \geqslant \mathsf{E}(A, B) - 2\big|(r + B) \cap A\big||B|^2$$

where $A' = A \setminus (r + B)$. Thus, iterating this procedure we obtain a set R of size $O(M^{3/2}|A|/|B|)$ such that

$$\big|A \cap (R + B)\big| \gg |A|/M^{3/2},$$

which completes the proof. □

Remark 61. It is easy to see that the proofs of Theorem 54 and Theorem 60 rely on the following general inequality

$$\Big(\sum_{x\in B}(A \circ A)(x)\Big)^8 \leqslant |A|^8\mathsf{E}(B)\mathsf{E}_4(A).$$

The same argument gives for all $l \geqslant 1$

$$\Big(\sum_{x\in B} (A\circ A)(x) \Big)^{4l} \leqslant |A|^{6l-4} \mathsf{E}_l(B) \mathsf{E}_{l+2}(A).$$

It is interesting to compare these inequalities for $B = A - A$ with Lemma 3.

We finish the paper with an exposition of a well-known result of Katz and Koester [15]. For a set $G \subseteq A \times B$, by $A \overset{G}{-} B$ we mean the set of all elements $a - b$ such that $(a, b) \in G$.

Theorem 62. *Suppose that $|A - A| = K|A|$. Then there is a set $B \subseteq A - A$ or $B \subseteq A$ such that $|B| \gg |A|/(K^{25/22} \log K)$ and $\mathsf{E}(B) \gg |B|^3/(K^{21/22} \log^{4/11} K)$.*

Proof. Let $1 \leqslant M \leqslant K^{1/22}$ be a real number. We assume that $\mathsf{E}(B) \leqslant M|B|^3/K$ for every $B \subseteq A - A$ or $B \subseteq A$ such that $|B| \gg |A|/(K^{25/22} \log K)$. Our aim is to show that M is large.

Suppose that $\mathsf{E}(A) \leqslant M|A|^3/K$. Again, let $P \subseteq A - A = D$ be the set of all differences with at least $|A|/2K$ representations. Then

$$\frac{1}{2}|A|^2 \leqslant \sum_{s\in P} (A\circ A)(s) \leqslant \mathsf{E}(A)^{1/2} |P|^{1/2},$$

hence $|P| \geqslant \frac{1}{4} K|A|/M$. We consider two cases. First assume that there exists a set $P' \subseteq P$ of size $|P|/2$ such that for every $s \in P'$ we have $|A - A_s| \geqslant K^{1/2} M|A|$. As in (37) we have

$$\mathsf{E}(D) \geqslant \sum_{s\in P} (D\circ D)(s)^2 \geqslant \sum_{s\in P'} |A - A_s|^2 \geqslant \big|P'\big| K M^2 |A|^2 \gg M|D|^3/K$$

and the assertion follows if we will show that M is large.

Now, assume that there exists a set $P'' \subseteq P$ of size $|P|/2$ such that for every $s \in P''$ we have $|A - A_s| < K^{1/2} M|A|$. Therefore, for each $s \in P''$, $\mathsf{E}(A, A_s) > |A||A_s|^2/K^{1/2}M$, so that

$$\sum_x (A\circ A)(x)(A_s \circ A_s)(x) > \frac{|A||A_s|^2}{K^{1/2} M}.$$

Pigeonholing, for each $s \in P''$ there is a $1 \leqslant i = i(s) \leqslant \frac{1}{2}\log(KM^2)$ such that

$$\sum_{\substack{x: \\ |A|/2^i < (A\circ A)(x) \leqslant |A|/2^{i-1}}} (A_s \circ A_s)(x) \gg \frac{2^i |A_s|^2}{K^{1/2} M \log K}. \tag{98}$$

Thus, there exist i_0 and a set $Q \subseteq P''$ of size $\gg |P|/\log K$ such that for every $s \in Q$, $i(s) = i_0$. Let $G_s \subseteq A_s^2$ consist of all pairs $(a, a') \in A_s^2$ such that $(A \circ A)(a - a') \geqslant |A|/2^{i_0}$. By (98) it follows that $|G_s| \gg 2^{i_0}|A_s|^2/(K^{1/2} M \log K)$. Again we may assume that

$$|A_s \overset{G_s}{-} A_s| \gg \frac{2^{2i_0}|A_s|}{M^3 \log K},$$

because otherwise after some choice of constants, we have $\mathsf{E}(A_s) \geqslant |G_s|^2/|A_s \overset{G_s}{-} A_s| \geqslant M|A_s|^3/K$. Put

$$X = \bigcup_{s\in Q} \bigl(A_s \overset{G_s}{-} A_s\bigr)$$

and observe that $|X|2^{-2i_0}|A|^2 \leqslant \mathsf{E}(A) \leqslant M|A|^3/K$, so $|X| \leqslant 2^{2i_0}M|A|/K$. Define

$$g(x) = \bigl|\bigl\{s \in Q : x \in A_s \overset{G_s}{-} A_s\bigr\}\bigr|$$

and notice that if $x \in A_s \overset{G_s}{-} A_s$ then $s \in D \cap (x + D)$. Therefore, assuming $\mathsf{E}(D) \leqslant M|D|^3/K$ and $\mathsf{E}(X) \leqslant M|X|^3/K$,

$$\begin{aligned}\frac{|A|^2 2^{2i_0}}{M^4 \log^2 K} &\ll \sum_{s\in Q} |A_s \overset{G_s}{-} A_s| = \sum_{x\in X} g(x) \leqslant \sum_{x\in X} (D \circ D)(x)\\ &= \sum_{d\in D} (D \circ X)(d) \leqslant |D|^{1/2}\mathsf{E}(D)^{1/4}\mathsf{E}(X)^{1/4}\\ &\leqslant M^{1/4}K|A|^{5/4}\mathsf{E}(X)^{1/4}. \qquad (99)\end{aligned}$$

On the other hand for each $x \in X$ we have $(A \circ A)(x) \geqslant |A|/2^{i_0}$, so that

$$2^{-i_0}|A||X| \leqslant \sum_{x\in X} (A \circ A)(x) \leqslant M^{1/4}K^{-1/4}|A|^{5/4}\mathsf{E}(X)^{1/4}. \qquad (100)$$

Combining (99) and (100), in view of $|A| \geqslant K|X|/(2^{2i_0}M)$, we see that

$$\mathsf{E}(X) \gg \frac{|X|^3}{M^{10}K^{1/2}\log^4 K}.$$

The assertion follows for $M \gg K^{1/22}/\log^{4/11} K$. □

Acknowledgments

I.D.S. is grateful to A.V. Akopyan and F. Petrov for useful discussions. Both authors are grateful to N.G. Moshchevitin and V.F. Lev. I.D.S. thanks Institute IITP RAN for excellent working conditions.

References

[1] N. Alon, B. Bukh, B. Sudakov, Discrete Kakeya-type problems and small bases, Israel J. Math. 174 (2009) 285–301.
[2] A. Balog, Many additive quadruples, in: Additive Combinatorics, in: CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 39–49.
[3] A. Balog, A note on sum-product estimates, preprint.
[4] A. Balog, E. Szemerédi, A statistical theorem of set addition, Combinatorica 14 (1994) 263–268.
[5] M. Bateman, N. Katz, New bounds on caps sets, arXiv:1101.5851v1 [math.CA], 31 January 2011.
[6] M. Bateman, N. Katz, Structure in additively nonsmoothing sets, arXiv:1104.2862v1 [math.CO], 14 April 2011.
[7] T. Cochraine, http://gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/#comment-10647.
[8] E. Croot, O. Sisask, A probabilistic technique for finding almost-periods of convolutions, Geom. Funct. Anal. 20 (2010) 1367–1396.
[9] E. Croot, I.Z. Ruzsa, T. Schoen, Arithmetic progressions in sparse sumsets, in: Combinatorial Number Theory, de Gruyter, Berlin, 2007, pp. 157–164.
[10] W.T. Gowers, A new proof of Szemerédi's theorem, Geom. Funct. Anal. 11 (2001) 465–588.
[11] W.T. Gowers, Quasirandom groups, Combin. Probab. Comput. 17 (2008) 363–387.
[12] J.A. Haight, Difference covers which have small k-sums for any k, Mathematika 20 (1973) 109–118.
[13] A. Iosevich, V.S. Konyagin, M. Rudnev, V. Ten, On combinatorial complexity of convex sequences, Discrete Comput. Geom. 35 (2006) 143–158.

[14] J. Johnsen, On the distribution of powers in finite fields, J. Reine Angew. Math. 251 (1971) 10–19.
[15] N.H. Katz, P. Koester, On additive doubling and energy, SIAM J. Discrete Math. 24 (2010) 1684–1693.
[16] S.V. Konyagin, Estimates for trigonometric sums and for Gaussian sums, in: IV International Conference "Modern Problems of Number Theory and Its Applications", Part 3, Moscow State University, 2002, pp. 86–114.
[17] S. Konyagin, I. Shparlinski, Character Sums with Exponential Functions, Cambridge University Press, Cambridge, 1999.
[18] S. Kopparty, V.F. Lev, S. Saraf, M. Sudan, Kakeya-type sets in finite vector spaces, arXiv:1003.3736v1 [math.NT].
[19] L. Li, On a theorem of Schoen and Shkredov on sumsets of convex sets, arXiv:1108.4382v1 [math.CO].
[20] G. Petridis, New proofs of Plünnecke-type estimates for product sets in non-abelian groups, preprint.
[21] W. Rudin, Fourier Analysis on Groups, Wiley, 1990, reprint of the 1962 original.
[22] I.Z. Ruzsa, On the cardinality of $A + A$ and $A - A$, in: Combinatorics, vol. II, Proc. Fifth Hungarian Colloq., Keszthely, 1976, in: Colloq. Math. Soc. János Bolyai, vol. 18, North-Holland, Amsterdam, New York, 1978, pp. 933–938.
[23] I.Z. Ruzsa, Sumsets and structure, in: Combinatorial Number Theory and Additive Group Theory, in: Adv. Courses Math. CRM Barcelona, Birkhäuser Verlag, Basel, 2009, pp. 87–210.
[24] T. Sanders, On the Bogolubov–Ruzsa lemma, preprint.
[25] T. Sanders, On Roth's theorem on progressions, Ann. of Math. 174 (1) (2011) 619–636.
[26] T. Sanders, Popular difference sets, Online J. Anal. Comb. 5 (2010), Article 5, 4 pp.
[27] T. Schoen, I.D. Shkredov, Additive properties of multiplicative subgroups of $\mathbb{F}_p$, Q. J. Math. 63 (3) (2012) 713–722.
[28] T. Schoen, I.D. Shkredov, On sumsets of convex sets, Combin. Probab. Comput. 20 (2011) 793–798.
[29] I.D. Shkredov, On sets of large exponential sums, Izv. Russ. Acad. Sci. 72 (1) (2008) 161–182.
[30] I.D. Shkredov, On sumsets of dissociated sets, Online J. Anal. Comb. 4 (2009) 1–26.
[31] I.D. Shkredov, Some applications of W. Rudin's inequality to problems of combinatorial number theory, Unif. Distrib. Theory 6 (2) (2011) 95–116.
[32] I.D. Shkredov, I.V. V'ugin, On additive shifts of multiplicative subgroups, Mat. Sb. 203 (6) (2012) 81–100.
[33] I.D. Shkredov, S. Yekhanin, Sets with large additive energy and symmetric sets, J. Combin. Theory Ser. A 118 (2011) 1086–1093.
[34] J. Solymosi, An upper bound for the multiplicative energy, arXiv:0806.1040v1 [math.CO], 5 June 2008.
[35] E. Szemerédi, W.T. Trotter, Extremal problems in discrete geometry, Combinatorica 3 (1983) 381–392.
[36] T. Tao, V. Vu, Additive Combinatorics, Cambridge University Press, 2006.