Труды Москов. Матем. Общ.
Том 74 (2013), вып. 1

Trans. Moscow Math. Soc.
2013, Pages 31–63
S 0077-1554(2014)00212-0
Article electronically published on April 9, 2014

SOME NEW RESULTS ON HIGHER ENERGIES

I. D. SHKREDOV

Abstract. This article is concerned with the method of higher energies from combinatorial number theory. Upper bounds are obtained for the additive energies of convex sets and of sets A with small $|AA|$ and $|A(A+1)|$. New structural results, involving the notion of a dual popular difference set, are proved in terms of higher energies.

Contents

§ 1. Introduction

The method of higher energies (or, in other words, the method of higher moments of convolutions of characteristic functions of sets) was proposed in [20], developed further in [22, 27] and, finally, found a series of applications in [10, 14, 15, 16, 21, 25, 26]. In this paper, we obtain some new results in this direction, using the so-called operator method (or method of eigenvalues) from [24, 25], which, for the convenience of the reader, we recall in § 4.

Our main results are contained in §§ 5–7. In § 5 we apply the method of eigenvalues and obtain new upper bounds for the additive energy of some families of sets. For example, we formulate a result which concerns the family of convex subsets (that is, images of convex mappings) of $\mathbb{R}$.

Theorem 1.1. *Let $A \subseteq \mathbb{R}$ be a convex set. Then*

$$\mathsf{E}(A) \ll |A|^{32/13} \log^{71/65} |A|. \tag{1.1}$$

Here, $\mathsf{E}(A)$ is the so-called *additive energy* of our set A, equal to the number of solutions of the equation $a_1 - a_2 = a_3 - a_4$, where $a_1, a_2, a_3, a_4 \in A$. Equation (1.1) was

2010 *Mathematics Subject Classification.* Primary 11B30; Secondary 11B75 .

Key words and phrases. Combinatorial number theory, higher energies, popular difference set.

This work was supported by the grant RFFI 11-01-00759, the Government grant RF 11.G34.31.0053, the Federal Program "Scientific and Scientific-Pedagogical Personnel in Russia" 2009–2013, the Grant for Scientific Projects Undertaken by Leading Youth Collectives 12-01-33080, and the Grant for Leading Scientific Schools 2519.2012.1.

obtained in [12] with the constant $5/2$ in place of $32/13$. This was further improved to $89/36$ in [25], also using the method of eigenvalues.

The next section of this article contains so-called structural results. In additive combinatorics, the most important example of this type of statement is, of course, Freiman's remarkable theorem on sets with small doubling or, in other words, on sets with small sum, which gives a complete description of the given family of sets (see [28]). Here we mean something a little different by structural results. In our theorems, proceeding from certain conditions on the set A (mostly on the higher energies of the set), it is proved that certain subsets of A have small doubling or large additive energy. As an example of this class of statements, we recall the strong structural theorem in [2].

In what follows, it is assumed that $\mathbf{G}$ is an Abelian group.

Theorem 1.2. *Let $A \subseteq \mathbf{G}$ be a symmetric set, and let τ_0, σ_0 be nonnegative real numbers. Assume further that A has the property that for every $A_* \subseteq A$ with $|A_*| \gg |A|$ the additive energy satisfies $\mathsf{E}(A_*) \gg \mathsf{E}(A) = |A|^{2+\tau_0}$. Suppose that $\mathsf{T}_4(A) \ll |A|^{4+3\tau_0+\sigma_0}$. Then there exists a function $f_{\tau_0}\colon (0,1) \to (0,\infty)$ such that $f_{\tau_0}(\eta) \to 0$ as $\eta \to 0$, and also a number $\alpha \geq 0$ and sets $X_j, H_j \subseteq \mathbf{G}$, $B_j \subseteq A$, for $j \in [|A|^{\alpha - f_{\tau_0}(\sigma_0)}]$, with the properties*

$$|H_j| \ll |A|^{\tau_0+\alpha+f_{\tau_0}(\sigma_0)}, \quad |X_j| \ll |A|^{1-\tau_0-2\alpha+f_{\tau_0}(\sigma_0)},$$
$$|H_j - H_j| \ll |H_j|^{1+f_{\tau_0}(\sigma_0)}, \quad |(X_j + H_j) \cap B_j| \gg |A|^{1-\alpha-f_{\tau_0}(\sigma_0)},$$

and, for all $i \neq j$, $B_i \cap B_j = \emptyset$.

Here, $\mathsf{T}_4(A)$ is the number of solutions of the equation

$$a_1 + a_2 + a_3 + a_4 = a_1' + a_2' + a_3' + a_4', \quad a_1, a_2, a_3, a_4, a_1', a_2', a_3', a_4' \in A.$$

In this article, we need to generalize the concept of the additive energy of a set: for every $s \geq 1$, we set

$$\mathsf{E}_s(A) = \sum_x |A \cap (A - x)|^s. \tag{1.2}$$

The values $\mathsf{E}_s(A)$ in (1.2) are precisely what we call higher energies.

We now formulate two of our structural results. Weaker variants of the first statement were proved in [22] and [25]. From a certain point of view, results of this type may be called optimal versions of the Balog–Szemerédi–Gowers Theorem; see [22].

Theorem 1.3. *Let $A \subseteq \mathbf{G}$ be some set, $\mathsf{E}(A) = |A|^3/K$, and $\mathsf{E}_3(A) = M|A|^4/K^2$. Then there exists a set $A' \subseteq A$ such that*

$$|A'| \gg M^{-10} \log^{-15} M \cdot |A| \tag{1.3}$$

and

$$|nA' - mA'| \ll (M^9 \log^{14} M)^{6(n+m)} K |A'|, \tag{1.4}$$

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

It is interesting that the generality of Theorem 1.3 permits the proof of a "nontrivial" bound in Theorem 1.1, that is, an inequality of the form $\mathsf{E}(A) \ll |A|^{5/2-\varepsilon_0}$, where $\varepsilon_0 > 0$ is an absolute constant. A similar reduction is valid also in the case of a multiplicative subgroup $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number (see Remark 6.2).

We now state our second structural result.

Theorem 1.4. *Let $A \subseteq \mathbf{G}$ be some set, $\mathsf{E}_{3/2}(A) = |A|^{5/2}/K^{1/2}$, and $\mathsf{T}_4(A) = M|A|^7/K^3$. Then there exists a set $A' \subseteq A$ such that*

$$|A'| \gg \frac{|A|}{MK} \tag{1.5}$$

and

$$\mathsf{E}(A') \gg \frac{|A'|^3}{M}. \tag{1.6}$$

It is easy to see that Theorem 1.4 is sharp (see, for example, Remark 6.5). Our condition on $\mathsf{E}_{3/2}(A)$ is, of course, stronger than the condition on $\mathsf{E}(A)$ in Theorem 1.2.

The popular difference set is a simple and important object in additive combinatorics (see, for example, [8, 9, 28]). In § 7, we develop an idea due to Bateman and Katz [1, 2] that every popular difference set corresponds to a certain other set, which we call the dual popular set. As an application, our method allows us to establish a nontrivial connection between the quantities $\mathsf{E}(A)$ and $\mathsf{E}_s(A)$, for $s \in [1,2]$; see Theorem 7.2 or Corollary 7.5. It is interesting that a similar relationship does not also hold for $s > 2$.

Finally, we note that the methods we use are entirely elementary, in the sense that they do not use Fourier transforms.

The author thanks Tomasz Schoen, Sergei Vladimirovich Konyagin and Misha Rudnev for fruitful discussions and explanations.

§ 2. Definitions

Let $\mathbf{G}$ be an Abelian group. If $\mathbf{G}$ is finite, then we denote its order by N. We define two types of convolution in $\mathbf{G}$:

$$(f*g)(x) := \sum_{y\in\mathbf{G}} f(y)g(x-y)$$

and

$$(f\circ g)(x) := \sum_{y\in\mathbf{G}} f(y)g(y+x) = (f*g^c)(-x),$$

where we set $h^c(x) := h(-x)$, for a function $h\colon \mathbf{G}\to\mathbb{C}$. Clearly,

$$(f*g)(x) = (g*f)(x) \quad \text{and} \quad (f\circ g)(x) = (g\circ f)(-x), \quad \text{for } x\in\mathbf{G}.$$

We denote by $*_k$ the result of applying the first type of convolution k times, for $k\in\mathbb{N}$; to put this another way, $*_k := *(*_{k-1})$.

In this article, we use the same letter to denote a set $S\subseteq\mathbf{G}$ and its characteristic function $S\colon \mathbf{G}\to\{0,1\}$. We denote the *additive energy* of two sets $A,B\subseteq\mathbf{G}$ by $\mathsf{E}(A,B)$ (see, for example, [28]); in other words,

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

If $A=B$, then we write $\mathsf{E}(A)$ in place of $\mathsf{E}(A,A)$. Clearly,

$$\mathsf{E}(A,B) = \sum_x (A*B)(x)^2 = \sum_x (A\circ B)(x)^2 = \sum_x (A\circ A)(x)(B\circ B)(x). \tag{2.1}$$

Let

$$\mathsf{T}_k(A) := \sum_x (A*_{k-1}A)^2(x)$$
$$= \big|\big\{a_1+\ldots+a_k = a_1'+\ldots+a_k'\colon a_1,\ldots,a_k,a_1',\ldots,a_k'\in A\big\}\big|.$$

Also let

$$\sigma_k(A) := (A*_{k-1}A)(0) = \big|\big\{a_1+\ldots+a_k = 0\colon a_1,\ldots,a_k\in A\big\}\big|.$$

We note that for a symmetric set A, that is, a set for which $A=-A$, we have $\sigma_2(A)=|A|$ and $\sigma_{2k}(A)=\mathsf{T}_k(A)$. If $\psi\colon\mathbf{G}\to\mathbb{C}$ is some function, then we write

$$\sigma_\psi(A) = \sigma(\psi,A) := \sum_x \psi(x)(A\circ A)(x).$$

In this way, if we take another set $P \subseteq \mathbf{G}$, then $\sigma_P(A)$ is equal to $\sigma_P(A) := \sum_{x\in P}(A\circ A)(x)$. Similarly, $\mathsf{E}_P(A) := \sum_{x\in P}(A\circ A)^2(x)$.

For a sequence $s = (s_1,\dots,s_{k-1})$, we put

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

If $B = A$, then we write A_s for A_s^A. Let

$$\mathsf{E}_k(A) = \sum_x |A\cap(A-x)|^s = \sum_{x\in\mathbf{G}}(A\circ A)(x)^k = \sum_{s_1\in\mathbf{G},\dots,s_{k-1}\in\mathbf{G}}|A_s|^2 \tag{2.2}$$

and

$$\mathsf{E}_k(A,B) = \sum_{x\in\mathbf{G}}(A\circ A)(x)(B\circ B)(x)^{k-1} = \sum_{s_1\in\mathbf{G},\dots,s_{k-1}\in\mathbf{G}}|B_s^A|^2 \tag{2.3}$$

be the higher energies of A and B. The first formulae of (2.2) and (2.3) can be regarded as defining the quantities $\mathsf{E}_k(A)$ and $\mathsf{E}_k(A,B)$ for an arbitrary, not necessarily integer, $k\ge 1$. As above, for a set $P\subseteq\mathbf{G}$, we write

$$\mathsf{E}_k^P(A) := \sum_{s\in P}|A_s|^k,$$

and for the set $\mathscr{P}$ from $\mathbf{G}^{k-1}$, we put

$$\mathsf{E}_k^{\mathscr{P}}(A) := \sum_{(s_1,\dots,s_{k-1})\in\mathscr{P}}|A_s|^2.$$

Clearly,

$$\begin{aligned}\mathsf{E}_{k+1}(A,B) &= \sum_x (A\circ A)(x)(B\circ B)(x)^k\\ &= \sum_{x_1,\dots,x_{k-1}}\Big(\sum_y A(y)B(y+x_1)\dots B(y+x_k)\Big)^2\\ &= \mathsf{E}(\Delta_k(A),B^k),\end{aligned} \tag{2.4}$$

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

The quantities $\mathsf{E}_k(A,B)$ can be written in terms of the above convolutions.

Definition 2.1. Let $k\ge 2$ be a positive integer and $f_0,\dots,f_{k-1}\colon \mathbf{G}\to\mathbb{C}$ be some functions. Let F be the vector $(f_0,\dots,f_{k-1})$ and x be the vector $(x_1,\dots,x_{k-1})$. We denote by $\mathcal{C}_k(f_0,\dots,f_{k-1})(x_1,\dots,x_{k-1})$ the function

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

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

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

The following lemma from [25] concerns the basic properties of the function $\mathscr{C}_k(f_0,\dots,f_{k-1})$.

Lemma 2.2. *In the above notation, we have*

$$\begin{aligned}\sum_{x_1,\dots,x_{l-1}} &\mathscr{C}_l(f_0,\dots,f_{l-1})(x_1,\dots,x_{l-1})\,\mathscr{C}_l(g_0,\dots,g_{l-1})(x_1,\dots,x_{l-1})\\ &= \sum_z (f_0\circ g_0)(z)\dots(f_{l-1}\circ g_{l-1})(z)\quad\text{(the inner product)}.\end{aligned} \tag{2.5}$$

Furthermore,

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

$$= \sum_{y_1,\dots,\,y_{k-1}} \mathscr{C}_k^l(f_0,\dots,f_{k-1})(y_1,\dots,y_{k-1}) \quad \text{(the generalized inner product)} \tag{2.6}$$

and

$$\sum_{x_1,\dots,\,x_{l-1}} \mathscr{C}_l(f_0)(x_1,\dots,x_{l-1})\big(\mathscr{C}_l(f_1)\circ\dots\circ\mathscr{C}_l(f_{k-1})\big)(x_1,\dots,x_{l-1}) = \sum_z (f_0\circ\dots\circ f_{k-1})^l(z) \quad (\sigma_k \textit{ for } \mathscr{C}_l). \tag{2.7}$$

Generalizing the quantities $\sigma_P(A)$, for $P\subseteq\mathbf{G}$, for an arbitrary set $\mathscr{P}\subseteq\mathbf{G}^{k-1}$ with $k\geq 2$, we define the sum

$$\sigma_{\mathscr{P}}(A) := \sum_{(s_1,\dots,s_{k-1})\in\mathscr{P}} \mathscr{C}_k(A)(s_1,\dots,s_{k-1}).$$

Let $f_1,\dots,f_t\colon \mathbf{G}\to\mathbb{C}$ be given functions. Their tensor product is defined by

$$(f_1\otimes f_2\otimes\dots\otimes f_t)(x_1,\dots,x_t) = f_1(x_1)f_2(x_2)\dots f_t(x_t).$$

For the tensor product of one function f, we write

$$(f^{\otimes})(x_1,\dots,x_t) = \prod_{j=1}^{t} f(x_j).$$

Thus, allowing some imprecision in the notation, we do not indicate the number t in the definition of the tensor power of a function. It is easy to see that

$$(g\circ f)^{\otimes} = (g^{\otimes}\circ f^{\otimes}) \quad \text{and} \quad (g*f)^{\otimes} = (g^{\otimes}*f^{\otimes}) \tag{2.8}$$

and, furthermore,

$$\mathscr{C}_k(f_0^{\otimes},\dots,f_{k-1}^{\otimes}) = \mathscr{C}_k^{\otimes}(f_0,\dots,f_{k-1}). \tag{2.9}$$

For a natural number n, we set $[n]=\{1,\dots,n\}$. All logarithms in this article are taken to base 2. We denote the usual Vinogradov symbols by $\ll$ and $\gg$. We write $\ll_M$ and $\gg_M$ if the symbols depend upon some constant M.

For arbitrary functions f and g, the expression $f\ll g^{1+}$ denotes the fact that for every $\varepsilon>0$, we have $f\ll g^{1+\varepsilon}$, and the expression $f\ll g^{1-}$ that for any $\varepsilon>0$, we have $f\ll g^{1-\varepsilon}$.

§ 3. Preliminaries

We begin this section by recalling several standard facts about matrices. The first statement that we need is the following lemma on singular value decompositions (see, for example, [22]).

Lemma 3.1. *Let n,m be natural numbers, with $n\leq m$, and let X,Y be sets with cardinalities n and m, respectively. Let $\mathbf{M}=\mathbf{M}(x,y)$, for $x\in X$ and $y\in Y$, be an $(n\times m)$ complex (real) matrix. Then there exist complex (real) functions u_j, defined in X, complex (real) functions v_j, defined in Y, and a nonnegative number λ_j such that*

$$\mathbf{M}(x,y) = \sum_{j=1}^{n} \lambda_j u_j(x)\overline{v_j(y)}, \tag{3.1}$$

where $\{u_j\}$ *for* $j \in [n]$ *and* $\{v_j\}$ *for* $j \in [n]$ *denote two orthonormalized sequences, and* (3.2)

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

Further:

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

$$\sum_{j=1}^n \lambda_j^4 = \sum_{x,\,x'} \Big| \sum_y \mathbf{M}(x,y)\overline{\mathbf{M}(x',y)} \Big|^2. \tag{3.3}$$

For $j \in [n]$, we call $\{u_j\}$ and $\{v_j\}$ singular functions.

We now recall the well-known Perron–Frobenius Theorem on the principal eigenvalues and corresponding nonnegative eigenvectors of nonnegative matrices (see, for example, [11, Chapter 8]). We denote the spectral radius of a square matrix M by $\rho(M)$.

Theorem 3.2. *Let* M *be a real square matrix with nonnegative elements. Then the eigenvalue* $\rho(M)$ *corresponds to a nonnegative eigenvector. Conversely, if the matrix* M *has a strictly positive eigenvector, then this corresponds to* $\rho(M)$.

We also need the convexity property of eigenvalues (see, for example, [11]).

Lemma 3.3. *Let* M *be a normal* $(n \times n)$*-matrix with eigenvalues* $\mu_1, \dots, \mu_n$, *and let* f *be an arbitrary convex function of* n *real variables. Then*

$$\max_{x_1,\dots,x_n} f\big(\langle Mx_1, x_1\rangle, \dots, \langle Mx_n, x_n\rangle\big) = \max_{i_1,\dots,i_n} f(\mu_{i_1}, \dots, \mu_{i_n}),$$

where the maximum on the left-hand side is taken over all orthonormalized systems of vectors $x_1, \dots, x_n$, *and the right-hand maximum over an arbitrary permutation of the numbers* $1, 2, \dots, n$.

We now recall some combinatorial results.

The first lemma we need is a special case of Lemma 2.8 in [27].

Lemma 3.4. *Let* A *be an arbitrary subset of an Abelian group. Then, for any* $k, l \in \mathbb{N}$, *we have*

$$\sum \mathsf{E}(A_s, A_t) = \mathsf{E}_{k+l}(A),$$

with the sum taken over all s, t *such that* $\|s\| = k-1$ *and* $\|t\| = l-1$, *where* $\|x\|$ *denotes the number of components of a vector* x.

We also need the Balog–Szemerédi–Gowers Theorem; see [28, Chapter 2.5]. The current bounds in this result are contained in [19].

Theorem 3.5. *Let* $\alpha \in (0, 1]$ *be a real number, and* A *and* B *be finite subsets of an Abelian group, with* $|A| \geq |B|$. *If* $\mathsf{E}(A, B) = \alpha|A|^3$, *then there exist sets* $A' \subseteq A$ *and* $B' \subseteq B$ *such that* $|A'| \gg \alpha|A|$, $|B'| \gg \alpha|B|$, *and*

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

We recall that a set $A = \{a_1, \dots, a_n\} \subseteq \mathbb{R}$ is called *convex* if $a_i - a_{i-1} < a_{i+1} - a_i$ for all $i \in \mathbb{N}$ with $2 \leq i \leq n-1$. We have the following lemma; see, for example, [21], [12] or [15].

Lemma 3.6. *Let A be a convex set, $A' \subseteq A$, and let B be an arbitrary set. Then*

$$|A'+B| \gg |A'|^{3/2}|B|^{1/2}|A|^{-1/2}. \tag{3.4}$$

If we arrange the quantities $(A *_{k-1} A)(x)$ in nonincreasing order,

$$(A *_{k-1} A)(x_1) \geq (A *_{k-1} A)(x_2) \geq \dots,$$

then

$$(A *_{k-1} A)(x_j) \ll_k |A|^{k-\frac{4}{3}(1-2^{-k})} j^{-1/3}. \tag{3.5}$$

In particular, $\mathsf{E}_3(A) \ll |A|^3 \log |A|$ and $\mathsf{E}(A,B) \ll |A| \cdot |B|^{3/2}$. An inequality similar to (3.5) also holds for the convolution $\circ$.

As noted in Li's paper [15] (see also [22]), sets A of real numbers with small multiplicative doubling behave very similarly to convex sets. More precisely, we have the following lemma from [22].

Lemma 3.7. *Let $A, B \subseteq \mathbb{R}$ be finite sets, and let $|AA| = M|A|$. If we arrange the quantities $(A \circ B)(x)$ in nonincreasing order,*

$$(A \circ B)(x_1) \geq (A \circ B)(x_2) \geq \dots,$$

then we have the inequality

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

In particular,

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

§ 4. Operators

In this section, we describe a certain family of operators (finite matrices). The use of these operators allows us to prove a whole series of inequalities from [15, 20, 21, 25], and others, using a single method. In this part of the article, we also prove several lemmas we need later on. We note that our definitions differ somewhat from those in [24]. In particular, we do not use Fourier transforms.

Let $g\colon \mathbf{G} \to \mathbb{C}$ be an arbitrary function and $A, B \subseteq \mathbf{G}$ some finite sets. We assume that $|B| \leq |A|$. We denote by $\mathrm{T}^g_{A,B}$ the rectangular matrix

$$\mathrm{T}^g_{A,B}(x,y) = g(x-y)A(x)B(y) \tag{4.1}$$

and by $\widetilde{\mathrm{T}}^g_{A,B}(x,y)$ the other rectangular matrix

$$\widetilde{\mathrm{T}}^g_{A,B}(x,y) = g(x+y)A(x)B(y). \tag{4.2}$$

We shall describe the simplest properties of the matrices $\mathrm{T}^g_{A,B}$ and $\widetilde{\mathrm{T}}^g_{A,B}$. By Lemma 3.1, we have

$$\mathrm{T}^g_{A,B}(x,y) = \sum_{j=0}^{|B|-1} \lambda_j(\mathrm{T}^g_{A,B}) u_j(x) v_j(y),$$

and similarly for $\widetilde{\mathrm{T}}^g_{A,B}$. Here, u_j, v_j are singular functions. We arrange the singular values in nonincreasing order,

$$\lambda_0(\mathrm{T}^g_{A,B}) \geq \lambda_1(\mathrm{T}^g_{A,B}) \geq \dots \geq \lambda_{|B|-1}(\mathrm{T}^g_{A,B}),$$

and similarly for $\widetilde{\mathrm{T}}^g_{A,\,B}$. We call λ_0 the principal singular value and the functions u_0, v_0 the principal singular functions. It is clear that

$$\mathrm{T}^g_{A,\,B}(\mathrm{T}^g_{A,\,B})^*(y,y') = B(y)B(y')\mathscr{C}_3(A,g,\overline{g})(-y,-y'), \tag{4.3}$$

$$\widetilde{\mathrm{T}}^g_{A,\,B}(\widetilde{\mathrm{T}}^g_{A,\,B})^*(y,y') = B(y)B(y')\mathscr{C}_3(A,g,\overline{g})(y,y'), \tag{4.4}$$

$$(\mathrm{T}^g_{A,\,B})^*\mathrm{T}^g_{A,\,B}(x,x') = A(x)A(x')\mathscr{C}_3(B,\overline{g}^c,g^c)(-x,-x'), \tag{4.5}$$

$$(\widetilde{\mathrm{T}}^g_{A,\,B})^*\widetilde{\mathrm{T}}^g_{A,\,B}(x,x') = A(y)A(y')\mathscr{C}_3(B,\overline{g},g)(x,x'). \tag{4.6}$$

For a real function g, we have $(\widetilde{\mathrm{T}}^g_{A,\,B})^* = \widetilde{\mathrm{T}}^g_{B,A}$. For an even real function g, we have $(\mathrm{T}^g_{A,\,B})^* = \mathrm{T}^g_{B,A}$. Using Lemma 3.1, we find

$$\begin{aligned}\sum_{j=0}^{|B|-1}\lambda_j^2(\mathrm{T}^g_{A,\,B}) &= \sum_{x,\,y}|g(x-y)|^2A(x)B(y),\\ \sum_{j=0}^{|B|-1}\lambda_j^2(\widetilde{\mathrm{T}}^g_{A,\,B}) &= \sum_{x,\,y}|g(x+y)|^2A(x)B(y).\end{aligned} \tag{4.7}$$

Further,

$$\begin{aligned}\sum_j\lambda_j^4(\mathrm{T}^g_{A,\,B}) &= \sum_{y,\,y'}B(y)B(y')\big|\mathscr{C}_3(A,g,\overline{g})(-y,-y')\big|^2\\ &= \sum_{x,\,x'}A(x)A(x')\big|\mathscr{C}_3(B,\overline{g}^c,g^c)(-x,-x')\big|^2\end{aligned} \tag{4.8}$$

and

$$\begin{aligned}\sum_j\lambda_j^4(\widetilde{\mathrm{T}}^g_{A,\,B}) &= \sum_{y,\,y'}B(y)B(y')\big|\mathscr{C}_3(A,g,\overline{g})(y,y')\big|^2\\ &= \sum_{x,\,x'}A(x)A(x')\big|\mathscr{C}_3(B,\overline{g},g)(x,x')\big|^2.\end{aligned} \tag{4.9}$$

In particular, in the following lemma we find all the singular values and the singular functions of the operators $\mathrm{T}^{A-B}_{A,\,B}$ and $\widetilde{\mathrm{T}}^{A+B}_{A,\,B}$.

Lemma 4.1. *Let $A, B \subseteq \mathbf{G}$ be finite sets with $|B| \le |A|$, and let $D, S \subseteq \mathbf{G}$ be two sets such that $A - B \subseteq D$ and $A + B \subseteq S$. Then the principal singular values and singular functions of the operators $\mathrm{T}^D_{A,\,B}$ and $\widetilde{\mathrm{T}}^S_{A,\,B}$ are equal to $\lambda_0 = (|A|\cdot|B|)^{1/2}$ and*

$$v_0(y) = \frac{B(y)}{|B|^{1/2}}, \quad u_0(x) = \frac{A(x)}{|A|^{1/2}},$$

respectively. The remaining singular values are equal to zero.

Proof. Applying formulae (4.3) and (4.4), it is easy to see that

$$(\mathrm{T}^D_{A,\,B}(\mathrm{T}^D_{A,\,B})^*B)(y) = B(y)\sum_{y'\in B}\mathscr{C}_3(A,D,D)(-y,-y') = |A|\cdot|B|B(y),$$

$$\begin{aligned}(\widetilde{\mathrm{T}}^S_{A,\,B}(\widetilde{\mathrm{T}}^S_{A,\,B})^*B)(y) &= B(y)\sum_{y'\in B}\mathscr{C}_3(A,S,S)(y,y')\\ &= |B|B(y)(A\circ S)(y) = |A|\cdot|B|B(y).\end{aligned}$$

Thus, $v_0(y) = B(y)/|B|^{1/2}$ and $\lambda_0 = (|A|\cdot|B|)^{1/2}$. Hence

$$u_0(x) = A(x)(|A|^{1/2}|B|)^{-1}\sum_y B(y)D(x-y) = \frac{A(x)}{|A|^{1/2}}$$

and

$$u_0(x) = A(x)(|A|^{1/2}|B|)^{-1}(B \circ S)(x) = \frac{A(x)}{|A|^{1/2}},$$

for $\mathrm{T}^{D}_{A,\,B}$ and $\widetilde{\mathrm{T}}^{S}_{A,\,B}$, respectively. By formula (4.7), we have

$$\sum_{j=0}^{|B|-1} \lambda_j^2 = |A| \cdot |B|.$$

This means that all the remaining singular values are equal to zero. □

We now apply an argument from [25, Proposition 28].

Lemma 4.2. *Let $A, B \subseteq \mathbf{G}$ be finite sets, and let $D, S \subseteq \mathbf{G}$ be arbitrary sets such that $A - B \subseteq D$ and $A + B \subseteq S$. Let ψ be some function on $\mathbf{G}$. Then*

$$|A|^2\sigma^2(\psi, B) \le \mathsf{E}_3(A, B)\sigma(\psi^2, D) \tag{4.10}$$

and

$$|A|^2\sigma^2(\psi, B) \le \mathsf{E}_3(A, B)\sigma(\psi^2, S). \tag{4.11}$$

Proof. We will prove the bound (4.11), since the proof of (4.10) is similar. We denote the singular values of the operator $\mathrm{T}^{S}_{A,\,B}$ by λ_j and the corresponding singular functions by u_j, v_j. Clearly, by Lemma 4.1 we have

$$S(x + y)A(x)B(y) = \sum_{j=0}^{|B|-1} \lambda_j u_j(x)v_j(y) = \lambda_0 u_0(x)v_0(y).$$

Applying Lemma 4.1 once again, we find

$$\sum_{x\in A}\sum_{y,\,z\in B} S(x + y)S(x + z)\psi(y - z) = \lambda_0^2 \sum_{y,\,z} \psi(y - z)v_0(y)v_0(z) = |A|\sigma(\psi, B).$$

Further,

$$\sum_{x\in A}\sum_{y,\,z\in B} S(x + y)S(x + z)\psi(y - z) = \sum_{\alpha,\beta} S(\alpha)S(\beta)\psi(\alpha - \beta)\mathscr{C}_3(-A, B, B)(\alpha, \beta).$$

By the Cauchy–Bunyakovskii inequality, we obtain

$$|A|^2\sigma^2(\psi, B) \le \mathsf{E}_3(A, B) \sum_{\alpha,\beta} S(\alpha)S(\beta)\psi^2(\alpha - \beta) = \mathsf{E}_3(A, B)\sigma(\psi^2, S), \tag{4.12}$$

as required. □

Corollary 4.3. *For any $A, B \subseteq \mathbf{G}$, we have*

$$|A|^2\mathsf{E}^2_{3/2}(B) \le \mathsf{E}_3(A, B)\mathsf{E}(B, A \pm B) \le \mathsf{E}_3^{1/3}(A)\mathsf{E}_3^{2/3}(B)\mathsf{E}(B, A \pm B). \tag{4.13}$$

This inequality was obtained in [15].

Corollary 4.4. *For any $A \subseteq \mathbf{G}$, we have*

$$|A|^6 \le \mathsf{E}_3(A) \sum_{x\in A-A} \big((A \pm A) \circ (A \pm A)\big)(x).$$

This inequality is from [21].

We now consider the symmetric variant of the above operators.

Let $g\colon \mathbf{G} \to \mathbb{C}$ be some function and $A \subseteq \mathbf{G}$ an arbitrary finite set. We let T^{g}_{A} denote the matrix

$$\mathrm{T}^{g}_{A}(x, y) = g(x - y)A(x)A(y), \tag{4.14}$$

and $\widetilde{\mathrm{T}}^g_A(x,y)$ the matrix

$$\widetilde{\mathrm{T}}^g_A(x,y) = g(x+y)A(x)A(y). \tag{4.15}$$

The general theory of the given operators was developed in [24], and applications can be found in [22, 24, 25, 26]. We shall describe the simplest properties of the matrices T^g_A and $\widetilde{\mathrm{T}}^g_A$. It is easy to see that T^g_A is Hermitian if and only if $\overline{g(-x)} = g(x)$ and $\widetilde{\mathrm{T}}^g_A$ is Hermitian if and only if g is a real function. Below, we shall only deal with Hermitian operators defined by real functions g. We arrange the eigenvalues in nonincreasing order,

$$|\mu_0(\mathrm{T}^g_A)| \geq |\mu_1(\mathrm{T}^g_A)| \geq \ldots \geq |\mu_{|A|-1}(\mathrm{T}^g_A)|,$$

and similarly for $\widetilde{\mathrm{T}}^g_A$. We call μ_0 the principal eigenvalue and the corresponding eigenfunction the principal eigenfunction. By Lemma 3.1, we have

$$\sum_j \mu_j(\mathrm{T}^g_A) = g(0)|A| \quad \text{and} \quad \sum_j \mu_j(\widetilde{\mathrm{T}}^g_A) = \sum_x A(x)g(2x). \tag{4.16}$$

Further, in the case of Hermitian (normal) matrices T^g_A, $\widetilde{\mathrm{T}}^g_A$ we obtain

$$\sum_j |\mu_j(\mathrm{T}^g_A)|^2 = \sum_z |g(z)|^2 (A\circ A)(z) \quad \text{and} \quad \sum_j |\mu_j(\widetilde{\mathrm{T}}^g_A)|^2 = \sum_x |g(z)|^2 (A * A)(z). \tag{4.17}$$

Let $f_0, f_1, \ldots, f_{|A|-1}$ be the sequence of corresponding eigenfunctions. Some results on these functions can be found in [25].

Of course, the singular values of the operators $\mathrm{T}^g_{A,\,A}$ and the eigenvalues of the operators T^g_A, in the case when T^g_A is Hermitian, are connected by the simple formula

$$\lambda_j(\mathrm{T}^g_{A,\,A}) = |\mu_j(\mathrm{T}^g_{A,\,A})|.$$

The same equality holds for the operators $\widetilde{\mathrm{T}}^g_{A,\,A}$ and $\widetilde{\mathrm{T}}^g_A$.

Example 4.5. One of the main reasons why the above operators were introduced was in an attempt to use them to find additive subsets, richer than A. We consider a typical example. Let $A = H \sqcup \Lambda \subseteq \mathbb{F}_p^n$, where H is a subspace and Λ is a dissociative set (basis). We suppose that $|H| \gg |A|^{2/3}$ and $|H| \ll |A|$. Then $\mathsf{E}(A) \sim \mathsf{E}(H)$ and, by the Courant–Fischer Theorem, A is not a principal eigenfunction of the operator $\mathrm{T}^{A\circ A}_A$ since $\mathsf{E}(A)/|A| < \mathsf{E}(H)/|H| \leq \mathsf{E}(A,H)/|H|$. Thus, in this case, the support of the principal eigenfunction belongs to H, and not to all of A. Another reason for the operator method is the attempt to carry out "local" analysis. Of course, this is a strong distinction between it and the method of Fourier transforms, which deals with the whole of the group $\mathbf{G}$.

The proof of the following analogue of Lemma 4.1 is almost word-for-word the same.

Lemma 4.6. *Let $A \subseteq \mathbf{G}$ be a finite set, and let $D, S \subseteq \mathbf{G}$ be arbitrary sets such that $A - A \subseteq D$ and $A + A \subseteq S$. Then, the operators T^D_A, $\widetilde{\mathrm{T}}^S_A$ have $\mu_0 = |A|$, $f_0(x) = A(x)/|A|^{1/2}$, and all their remaining eignevalues are equal to zero.*

Proof. We see that in both cases $\mu_0 = |A|$ and $f_0 = A(x)/|A|^{1/2}$. Further, by formulae (4.16) and (4.17) the eigenvalues of T^D_A and $\widetilde{\mathrm{T}}^S_A$ satisfy

$$\sum_j \mu_j = |A| \quad \text{and} \quad \sum_j |\mu_j|^2 = |A|^2.$$

Thus, the remaining eigenvalues of both operators are equal to zero. $\square$

Remark 4.7. If, in (4.10) and (4.11), we take a single set $A = B$ and we set

$$\psi(x) = (A \circ A)(x)/(D \circ D)(x) \text{ or } \psi(x) = (A \circ A)(x)/(S \circ S)(x),$$

then we obtain

$$\sum_{x \in D} \frac{(A \circ A)^2(x)}{(D \circ D)(x)} \le \frac{\mathsf{E}_3(A)}{|A|^2} \quad \text{and} \quad \sum_{x \in D} \frac{(A \circ A)^2(x)}{(S \circ S)(x)} \le \frac{\mathsf{E}_3(A)}{|A|^2}.$$

A slightly more precise inequality was proved in [25].

In addition to formulae (4.16) and (4.17), there exists an interesting interrelation between the eigenvalues $\mu_\alpha(\mathrm{T}_A^g)$ and eigenfunctions f_α of our operators. We denote the average value of the corresponding eigenfunction by g_α, that is,

$$g_\alpha = \sum_x f_\alpha(x).$$

We shall formulate our result for the operators T_A^g. It goes without saying that a similar statement holds for $\widetilde{\mathrm{T}}_A^g$.

Proposition 4.8. *Let $g\colon \mathbf{G} \to \mathbb{C}$ be an arbitrary function such that $\overline{g(-x)} = g(x)$. Then*

$$\sum_\alpha \mu_\alpha |g_\alpha|^2 = \sum_x g(x)(A \circ A)(x), \tag{4.18}$$

$$\sum_\alpha |\mu_\alpha|^2 |g_\alpha|^2 = \sum_{x \in A} |(g \circ A)(x)|^2. \tag{4.19}$$

Further, if g is a real even function, then

$$\sum_\alpha \mu_\alpha |\mu_\alpha g_\alpha|^2 \ge \frac{1}{|A|^2} \Big(\sum_x g(x)(A \circ A)(x) \Big)^3. \tag{4.20}$$

Proof. Formula (4.18) follows from the definition of the operator T_A^g, since $\langle \mathrm{T}_A^g A, A\rangle = \sum_x g(x)(A \circ A)(x)$. To prove (4.19), note that

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

Thus,

$$\mu_\alpha g_\alpha = \sum_x A(x)(g * f_\alpha)(x). \tag{4.21}$$

Taking the square of formula (4.21), summing the resulting equalities over α, and using the orthogonality of the functions f_α, we find

$$\begin{aligned} \sum_\alpha |\mu_\alpha|^2 \cdot |g_\alpha|^2 &= \sum_\alpha \sum_{x,\, x' \in A} f_\alpha(z)\overline{f_\alpha(z')} g(x - z)\overline{g(x' - z')} \\ &= \sum_{x,\, x' \in A} \sum_{z \in A} g(x - z)\overline{g(x' - z)} = \sum_{x \in A} |(g \circ A)(x)|^2. \end{aligned}$$

To prove (4.20), we recall a useful inequality due to A. Carbery [5] (see also [6]), namely,

$$\langle \mathrm{T} f_1, f_2\rangle^3 \le \|f_1\|_3^3 \cdot \|f_2\|_3^3 \cdot \sum_{x,\, y} \mathrm{T}(x, y) \Big(\sum_a \mathrm{T}(x, a) \Big) \Big(\sum_b \mathrm{T}(b, y) \Big), \tag{4.22}$$

valid for $\mathrm{T}, f_1, f_2 \ge 0$. Since

$$\mathrm{T}_A^g(x, y) = \sum_\alpha \mu_\alpha f_\alpha(x)\overline{f_\alpha(y)},$$

substituting $\mathrm{T} = \mathrm{T}^g_A$ and $f_1 = f_2 = A$ into (4.22) gives us

$$\Big(\sum_x g(x)(A\circ A)(x)\Big)^3 \le |A|^2\cdot\sum_{x,\,y}\sum_\alpha \mu_\alpha f_\alpha(x)\overline{f_\alpha(y)}\Big(\sum_\beta \overline{\mu_\beta f_\beta(x)}g_\beta\Big)\Big(\sum_\gamma \overline{\mu_\gamma g_\gamma}f_\gamma(y)\Big)$$
$$= |A|^2\cdot\sum_\alpha \mu_\alpha|\mu_\alpha g_\alpha|^2. \quad \square$$

Let t be a natural number. We denote the operator $\mathrm{T}^{g^\otimes}_{A^\otimes}$, where the tensor power of the functions g and A is taken t times, by $(\mathrm{T}^g_A)^\otimes$. We call the operator that we have obtained the t-th tensor power of T^g_A. It is easy to see that the tensor power thus defined coincides with the usual tensor power. It is clear that if T^g_A is Hermitian, then the operator $(\mathrm{T}^g_A)^\otimes$ is also Hermitian. We will prove a result on tensor powers of the operator T^g_A.

Lemma 4.9. *Let t be a natural number, and let $g\colon \mathbf{G}\to\mathbb{C}$ be an arbitrary function such that $\overline{g(-x)} = g(x)$. Then the eigenvalues and eigenfunctions of the t-th tensor powers $(\mathrm{T}^g_A)^\otimes$ are given by all the possible products of t eigenvalues and eigenfunctions of the operator T^g_A. In particular, $\mu_0((\mathrm{T}^g_A)^\otimes) = \mu_0^t(\mathrm{T}^g_A)$.*

Proof. Since $\overline{g(-x)} = g(x)$, the operator T^g_A is Hermitian. Let $\{f_\alpha\}$, for $\alpha\in[|A|]$, be an orthonormal family of eigenfunctions of the operator T^g_A. Using (2.8) and the definition of the operator T^g_A, it is easy to see that the $|A|^t$ products of the form $\prod_{j=1}^{|A|} f_{\alpha_j}$, for $\alpha_j\in\{0,1,\dots,|A|-1\}$, are orthonormalized eigenfunctions of $(\mathrm{T}^g_A)^\otimes$. The lemma is proved. $\square$

It will be very convenient to formulate the results of [22, 25] in terms of eigenvalues of operators. As an example, we state an operator version of Theorem 56 from [25].

Theorem 4.10. *Let $A\subseteq\mathbf{G}$ be a set, $\mu_0 = \mu_0(\mathrm{T}^{A\circ A}_A)$, and $\mathsf{E}_3(A) = M\mu_0^2$. Suppose that $M\le \mu_0/(6|A|)$. Then there exists a real number r such that*

$$1\le r\le \frac{1}{|A|}\max_{x\ne 0}(A\circ A)(x)\cdot\frac{|A|^2}{\mu_0}M^{1/2}\le \frac{|A|^2}{\mu_0}M^{1/2}, \tag{4.23}$$

and a set $A'\subseteq A$ for which

$$|A'|\gg M^{-23/2}r^{-2}\log^{-9}|A|\cdot|A| \tag{4.24}$$

and

$$|nA'-mA'|\ll (M^9\log^6|A|)^{7(n+m)}r^{-1}M^{1/2}\frac{|A|^2}{\mu_0}|A'|, \tag{4.25}$$

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

We recall a lemma from [25].

Lemma 4.11. *Let $A\subseteq\mathbf{G}$ be a set, g a nonnegative function, and let $\mu_0 = \mu_0(\mathrm{T}^g_A)$. Then*

$$|A|\ge\Big(\sum_x f_0(x)\Big)^2\ge\max\Big\{\frac{\mu_0}{\|g\|_\infty},\frac{\mu_0^2}{\|g\|_2^2}\Big\} \tag{4.26}$$

and

$$\|f_0\|_\infty\le\frac{\|g\|_2}{\mu_0}. \tag{4.27}$$

If $\widehat{g} \geq 0$ *and* $g = g_1 \circ \overline{g}_1$, *then*

$$\|f_0\|_\infty \leq \frac{\|g_1\|_2}{\mu_0^{1/2}}. \tag{4.28}$$

The operator $\mathrm{T}_A^{A\circ A}$ is the simplest example of a nonnegatively defined operator on the set A. On the other hand, it is connected with the additive energy of A, since $|A|^{-1}\mathsf{E}(A) \leq \mu_0(\mathrm{T}_A^{A\circ A})$ by Theorem 3.2. Thus, it is natural to try to obtain bounds for the principal eigenvalues of this operator. We use Lemma 4.11 for this. Other lower bounds for the quantities $\mu_0(\mathrm{T}_A^{A\circ A})$ are contained in Theorem 7.2.

Corollary 4.12. *For any set* $A \subseteq \mathbf{G}$, *we have*

$$\mu_0(\mathrm{T}_A^{A\circ A}) \geq \max_{g\geq 0} \frac{\mu_0^3(\mathrm{T}_A^g)}{\|g\|_2^2 \cdot \|g\|_\infty}. \tag{4.29}$$

Proof. Let $\mu = \mu_0(\mathrm{T}_A^g)$, and let $f = f_0$ be the corresponding eigenfunction. We will prove an even stronger inequality than (4.29), namely, that the given lower bound is valid for $\langle \mathrm{T}_A^{A\circ A} f_0, f_0\rangle$. We have

$$\mu f(x) = A(x)(g * f)(x),$$

so that

$$\mu^2 \Big(\sum_x f(x)\Big)^2 \leq \Big(\sum_x g(x)(f\circ A)(x)\Big)^2 \leq \|g\|_2^2\, \mathsf{E}(A,f) \leq \|g\|_2^2\, \mu_0(\mathrm{T}_A^{A\circ A}).$$

Applying inequality (4.26) from Lemma 4.11, we find

$$\Big(\sum_x f(x)\Big)^2 \geq \frac{\mu}{\|g\|_\infty},$$

which it was required to prove. □

To conclude this section, we recall Proposition 22 from [25] (or see the proof of Proposition 4.8 above).

Proposition 4.13. *Let* $A \subseteq \mathbf{G}$ *be a set,* g_1, g_2 *real functions,* $g_1^c = g_1$, *and let* $\{f_\alpha\}$ *be the eigenfunctions of the operator* $\mathrm{T}_A^{g_1}$. *Then*

$$\sum_{x,\,y,\,z\in A} g_1(x-y)g_1(x-z)g_2(y-z) = \sum_{\alpha=0}^{|A|-1} \mu_\alpha^2(\mathrm{T}_A^{g_1}) \cdot \langle \mathrm{T}_A^{g_2} f_\alpha, f_\alpha\rangle.$$

§ 5. Convex sets and sets with small multiplicative doubling

In this part of the article, we apply the techniques of § 4 to obtain upper bounds for the additive energies of certain families of sets. We begin with a family of convex subsets of $\mathbb{R}$.

Theorem 5.1. *Let* $A \subseteq \mathbb{R}$ *be a convex set. Then*

$$\mathsf{E}(A) \ll |A|^{\,32/13} \log^{71/65} |A|. \tag{5.1}$$

Proof. Let $\mathsf{E} = \mathsf{E}(A) = |A|^3/K$, $\mathsf{E}_3 = \mathsf{E}_3(A)$, and $L = \log|A|$. Using formula (3.5) from Lemma 3.6 with parameter $k = 1$, we obtain

$$2^{-2}\mathsf{E} \leq \sum_s |A_s|^2, \tag{5.2}$$

where the summation is taken over all $s\colon 2^{-1}|A|K^{-1} < |A_s| \le cK$ and where $c > 0$ is an absolute constant. We put

$$D_j = \big\{s \in A - A\colon 2^{j-2}|A|K^{-1} < |A_s| \le 2^{j-1}|A|K^{-1}\big\},$$

where $j \in [l]$ and $2^l \le 2cK^2|A|^{-1} \ll K^2|A|^{-1}$. Thus, it follows from inequality (5.2) that

$$2^{-2}\mathsf{E} \le \sum_{j=1}^{l} \sum_{s\in D_j} |A_s|^2.$$

By Dirichlet's principle, there exists $j \in [l]$ for which we have

$$2^{-2}l^{-1}\mathsf{E} \le \sum_{s\in D_j} |A_s|^2 \le |D_j|\big(2^{j-1}|A|K^{-1}\big)^2. \tag{5.3}$$

Set $D = D_j$, $\Delta = 2^{j-1}|A|K^{-1}$, and $g(x) = (A\circ A)(x)D(x)$. We consider the operators $\mathrm{T}_1 = \mathrm{T}^g_A$, $\mathrm{T}_2 = \mathrm{T}^A_{A,D}$, and $\mathrm{T}_3 = \mathrm{T}^{A\circ A}_A$. It is clear that the elements of the matrices T_1 and $(\mathrm{T}_2)^*\mathrm{T}_2$ do not outnumber those of T_3. It is also clear that the operator T_3 is nonnegatively defined. By formula (5.3), we find

$$\frac{\mathsf{E}}{4l|A|} \le \mu_0(\mathrm{T}_1). \tag{5.4}$$

Similarly,

$$\frac{\mathsf{E}}{4l|A|} \le \mu_0(\mathrm{T}_1) \le \langle \mathrm{T}_3 f_0, f_0\rangle, \tag{5.5}$$

where $f_0 \ge 0$ is the principal eigenfunction of the operator T_1. Applying Proposition 4.13 with parameters $A = A$, $g_1 = g$, and $g_2 = A\circ A$, we obtain

$$\mu_0^3(\mathrm{T}_1) \le \sum_{x,y,z\in A} g(x-y)g(x-z)(A\circ A)(y-z),$$

since the operator T_3 is nonnegatively defined. Further,

$$\mu_0^3(\mathrm{T}_1) \le \sum_{\alpha,\beta} g(\alpha)g(\beta)(A\circ A)(\alpha-\beta)\mathscr{C}_3(A)(\alpha,\beta). \tag{5.6}$$

The summation in formula (5.6) can be carried out over α, β such that

$$(A\circ A)(\alpha-\beta) \ge \frac{\mathsf{E}^2}{32L^2|A|^3\mathsf{E}_3^{1/2}} := d.$$

In fact, on the contrary, it follows from (4.3) and (4.8) that

$$\mu_0^3(\mathrm{T}_1) < d\Delta^2 \cdot \sum_{\alpha,\beta} D(\alpha)D(\beta)\mathscr{C}_3(A)(\alpha,\beta) = d\Delta^2 \cdot \langle \mathrm{T}_2(\mathrm{T}_2)^* D, D\rangle$$
$$\le d\Delta^2|D|\mu_0(\mathrm{T}_2(\mathrm{T}_2)^*) \le d\Delta^2|D|\mathsf{E}_3^{1/2},$$

and we obtain a contradiction in view of the definition of the set D and the inequality (5.4). Thus,

$$2^{-1}\mu_0^3(\mathrm{T}_1) \le \sum_{\alpha,\beta\colon (A\circ A)(\alpha-\beta)\ge d} g(\alpha)g(\beta)(A\circ A)(\alpha-\beta)\mathscr{C}_3(A)(\alpha,\beta).$$

By the Cauchy–Bunyakovskii inequality and Lemmas 2.2 and 3.6, we find

$$\mu_0^6(\mathrm{T}_1) \ll \mathsf{E}_3 \sum_{\alpha,\beta\in D:\ (A\circ A)(\alpha-\beta)\geq d} (A\circ A)^2(\alpha)(A\circ A)^2(\beta)(A\circ A)^2(\alpha-\beta)$$

$$\ll |A|^3 L\Delta^3 \sum_{\alpha,\beta:\ (A\circ A)(\alpha-\beta)\geq d} D(\alpha)(A\circ A)(\alpha)D(\beta)(A\circ A)^2(\alpha-\beta) = |A|^3 L\Delta^3\cdot\sigma. \tag{5.7}$$

We bound the quantities σ in two different ways. We consider the sets S_i:

$$S_i = \bigl\{x\colon 2^{i-1}d < (A\circ A)(x) \leq 2^i d\bigr\}. \tag{5.8}$$

It follows immediately from Lemma 3.6 that $|S_i| \ll |A|^3/(2^i d)^3$. Thus, for some i,

$$\sigma \ll L \sum_{\alpha,\beta,\alpha-\beta\in S_i} D(\alpha)(A\circ A)(\alpha)D(\beta)(A\circ A)^2(\alpha-\beta) = L\sigma_*\,, \tag{5.9}$$

and it is sufficient to bound the quantity σ_*. We put $\tau = 2^i d$ and write S_τ for S_i. By Lemma 3.6, we have

$$\sigma_* \ll \Delta\tau\mathsf{E}(D,A) \ll \Delta\tau|A|\cdot|D|^{3/2}. \tag{5.10}$$

Further, applying the same lemma twice, and also the inequality $|S_\tau| \ll |A|^3/\tau^3$, we obtain

$$\sigma_* \ll \tau^2\sum_\alpha (A\circ A)(\alpha)(D\circ S_\tau)(\alpha) \ll \tau^2|A|\cdot|D|^{3/4}|S_\tau|^{3/4} \ll \tau^{-1/4}|A|^{13/4}|D|^{3/4}. \tag{5.11}$$

Combining the bounds (5.10) and (5.11), and optimizing for the parameter τ, we find

$$\sigma_* \ll \Delta^{1/5}|A|^{14/5}|D|^{9/10}. \tag{5.12}$$

Returning to the inequality (5.7), recalling (5.4) and (5.5), and substituting the latter formula into (5.9), we obtain

$$\frac{\mathsf{E}^6}{|A|^6L^6} \ll \mu_0^6(\mathrm{T}_1) \ll |A|^3L^2\Delta^3\cdot\Delta^{1/5}|A|^{14/5}|D|^{9/10}.$$

Accurate calculations, using (5.3), give us

$$\Bigl(\frac{\mathsf{E}}{|A|L}\Bigr)^{51/10} \ll |A|^{29/5+9/10}L^2\Delta^{7/5}.$$

Applying the bound $\Delta \ll K$, after a short calculation, we verify the inequality (5.1). The theorem is proved. □

Corollary 5.2. *Let $A\subseteq\mathbb{Z}$ be a convex set, and let $P_A(\theta) = \sum_{a\in A} e^{2\pi i a\theta}$. Then*

$$\int_0^{2\pi} |P_A(\theta)|^4\,d\theta \ll |A|^{32/13}\log^{71/65}|A|.$$

Remark 5.3. The argument used in the proof of Theorem 5.1 is sufficiently precise modulo our current knowledge of convex sets. In fact, if we consider the special case where the parameter τ is $\tau = \Delta = K$, and hence, by Lemma 3.6, we have $|D| \ll |A|^3/K^3$, then, calculating as above, we obtain the bound $K \gg |A|^{7/13-}$ precisely. The same situation occurs in the case of a multiplicative subgroup $\mathbb{Z}/p\mathbb{Z}$, for p a prime number (see [25]), where the choice $\tau = \Delta = K$ gives $K \gg |A|^{5/9-}$.

It is likely that similar reasoning will allow us to prove new upper bounds for the values $\mathsf{T}_k(A)$ too, just as was done in [25]. We will not give the analogous calculations here. It seems likely that even better inequalities for $\mathsf{T}_k(A)$ can be obtained by applying the Szemerédi–Trotter theorem with weights.

We now formulate a general result on additive energies of sets with small multiplicative doubling.

Theorem 5.4. *Let $A \subseteq \mathbb{R}$ be some set. We assume that $|AA| = M|A|$, for $M \geq 1$. Then*

$$\mathsf{E}(A) \ll (M\log M)^{14/13}|A|^{32/13}\log^{71/65}|A|. \tag{5.13}$$

Proof. Let $\mathsf{E} = \mathsf{E}(A) = |A|^3/K$, $\mathsf{E}_3 = \mathsf{E}_3(A)$, and $L = \log|A|$. By Lemma 3.7, we have $\mathsf{E}_3(A) \ll (M\log M)^2 \cdot |A|^3\log|A|$. Thus, for small M, the quantities $\mathsf{E}_3(A)$ are small, and we can apply the argument from the proof of Theorem 5.1. Using the first inequality of Lemma 3.7, we obtain

$$2^{-2}\mathsf{E} \leq \sum_{j=1}^{l}\sum_{s\in D_j}|A_s|^2,$$

where $D_j = \{s \in A-A\colon 2^{j-2}|A|K^{-1} < |A_s| \leq 2^{j-1}|A|K^{-1}\}$, $c > 0$ is an absolute constant, and $j \in [l]$, $2^l \ll (M\log M)^2K^2|A|^{-1}$. By Dirichlet's principle, there exists $j \in [l]$ such that

$$2^{-2}l^{-1}\mathsf{E} \leq \sum_{s\in D_j}|A_s|^2. \tag{5.14}$$

We put $D = D_j$, $\Delta = 2^{j-1}|A|K^{-1}$, and $g(x) = (A\circ A)(x)D(x)$. We next apply the arguments we used between (5.3) and (5.7). Using the operators $\mathrm{T}_1 = \mathrm{T}^g_A$, $\mathrm{T}_2 = \mathrm{T}^A_{A,D}$ and $\mathrm{T}_3 = \mathrm{T}^{A\circ A}_A$, formula (2.5) from Lemma 2.2, and the upper bound for E_3, we find

$$\begin{aligned}\mu_0^6(\mathrm{T}_1) &\ll \mathsf{E}_3 \sum_{\alpha,\beta\in D\colon (A\circ A)(\alpha-\beta)\geq d}(A\circ A)^2(\alpha)(A\circ A)^2(\beta)(A\circ A)^2(\alpha-\beta)\\ &\ll |A|^3M^2(\log M)^2L\Delta^3\sum_{\alpha,\beta\colon (A\circ A)(\alpha-\beta)\geq d}D(\alpha)(A\circ A)(\alpha)D(\beta)(A\circ A)^2(\alpha-\beta)\\ &= |A|^3M^2(\log M)^2L\Delta^3\cdot\sigma.\end{aligned}$$

As in Theorem 5.1, the number d can be taken to be equal to $\mathsf{E}^2/32L^2|A|\mathsf{E}_3^{1/2}$. Using the corollary to the first inequality in Lemma 3.7, namely, $|S_i| \ll (M\log M)^2|A|^3/(d^3 2^{3i})$, the second bound in Lemma 3.7, and applying the argument we used between (5.8) and (5.12), we obtain

$$\begin{aligned}\sigma &\ll \min_\tau\left\{\Delta\tau|A|\cdot|D|^{3/2}(M\log M), \tau^{-1/4}|A|^{13/4}|D|^{3/4}(M\log M)^{5/2}\right\}\\ &\ll \Delta^{1/4}|A|^{14/5}|D|^{9/10}(M\log M)^{11/5}.\end{aligned}$$

Thus,

$$\frac{\mathsf{E}^6}{|A|^6L^6} \ll |A|^3L^2\Delta^3(M\log M)^2\cdot\Delta^{1/5}|A|^{14/5}|D|^{9/10}(M\log M)^{11/5}.$$

As in Theorem 5.1, accurate calculation gives us

$$\Big(\frac{\mathsf{E}}{|A|L}\Big)^{51/10} \ll |A|^{29/5+9/10}L^2\Delta^{7/5}(M\log M)^{21/5}.$$

Using the inequality $\Delta \ll K(M\log M)^2$, after some calculation we find

$$K \gg |A|^{7/13}L^{-71/65}(M\log M)^{-14/13},$$

as required. The theorem is proved. □

It is easy to see that Theorem 5.4 gives a better bound for the additive energy than Lemma 3.7 (namely, $\mathsf{E}(A) \ll M\log M|A|^{5/2}$) if, roughly speaking, $M \ll |A|^{1/2-}$.

The following theorem was proved in [25].

Theorem 5.5. *Let $A \subseteq \mathbb{R}$ be a set, and let $\varepsilon \in [0,1)$ be a real number. Assume that $|AA| = M|A|$, $M \geq 1$, and*

$$\bigl|\bigl\{x \neq 0\colon (A\circ A)(x) \geq |A|^{1-\varepsilon}\bigr\}\bigr| \ll (M\log M)^{5/3}|A|^{1/6-\varepsilon/4}\log^{5/6}|A|. \tag{5.15}$$

Then

$$\mathsf{E}(A) \ll M\log M|A|^{5/2-\varepsilon/12}\log^{1/2}|A|. \tag{5.16}$$

Thus, Theorem 5.4 gives a better bound than Theorem 5.5 if, roughly speaking, $M \ll |A|^{1/2-13\varepsilon/12}$. Of course, the advantage of Theorem 5.4 lies in the absence of the parameter ε or, in other words, in the absence, in a certain sense, of a uniform upper bound for the convolution of the set A.

We will apply the argument from the proof of Theorem 5.4 to another family of sets A, namely sets for which the quantity $|A(A+1)|$ is small. Such sets were considered in [10], where the following lemma was proved.

Lemma 5.6. *Let $A, B \subseteq \mathbb{R}$ be arbitrary finite sets, and let $\tau \leq |A|, |B|$ be a real parameter. Then*

$$\bigl|\bigl\{s \in AB\colon |A\cap sB^{-1}| \geq \tau\bigr\}\bigr| \ll \frac{|A(A+1)|^2|B|^2}{|A|\tau^3}. \tag{5.17}$$

It follows from the above lemma that, for every $A \subseteq \mathbb{R}$, we have

$$\mathsf{E}^{\times}(A) \ll |A(A+1)|\cdot|A|^{3/2}.$$

Besides this inequality, a series of interesting results were proved in [10]. Here we state just one.

Theorem 5.7. *Let $A \subseteq \mathbb{R}$ be some set. Then*

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

All the inequalities in Theorem 5.7 were strengthened in [25], in the case where an analogue of inequality (5.15) holds. We prove a result where this additional condition is not assumed.

Corollary 5.8. *Let $A \subseteq \mathbb{R}$ be some set, let $a \in \mathbb{R}$ be an arbitrary number, $|A(A+1)| = M|A|$, and $M \geq 1$. Then*

$$\mathsf{E}^{\times}(A, A+a) \ll M^{14/13}|A|^{32/13}\log^{71/65}|A|. \tag{5.18}$$

In particular,

$$\mathsf{E}^{\times}(A) \ll M^{14/13}|A|^{32/13}\log^{71/65}|A|. \tag{5.19}$$

Proof. We put $A' = A + a$, and now let the convolution have the cardinality of the set $\{a_1, a_2 \in A\colon x = a_1a_2^{-1}\}$. Lemma 5.6 gives us

$$\mathsf{E}^{\times}_3(A') \ll M^2|A|^3\log|A|.$$

We then apply the arguments from the proof of Theorem 5.4. □

§ 6. Structural results

The results of § 5 assert that if the quantity $\mathsf{E}_3(A)$ is small and the set A has some additional properties of "nonorderability", then we can say something nontrivial about the additive energy of A. We shall formulate a certain variant of this principle (see Theorem 6.1 below). Using just the smallness of $\mathsf{E}_3(A)$, we show that A has a structured subset. Several results of this kind have been proved in earlier works; see [22, 25]. Our new theorem is stronger than the earlier statements, in the sense that the requirements

in it are minimal. From a certain point of view, results of this kind can be called optimal versions of the Balog–Szemerédi–Gowers Theorem; see [22].

Theorem 6.1. *Let $A \subseteq \mathbf{G}$ be some set, $\mathsf{E}(A) = |A|^3/K$, and $\mathsf{E}_3(A) = M|A|^4/K^2$. Then there exists a set $A' \subseteq A$ such that*

$$|A'| \gg M^{-10}\log^{-15} M \cdot |A| \tag{6.1}$$

and

$$|nA' - mA'| \ll (M^9\log^{14} M)^{6(n+m)}K|A'|, \tag{6.2}$$

for all $n, m \in \mathbb{N}$. Moreover, if $s \in (1,3)$ is a real number and $\mathsf{E}_s(A) = |A|^{s+1}/K^{s-1}$, then, for all $s \in (1, 3/2]$, there exists a set $A' \subseteq A$ with the properties

$$|A'| \gg M^{-(14-4s)/(3-s)}(s-1)^{21}\log^{-21}(M(s-1)^{-1}) \cdot |A| \tag{6.3}$$

and

$$|nA' - mA'| \ll \big(M^5(s-1)^{-20}\log^{20}(M(s-1)^{-1})\big)^{6(n+m)}K|A'|. \tag{6.4}$$

Finally, if $s \in (3/2, 3)$, then there exists a set $A' \subseteq A$ such that

$$|A'| \gg M^{-(44-24s)/(3-s)}(3-s)^{21}\log^{-21} M \cdot |A| \tag{6.5}$$

and

$$|nA' - mA'| \ll \big(M^{(45-25s)/(3-s)}(3-s)^{-20}\log^{20} M\big)^{6(n+m)}K|A'|, \tag{6.6}$$

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

Proof. Let

$$\mathsf{E}_s = \mathsf{E}_s(A) = \frac{|A|^{s+1}}{K^{s-1}}, \quad \mathsf{E}_3 = \mathsf{E}_3(A), \quad L = 2(3-s)^{-1}\log(4M(s-1)^{-1}).$$

Since E_3 is small, we can apply the argument in the proof of Theorem 5.4. We put

$$D_j = \big\{x \in A - A\colon 2^{j-2}|A|K^{-1} < |A_x| \le 2^{j-1}|A|K^{-1}\big\}.$$

It is clear that $|D_j|(2^{j-2}|A|K^{-1})^3 \le \mathsf{E}_3$ and, consequently,

$$|D_j| \ll \frac{\mathsf{E}_3}{|A|^3K^{-3}2^{3j}}. \tag{6.7}$$

Thus,

$$(s-1)\mathsf{E}_s \ll \sum_{j=1}^{l}\sum_{s}|A_s|^s,$$

where l is bounded above by $\log M^{1/(3-s)} = L$. By Dirichlet's principle, there exists $j \in [l]$ such that

$$(s-1)L^{-1}\mathsf{E}_s \ll \sum_{s\in D_j}|A_s|^s. \tag{6.8}$$

We put $D = D_j$, $\Delta = 2^{j-1}|A|K^{-1}$, and $g(x) = (A\circ A)^{s-1}(x)D(x)$. It follows from the bound (6.8) that

$$|D| \gg \frac{(s-1)|A|K}{LM^{s/(3-s)}} \tag{6.9}$$

and

$$\sum_{x\in D}(A\circ A)(x) \gg \frac{(s-1)|A|^2}{LM^{(s-1)/(3-s)}}. \tag{6.10}$$

We next consider the operators $\mathrm{T}_1 = \mathrm{T}^g_A$, $\mathrm{T}_2 = \mathrm{T}^A_{A,\,D}$, $\mathrm{T}_3 = \mathrm{T}^{A\circ A}_A$ and apply the arguments used between (5.3) and (5.7). Using Corollary 4.12, we find

$$\langle \mathrm{T}_3 f_0, f_0\rangle \geq \frac{\mu_0^3(\mathrm{T}_1)}{\|g\|_2^2\cdot\|g\|_\infty} \gg \frac{|D|^2\Delta^3}{|A|^3} := \sigma. \tag{6.11}$$

In the case $s=2$ (see the proofs of Theorems 5.1 and 5.4), we have $\sigma \geq \mu_0(\mathrm{T}_1)$. Further, by Proposition 4.13 and formula (2.5) in Lemma 2.2, we obtain

$$\begin{aligned}(s-1)^6\mu_0^4(\mathrm{T}_1)\sigma^2 &\\ \ll \mathsf{E}_3 \sum_{\alpha,\beta\in D\colon\,(A\circ A)(\alpha-\beta)\geq d} &(A\circ A)^{2s-2}(\alpha)(A\circ A)^{2s-2}(\beta)(A\circ A)^2(\alpha-\beta)\\ &\ll \mathsf{E}_3\Delta^{4s-4}\sum_{x\colon\,(A\circ A)(x)\geq d}(D\circ D)(x)(A\circ A)^2(x),\end{aligned} \tag{6.12}$$

where d can be taken as $d=\frac{(s-1)^3\sigma\mu_0(\mathrm{T}_1)}{2^{13}L\Delta^{s-2}\mathsf{E}_3^{1/2}}$ (and $d=\frac{\mu_0^2(\mathrm{T}_1)}{32|A|\mathsf{E}_3^{1/2}}$ in the case $s=2$). Applying Hölder's inequality, we have

$$\sum_x (A\circ A)^2(x)(D\circ D)(x) \leq \mathsf{E}_3^{2/3}\Big(\sum_x (D\circ D)^3(x)\Big)^{1/3} \leq \mathsf{E}_3^{2/3}|D|^{1/3}\mathsf{E}^{1/3}(D).$$

We put $\mathsf{E}(D)=\mu|D|^3$. Recalling (6.12), we find that

$$(s-1)^6\mu_0^4(\mathrm{T}_1)\sigma^2 \ll \Big(\frac{M|A|^4}{K^2}\Big)^{5/3}\Delta^{4s-4}|D|^{4/3}\mu^{1/3}. \tag{6.13}$$

We have $\Delta \ll M^{1/(3-s)}|A|/K$. We begin with the case $s=2$. In this situation, we have $\sigma\geq\mu_0(\mathrm{T}_1)$. Doing some accurate calculations, we obtain

$$\mathsf{E}(D)=\mu|D|^3 \gg \frac{|D|^3}{M^9L^{14}}.$$

By Theorem 3.5 (the Balog–Szemerédi–Gowers Theorem), there exists a set $D'\subseteq D$ such that $|D'|\gg\mu|D|$ and $|D'+D'|\ll\mu^{-6}|D'|$. The Plünnecke–Ruzsa inequality (see, for example, [28]) gives us the bound

$$|nD'-mD'|\ll\mu^{-6(n+m)}|D'|, \tag{6.14}$$

valid for all $n,m\in\mathbb{N}$. Using the definition of the set $D=D_j$, and also inequality (6.10) (recall that we are in the case $s=2$), we find $x\in\mathbf{G}$ such that

$$|(A-x)\cap D'|\gg\mu|A|L^{-1}M^{-1}\gg M^{-10}L^{-15}\cdot|A|. \tag{6.15}$$

We put $A'=A\cap(D'+x)$. Using (6.14), (6.15), and also the definition of the set Δ, we obtain, for all $n,m\in\mathbb{N}$,

$$|nA'-mA'|\leq|nD'-mD'|\ll\mu^{-7(n+m)}|A|\cdot|A'|\Delta^{-1}\ll\mu^{-6(n+m)}K|A'|, \tag{6.16}$$

and the theorem is proved for $s=2$.

We now choose an arbitrary $s\in(1,3)$. Returning to (6.13), using (6.11), and carrying out similar calculations, we find

$$\Big(\frac{(s-1)\mathsf{E}_s}{L|A|}\Big)^{20/3}\Delta^{10-20s/3}\ll|A|^{10/3}\mu^{1/3}\Big(\frac{M|A|^4}{K^2}\Big)^{5/3}. \tag{6.17}$$

We suppose that $s\in(1,3/2]$. In this case,

$$\mu\gg\frac{(s-1)^{20}}{M^5L^{20}},$$

since $\Delta \gg |A|/K$. We next repeat the above arguments. If $s \in [3/2, 3)$, then inequality (6.17) gives us

$$\left(\frac{(s-1)\mathsf{E}_s}{L|A|}\right)^{20/3}(M^{1/(3-s)}|A|K^{-1})^{10-20s/3} \ll |A|^{10/3}\mu^{1/3}\left(\frac{M|A|^4}{K^2}\right)^{5/3},$$

since in this case $\Delta \ll M^{1/(3-s)}|A|/K$. Minor calculations show that

$$\mu \gg \frac{1}{M^{(45-25s)/(3-s)}L^{20}}.$$

We next repeat the preceding arguments once more. The theorem is proved. □

It undoubtedly follows from inequality (6.1) and the condition $\mathsf{E}(A) = |A|^3/K$ from Theorem 6.1 that $|A'-A'| \gg_M K|A'|$. Thus, the factor K in inequality (6.6) is essential.

Of course, using the definition of Δ more accurately can improve the bounds (6.1) and (6.2) slightly.

Remark 6.2. For every convex set A, Theorem 6.1 gives an easy proof of a "nontrivial" bound of the form $\mathsf{E}(A) \ll |A|^{5/2-\varepsilon_0}$, where $\varepsilon_0 > 0$ is an absolute constant. In fact, putting $M = \log|A|$ and using (3.4) from Lemma 3.6 and the upper bound for the energy $\mathsf{E}_3(A)$ arising from this lemma, we see from Theorem 6.1 that the set A' satisfies

$$|A|^{7/4} \ll_M |A'+A'-A'| \ll_M |A|^4\mathsf{E}^{-1}(A),$$

and the statement is proved. Applying arguments from [21], we can obtain an even simpler proof. Indeed, for a subset $A' \subseteq A$ of such a large size, we have

$$|A|^{3/2+\varepsilon_1} \ll_M |A'-A'| \ll_M |A|^4\mathsf{E}^{-1}(A),$$

where $\varepsilon_1 > 0$ is an absolute constant, and we again find a lower bound for ε_0. It is interesting that, in this case, the lower bounds on the doubling constants give upper bounds for the additive energy.

The same proof also holds in the case of a multiplicative subgroup $\Gamma \subseteq \mathbb{Z}/p\mathbb{Z}$, where p is a prime number. In this case, it is necessary to apply Stepanov's method (see, for example, [13] or [27]) or a combination of Stepanov's method and the method, from the recent works [20, 27, 25], for obtaining lower bounds for the doubling constants. We note that a bound of the form $\mathsf{E}(\Gamma) \ll |\Gamma|^{5/2-\varepsilon}$ was already known; see [25], where the proof uses another variant of the method of eigenvalues. Finally, any multiplicative subgroup Γ of order $|\Gamma| > p^{\varepsilon}$ is an additive basis of $\mathbb{Z}/p\mathbb{Z}$ of order $C(\varepsilon)$ (see, for example, [7, 3], and the general inequality from [17] on sums of products). The same is also true for arbitrary sets with small multiplicative doubling; see [4] (a more precise statement was proved by Bourgain, consisting of the fact that, in the mean, the Fourier coefficients of such sets have a nontrivial estimate). It also follows that we can derive a "nontrivial" upper bound for $\mathsf{E}(\Gamma)$.

The above reasoning makes it easy to replace the condition on E_3 in Theorem 6.1 by a similar condition for E_4. Due to the parity, the proof is even easier in this case. A general result of similar type but with slightly different constants was obtained in [22]; see Theorem 54. We give a new proof here, since the following important Theorem 6.4 is obtained using almost the same arguments.

Theorem 6.3. *Let $s \in [8/5, 4)$ be a real number, $A \subseteq \mathbf{G}$ be some set, $\mathsf{E}_s(A) = |A|^{s+1}/K^{s-1}$, and $\mathsf{E}_4(A) = M|A|^5/K^3$. Then there exists a set $A' \subseteq A$ such that*

$$|A'| \gg M^{-(5s-5)/(4-s)}(4-s)^6\log^{-6}M \cdot |A| \tag{6.18}$$

and

$$|nA'-mA'| \ll \left(M^{(4s-4)/(4-s)}(4-s)^{-5}\log^5 M\right)^{6(n+m)}K|A'|, \tag{6.19}$$

for all $n, m \in \mathbb{N}$. If $s \in (1, 8/5]$, then there exists a set $A' \subseteq A$ for which we have

$$|A'| \gg M^{-3/(4-s)}(s-1)^6 \log^{-6}(M(s-1)^{-1}) \cdot |A| \tag{6.20}$$

and

$$|nA' - mA'| \ll \big(M(s-1)^{-5}\log^5(M(s-1)^{-1})\big)^{6(n+m)} K|A'|, \tag{6.21}$$

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

Proof. Let $\mathsf{E}_4 = \mathsf{E}_4(A)$, and $L = 2(4-s)^{-1}\log(4M(s-1)^{-1})$. In the terminology of Theorem 6.1, we have

$$\begin{aligned}(s-1)^8\mu_0^8(\mathrm{T}_1) &\ll \Big(\sum_{x,\,y,\,z,\,w\in A} g(x-y)g(y-z)g(z-w)g(w-x)\Big)^2\\ &= \Big(\sum_{\alpha,\,\beta,\,\gamma} \mathscr{C}_4(A)(\alpha,\beta,\gamma)g(\alpha)g(\beta-\alpha)g(\gamma-\beta)g(\gamma)\Big)^2\\ &\ll \mathsf{E}_4 \cdot \sum_{\alpha,\,\beta,\,\gamma} g^2(\alpha)g^2(\beta-\alpha)g^2(\gamma-\beta)g^2(\gamma)\\ &\ll \mathsf{E}_4\cdot\Delta^{8s-8}\mathsf{E}(D) \ll \frac{M|A|^5}{K^3}\cdot\Delta^{8s-8}\mathsf{E}(D).\end{aligned}$$

Here,

$$g(x) = D(x)(A\circ A)^{s-1}(x), \quad \mathrm{T}_1 = \mathrm{T}_A^g, \quad D = D_j, \quad \Delta = 2^{j-1}|A|K^{-1}.$$

We have $2^j \ll M^{1/(4-s)}$, and, consequently, $\Delta \ll M^{1/(4-s)}|A|K^{-1}$. We note that the number j can be bounded above by $\log M^{1/(4-s)} = L$. We put $\mathsf{E}(D) = \mu|D|^3$. After accurate calculations, we find, in the case $s \in [8/5, 4)$, that

$$\begin{aligned}\Big(\frac{|A|^s}{K^{s-1}L}\Big)^5 \ll \Big((s-1)\frac{|A|^s}{K^{s-1}L}\Big)^5 &\ll \frac{M|A|^5}{K^3}\Delta^{5s-8}|A|^3\mu\\ &\ll \frac{M|A|^5}{K^3}(M^{1/(4-s)}|A|K^{-1})^{5s-8}|A|^3\mu.\end{aligned}$$

Thus $\mu \gg 1\big/(M^{(4s-4)/(4-s)}L^5)$. We next apply the arguments used between (6.14) and (6.16) in the proof of Theorem 6.1.

If $s \in (1, 8/5)$, then it is easy to see that $\mu \gg (s-1)^5\big/(ML^5)$. Repeating the above argument, we obtain the required result. The theorem is proved. □

Theorems 6.1 and 6.3 can undoubtedly be generalized to higher moments. Nevertheless, such generalizations become weaker for large k, since it becomes necessary to deal with $\mathsf{T}_k(D)$ rather than $\mathsf{E}(D)$.

Instead of this, we consider another characteristic of the set A, namely the energy $\mathsf{T}_4(A)$, and obtain a structural result in this situation. A similar statement has also been proved in [22]; see Theorem 60. Theorem 1.2 in the Introduction has a similar form but, of course, starts from from weaker assumptions.

Theorem 6.4. *Let $A \subseteq \mathbf{G}$ be some set, $\mathsf{E}_{3/2}(A) = |A|^{5/2}/K^{1/2}$, and $\mathsf{T}_4(A) = M|A|^7/K^3$. Then there exists a set $A' \subseteq A$ such that*

$$|A'| \gg \frac{|A|}{MK} \tag{6.22}$$

and

$$\mathsf{E}(A') \gg \frac{|A'|^3}{M}. \tag{6.23}$$

If s is a real number, $s \in (1,3/2]$, and the equality

$$\mathsf{E}_s(A) = |A|^{s+1}/K^{s-1}$$

holds, then there exists a set $A' \subseteq A$ for which

$$|A'| \gg \frac{(s-1)^8|A|}{MK\log^8 K} \tag{6.24}$$

and

$$\mathsf{E}(A') \gg \frac{(s-1)^8|A'|^3}{M\log^8 K}. \tag{6.25}$$

Proof. Let $\mathsf{E}_4 = \mathsf{E}_4(A)$, and $\mathsf{T}_4 = \mathsf{T}_4(A)$. In the terminology of Theorems 6.1 and 6.3, we have

$$\mu_0^8(\mathrm{T}_1) \ll \Big(\sum_{x,\,y,\,z,\,w\,\in\,A} g(x-y)g(y-z)g(z-w)g(w-x)\Big)^2$$
$$\ll \mathsf{E}_4 \cdot \sum_{\alpha,\,\beta,\,\gamma} g^2(\alpha)g^2(\beta-\alpha)g^2(\gamma-\beta)g^2(\gamma) \ll \mathsf{E}_4\cdot\mathsf{T}_4 \ll \mathsf{E}_4\cdot\frac{M|A|^7}{K^3}.$$

Here, $g(x) = (A\circ A)^{s-1}(x)$ and $\mathrm{T}_1 = \mathrm{T}_A^g$. We put $\mathsf{E}_4 = \mu|A|^5$. We first consider $s = 3/2$. After minor calculations, we find $\mu \gg 1/(MK)$. It is clear that

$$\sum_{s\colon\,|A_s|<2^{-2}\mu|A|}\sum_t \mathsf{E}(A_s,A_t) \le \sum_{s\colon\,|A_s|<2^{-2}\mu|A|}\sum_t |A_s|^2\cdot|A_t| < 2^{-2}\mathsf{E}_4.$$

Thus, by Lemma 3.4, we have

$$\sum_{s,t\colon\,|A_s|,\,|A_t|\ge 2^{-2}\mu|A|} \mathsf{E}(A_s,A_t) \ge 2^{-1}\mathsf{E}_4. \tag{6.26}$$

We put

$$\nu := \max_{|A_s|,\,|A_t|\ge 2^{-2}\mu|A|} \frac{\mathsf{E}(A_s,A_t)}{|A_s|^{3/2}\cdot|A_t|^{3/2}}.$$

By inequality (6.26), we have

$$2^{-1}\mathsf{E}_4 \le \nu\sum_{s,t}|A_s|^{3/2}\cdot|A_t|^{3/2} = \nu\mathsf{E}^2_{3/2}(A),$$

and, consequently, $\nu \ge 2^{-1}\mu K$. It follows that there exist s,t such that $|A_s|,|A_t| \ge 2^{-2}\mu|A|$ and

$$\mathsf{E}(A_s,A_t) \ge \nu|A_s|^{3/2}|A_t|^{3/2} \gg \frac{|A_s|^{3/2}\cdot|A_t|^{3/2}}{M}.$$

Applying the Cauchy–Bunyakovskii inequality, we obtain the required result.

Now let $s \in (1,3/2)$. In this case, we put $g(x) = D(x)(A\circ A)^{s-1}(x)$, where the set D is defined as in Theorems 6.1 and 6.3. We have

$$(s-1)^8\left(\frac{\mathsf{E}_s(A)}{|A|L}\right)^8 \ll \mathsf{E}_4\mathsf{T}_4\Delta^{8s-12},$$

where $\Delta \gg |A|/K$ and $L \ll \log K$. Consequently, $\mu \gg (s-1)^8/(ML^8K)$. Repeating the above arguments, we obtain the required result. The theorem is proved. □

Remark 6.5. The bounds in Theorem 6.4 are sharp, as the example of the set $A = H + \Lambda \subseteq \mathbb{F}_2^n$ shows. Here, $H \le \mathbb{F}_2^n$ is an arbitrary subspace and Λ is a dissociative set (basis) (see also Example 7.1 in §7). This set A corresponds to the case $\alpha = 0$ in Theorem 1.2. There are also other, more complicated, examples which illustrate the same point.

Remark 6.6. The proof of Theorem 6.4 shows, in particular, that

$$\left(\frac{\mathsf{E}_{3/2}(A)}{|A|}\right)^{2k} \le \mathsf{E}_k(A)\mathsf{T}_k(A)$$

and

$$\left(\frac{\sum_{x\in D}(A\circ A)(x)}{|A|}\right)^{2k} \le \mathsf{E}_k(A)\mathsf{T}_{k/2}(D), \tag{6.27}$$

for any sets $A, D \subseteq \mathbf{G}$ and an even natural number k. Special cases of the last formula are contained in [22]; see Lemma 3 and Remark 61 there.

Remark 6.7. Theorem 6.4 tells us that the set A has a subset A' with large additive energy. So, by the Balog–Szemerédi–Gowers Theorem, A' has a subset with small doubling, just as in Theorem 1.2. Remark 6.5 gives an example showing that our theorem is sharp, and, furthermore, the parameter α from Theorem 1.2 is equal to zero. It is easy to construct a similar counterexample, corresponding to the opposite situation $\alpha = (1-\tau_0)/2$. In fact, let $H_1, \dots, H_k$, where $k = [K^{1/2}]$, be some completely additive disjoint subspaces of $\mathbb{F}_2^n$ in the sense that $|H_1 + \ldots + H_k| = |H_1| \dots |H_k|$ (see, for example, [18]). We put $A = \bigsqcup_{j=1}^k H_j$. Then $\mathsf{T}_t(A) \sim |A|^{2t-1}/K^{t-1}$ and $\mathsf{E}_s(A) \sim |A|^{s+1}/K^{s/2}$, but, of course, there are no nontrivial sets X_j here. Thus, this example shows once again that, in terms of the values $\mathsf{E}_4(A)$ and $\mathsf{T}_4(A)$, our Theorem 6.4 is sharp (even if $\mathsf{E}_{3/2}(A)$ is smaller). Of course, if there is information about the "height" of the set A (see [1], [2] or § 7), then sets X_j may also appear. An example with additive disjoint subspaces $H_1, \dots, H_k$ is discussed in detail in the following section.

The special case of the theorems in this section, when the parameter s is equal to 1, was considered in [25]; see also [22].

§ 7. Dual popular sets

Let $k \ge 2$ be an integer and $c \in (0,1]$ a real number. Suppose that we are also given a set $A \subseteq \mathbf{G}$. We call the set $\mathscr{P} \subseteq \mathbf{G}^{k-1}$ a (k,c)-*dual* (or simply a dual) for the set $P \subseteq \mathbf{G}$ if

$$\begin{aligned} c\mathsf{E}_k^P(A) \le \sum_{x,\,y} P(x-y)A(x)A(y) \\ \times \sum_{z_1,\dots,z_{k-1}} \mathscr{P}(z_1,\dots,z_{k-1})A(x+z_1)\dots A(x+z_{k-1})A(y+z_1)\dots A(y+z_{k-1}). \end{aligned} \tag{7.1}$$

We also say that the set $P \subseteq \mathbf{G}$ is a (k,c)-*dual* for the set $\mathscr{P} \subseteq \mathbf{G}^{k-1}$ if

$$\begin{aligned} c\mathsf{E}_k^{\mathscr{P}}(A) \le \sum_{x,\,y} P(x-y)A(x)A(y) \\ \times \sum_{z_1,\dots,z_{k-1}} \mathscr{P}(z_1,\dots,z_{k-1})A(x+z_1)\dots A(x+z_{k-1})A(y+z_1)\dots A(y+z_{k-1}). \end{aligned} \tag{7.2}$$

Of course, a dual set defined in this way is not unique. We record the fact that $\mathscr{P}$ belongs to the family of dual sets for P, as $\mathscr{P} = P^*$, and conversely.

Pairs of dual sets are very easy to find. For example, for any $P \subseteq \mathbf{G}$, we can take the set $\mathscr{P} = A^{k-1} - \Delta_{k-1}(A)$, and for arbitrary $\mathscr{P} \subseteq \mathbf{G}^{k-1}$, the set $P = A - A$. We consider other examples. Let $P \subseteq \mathbf{G}$ be a popular difference set, in the sense that

$$P = \bigl\{z\colon |A_z|^{k-1} \ge \mathsf{E}_k(A)(2|A|^2)^{-1}\bigr\}.$$

Then

$$2^{-1}\mathsf{E}_k(A) \le \mathsf{E}_k^P(A) = \sum_{z\in P}|A_z|^k = \sum_{z_1,\dots,z_k} A(z_1)\dots A(z_k)\mathscr{C}_{k+1}(P,A)(z_1,\dots,z_k). \tag{7.3}$$

If we take

$$\mathscr{P} = \big\{(z_1,\dots,z_{k-1})\colon \mathscr{C}_k(A)(z_1,\dots,z_{k-1}) \ge \mathsf{E}_k(A)(4|A|^k)^{-1}\big\},$$

then

$$\begin{aligned}2^{-2}\mathsf{E}_k(A) &\le 2^{-1}\mathsf{E}_k^P(A)\\ &\le \sum_{z_1,\dots,z_k} A(z_1)\dots A(z_k)\mathscr{P}(z_1-z_k,\dots,z_{k-1}-z_k)\mathscr{C}_{k+1}(P,A)(z_1,\dots,z_k)\\ &= \sum_{x,\,y} P(x-y)A(x)A(y)\\ &\quad\times \sum_{z_1,\dots,z_{k-1}} \mathscr{P}(z_1,\dots,z_{k-1})A(x+z_1)\dots A(x+z_{k-1})A(y+z_1)\dots A(y+z_{k-1}).\end{aligned}$$

We have thus constructed a pair of $(k,1/2)$-dual sets. Similarly, we could have started with the inequality

$$2^{-1}\mathsf{E}_k(A) \le \mathsf{E}_k^{\mathscr{P}} = \sum_{(z_1,\dots,z_{k-1})\in\mathscr{P}} \mathscr{C}_k^2(A)(z_1,\dots,z_{k-1})$$

and then defined the set P, so as to again give the inclusion $P=\mathscr{P}^*$. In the last two examples, the sets P and $\mathscr{P}$ are popular difference sets. In this case, we say that $P,\mathscr{P}$ is a pair of $(k,1/4)$-popular dual sets. In other words, $P,\mathscr{P}$ is a pair of (k,c)-*popular dual* sets if

$$\begin{aligned}c\mathsf{E}_k(A) &\le \sum_{x,\,y} P(x-y)A(x)A(y)\\ &\quad\times \sum_{z_1,\dots,z_{k-1}} \mathscr{P}(z_1,\dots,z_{k-1})A(x+z_1)\dots A(x+z_{k-1})A(y+z_1)\dots A(y+z_{k-1}).\end{aligned} \tag{7.4}$$

The latter inequality clearly implies the bounds

$$c\mathsf{E}_k(A) \le \sum_{z\in P}|A_z|^k \quad\text{and}\quad c\mathsf{E}_k(A) \le \sum_{(z_1,\dots,z_{k-1})\in\mathscr{P}} \mathscr{C}_k^2(A)(z_1,\dots,z_{k-1}).$$

Thus, the converse statement is also true in a certain sense.

We note also that if P, $\mathscr{P}$ are (k,c)-popular dual sets, then it follows from formulae (2.8) and (2.9) that for every natural number t the tensor powers $P^{\otimes}$, $\mathscr{P}^{\otimes}$ are (k,c^t)-popular dual sets for $A^{\otimes}$. Another example of popular dual sets is that of the popular dual sets of levels, that is, the sets

$$P_i = \big\{s\colon 2^{i-1}\mathsf{E}_k(A)(2|A|^2)^{-1} < |A_s|^{k-1} \le 2^i\mathsf{E}_k(A)(2|A|^2)^{-1}\big\}$$

and

$$\mathscr{P}_j = \big\{(z_1,\dots,z_{k-1})\colon 2^{j-1}\mathsf{E}_k(A)(4|A|^k)^{-1} < \mathscr{C}_k(A)(z_1,\dots,z_{k-1}) \le 2^j\mathsf{E}_k(A)(4|A|^k)^{-1}\big\},$$

in the sense that there exist $i,j\in[L]$ for which P_i and $\mathscr{P}_j$ are $(k,2^{-2}L^{-2})$-popular dual sets, where

$$L = L(A) = \log\big(4|A|^{k+1}\mathsf{E}_k^{-1}(A)\big).$$

In this case, we put

$$\Delta = \Delta(P) = \Delta(A,P) = 2^i\mathsf{E}_k(A)(2|A|^2)^{-1}$$

and

$$\Delta^* = \Delta(P^*) = \Delta(A,P^*) = 2^j \mathsf{E}_k(A)(4|A|^k)^{-1}.$$

The case when $k=2$ is the most interesting. In this situation, the dual formula

$$\sum_{x,\,y} A(x)A(y)g(x-y)\mathscr{C}_3(h,A,A)(x,y) = \sum_{x,\,y} A(x)A(y)h(x-y)\mathscr{C}_3(g,A,A)(x,y) \tag{7.5}$$

holds, where $g,h\colon \mathbf{G}\to\mathbb{C}$ are arbitrary functions. It follows from the above formula that $(P^*)^* = P$, in the sense that the set P is a popular dual from the family of all popular dual sets of P^*. In this case, we write P^* instead of $\mathscr{P}$ and also speak of c-popular sets instead of $(2,c)$-popular dual.

Example 7.1. We consider the set A from Remark 6.5. The popular difference set of A divides naturally into two parts:

$$P_1 = H = \{x\colon |A_x| = |A|\} \quad \text{and} \quad P_2 = \{x\in (A-A)\setminus H\colon |A_x| = |H|\}.$$

It is easy to see that $P_2 = P_1^*$, and conversely. We note also that for $s\geq 1$, we have

$$\mathsf{E}_s(A) \sim |H|\cdot|A|^s + |A|^2\cdot|H|^{s-1} \sim \begin{cases} |H|\cdot|A|^s, & \text{if} \quad s\geq 2,\\ |A|^2\cdot|H|^{s-1}, & \text{if} \quad s<2. \end{cases}$$

Hence, any x from the set P_1 gives a greater contribution to the sum $\mathsf{E}_s(A) = \sum_x (A\circ A)^s(x)$ for large s, and x from P_2 a greater contribution for small s.

We now prove a basic result on the properties of dual sets. The most interesting statement is the inequality (7.11), which points to a nontrivial connection between $\mathsf{E}(A)$ and $\mathsf{E}_s(A)$, for $s\in[1,2]$. Further, the bounds (7.7)–(7.10) and (7.12) demonstrate the existence of a different correspondence between characteristics of dual sets. It follows from this, for example, that for any "connected" set A (we give an exact definition of this below), there exists a set $Q\subseteq A-A$, for which we have $\mathsf{E}_Q(A) \gg \mathsf{E}^{1-}(A) := |A|^{3-}/K$ and $\sigma_Q(A) \gg |A|^{2-}/K^{1/2}$ (see [1], [2], or the corollary and proposition below).

We consider the Hermitian operator

$$\mathrm{T}(x,y) = A(x)A(y) \times \sum_{z_1,\dots,z_{k-1}} \mathscr{P}(z_1,\dots,z_{k-1})A(x+z_1)\dots A(x+z_{k-1})A(y+z_1)\dots A(y+z_{k-1}). \tag{7.6}$$

It is easy to see that T is nonnegative definite. It follows from formula (4.5) that, in the case $k=2$, this operator is equal to $(\mathrm{T}^A_{A,\,\mathscr{P}^c})^*\mathrm{T}^A_{A,\,\mathscr{P}^c}$.

Theorem 7.2. *Let $A\subseteq\mathbf{G}$ be some set. In the above notation, there exists a pair of $(k, 2^{-2}L^{-2})$-popular dual sets P, $\mathscr{P}$ such that*

$$\Delta\Delta^* \leq 16L\mu_0\big(\mathrm{T}_A^{(A\circ A)^{k-1}}\big), \tag{7.7}$$

and

$$\mathsf{E}_k^2(A) \leq 16L^2\mu_0\big(\mathrm{T}_A^{(A\circ A)^{k-1}}\big)\sigma_P(A)\sigma_{\mathscr{P}}(A), \tag{7.8}$$

$$\mathsf{E}_k^2(A) \leq 2^8L^3\mu_0^2\big(\mathrm{T}_A^{(A\circ A)^{k-1}}\big)\cdot|P|\cdot|\mathscr{P}|, \tag{7.9}$$

$$\mathsf{E}_k^2(A) \leq 16L^4\sigma_P(A)\sigma_{\mathscr{P}}(A)\mu_0(\mathrm{T}). \tag{7.10}$$

In the case $k=2$, for any $s\in[1,2]$,

$$\mathsf{E}(A) \leq \mu_0\big(\mathrm{T}_A^{A\circ A}\big)^{1-s/2}\mathsf{E}_s(A), \tag{7.11}$$

and if P^* is c-dual to P, then

$$c^2\mathsf{E}_P^2(A) \le \sigma_{P^*}(A)\cdot \sum_{x,\,y\in P}\mathscr{C}_3^2(A)(x,y). \tag{7.12}$$

Proof. We first prove the required formulae up to additional factors (constants and logarithms) and then apply the method of exponentiation (see, for example, [28]); that is, we replace A by A^t, where t is a large integer, and rid ourselves of these factors by taking the root of degree t. By formula (2.8), we have $\mathsf{E}_s(A^t)=\mathsf{E}_s^t(A)$, for any s. Applying Lemma 4.9, we find $\mu_0\big(\mathrm{T}_{A^\otimes}^{(A\circ A)^\otimes}\big)=\mu_0^t(\mathrm{T}_A^{A\circ A})$. Finally, $L(A^t)\le tL(A)$, where $L=\log\big(4|A|^{k+1}\mathsf{E}_k^{-1}(A)\big)$.

We prove the inequality (7.7). Let $P=P_i$, $\mathscr{P}=\mathscr{P}_j$ be two $(k,2^{-2}L^{-2})$-popular dual sets, where L is the same as before. By the definition of the operator T and formula (7.4), we have

$$\mathsf{E}_k(A)2^{-2}L^{-2}\le \sum_\alpha \mu_\alpha(\mathrm{T}_A^P)\langle \mathrm{T}f_\alpha, f_\alpha\rangle \tag{7.13}$$

$$\le \mu_0(\mathrm{T}_A^P)\sum_\alpha\langle \mathrm{T}f_\alpha,f_\alpha\rangle=\mu_0(\mathrm{T}_A^P)\cdot\sum_{(z_1,\dots,z_{k-1})\in\mathscr{P}}\mathscr{C}_k(A)(z_1,\dots,z_{k-1}), \tag{7.14}$$

where the $\{f_\alpha\}_{\alpha\in[|A|]}$ are eigenfunctions of the operator T_A^P. In deriving the last formula, we used the fact that the set P is symmetric. Multiplying inequality (7.14) by $\Delta\Delta^*$ and applying the definitions of the sets P and $\mathscr{P}$, we find

$$\Delta\Delta^*\le 16L\mu_0\big(\mathrm{T}_A^{P(A\circ A)^{k-1}}\big)\le 16L\mu_0\big(\mathrm{T}_A^{(A\circ A)^{k-1}}\big).$$

We now prove (7.8), (7.9) and (7.10). Multiplying (7.14) by $\Delta\sigma_P(A)$, we obtain (7.8). Combining (7.7) and (7.8), we have (7.9). Returning to (7.13) and using the Cauchy–Bunyakovskii inequality, we find

$$\mathsf{E}_k^2(A)2^{-4}L^{-4}\le\sum_\alpha\mu_\alpha^2(\mathrm{T}_A^P)\cdot\sum_\alpha\langle\mathrm{T}f_\alpha,f_\alpha\rangle^2.$$

Now applying (4.17) and Lemma 3.3, we see that

$$\mathsf{E}_k^2(A)2^{-4}L^{-4}\le\sigma_P(A)\sum_\alpha\mu_\alpha^2(\mathrm{T})\le\sigma_P(A)\mu_0(\mathrm{T})\sum_\alpha\mu_\alpha(\mathrm{T})=\sigma_P(A)\sigma_{\mathscr{P}}(A)\mu_0(\mathrm{T}),$$

and the bound (7.10) is proved.

When $k=2$, we have $\widetilde{\Delta}:=\min\{\Delta,\Delta^*\}\le\big(16L\mu_0(\mathrm{T}_A^{A\circ A})\big)^{1/2}$. We can assume that this minimum is attained in P^*, since the opposite situation is considered similarly. Hence

$$\mathsf{E}(A)\le 4L^2\sum_{x\in P^*}|A_x|^2\le 4L^2(\widetilde{\Delta})^{2-s}\mathsf{E}_s(A)\le 4L^2(16L)^{1-s/2}\mu_0(\mathrm{T}_A^{A\circ A})^{1-s/2}\mathsf{E}_s(A).$$

Using the method of exponentiation, we obtain (7.11). Inequality (7.12) is proved analogously. The theorem is completely proved. □

The example from Remark 6.7 tells us that all the inequalities in the above theorem are sharp. Furthermore, it follows from Example 4.5 that the presence of the quantities $\mu_0(\mathrm{T}_A^{A\circ A})$ is essential in the estimates we have proved

In Theorem 7.2, the quantity $\mu_0\big(\mathrm{T}_A^{(A\circ A)^{k-1}}\big)$ appears. More precisely, we deal with the principal eigenvalue $\mu_0(\mathrm{T}_A^P)$, for some popular set P. The following lemma shows us that this can easily be bounded on large subsets of the set A.

Lemma 7.3. *Let $A \subseteq \mathbf{G}$ be some set. There exists a set $A' \subseteq A$ with $|A'| \geq |A|/2$ such that*

$$\mu_0(\mathrm{T}^P_{A'}) \leq \frac{2\mathsf{E}(A)}{\Delta|A|},$$

for any set $P \subseteq \{x\colon |A_x| \leq \Delta\}$ and an arbitrary real number $\Delta > 0$. In particular,

$$\mu_0(\mathrm{T}^{A\circ A}_{A'}) \leq \frac{2\mathsf{E}(A)}{|A|}.$$

Proof. Let

$$A_1 = \left\{x\colon ((A*A)\circ A)(x) > \frac{2\mathsf{E}(A)}{|A|}\right\}.$$

It is easy to see that $|A_1| < |A|/2$. We put $A' = A \setminus A_1$, and let f be the principal eigenfunction of the operator $\mathrm{T}^P_{A'}$. We also set $\mu_0 = \mu_0(\mathrm{T}^P_{A'})$. We have

$$\mu_0 f(x) = A'(x)(P*f)(x).$$

Summing over $x \in A'$ and applying the definition of the set A', we find

$$\begin{aligned}\mu_0 \sum_x f(x) &= \sum_x f(x)(P\circ A')(x) \leq \Delta^{-1}\sum_x f(x)((A\circ A)\circ A)(x)\\ &= \Delta^{-1}\sum_x f(x)((A*A)\circ A)(x) \leq \Delta^{-1}\frac{2\mathsf{E}(A)}{|A|}\cdot\sum_x f(x),\end{aligned}$$

as required. □

We need an analogue of one of the definitions in [23].

Definition 7.4. Let $\alpha > 1$ be a real number, and $\beta, \gamma \in [0,1]$. A set $A \subseteq \mathbf{G}$ is called (α,β,γ)-connected if, for any $B \subseteq A$ with $|B| \geq \beta|A|$, we have

$$\mathsf{E}_\alpha(B) \geq \gamma\left(\frac{|B|}{|A|}\right)^{2\alpha}\mathsf{E}_\alpha(A).$$

Thus, the set in Theorem 1.2 is a $(2,\beta,\gamma)$-connected set with parameters $\beta,\gamma \gg 1$. As was proved in [23], when $\alpha = 2$ any set contains a large connected subset.

We shall obtain a corollary to Theorem 7.2 for connected sets A. Our inequality (7.18) below shows that, in this case, there exists a nontrivial connection between the quantities $\mathsf{E}(A)$ and $\mathsf{E}_s(A)$, for $1 \leq s \leq 2$.

Corollary 7.5. *Let $A \subseteq \mathbf{G}$ be some set, and $\beta,\gamma \in [0,1]$. Suppose that A is $(2,\beta,\gamma)$-connected, with $\beta \leq 1/2$. Then there exist two $2^{-6}\gamma L^{-2}$-popular dual sets P, P^* such that*

$$\Delta\Delta^* \leq \frac{2^8 L^2\mathsf{E}(A)}{\gamma|A|}, \tag{7.15}$$

$$L^{-5}\gamma^3 2^{-21}|A|^2 \leq |P|\cdot|P^*|, \tag{7.16}$$

and

$$L^{-3}\gamma^2 2^{-13}\mathsf{E}(A)|A| \leq \sigma_P(A)\sigma_{P^*}(A). \tag{7.17}$$

Further, for any $s \in [1,2]$, we have

$$\mathsf{E}_s(A) \geq 2^{-5}\gamma|A|^{1-s/2}\mathsf{E}^{s/2}(A). \tag{7.18}$$

Proof. Let

$$P_j = \Big\{ x\colon \frac{2^{j-1}\gamma \mathsf{E}(A)}{2^5|A|^2} < |A_x| \le \frac{2^j \gamma \mathsf{E}(A)}{2^5|A|^2} \Big\}, \quad j \in [L].$$

Applying Lemma 7.3, we find a set $A' \subseteq A$ with $|A'| \ge |A|/2$ such that, for every j, we have $\mu_0\big(\mathrm{T}_{A'}^{P_j}\big) \le \frac{2\mathsf{E}(A)}{\Delta_j |A|}$. Here, as earlier, $\Delta_j = \frac{2^j\gamma \mathsf{E}(A)}{2^5|A|^2}$. By connectedness, we have

$$\gamma 2^{-5}\mathsf{E}(A) \le 2^{-1}\mathsf{E}(A') \le \sum_{j=1}^{L} \sum_{x\in P_j} (A'\circ A')^2(x),$$

and, for some $j \in [L]$, there exists $P = P_j$ such that

$$\gamma 2^{-5} L^{-1}\mathsf{E}(A) \le 2^{-1}L^{-1}\mathsf{E}(A') \le \sum_{x\in P} (A'\circ A')^2(x) = \mathsf{E}_P(A'). \tag{7.19}$$

Of course, $\mathsf{E}_P(A') \le \mathsf{E}_P(A) \le \Delta \sigma_P(A)$.

We consider the set P^* and put $\Delta = \Delta_j$. It follows from inequality (7.19) that the sets P, P^* are $2^{-6}\gamma L^{-2}$-popular dual sets. Applying the argument from Theorem 7.2 and the bound (7.19), we obtain

$$2^{-2}L^{-2}\mathsf{E}(A') \le \mu_0(\mathrm{T}_{A'}^P)\sigma_{P^*}(A') \le \frac{2\mathsf{E}(A)}{\Delta|A|}\cdot \sigma_{P^*}(A). \tag{7.20}$$

Multiplying the last inequality by Δ^* and again using connectedness, we find

$$2^{-2}L^{-2}\Delta\Delta^*\mathsf{E}(A') \le \frac{2\mathsf{E}(A)}{|A|} 2\mathsf{E}(A) \le 2^6\gamma^{-1}\mathsf{E}(A')\frac{\mathsf{E}(A)}{|A|},$$

which gives us (7.15) for the sets P, P^* we have constructed.

Further, multiplying (7.20) by $\sigma_P(A)$ and recalling (7.19), we obtain

$$\gamma 2^{-6}L^{-2}\mathsf{E}(A)\sigma_P(A)\Delta \le \frac{2\mathsf{E}(A)}{|A|}\cdot \sigma_{P^*}(A)\sigma_P(A).$$

Using the definition of the set P and inequality (7.19), we find

$$\gamma 2^{-6}L^{-2}\mathsf{E}(A)\cdot \gamma 2^{-6}L^{-1}\mathsf{E}(A) \le \frac{2\mathsf{E}(A)}{|A|}\cdot \sigma_{P^*}(A)\sigma_P(A),$$

which gives us the bound (7.17). Combining (7.15) and (7.17), we have (7.16).

Finally, applying inequality (7.11) of Theorem 7.2, we obtain

$$\begin{aligned} 2^{-4}\gamma\mathsf{E}(A) \le \mathsf{E}(A') &\le \mu_0^{1-s/2}\big(\mathrm{T}_{A'}^{A'\circ A'}\big)\mathsf{E}_s(A') \\ &\le \mu_0^{1-s/2}\big(\mathrm{T}_{A'}^{A\circ A}\big)\mathsf{E}_s(A) \le \left(\frac{2\mathsf{E}(A)}{|A|}\right)^{1-s/2}\mathsf{E}_s(A), \end{aligned}$$

and this shows that (7.18) holds. The proof of the corollary is complete. □

The example from Remark 6.7 shows that the inequality (7.18) cannot be strengthened. In this situation, $P = P^* = \bigsqcup_{j=1}^k H_j$, and so it is natural to call the set A from this example a "self-dual". Such sets possess interesting properties. For example, by the above corollary, the quantity $\sigma_P(A)$ is always large and Δ is small. The set from Remark 6.5 (see also Example 7.1) shows that even if A is connected, (7.18) cannot hold for $s > 2$. Thus, in this domain of values of the parameter s, the trivial bounds $\mathsf{E}_{s_2}(A) \le \mathsf{E}_{s_1}(A)|A|^{s_2-s_1}$, for $s_2 \ge s_1$, sometimes turn out to be sharp. Finally, Example 4.5 tells us that the inequality (7.18) cannot hold for arbitrary A. Generally speaking, in order to apply inequalities of the form (7.11), we need the set A to be connected or to have bounds on $\mu_0(\mathrm{T}_A^{A\circ A})$, and not simply on $\mathsf{E}(A)/|A|$.

Thus, even for connected sets A it is not always possible to find a set $P \subseteq A-A$ such that, roughly speaking, $\mathsf{E}_P(A) \gg \mathsf{E}(A) = |A|^3/K$ and $\sigma_P(A) \gg |A|^2/K^{1/2}$, but $\Delta \ll |A|/K^{1/2}$. Nevertheless, if lower bounds are known for $\mathsf{E}_s(A)$, for $s<2$, then the inequality in Corollary 7.5 can be strengthened. This is proved in the following two statements.

Proposition 7.6. *Let $A \subseteq \mathbf{G}$ be some set, $s \in (1,2]$ and $\beta, \gamma \in [0,1]$. Suppose that A is (s,β,γ)-connected, with $\beta \le 1/2$. Then, for*

$$Q = (2^{3s}\gamma^{-1}L^s)^{-1/(s-1)}\mathsf{E}_s^{1/(s-1)}(A)|A|^{-(4-2s)/(s-1)}\mathsf{E}^{-1}(A),$$

there exist two Q-popular dual sets P, P^* such that

$$\mathsf{E}_s(A)|A|^{s-1}\Delta(\Delta^*)^{s-1} \le 2^{4s+3}\gamma^{-1}L^{s+1}\mathsf{E}^s(A) \tag{7.21}$$

and

$$\mathsf{E}_s^2(A)|A|^{s-1} \le 2^{6s+1}\gamma^{-2}L^{s+1}\mathsf{E}^{s-1}(A)\sigma_P^{s-1}(A)\sigma_{P^*}^{3-s}(A). \tag{7.22}$$

Proof. Let

$$P_j = \left\{x\colon \frac{2^{j-1}\gamma\mathsf{E}_s(A)}{2^{1+2s}|A|^2} < |A_x|^{s-1} \le \frac{2^j\gamma\mathsf{E}_s(A)}{2^{1+2s}|A|^2}\right\}, \quad j \in [L].$$

Applying Lemma 7.3, we find a set $A' \subseteq A$ with $|A'| \ge |A|/2$ such that, for all j, we have $\mu_0(\mathrm{T}_{A'}^{P_j}) \le \frac{2\mathsf{E}(A)}{\Delta_j|A|}$. Here, $\Delta_j^{s-1} = \frac{2^j\gamma\mathsf{E}_s(A)}{2^{1+2s}|A|^2}$. Using connectedness, we obtain

$$\gamma 2^{-1-2s}\mathsf{E}_s(A) \le 2^{-1}\mathsf{E}_s(A') \le \sum_{j=1}^{L}\sum_{x\in P_j}(A'\circ A')^s(x), \tag{7.23}$$

and so, for some $j \in [L]$, there exists $P = P_j$ such that

$$\gamma 2^{-1-2s}L^{-1}\mathsf{E}_s(A) \le 2^{-1}L^{-1}\mathsf{E}_s(A') \le \sum_{x\in P}(A'\circ A')^s(x) = \mathsf{E}_s^P(A'). \tag{7.24}$$

Clearly, $\mathsf{E}_s^P(A') \le \mathsf{E}_s^P(A) \le \Delta^{s-1}\sigma_P(A)$. By Hölder's inequality, we have

$$\mathsf{E}_s^P(A') \le \mathsf{E}_P^{s-1}(A')\sigma_P^{2-s}(A'). \tag{7.25}$$

Now let P^* be a dual set to P. Then

$$\mathsf{E}_P(A') \le 2L\sum_\alpha \mu_\alpha(\mathrm{T}_{A'}^P)\langle \mathrm{T}f_\alpha, f_\alpha\rangle \le \frac{4L\mathsf{E}(A)}{\Delta|A|}\sigma_{P^*}(A), \tag{7.26}$$

where the $\{f_\alpha\}$ are eigenfunctions of the operator $\mathrm{T}_{A'}^P$ and T is the operator defined by formula (7.6) with $\mathscr{P} = P^*$. Using (7.24), (7.25), and the trivial upper bound for $\sigma_P(A)$, $\sigma_P(A) \le |A|^2$, we see that P and P^* are Q-popular dual sets, where

$$Q = (2^{3s}\gamma^{-1}L^s)^{-1/(s-1)}\mathsf{E}_s^{1/(s-1)}(A)|A|^{-(4-2s)/(s-1)}\mathsf{E}^{-1}(A).$$

We put $\sigma = \sigma_P(A)$ and $\sigma^* = \sigma_{P^*}(A)$. Substituting (7.26) into (7.25), in view of inequality (7.24) we see that

$$\mathsf{E}_s(A)\Delta^{s-1} \le 2^{4s-1}\gamma^{-1}L^s\left(\frac{\mathsf{E}(A)}{|A|}\right)^{s-1}(\sigma^*)^{s-1}\sigma^{2-s}. \tag{7.27}$$

Multiplying by σ and using (7.23), we find

$$\mathsf{E}_s^2(A) \le 2^{6s+1}\gamma^{-2}L^{s+1}\left(\frac{\mathsf{E}(A)}{|A|}\right)^{s-1}(\sigma^*)^{s-1}\sigma^{3-s},$$

and inequality (7.22) is proved.

Multiplying (7.27) by $(\Delta^*)^{s-1}(\Delta)^{2-s}$ and using the bounds

$$\Delta\sigma \le 2\mathsf{E}(A), \quad \Delta^*\sigma^* \le 2\mathsf{E}(A),$$

we similarly have

$$\mathsf{E}_s(A)|A|^{s-1}\Delta(\Delta^*)^{s-1} \le 2^{4s+3}\gamma^{-1}L^{s+1}\mathsf{E}^s(A). \qquad \square$$

For example, if

$$\mathsf{E}(A) = \frac{|A|^3}{K}, \quad \mathsf{E}_{3/2}(A) = \frac{|A|^{5/2}}{K^{1/2}},$$

then it follows from (7.21) that $\min\{\Delta,\Delta^*\} \ll_L |A|/K^{2/3}$. This is, of course, stronger than the bound $\min\{\Delta,\Delta^*\} \ll_L |A|/K^{1/2}$, which can be deduced from Theorem 7.2 (assuming the presence of the corresponding bound on $\mu_0(\mathrm{T}_A^{A\circ A})$) or from Corollary 7.5.

Corollary 7.7. *Let $A \subseteq \mathbf{G}$ be some set, $|A-A| \le K|A|$ and let $s \in (1,2]$ be a real number. Then there exist two*

$$(cL^s)^{1/(s-1)}\frac{|A|^3}{K\mathsf{E}(A)}\text{-popular} \tag{7.28}$$

sets P, P^*, where $c>0$ is an absolute constant, with the properties

$$\Delta(\Delta^*)^{s-1} \ll L^{s+1}\cdot\frac{K^{s-1}\mathsf{E}^s(A)}{|A|^{2s}} \tag{7.29}$$

and

$$|A|^{3s+1} \ll K^{2(s-1)}L^{s+1}\mathsf{E}^{s-1}(A)\sigma_P^{s-1}(A)\sigma_{P^*}^{3-s}(A). \tag{7.30}$$

Proof. Let

$$P_j = \left\{x\colon \frac{2^{j-1}|A|^{s-1}}{2^{2s+1}K^{s-1}} < |A_x|^{s-1} \le \frac{2^j|A|^{s-1}}{2^{2s+1}K^{s-1}}\right\}, \quad j\in[L].$$

Appling Lemma 7.3, we find a set $A'\subseteq A$ with $|A'|\ge|A|/2$ such that, for all j, we have $\mu_0\big(\mathrm{T}_{A'}^{P_j}\big) \le \frac{2\mathsf{E}(A)}{\Delta_j|A|}$. Here, $\Delta_j^{s-1} = \frac{2^j|A|^{s-1}}{2^{2s+1}K^{s-1}}$. Using Hölder's inequality, we obtain

$$\mathsf{E}_s(A') \ge \frac{2^{-2s}|A|^{s+1}}{K^{s-1}}.$$

Then, for some $j\in[L]$ and $P_j = P$, we have the inequality

$$\mathsf{E}_s(A') \le 2L\sum_{x\in P}|A'_x|^s.$$

We can next apply the argument from Proposition 7.6. The lemma is proved. $\square$

We now try to prove an analogue of Theorem 6.4 under weaker assumptions on the set A, namely, that it has only a lower bound for its additive energy. More precisely, we obtain a lower bound for $\mathsf{E}_4(A)$, and the existence of a structural subset $A'\subseteq A$ follows from this in the same manner as in Theorem 6.4. Our result is quite simple, and the reasons why the method does not give the same bounds as in Theorem 6.4 are discussed after Proposition 7.8.

Proposition 7.8. *Let $A\subseteq\mathbf{G}$ be some set, $\mathsf{E}(A) = |A|^3/K$, and $\mathsf{T}_4(A) = M|A|^7/K^3$. Then*

$$\mathsf{E}_4(A) \ge \frac{|A|^5}{2^5L^{10/3}M^{1/3}K^{7/3}}. \tag{7.31}$$

Proof. Let P be a popular difference set such that

$$\mathsf{E}(A) \le 2L \sum_{x\in P} |A_x|^2. \tag{7.32}$$

From inequality (7.32), we clearly have

$$\mathsf{E}_4(A) \ge (8L)^{-1}K^{-1}\Delta^2|A|^3. \tag{7.33}$$

On the other hand, from the arguments in Theorem 6.4 it follows that

$$\left(\frac{\mathsf{E}(A)}{2L|A|}\right)^8 \le \mathsf{E}_4(A)\Delta^4\mathsf{T}_4(A) \le \mathsf{E}_4(A)\Delta^4\frac{M|A|^7}{K^3}. \tag{7.34}$$

Combining (7.33), (7.34), and optimizing for Δ, we obtain the required result. □

The example in Remark 6.7 shows that the value $K^{7/3}$ in inequality (7.31) cannot be replaced by anything smaller than K^2. The reason why we have precisely K^2 in this example is entirely clear. Indeed, it is easy to see that, in this case, there exist $[K^{1/2}]$ eigenvalues, equal, in order, to $\mu_0(\mathrm{T}_A^{A\circ A})$, and our approximation of the sum $\sum_\alpha \mu_\alpha^4(\mathrm{T}_A^{A\circ A})$ by one zero term is very rough. Simple calculations show that, using the contribution of all $[K^{1/2}]$ eigenvalues in the sum $\sum_\alpha \mu_\alpha^4(\mathrm{T}_A^{A\circ A})$, we obtain precisely K^2.

The same example shows us that the approach connected with obtaining lower bounds for $\mathsf{E}_4(A)$ does not always work for determining the structural subset $A' \subseteq A$. Indeed, in the proof of Theorem 6.4 we used Lemma 3.4, which says that $\mathsf{E}_4(A) = \sum_{s,t} \mathsf{E}(A_s, A_t)$. But in our example, for a typical pair (s,t), the combined energy $\mathsf{E}(A_s, A_t)$ is very small, and therefore the intermediate arguments give almost nothing.

It would be interesting to find a better bound than (7.31).

Remark 7.9. The conditions in Theorem 6.4 are undoubtedly stronger than those in Proposition 7.8. This kind of inequality, namely a lower bound on $\mathsf{E}_s(A)$, for $s \le 2$, can be interpreted as the closeness of A to a set with small doubling. Indeed, by Hölder's inequality, all such inequalities are included in each other, and, on the other hand, if A has small doubling, then all $\mathsf{E}_s(A)$ are large, for $s \ge 1$.

To conclude this section, we consider another example of dual sets. Let

$$P = \bigl\{x\colon \mathsf{E}(A, A_x) \ge |A_x|^2\mathsf{E}_3(A)(2\mathsf{E}(A))^{-1}\bigr\}.$$

Then, by Lemma 3.4,

$$2^{-1}\mathsf{E}_3(A) \le \sum_{x\in P} \mathsf{E}(A, A_x) = \sum_{x,\,y} A(x)A(y)(A\circ A)(x-y)\mathscr{C}_3(P,A,A)(x,y).$$

The last expression is very similar to (7.3). As above, we define a popular set P^* by the formula $P^* = \bigl\{x\colon |A_x| \ge \mathsf{E}_3(A)(4\mathsf{E}(A))^{-1}\bigr\}$. Thus,

$$2^{-2}\mathsf{E}_3(A) \le \sum_{x,\,y} A(x)A(y)(A\circ A)(x-y)P^*(x-y)\mathscr{C}_3(P,A,A)(x,y). \tag{7.35}$$

Applying the Cauchy–Bunyakovskii inequality for the bound (7.35), we find

$$2^{-4}\mathsf{E}_3^2(A) \le \mathsf{E}_3^{P^*}(A)\cdot \sum_{x,\,y\in P} \mathscr{C}_3^2(A)(x,y).$$

In particular, for a dual set P^*, we have

$$\sum_{x\in P^*} |A_x|^3 \gg \mathsf{E}_3(A).$$

Using formula (7.35) for dual sets of this type, we can undoubtedly obtain an analogue of Theorem 7.2.

References

[1] M. Bateman and N. Katz, *New bounds on cap sets*, J. Amer. Math. Soc. **25** (2012), no. 2, 585–613. MR2869028

[2] M. Bateman and N. Katz, *Structure in additively nonsmoothing sets*, arXiv:1104.2862v1 [math.CO], 14 Apr 2011.

[3] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, Int. J. Number Theory **1** (2005), no. 1, 1–32. MR2172328 (2006g:11041)

[4] J. Bourgain, *Estimates on exponential sums related to the Diffie–Hellmann distributions*, Geom. Funct. Anal. **15** (2005), no. 1, 1–34. MR2140627 (2006h:11095)

[5] A. Carbery, *A multilinear generalization of the Cauchy–Schwarz inequality*, Proc. Amer. Math. Soc. **132** (2004), no. 11, 3141–3152. MR2073287 (2005e:26022)

[6] A. Carbery, *An automatic proof of a multilinear generalization of the Cauchy–Schwarz inequality*, preprint.

[7] A. A. Glibichuk and S. V. Konyagin, *Additive properties of product sets in fields of prime order*, in *Additive combinatorics*, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, 279–286. MR2359478 (2009a:11054)

[8] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), 529–551. MR1631259 (2000d:11019)

[9] W. T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), 465–588. MR1844079 (2002k:11014)

[10] T. G. F. Jones and O. Roche-Newton, *Improved bounds on the set $A(A+1)$*, J. Combin. Theory Ser. A **120** (2013), no. 3, 515–526. MR3007133

[11] R. Horn and C. Johnson, *Matrix analysis*, Cambridge University Press, Cambridge, 1985. MR832183 (87e:15001)

[12] A. Iosevich, S. V. Konyagin, M. Rudnev and V. Ten, *On combinatorial complexity of convex sequences*, Discrete Comput. Geom. **35** (2006), 143–158. MR2183494 (2006k:11036)

[13] S. V. Konyagin, *Estimates for trigonometric sums over subgroups and for Gauss sums*, IV International Conference "Modern Problems in Number Theory and its Applications": Current Problems, Part III (Tula, 2001), Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002, 86–114. (Russian) MR1985950 (2004d:11073)

[14] S. V. Konyagin and M. Rudnev, *On new sum-product type estimates*, SIAM J. Discrete Math. **27** (2013), no. 2, 973–990. MR3056747

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

[16] L. Li and O. Roche-Newton, *Convexity and a sum-product type estimate*, Acta Arith. **156** (2012), no. 3, 247–255. MR2999071

[17] M. Rudnev, *An improved sum-product inequality in fields of prime order*, Int. Math. Res. Not. IMRN 2012, no. 16, 3693–3705. MR2959023

[18] T. Sanders, *Approximate (abelian) groups*, arXiv:1212.0456v1 [math.CA], 3 Dec 2012.

[19] T. Schoen, *New bounds in Balog–Szemerédi–Gowers theorem*, preprint.

[20] T. Schoen and I. D. Shkredov, *Additive properties of multiplicative subgroups of $\mathbb{F}_p$*, Quart. J. Math. **63** (2012), no. 3, 713–722. MR2967172

[21] T. Schoen and I. D. Shkredov, *On sumsets of convex sets*, Combin. Probab. Comput. **20** (2011), 793–798. MR2825592 (2012g:11021)

[22] T. Schoen and I. D. Shkredov, *Higher moments of convolutions*, J. Number Theory **133** (2013), no. 5, 1693–1737. MR3007128

[23] I. D. Shkredov, *On sets with small doubling*, Mat. Zametki **84** (2008), no. 6, 927–947; English transl., Math. Notes **84** (2008), no. 5–6, 859–878. MR2492806 (2010c:11015)

[24] I. D. Shkredov, *Some applications of W. Rudin's inequality to problems of combinatorial number theory*, Unif. Distrib. Theory **6** (2011), no. 2, 95–116. MR2904042

[25] I. D. Shkredov, *Some new inequalities in additive combinatorics*, arXiv:1208.2344v2 [math.CO].

[26] I. D. Shkredov, *On Heilbronn's exponential sum*, Quart. J. Math., doi 10.1093qmathhas037.

[27] I. V. V'yugin and I. D. Shkredov, *On additive shifts of multiplicative subgroups*, Mat. Sb. **203** (2012), no. 6, 81–100; English transl., Sb. Math. **203** (2012), no. 5–6, 844–863. MR2984656

[28] T. Tao and V. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, 2006. MR2289012 (2008a:11002)

Department of Algebra and Number Theory, Russian Academy of Sciences, Steklov Mathematical Institute, Moscow

Delone Laboratory of Discrete and Computational Geometry, Yaroslavl State University, Yaroslavl

Kharkevich Institute of Information Transmission Problems, Russian Academy of Sciences
E-mail address: ilya.shkredov@gmail.com

Translated by CHRISTOPHER HOLLINGS