J. Aust. Math. Soc. **100** (2016), 124–144
doi:10.1017/S1446788715000324

ADDITIVE DIMENSION AND A THEOREM OF SANDERS

TOMASZ SCHOEN and ILYA D. SHKREDOV✉

(Received 9 April 2014; accepted 1 June 2015; first published online 22 October 2015)

Communicated by B. Martin

Abstract

We prove some new bounds for the size of the maximal dissociated subset of structured (having small sumset, large energy and so on) subsets of an abelian group.

2010 *Mathematics subject classification*: primary 11B13; secondary 11B75.

Keywords and phrases: additive dimension, sumset, additive energy, dissociated sets.

1. Introduction

Let $\mathbf{G}$ be an abelian group. A finite set $\Lambda \subseteq \mathbf{G}$ is called *dissociated* if any equality of the form

$$\sum_{\lambda\in\Lambda} \varepsilon_\lambda \lambda = 0$$

for $\varepsilon_\lambda \in \{-1, 0, 1\}$ implies $\varepsilon_\lambda = 0$ for all λ. The notion of dissociativity appeared naturally in analysis; see [12]. In many problems of additive combinatorics (see for example [1, 2, 4, 5, 8, 17, 19, 20]) it is important to control the size of the largest dissociated subset of A, which we call the (additive) *dimension* of the set A and denote by $\dim(A)$. There are other possible variants of additive dimension and we discuss them in Section 8, for example

$$d(A) = \min\{|S| : S \subseteq A,\ A \subseteq \operatorname{Span} S\}, \quad d_*(A) = \min\{|S| : A \subseteq \operatorname{Span} S\},$$

and

$$\tilde{d}(A) = \min\{|\Lambda| : \Lambda \subseteq A, \Lambda \text{ is a maximal (by inclusion) dissociated subset of } A\},$$

The first author was supported by NCN 2012/07/B/ST1/03556. The second author's work was supported by grant RFFI NN 11-01-00759, the Russian Government project 11.G34.31.0053, the Federal Program 'Scientific and scientific–pedagogical staff of innovative Russia' 2009–2013, grant mol_a_ved 12–01–33080 and grant Leading Scientific Schools N 2519.2012.1.

where, for $S = \{s_1, \dots, s_l\}$, we define

$$\mathrm{Span}\,(S) := \Big\{ \sum_{j=1}^{l} \varepsilon_j s_j : \varepsilon_j \in \{0, -1, 1\} \Big\}.$$

In the group $\mathbb{F}_2^n$, all these dimensions coincide with the usual dimension. Thus, the notions of dissociativity and additive dimension generalize the ordinary linear dependence and dimension, correspondingly, and $\mathrm{Span}\,(S)$ corresponds to the linear span. All the dimensions are closely connected to each other, see Section 8, and we refer the interested reader to the recent paper [7].

Additive dimension can be considered as a measure of the 'structure' of a set and the main aim of the paper is to find some connections between the dimension and other natural quantitative measures of structure such as doubling constant and various types of additive energy; see for example Theorems 1.1 and 1.2 below.

Historically, the first general theorem on dimension of the so-called large spectrum of a set, that is, the characters at which the Fourier transform of a set is large, was obtained by Chang [8]. Chang used dimension dim in her proof and that is why we are concentrating on this definition of dimension in our paper. For further results in this direction, see [1–3, 5, 16, 20, 27]. For example, new theorems of Bateman and Katz [1, 2] on the structure of the large spectrum of sets having no arithmetic progressions of length three, namely, new results on dimensions of subsets of such sets, allowed them to achieve remarkable progress in the long-standing cap set problem. Here we use the additive dimension as a measure of additive structure; however, there other natural measures of structure like doubling constant and additive energy. The following theorems, proved in [20, 27], offer a useful connection between the types of additive structure.

THEOREM 1.1. *Let* $A, B \subseteq \mathbf{G}$ *be finite sets and suppose that* $|A + B| \leqslant K|A|$. *Then* $\dim(B) \ll K \log |A|$.

THEOREM 1.2. *Let* $A, B \subseteq \mathbf{G}$ *be finite sets and suppose that* $\mathsf{E}(A, B) \geqslant |A||B|^2/K$. *Then there exists a set* $B_1 \subseteq B$ *such that* $\dim(B_1) \ll K \log |A|$ *and*

$$\mathsf{E}(A, B_1) \geqslant 2^{-5}\mathsf{E}(A, B). \tag{1.1}$$

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

One of the aims of this paper is to obtain some further estimates on dimensions of sets. First of all, we give a simple combinatorial proof of Theorem 1.1 and refine the result in the case of small doubling constant K (see Theorem 4.2). Furthermore, we generalize Theorem 1.2 for the case of another type of energy and improve it by finding a subset having even smaller additive dimension (see Theorems 5.2 and 5.5). As a demonstration of how our method could be used, we present an application of our results to obtain a new bound in an interesting problem of Konyagin. We show

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

that for every $A \subseteq \mathbb{F}_p$ such that $|A| \leqslant e^{c\sqrt{\log p}}$, there exists x with $0 < (A * A)(x) \ll e^{-O(\log^{1/4}|A|)}|A|$. In the last section we reformulate some results from the papers [1, 2] in terms of the additive dimensions and prove them for general abelian groups.

The polynomial Freiman–Ruzsa conjecture (PFRC) roughly states (see [9] for details) that every set A with $|A + A| \leqslant K|A|$ contains a highly structured subset of size $|A|/K^{O(1)}$. This is a very important conjecture in additive combinatorics, which implies a series of new results in number theory, theory of functions, computer science and additive combinatorics of course; see for example [9, 18, 21]. Roughly speaking, it states that any set with small doubling contains a polynomially large subset which is really structured. So, it is not surprising that such strong structural results have many applications in different fields.

If PFRC holds, then for every set A with $|A + A| \leqslant K|A|$ there is a subset $B \subseteq A$, $|B| \gg K^{-C}|A|$ with $\dim(B) \ll K^{o(1)} \log |A|$, as $K \to \infty$. Our results provide bounds of the form $\dim(B) \ll K^c \log |A|$, where $c > 0$ is some constant, which is much weaker than one could expect from PFRC. However, our theorems are still applicable because in our results the size of the set B is large and explicit, which is crucial, for example, in problems concerning sets without solutions to a linear equation (see for example [2, 20]).

2. Notation

Let $\mathbf{G}$ be a finite abelian group and denote by N the cardinality of $\mathbf{G}$. It is well known [12] that the dual group $\widehat{\mathbf{G}}$ is isomorphic to $\mathbf{G}$ in this case. Let f be a function from $\mathbf{G}$ to $\mathbb{C}$. We denote the Fourier transform of f by $\widehat{f}$,

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

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

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

$$\sum_{y\in\mathbf{G}} \Big| \sum_{x\in\mathbf{G}} f(x)g(y - x) \Big|^2 = \frac{1}{N} \sum_{\xi\in\widehat{\mathbf{G}}} |\widehat{f}(\xi)|^2 |\widehat{g}(\xi)|^2, \tag{2.1}$$

and

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

If

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

then

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

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

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

We denote the characteristic function of a set $S \subseteq \mathbf{G}$ by $S(x)$. Write $\mathsf{E}(A, B)$ for the *additive energy* of sets $A, B \subseteq \mathbf{G}$ (see for example [28]), that is,

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

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

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

and, by (2.1),

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

Let

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

Clearly, $\mathsf{T}_k(A) = (1/N) \sum_\xi |\widehat{A}(\xi)|^{2k}$. For $A_1, \ldots, A_{2k} \subseteq \mathbf{G}$, let

$$\mathsf{T}_k(A_1, \ldots, A_{2k}) := |\{a_1 + \cdots + a_k = a_{k+1} + \cdots + a_{2k} : a_i \in A_i,\ i \in [2k]\}|.$$

Put also

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

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

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

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

and

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

be the higher energies of A and B. The second formulas in (2.2) and (2.3) can be considered as the definitions of $\mathsf{E}_k(A)$ and $\mathsf{E}_k(A, B)$ for noninteger k, $k \geqslant 1$.

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

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

3. Preliminaries

In this section we recall some results that we will need in the paper.

First of all, it was proved by Rudin [12] that all L^p norms of the Fourier transform of a function whose transform is supported on a dissociated set are equivalent.

LEMMA 3.1. *Let $\Lambda \subseteq \mathbb{Z}_N$ be a dissociated set and let a_n be any complex numbers. Then, for each $p \geqslant 2$,*

$$\frac{1}{N}\sum_{x=0}^{N-1}\Big|\sum_{n\in\Lambda} a_n e^{-2\pi i n x/N}\Big|^p \leqslant (Cp)^{p/2}\Big(\sum_{n\in\Lambda}|a_n|^2\Big)^{p/2}$$

for some absolute constant C.

A consequence of the above lemma is the following result due to Sanders [16]. (Similar results were obtained by Bourgain [3] and by the second author [24].)

LEMMA 3.2. *Let $\mathbf{G}$ be a finite abelian group, $Q \subseteq \mathbf{G}$ be a set and l be a positive integer. There is a partition $Q = Q^{\mathrm{str}} \cup Q^{\mathrm{diss}}$ such that $\dim(Q^{\mathrm{str}}) < l$ and Q^{diss} is a union of dissociated sets of size l. Moreover, for all $p \geqslant 2$, the following holds:*

$$\Big(\frac{1}{N}\sum_{\xi}|\widehat{Q}^{\mathrm{diss}}(\xi)|^p\Big)^{1/p} \ll \sqrt{p/l}\cdot|Q|.$$

We will also make use of a covering lemma due to Chang [8] and the Plünnecke–Ruzsa inequality; see [15], [14] or [28].

LEMMA 3.3. *Let L, K be real numbers, and $A, B \subseteq \mathbf{G}$ be two sets. If $|A + A| \leqslant K|A|$ and $|A + B| \leqslant L|B|$, then there are sets $S_1, \ldots, S_l$ each of size at most $2K$ such that $A \subseteq B - B + (S_1 - S_1) + \cdots + (S_l - S_l)$ and $l \leqslant \log(2KL)$.*

LEMMA 3.4. *Let $j < k$ be positive integers. Let also A, B be finite set of an abelian group such that $|A + jB| \leqslant K|A|$. Then there is a nonempty set $X \subseteq A$ such that*

$$|X + kB| \leqslant K^{k/j}|X|.$$

Furthermore, if $|A + A| \leqslant K|A|$, then

$$|mA - nA| \leqslant K^{n+m}|A| \tag{3.1}$$

for all $n, m \in \mathbb{N}$. Moreover, for fixed $j \geqslant 1$ and arbitrary $0 < \delta < 1$, there exists $X \subseteq A$ such that $|X| \geqslant (1 - \delta)|A|$ and

$$|X + kB| \leqslant (K/\delta)^k|X|.$$

We will also make use of some results concerning higher additive energies (see [23] and [26]).

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

Lemma 3.5. *Let A be a subset of an abelian group. Then, for every $k, l \in \mathbb{N}$,*

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

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

Theorem 3.6. *Let A be a finite subset of an abelian group. Suppose that $\mathsf{E}(A) = |A|^3/K$, and $\mathsf{E}_{3+\varepsilon}(A) = M|A|^{4+\varepsilon}/K^{2+\varepsilon}$, where $\varepsilon \in (0, 1]$. Put $P := \{x : (A \circ A)(x) \geqslant |A|/2K\}$. Then $|P| \gg K|A|/M^{2/(1+\varepsilon)}$ and $\mathsf{E}(P) \gg M^{-\beta}|P|^3$, where $\beta = (3 + 4\varepsilon)/(\varepsilon(1 + \varepsilon))$.*

Theorem 3.7. *Let $A \subseteq \mathbf{G}$ be a finite set and $l \geqslant 2$ be a positive integer. Then*

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

Other relations between E_s and T_s can be found in [23, 25].

Theorem 3.8. *Let $A \subseteq \mathbf{G}$ be a finite set. Suppose that $\mathsf{E}_s(A) = |A|^{s+1}/K^{s-1}$, $s \in (1, 3/2]$ and $\mathsf{T}_4(A) := M|A|^7/K^3$; then*

$$\mathsf{E}_4(A) \gg_{s-1} \frac{|A|^5}{MK}.$$

By an arithmetic progression of dimension d and size L, we mean a set of the form

$$Q = \{a_0 + a_1x_1 + \cdots + a_dx_d : 0 \leqslant x_j < l_j\}, \tag{3.2}$$

where $L := l_1 \cdots l_d$. The progression Q is said to be *proper* if all of the sums in (3.2) are distinct. In the latter case we have, in particular, $|Q| = L$. It is easy to see that any proper progression Q of dimension d satisfies $|mQ| \leqslant m^d|Q|$ for any positive integer m. By a *proper coset progression* of dimension d, we will mean a subset of $\mathbf{G}$ of the form $Q + H$, where $H \subseteq \mathbf{G}$ is a subgroup, Q is a proper progression of dimension d and the sum is direct in the sense that $q + h = q' + h'$ if and only if $h = h'$ and $q = q'$. By the size of a proper coset progression, we mean simply its cardinality.

Finally, let us recall the main result proved in [18].

Theorem 3.9. *Suppose that $\mathbf{G}$ is an abelian group and $A, S \subseteq \mathbf{G}$ are finite nonempty sets such that $|A + S| \leqslant K \min\{|A|, |S|\}$. Then $(A - A) + (S - S)$ contains a proper symmetric $d(K)$-dimensional coset progression P of size $\exp(-h(K))|A + S|$. Moreover, we may take $d(K) = O(\log^6 K)$ and $h(K) = O(\log^6 K \log\log K)$.*

4. Additive dimension of sets with small doubling

In the beginning, we derive a consequence of Theorem 3.9.

Lemma 4.1. *Let A be a subset of an abelian group such that $|A + A| \leqslant K|A|$. Then*

$$|kA| \leqslant \left(\frac{3ek}{K}\right)^{O(K\log^6(2K)\log\log(4K))}|A|$$

for every $k \geqslant K$.

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

Proof. By Theorem 3.9, there exists a proper generalized arithmetic progression P of dimension $d \ll \log^6 K$ and size at least $|A|/K^{O(\log^5(2K)\log\log(4K))}$ such that $P \subseteq 2A - 2A$. Thus, applying the Plünnecke–Ruzsa inequality (3.1),

$$|A + P| \leqslant |3A - 2A| \leqslant K^5|A| \leqslant K^{O(\log^5(2K)\log\log(4K))}|P|.$$

By Lemma 3.3,

$$A \subseteq P - P + (S_1 - S_1) + \cdots + (S_l - S_l)$$

with $l \ll \log^6(2K)\log\log(4K)$. Therefore,

$$|kA| \leqslant |kP - kP + (kS_1 - kS_1) + \cdots + (kS_l - kS_l)| \leqslant \binom{2K+k-1}{k}^{2l} |kP - kP|$$
$$\leqslant \binom{2K+k-1}{k}^{2l} (2k)^d|P| \leqslant \Big(\frac{3ek}{2K-1}\Big)^{4lK} (2k)^d|P| \leqslant \Big(\frac{3ek}{K}\Big)^{O(K\log^6(2K)\log\log(4K))} |A|,$$

provided that $k \geqslant K$. □

Our first result refines Sanders' theorem (Theorem 1.1), provided that K is not too large.

Theorem 4.2. *Let $A \subseteq \mathbf{G}$ be a finite set and suppose that $|A + A| \leqslant K|A|$. Then*

$$\dim(A) \ll K \log |A|$$

and

$$\dim(A) \ll \log |A| + K \log^6(2K)\log\log(4K) \cdot \log\log |A|.$$

Proof. Let $\Lambda \subseteq A$ be a dissociated set such that $|\Lambda| = \dim(A)$. Then, by Lemma 3.1 (or simple counting arguments) and Lemma 3.4, we have for some absolute constant $C > 0$,

$$\frac{|\Lambda|^k}{(Ck)^k} \leqslant |k\Lambda| \leqslant |kA| \leqslant K^k|A|.$$

Taking $k \sim \log |A|$, we obtain the first assertion.

Similarly, by Lemma 4.1,

$$\frac{|\Lambda|^k}{(Ck)^k} \leqslant \Big(\frac{3ek}{K}\Big)^{O(K\log^6(2K)\log\log(4K))} |A|$$

for $k \geqslant K$. Thus, putting

$$k \sim \log |A| + K \log^6(2K)\log\log(4K)\log\log |A|,$$
$$|\Lambda| \ll \log |A| + K \log^6(2K)\log\log(4K)\log\log |A|,$$

as required. □

Note that using recent advances of Konyagin, see [21], one can obtain further improvements of powers of logarithms in Lemma 4.1 and Theorem 4.2.

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

In the above proof the hardest case is when the size of kA attains its maximal value $K^k|A|$. However, we show that if it is the case then one can find a huge subset of A with very small additive dimension.

Theorem 4.3. *Let $A \subseteq \mathbf{G}$ be a set and $K \geqslant 1$, $\varepsilon > 0$ be real numbers. Suppose that $|A + A| \leqslant K|A|$ and $|kA| \geqslant K^{k-\varepsilon}|A|$ for some $k \geqslant 3$. Then there exists a set $A' \subseteq A$ of size at least $|A|/2$ such that* $\dim(A') \ll 2^k K^{\varepsilon} \log |kA|$.

Proof. From Lemma 3.4, it follows that there exists a set X, $|X| \geqslant |A|/2$ such that $|X + kA| \leqslant (2K)^k|A|$. Therefore,

$$|X + kA| \leqslant 2^k K^{\varepsilon}|kA|.$$

By Sanders' theorem (Theorem 1.1), we have $\dim(X) \ll 2^k K^{\varepsilon} \log |kA|$. This completes the proof. □

We recall the following result, which appeared as [22, Lemma 3].

Theorem 4.4. *Let A be a finite set of an abelian group such that $|A + A| \leqslant K|A|$. Then, for every $k \in \mathbb{N}$, there exist sets $X \subseteq A$ and $Y \subseteq A + A$ such that $|X| \geqslant (2K)^{-2^{k+1}}|A|$, $|Y| \geqslant |A|$ and $\mathsf{E}(X, Y) \geqslant K^{-2/k}|X|^2|Y|$.*

Combining Theorem 4.4 with Theorem 1.2, we obtain the following consequence.

Corollary 4.5. *Let A be a finite set of an abelian group such that $|A + A| \leqslant K|A|$. Then, for every $k \in \mathbb{N}$, there exists a set $X \subseteq A$ such that $|X| \gg (2K)^{-2^{k+1}}|A|/K^{1/2}$ and* $\dim(X) \ll K^{2/k} \log |A|$.

Using a well-known lemma of Croot and Sisask, Sanders proved the following result [18, Proposition 3.1].

Theorem 4.6. *Let A be a finite subset of an abelian group with $|A + A| \leqslant K|A|$. Then, for every $k \in \mathbb{N}$, there exists a set $X \subseteq A - t$ for some t of size at least $e^{-O(k^2 \log^2 2K)}|A + A|$ such that $kX \subseteq 2A - 2A$.*

Applying Theorem 4.6, we show that every set with small sumset contains a relatively large subset with very small additive dimension.

Corollary 4.7. *Let A be a finite subset of an abelian group with $|A + A| \leqslant K|A|$. Then, for every $k \in \mathbb{N}$, there exists a set $X \subseteq A$ of size at least $e^{-O(k^2 \log^2 2K)}|A + A|$ such that*

$$\dim(X) \ll K^{4/k} \log |A|.$$

Proof. Observe that we can assume that $k \leqslant \log |A|$, because otherwise our theorem is trivial. Let X be the set given by Theorem 4.6. By the Plünnecke–Ruzsa inequality,

$$|klX| \leqslant |2lA - 2lA| \leqslant K^{4l}|A|.$$

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

Now, we argue as in Theorem 4.2. Let $\Lambda \subseteq X$ be a dissociated set with $|\Lambda| = \dim(X)$. By Rudin's inequality, we have for some absolute constant $C_1 > 0$,

$$\frac{|\Lambda|^{kl}}{(C_1 kl)^{kl}} \leqslant |kl\Lambda| \leqslant |klX| \leqslant K^{4l}|A|.$$

Putting $l = [\log |A|/k]$,

$$\dim(X) \ll K^{4/k} \log |A|,$$

which completes the proof. □

5. Additive dimension of sets with large additive energy

The aim of this section is to refine Theorem 1.2, in the sense that under the same assumption $\mathsf{E}(A) = |A|^3/K$, we find a possibly large subset of A having additive dimension $O(K^{1-\gamma} \log |A|)$, where $\gamma > 0$ is an absolute constant. Observe that in the symmetric case $A = B$ such, although quantitatively weaker, results would follow from the previous section combined with the Balog–Szemerédi–Gowers theorem; see for example [28]. The point of the current section is that it is far more efficient to work with the assumption of large energy directly. Moveover, as we mentioned in the introduction, our results give an explicit effective lower bound for the size of the structured subset B, which is crucial in some additive-combinatorial problems [2, 20].

Our first result refines Theorem 1.2.

THEOREM 5.1. *Let A, B be subsets of a finite abelian group. Suppose that $\mathsf{E}(A, B) = |A||B|^2/K$; then there exist a set $B_* \subseteq B$ such that*

$$\dim(B_*) \ll K(\log K)^2 \log |A| \cdot \left(\frac{|B_*|}{|B|}\right)^2 \tag{5.1}$$

and

$$\mathsf{E}(A, B_*) \geqslant 2^{-2}\mathsf{E}(A, B). \tag{5.2}$$

PROOF. We establish Theorem 5.1 using the following algorithm.

At zero step we put $B_0 := B$, $\varepsilon_0(x) = 0$ and $\beta_0 = 1$. At step $j \geqslant 1$ we apply Lemma 3.2 to the set B_{j-1} with parameters $p = 2 + \log |A|$ and

$$l_j = K(\log K)^2 \beta_{j-1}^2 \log |A|.$$

Lemma 3.2 gives us a new set $B_j \subseteq B_{j-1}$, where $B_j = B^{\mathrm{str}}$; in other words, $B_{j-1} \setminus B_j$ is a disjoint union of all dissociated subsets each of size l_j. After that, put $\varepsilon_j(x) = B_{j-1}(x) - B_j(x)$, $\beta_j = |B_j|/|B|$ and iterate the procedure. The described algorithm will satisfy the following property:

$$\mathsf{E}(A, B_j) \geqslant 2^{-2}\mathsf{E}(A, B). \tag{5.3}$$

Obviously, at the first step inequality (5.3) is satisfied. If at some step j we get $\beta_j \geqslant \frac{1}{2}\beta_{j-1}$, then our algorithm terminates with the output $B_* = B_j$. In view of inequality

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

(5.3), it is clear that the total number of steps k does not exceed $\log K$. Further, if our iteration procedure terminates with the output B_*, then $\mathsf{E}(A, B_*) \geqslant 2^{-2}\mathsf{E}(A, B)$ and

$$\begin{aligned} \dim(B_*) &= \dim(B_j) \leqslant l_j = K(\log K)^2 \beta_{j-1}^2 \log|A| \\ &\leqslant 4K(\log K)^2 \beta_j^2 \log|A| \\ &\ll K(\log K)^2 \log|A| \cdot \Big(\frac{|B_*|}{|B|}\Big)^2. \end{aligned}$$

Thus, the constructed set B_* satisfies (5.1), (5.2).

It remains to check (5.3) and, clearly, it is sufficient to do it for the final step k. We have

$$\begin{aligned} N \cdot \mathsf{E}(A, B) &= \sum_\xi |\widehat{A}(\xi)|^2 |\widehat{B}(\xi)|^2 \\ &= \sum_\xi |\widehat{A}(\xi)|^2 |\widehat{B}_k(\xi)|^2 \\ &\quad + \Big(\sum_{j=1}^k \sum_\xi |\widehat{A}(\xi)|^2 \overline{\widehat{B}_j(\xi)} \widehat{\varepsilon}_j(\xi) + \sum_{j=1}^k \sum_\xi |\widehat{A}(\xi)|^2 \widehat{B}_j(\xi) \overline{\widehat{\varepsilon}_j(\xi)} \Big) \\ &\quad + \sum_{j=1}^k \sum_\xi |\widehat{A}(\xi)|^2 |\widehat{\varepsilon}_j(\xi)|^2 \\ &= \sigma_0 + \sigma_1 + \sigma_2. \end{aligned} \tag{5.4}$$

By the Hölder inequality, the Parseval identity and our choice of parameters,

$$\begin{aligned} \sigma_2 &\leqslant \sum_{j=1}^k \Big(\sum_\xi |\widehat{\varepsilon}_j(\xi)|^{2p} \Big)^{1/p} \cdot \Big(\sum_\xi |\widehat{A}(\xi)|^{2p/(p-1)} \Big)^{1-1/p} \\ &\leqslant \sum_{j=1}^k |A|^{1+1/p} |B_{j-1}|^2 N \frac{p}{l_j} \ll k(\log K)^{-2} K^{-1} |A||B|^2 N \\ &\leqslant 2^{-4} k^{-1} K^{-1} |A||B|^2 N. \end{aligned}$$

Next, we estimate σ_1 in a similar way. Let us consider only the first term in σ_1; the second one can be bounded in the same manner. By the Cauchy–Schwarz inequality,

$$\begin{aligned} N^{-1} \Big| \sum_{j=1}^k \sum_\xi |\widehat{A}(\xi)|^2 \overline{\widehat{B}_j(\xi)} \widehat{\varepsilon}_j(\xi) \Big| &\leqslant \sum_{j=1}^k \mathsf{E}^{1/2}(A, B_j) \mathsf{E}^{1/2}(A, \varepsilon_j) \\ &\leqslant \Big(\sum_{j=1}^k \mathsf{E}(A, B_j) \Big)^{1/2} \cdot \Big(\sum_{j=1}^k \mathsf{E}(A, \varepsilon_j) \Big)^{1/2} \\ &\leqslant k^{1/2} \mathsf{E}^{1/2}(A, B) \sigma_2^{1/2} \leqslant 2^{-2} \mathsf{E}(A, B). \end{aligned}$$

So, by (5.4), we obtain $\mathsf{E}(A, B_k) \geqslant 2^{-2} K^{-1} |A||B|^2$. This completes the proof. □

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

THEOREM 5.2. *Let A be a finite subset of an abelian group. Suppose that* $\mathsf{E}(A) = |A|^3/K$; *then there exists a set $B \subseteq A$ such that $|B| \gg |A|/K^{25/8}$ and* $\dim(B) \ll K^{7/8} \log |A|$.

PROOF. Let $\mathsf{E}_4(A) = M|A|^5/K^3$ and $P := \{x : (A \circ A)(x) \geqslant |A|/2K\}$. By Theorem 3.6, $|P| \gg K|A|/M$ and $\mathsf{E}(P) \gg |P|^3/M^{7/2}$. By Theorem 1.2, there exists $P' \subseteq P$ of size $\gg |P|/M^{7/6}$ such that $\dim(P') \ll M^{7/2} \log |P|$. We have

$$\sum_{x\in A}(P' \circ A)(x) \geqslant \frac{|A|}{2K}|P'| \gg \frac{|A|}{K}\frac{|P|}{M^{7/6}} \gg \frac{|A|^2}{M^{13/6}}.$$

Therefore, $(P' \circ A)(x) \gg |A|/M^{13/6}$ for some x. Putting $B = A \cap (P' + x)$,

$$|B| \gg |A|/M^{13/6} \tag{5.5}$$

and

$$\dim(B) \ll M^{7/2} \log(K|A|) \ll M^{7/2} \log |A|. \tag{5.6}$$

On the other hand, by Lemma 3.5,

$$\begin{aligned}
\kappa_4|A|^5 = \frac{M|A|^5}{K^3} &= \mathsf{E}_4(A) = \sum_{\|s\|=2} \mathsf{E}(A, A_s) \leqslant 2 \sum_{|A_s|\geqslant(1/2)\kappa_4|A|} \mathsf{E}(A, A_s)\\
&\leqslant 2 \max_{|A_s|\geqslant(1/2)\kappa_4|A|} \frac{\mathsf{E}(A, A_s)}{|A_s|^2} \cdot \sum |A_s|^2 \leqslant \max_{|A_s|\geqslant(1/2)\kappa_4|A|} \frac{\mathsf{E}(A, A_s)}{|A_s|^2} \cdot \mathsf{E}_3(A)
\end{aligned}$$

and similarly

$$\kappa_3|A|^4 = \mathsf{E}_3(A) = \sum_{\|t\|=1} \mathsf{E}(A, A_t) \leqslant 2 \max_{|A_t|\geqslant(1/2)\kappa_3|A|} \frac{\mathsf{E}(A, A_t)}{|A_t|^2} \cdot \mathsf{E}(A),$$

so there exist $|A_s| \geqslant \frac{1}{2}\kappa_4|A|$ and $|A_t| \geqslant \frac{1}{2}\kappa_3|A|$ such that $\mathsf{E}(A, A_s) \gg \kappa_4\kappa_3^{-1}|A||A_s|^2$ and $\mathsf{E}(A, A_t) \gg \kappa_3 K|A||A_t|^2$. But $\kappa_4\kappa_3^{-1}\kappa_3 K = M/K^2$, so either $\kappa_4\kappa_3^{-1} \geqslant M^{1/2}/K$ or $\kappa_3 K \geqslant M^{1/2}/K$. Hence, by Theorem 1.2, there is a set $B \subseteq A$ such that

$$\frac{|B|}{|A|} \gg \min\{\kappa_4(\kappa_4\kappa_3^{-1})^{1/2}, \kappa_3(\kappa_3 K)^{1/2}\} \geqslant \min\{M^{3/2}K^{-7/2}, M^{3/2}K^{-5/2}\} = M^{3/2}K^{-7/2} \tag{5.7}$$

and

$$\dim(B) \ll \frac{K}{M^{1/2}} \log |A|. \tag{5.8}$$

Combining (5.6), (5.8) and (5.5), (5.7), we obtain the required result. □

Clearly, using Theorem 5.1 instead of Theorem 1.2 in the proof, one can estimate the dimension of the set B in terms of the size of B.

To prove the next result, we need a generalization of Theorem 1.2 for the energies $\mathsf{T}_k(A)$.

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

Proposition 5.3. *Let $A \subseteq \mathbf{G}$ be a finite set, $k \geqslant 2$ be a positive integer and suppose that $\mathsf{T}_k(A) = c|A|^{2k-1}$. Then there is a set $A_* \subseteq A$ such that*

$$\mathsf{T}_k(A, \ldots, A, A_*, A_*) \geqslant 2^{-5}\mathsf{T}_k(A) \tag{5.9}$$

and

$$\dim(A_*) \ll \frac{\mathsf{T}_{k-1}(A)|A|^2}{\mathsf{T}_k(A)} \log(c^{-1}|A|) \leqslant c^{-1/(k-1)} \log(c^{-1}|A|). \tag{5.10}$$

In particular, $|A_*| \gg c^{1/(2k-1)}|A|$.

Proof. For any $l \leqslant k$, let $\mathsf{T}_l(A) = c_l|A|^{2l-1}$ and hence $c_k = c$. By Fourier transform,

$$\mathsf{T}_k(A) = \frac{1}{N}\sum_{\xi} |\widehat{A}(\xi)|^{2k}.$$

We apply Lemma 3.2 to the set A with parameters $p = 2 + \log(c^{-1}|A|)$ and $l = \eta^{-1}c^{-1}c_{k-1}\log(c^{-1}|A|)$, where $\eta > 0$ is an appropriate constant to be specified later. Write $\varepsilon(x) = A(x) - A_*(x)$, where $A_* = A^{\mathrm{str}}$; in other words, $A \setminus A_*$ is a disjoint union of all dissociated subsets each of size l. We have

$$\begin{aligned}
N \cdot \mathsf{T}_k(A) &= \sum_{\xi} |\widehat{A}(\xi)|^{2k-2}|\widehat{A}(\xi)|^2 \\
&= \sum_{\xi} |\widehat{A}(\xi)|^{2k-2}|\widehat{A}_*(\xi)|^2 \\
&\quad + \Big(\sum_{\xi} |\widehat{A}(\xi)|^{2k-2}\overline{\widehat{A}_*(\xi)}\widehat{\varepsilon}(\xi) + \sum_{\xi} |\widehat{A}(\xi)|^{2k-2}\widehat{A}_*(\xi)\overline{\widehat{\varepsilon}(\xi)}\Big) \\
&\quad + \sum_{\xi} |\widehat{A}(\xi)|^{2k-2}|\widehat{\varepsilon}(\xi)|^2 \\
&= \sigma_0 + \sigma_1 + \sigma_2.
\end{aligned}$$

By the Hölder inequality, the Parseval identity and our choice of parameters,

$$\begin{aligned}
\sigma_2 &\leqslant \Big(\sum_{\xi} |\widehat{\varepsilon}(\xi)|^{2p}\Big)^{1/p} \cdot \Big(\sum_{\xi} |\widehat{A}(\xi)|^{(2k-2)p/(p-1)}\Big)^{1-1/p} \\
&\ll \frac{p}{l}|A|^2 \cdot \mathsf{T}_{k-1}(A)\Big(\frac{|A|^{2k-2}}{\mathsf{T}_{k-1}(A)}\Big)^{1/p} N \\
&\leqslant 2^{-1}c_k|A|^{2k-1}N.
\end{aligned} \tag{5.11}$$

To obtain the last inequality, we have used a simple bound $\mathsf{T}_{k-1}(A) \geqslant c|A|^{2k-3}$. Hence, either σ_0 or σ_1 is at least $2^{-2}c_k|A|^{2k-1}N$. In the first case we are done. In the second case an application of the Cauchy–Schwarz inequality yields

$$2^{-6}N^2\mathsf{T}_k^2(A) \leqslant N \cdot \mathsf{T}_k(A, \ldots, A, A_*, A_*) \cdot \sigma_2.$$

Combining the inequality above with (5.11),

$$\mathsf{T}_k(A, \ldots, A, A_*, A_*) \geqslant 2^{-5}\mathsf{T}_k(A).$$

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

Using the last estimate and the Hölder inequality, we see that $|A_*| \gg c^{1/(2k-1)}|A|$. Furthermore, we have $\dim(A_*) \leqslant l = \eta^{-1}c^{-1}c_{k-1}\log(c^{-1}|A|)$, which proves the first inequality in (5.9). Applying the Hölder inequality again, we see that $c_{k-1} \leqslant c^{(k-2)/(k-1)}$, which gives the second inequality in (5.9). This completes the proof of Proposition 5.3. □

REMARK 5.4. One can also obtain an asymmetric version of the result above as well as a variant of Theorem 5.1 for the energies T_k.

Let us also remark that the bound on the size of A_* in Proposition 5.3 is sharp up to a constant factor (see example at the end of Section 2 in [27]). Indeed, let $\mathbf{G} = \mathbb{F}_2^n$ and $A = H \cup \Lambda$, where H is a subspace, $|H| \sim c^{1/(2k-1)}|A|$, Λ is a dissociated set (basis) and c is an appropriate parameter. Then $\mathsf{T}_k(A) \geqslant \mathsf{T}_k(H) = |H|^{2k-1} \gg c|A|^{2k-1}$, any set $A_* \subseteq A$ satisfying (5.10) has large intersection with H and hence it cannot have size much greater than $c^{1/(2k-1)}|A|$.

If one replaces the condition of Theorem 5.2 on $\mathsf{E}(A)$ by a similar one on $\mathsf{E}_{3/2}(A)$, then the the following result can be proved.

THEOREM 5.5. *Let A be a finite subset of an abelian group and suppose that $\mathsf{E}_{3/2}(A) = |A|^{5/2}/K^{1/2}$. Then there exists a set $B \subseteq A$ such that*

$$|B| \gg |A|/K^2$$

and

$$\dim(B) \ll K^{3/4}\log|A|.$$

PROOF. Write $\mathsf{T}_4(A) = M|A|^7/K^3$, $M \geqslant 1$; then, by Theorem 3.8,

$$\mathsf{E}_4(A) := \kappa_4|A|^5 \gg \frac{|A|^5}{MK}.$$

Furthermore,

$$\sum_{|A_s| \leqslant (1/4)\kappa_4|A|} \mathsf{E}(A_s, A_t) \leqslant \sum_{|A_s| \leqslant (1/4)\kappa_4|A|} |A_s|^2|A_t| \leqslant \frac{1}{4}\mathsf{E}_4(A)$$

and hence by Lemma 3.5

$$\frac{1}{2}\mathsf{E}_4(A) \leqslant \sum_{|A_s|,\,|A_t| \geqslant (1/4)\kappa_4|A|} \mathsf{E}(A_s, A_t) \leqslant \max_{|A_s|,\,|A_t| \geqslant (1/4)\kappa_4|A|} \frac{\mathsf{E}(A_s, A_t)}{|A_s|^{3/2}|A_t|^{3/2}} \cdot \sum_{s,t} |A_s|^{3/2}|A_t|^{3/2}.$$

Therefore, there are $|A_s|, |A_t| \gg \frac{1}{4}\kappa_4|A|$ such that

$$\mathsf{E}(A_s, A_t) \gg |A_s|^{3/2}|A_t|^{3/2} \cdot \frac{\mathsf{E}_4(A)}{\mathsf{E}_{3/2}(A)^2} \geqslant \frac{|A_s|^{3/2}|A_t|^{3/2}}{M}$$

and, by the Cauchy–Schwarz inequality, we see that either $\mathsf{E}(A_s) \gg |A_s|^3/M$, or $\mathsf{E}(A_t) \gg |A_t|^3/M$. Applying Theorem 1.2 in the symmetric case, we find $B \subseteq A$ such that

$$|B| \gg \frac{\kappa_4|A|}{M^{1/3}} \gg \frac{|A|}{M^{4/3}K} \tag{5.12}$$

and

$$\dim(B) \ll M \log|A|. \tag{5.13}$$

On the other hand, using Proposition 5.3, we get a set $B' \subseteq A$ such that $|B'| \gg M^{1/7}K^{-3/7}|A|$ and

$$\dim(B') \ll KM^{-1/3}\log|A|.$$

Combining the last inequalities with (5.12) and (5.13), we obtain the required result. □

Again, using Theorem 5.1 instead of Theorem 1.2 in the proof, one can estimate the dimension of the set B in terms of the size of B.

The last result of this section shows that small $\mathsf{E}_3(A)$ energy implies that a large subset of A has small dimension.

THEOREM 5.6. *Let A be a finite subset of an abelian group. Suppose that $|A-A| \leqslant K|A|$ and $\mathsf{E}_3(A) = M|A|^4/K^2$. Then there exists $A_* \subseteq A$ such that $|A_*| \gg |A|/M^{1/2}$ and*

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

PROOF. By Theorem 3.7, for every $l \geqslant 2$ we have $\mathsf{T}_l(A) \geqslant |A|^{2l-1}/(K(8M)^l)$. Applying Proposition 5.3 with $l \sim \log K$, we obtain the result. □

6. An application

Konyagin posed the following interesting problem. Is it true that there is a constant $c > 0$ such that if $A \subseteq \mathbb{F}_p$ and $|A| \leqslant \sqrt{p}$, then there exists x such that $0 < (A * A)(x) \ll |A|^{1-c}$? The first nontrivial results toward this conjecture were obtained in [11]. It was proved that there exists x such that $0 < (A * A)(x) \ll e^{-O((\log\log|A|)^2)}|A|$ provided that $|A| \leqslant e^{c\log^{1/5} p}$. Our next result improves the above estimate as well as the condition on the size of A.

THEOREM 6.1. *Suppose that $A \subseteq \mathbb{F}_p$ and $|A| \leqslant e^{c\sqrt{\log p}}$. Then there exists x such that*

$$0 < (A * A)(x) \ll e^{-O(\log^{1/4}|A|)}|A|$$

for some absolute constant $c > 0$.

PROOF. Let us write $|A|/K = \min_{x \in A+A}(A * A)(x)$; then clearly $|A + A| \leqslant K|A|$. Let $X \subseteq A$ be a set given by Corollary 4.7 for $k = [\log K]$. Then $|X| \gg e^{-O(\log^4 K)}|A|$ and $\dim(X) \ll \log|A|$. Suppose that Λ satisfies $|\Lambda| = \dim(X)$ and $X \subseteq \operatorname{Span}(\Lambda)$. By the Dirichlet approximation theorem, there exists $r \in \mathbb{F}_p^*$ such that

$$\|rt/p\| \leqslant p^{-1/|\Lambda|}$$

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

for every $t \in \Lambda$ and therefore

$$\|rx/p\| \leqslant |\Lambda| p^{-1/|\Lambda|} \ll (\log |A|) p^{-O(1/\log |A|)} < \frac{1}{K|A|}$$

for every $x \in X$. We can assume that there is a set $X' \subseteq X \subseteq A$ of size at least $|X|/2$ such that for each $x \in X'$ we have $\{rx/p\} < 1/(K|A|)$.

Notice that for every $r \in \mathbb{F}_p^*$ there is a large gap in the set $r \cdot (A + A)$, that is, there exists $s \in A + A$ such that

$$\{rs + 1, \ldots, rs + l\} \cap r \cdot (A + A) = \emptyset,$$

where $l = p - |A + A|/|A + A| \gg p/K|A|$. Since $(A * A)(s) \geqslant |A|/K$, it follows that there are at least $|A|/K$ elements $a \in A$ such that

$$\{ra + 1, \ldots, ra + l\} \cap (r \cdot A) = \emptyset.$$

Denote the set of such a by $Y \subseteq A$. Thus,

$$K|A| \geqslant |A + A| = |r \cdot A + r \cdot A| \geqslant |X' + Y| = |X'||Y| \geqslant e^{-O(\log^4 2K)} |A|^2,$$

so that $K \gg e^{O(\log^{1/4} |A|)}$ and the assertion follows. □

Bukh proved [6] that if $A \subseteq \mathbf{G}$ and $\lambda_i \in \mathbb{Z} \setminus \{0\}$, then

$$|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leqslant K^{O(\sum_i \log(1+|\lambda_i|))} |A|,$$

where $K = |A \pm A|/|A|$. We also prove here an estimate for sums of dilates. It is not directly related with the additive dimension of sets but it is another consequence of Theorem 3.9.

Theorem 6.2. *Let $A \subseteq \mathbf{G}$ be a finite set and $\lambda_i \in \mathbb{Z} \setminus \{0\}$. Suppose that $|A + A| \leqslant K|A|$; then*

$$|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leqslant e^{O(\log^6(2K) \log\log(4K))(k + \log(\sum_i |\lambda_i|))} |A|.$$

Proof. From Sanders' theorem (Theorem 3.9), it follows that there is a $O(\log^6 K)$-dimensional arithmetic progression P of size $|P| \gg |A|/K^{O(\log^5(2K) \log\log(4K))}$ contained in $2A - 2A$. By the well-known Ruzsa covering lemma, there is a set S with $|S| \ll K^{O(\log^5(2K) \log\log(4K))}$ such that

$$A \subseteq S + P - P.$$

Therefore,

$$\begin{aligned}
|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| &\leqslant K^{O(k \log^5(2K) \log\log(4K))} |\lambda_1 \cdot (P - P) + \cdots + \lambda_k \cdot (P - P)| \\
&\leqslant K^{O(k \log^5(2K) \log\log(4K))} \Big| \Big(\sum_{\lambda_i > 0} \lambda_i\Big)(P - P) + \Big(\sum_{\lambda_i < 0} \lambda_i\Big)(P - P) \Big| \\
&\leqslant K^{O(k \log^5(2K) \log\log(4K))} (|\lambda_1| + \cdots + |\lambda_k|)^{\log^6 K} |P - P| \\
&\leqslant e^{O(\log^6(2K) \log\log(4K))(k + \log(\sum_i |\lambda_i|))} |A|,
\end{aligned}$$

which completes the proof. □

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

7. A result of Bateman and Katz

In this section we reformulate some results from [1, 2] in terms of additive dimension. Although in [1, 2] the authors deal with the case $\mathbf{G} = \mathbb{F}_p^n$, where p is a prime number, it is easy to see that their arguments work in more general groups. We will follow their arguments with some modifications.

The main result of the section is Corollary 7.5 below and it was an important step of the Bateman–Katz proof of a new bound for the size of a set in $\mathbb{F}_3^n$ without arithmetic progressions of length three.

Let $A \subseteq \mathbf{G}$ and s be a positive integer. A $2s$-tuple $(x_1, \ldots, x_{2s}) \in A^{2s}$ is called an *additive* $2s$*-tuple* if $x_1 + \cdots + x_s = x_{s+1} + \cdots + x_{2s}$. We say that an additive $2s$-tuple $(x_1, \ldots, x_{2s})$ is *trivial* if at least two variables are equal. Otherwise we say that the $2s$-tuple is *nontrivial*. Let $\mathsf{T}_s^*(A)$ denote the number of nontrivial $2s$-tuples. We will often use the following inequality: $\mathsf{T}_l(A)^{s-1} \leqslant \mathsf{T}_s(A)^{l-1}|A|^{s-l}$, which holds for every $s \geqslant l \geqslant 2$.

LEMMA 7.1. *Let $A \subseteq \mathbf{G}$ and $s \geqslant 4$. Suppose that $\mathsf{T}_s(A) \gg 10^s s^{2s}|A|^s$. Then $\mathsf{T}_s^*(A) \geqslant \frac{1}{2}\mathsf{T}_s(A)$.*

PROOF. We proceed as in the proof of [13, Theorem 5.1]. Let $(A \tilde{*}_s A)(x)$ denote the number of representations $x = x_1 + \cdots + x_s$ in distinct $x_i \in A$. Observe that $\sum_x (A \tilde{*}_s A)(x)^2$ equals $\mathsf{T}_s^*(A)$ plus the number of additive tuples $(x_1, \ldots, x_{2s})$ such that for some $i \leqslant s$ and $j > s$ we have $x_i = x_j$. Hence,

$$\sum_x (A \tilde{*}_s A)(x)^2 - \mathsf{T}_s^*(A) \leqslant s^2|A| \sum_x (A \tilde{*}_{s-1} A)(x)^2 \leqslant s^2|A|\mathsf{T}_{s-1}(A). \tag{7.1}$$

Notice that $(A *_s A)(x) - (A \tilde{*}_s A)(x)$ is the number of representations $x = x_1 + \cdots + x_s$ for which $x_i = x_j$ for some $i < j$. Thus,

$$(A *_s A)(x) - (A \tilde{*}_s A)(x) \leqslant s^2 q(x), \tag{7.2}$$

where $q(x)$ is the number of solutions of $x = 2x_1 + \cdots + x_{s-1}$. By Fourier inversion,

$$\begin{aligned}\sum_x q(x)^2 &= \int |\widehat{A}(2\alpha)|^2 |\widehat{A}(\alpha)|^{2s-4}\, d\alpha \leqslant |A|^2 \mathsf{T}_{s-2}(A) \leqslant |A|^{2+2/(s-1)} \mathsf{T}_s(A)^{(s-3)/(s-1)} \\ &= |A|^{2+2/(s-1)} \mathsf{T}_s(A)^{-2/(s-1)} \mathsf{T}_s(A) \leqslant \frac{1}{100} s^{-4} \mathsf{T}_s(A).\end{aligned} \tag{7.3}$$

Therefore, by the triangle inequality and the inequalities (7.2) and (7.3),

$$\begin{aligned}\sum_x (A \tilde{*}_s A)(x)^2 &\geqslant \mathsf{T}_s(A)^{1/2}\Big(\mathsf{T}_s(A)^{1/2} - 2s^2\Big(\sum_x q(x)^2\Big)^{1/2}\Big) \\ &\geqslant \mathsf{T}_s(A)^{1/2}\Big(\mathsf{T}_s(A)^{1/2} - \frac{1}{5}\mathsf{T}_s(A)^{1/2}\Big) \\ &\geqslant \frac{4}{5}\mathsf{T}_s(A).\end{aligned} \tag{7.4}$$

Finally, using the assumption that $\mathsf{T}_s(A) \gg 10^s s^{2s}|A|^s$ and the bounds (7.1) and (7.4),

$$\mathsf{T}_s^*(A) \geqslant \tfrac{4}{5}\mathsf{T}_s(A) - s^2|A|\mathsf{T}_{s-1}(A) \geqslant \tfrac{4}{5}\mathsf{T}_s(A) - s^2|A|^{s/(s-1)}\mathsf{T}_s(A)^{(s-2)/(s-1)} \geqslant \tfrac{1}{2}\mathsf{T}_s(A)$$

and the assertion follows. □

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

We will also use the following simple lemmas.

Lemma 7.2. *Let $A \subseteq \mathbf{G}$ be a finite set and let $s > 0$ be an even integer. Suppose that A contains a family of nontrivial s-tuples, involving at least rs elements of A. Then* $\dim(A) \leqslant |A| - r$.

Proof. Let $\mathcal{S}$ denote the given family of s-tuples and let $M \subseteq A$ be the set of all elements of A involved in some s-tuple of $\mathcal{S}$. To prove the lemma, it is sufficient to show that there are s-tuples $S_1, \ldots, S_r \in \mathcal{S}$ and elements $a_j \in S_j$, $j \in [r]$ such that each a_j does not belong to S_i, $i \neq j$. Indeed, it is easy to see that $A \subseteq \operatorname{Span}(A \setminus \{a_1, \ldots, a_r\})$.

We use induction on $r \geqslant 0$. The result is trivial for $r = 0$. Now assume that $r \geqslant 1$. In view of the assumption $|M| \geqslant rs$, there is an element $a \in M$ belonging to at most $k := s|\mathcal{S}|/|M| \leqslant |\mathcal{S}|/r$ tuples from $\mathcal{S}$. Let $S_1, \ldots, S_k$ be all these tuples and put $\mathcal{S}' = \mathcal{S} \setminus \{S_1, \ldots, S_k\}$. One can suppose that the minimum of such k is attained on the element $a \in M$. Notice that $\mathcal{S}'$ involves at least $rs - s$ elements of A. Indeed, otherwise $|S_1 \cup \cdots \cup S_k| \geqslant s + 1$ and each element of $S_1 \cup \cdots \cup S_k$ belongs to at least k sets from $\mathcal{S}$, so that it belongs to all sets $S_1, \ldots, S_k$. But this implies that $|S_1 \cup \cdots \cup S_k| \leqslant ks/k = s$, which gives a contradiction. By the induction assumption, there are tuples $S'_1, \ldots, S'_r \in \mathcal{S}'$ and elements $a'_j \in S'_j$, $j \leqslant r - 1$ such that each a'_j does not belong to S'_i, $i \neq j$. Hence, the sets $S_1, S'_1, \ldots, S'_r \in \mathcal{S}$ and the elements $a_1, a'_1, \ldots, a'_{r-1}$ possess the required property. □

Lemma 7.3. *Let $M \subseteq \mathbf{G}$ be a finite set and suppose that $M = X \cup D$, where D is a dissociated set. Then there is an absolute constant $C > 0$ such that $\mathsf{T}_s(M) \leqslant C^s s^s |D|^s + 2^{2s}|X|^{2s-1}$.*

Proof. By Rudin's inequality,

$$\begin{aligned}\mathsf{T}_s(M) &= \int |\widehat{M}(\alpha)|^{2s}\, d\alpha \leqslant 2^{2s} \int |\widehat{D}(\alpha)|^{2s}\, d\alpha + 2^{2s} \int |\widehat{X}(\alpha)|^{2s}\, d\alpha \\ &\leqslant C^s s^s |D|^s + 2^{2s}|X|^{2s-1}.\end{aligned}$$ □

Proposition 7.4. *Let $A \subseteq \mathbf{G}$ be a finite set such that $\mathsf{T}_k(A) \geqslant 10^k s^{2k} |A|^k$, where $2 \leqslant k < s = \lfloor \log |A| \rfloor$. Furthermore, let $\sigma \geqslant 1$ and d be such that*

$$\frac{|A|^{1-(s-k)/2s(k-1)} \log^{3/2}|A|}{\mathsf{T}_k(A)^{(s-1)/2s(k-1)}} \ll d \leqslant \frac{|A|^{1/2}}{\sigma^{1/2}}. \tag{7.5}$$

Then there is a set $A' \subseteq A$ such that $\dim(A') \leqslant d$ *and*

$$|A'| \geqslant \sigma d.$$

Proof. Suppose that for all sets $A' \subseteq A$ such that $\dim A' = m \leqslant d$ we have $|A'| < d\sigma$. We choose d elements from A uniformly and at random. We show that

$$\mathbb{P}(\dim(\{x_1, \ldots, x_d\}) \leqslant d - l) = O(l)^{-l}. \tag{7.6}$$

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

Indeed, suppose that we have chosen $x_1, \ldots, x_m$ for some $m \leqslant d$. Put

$$A' := \mathrm{Span}\,(W) \cap A,$$

where W is a maximal dissociated subset of $\{x_1, \ldots, x_m\}$. Clearly, $|W| \leqslant m$ and hence $\dim(A') \leqslant m$. By our assumption, $d \leqslant |A|^{1/2}/\sigma^{1/2}$ and therefore the probability that x_{m+1} belongs to A' is at most $|A'|/|A| \lll d\sigma/|A| \leqslant 1/d$. Observe that if $\dim(\{x_1, \ldots, x_d\}) \leqslant d - l$, then there are at least l elements x_{i+1} such that $x_{i+1} \in \mathrm{Span}\,(W_i) \cap A$, where W_i is a maximal dissociated subset of $\{x_1, \ldots, x_i\}$. Thus, the required probability is bounded from above by

$$\sum_{j=l}^{d} \binom{d}{j} \frac{1}{d^j} \leqslant \sum_{j=l}^{\infty} \Big(\frac{ed}{j}\Big)^j \frac{1}{d^j} = O(l)^{-l}$$

and (7.6) is proved.

Next, suppose that the tuple $(x_1, \ldots, x_d) \in A^d$ has dimension $d - l$. Let M be the set that consists of all elements of $\{x_1, \ldots, x_d\}$ which are involved in some nontrivial $2s$-tuple. Then, by Lemma 7.2, $|M| \leqslant 2sl$. Since M contains an $(|M| - l)$-element dissociated subset, it follows by Lemma 7.3 that $\mathsf{T}^*_s(M) \leqslant \mathsf{T}_s(M) \leqslant C^s s^s (2sl)^s + 2^{2s} l^{2s-1}$. Therefore, the expected number of nontrivial $2s$-tuples in $(x_1, \ldots, x_d)$ is bounded from above by

$$C_1^s \sum_{l=0}^{d} (s^{2s} l^s + l^{2s-1}) O(l)^{-l} \leqslant C_2^s s^{3s}, \tag{7.7}$$

where $C_1, C_2 > 0$ are absolute constants.

On the other hand, the expected number of nontrivial $2s$-tuples in $(x_1, \ldots, x_d)$ equals $\mathsf{T}^*_s(A)(d/|A|)^{2s}$ and, by Lemma 7.1,

$$\mathsf{T}^*_s(A)\Big(\frac{d}{|A|}\Big)^{2s} \geqslant \frac{1}{2}\mathsf{T}_s(A)\Big(\frac{d}{|A|}\Big)^{2s} \geqslant \frac{\mathsf{T}_k(A)^{(s-1)/(k-1)}}{2|A|^{(s-k)/(k-1)}}\Big(\frac{d}{|A|}\Big)^{2s}.$$

Comparing the last estimate with (7.7) (recalling that $s = \lfloor \log |A| \rfloor$), we obtain a contradiction. This completes the proof. □

Finally, let us formulate the Bateman–Katz theorem for a general abelian group $\mathbf{G}$.

Corollary 7.5. *Let $A \subseteq \mathbf{G}$ be a finite set and let k be a fixed integer, $2 \leqslant k < \lfloor \log |A| \rfloor$. Suppose that $\mathsf{T}_k(A) = c|A|^{2k-1} \geqslant 10^k |A|^k \log^{2k} |A|$. Then there is a set $A' \subseteq A$ such that*

$$|A'| \gg \frac{c^{1/2(k-1)}|A|}{\log^{3/2} |A|}$$

and

$$\dim(A') \ll_k c^{-1/2(k-1)} \cdot \log^{3/2} |A|.$$

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

Proof. As in Proposition 7.4, put $s = \lfloor \log |A| \rfloor$. In view of $k < s$, we have $\mathsf{T}_s(A) \gg 10^s s^{2s} |A|^s$ and $\mathsf{T}_s(A) \geqslant c^{(s-1)/(k-1)} |A|^{2s-1}$. We apply Proposition 7.4 with

$$d \sim |A| \mathsf{T}_s^{-1/2s}(A) \log^{3/2} |A| \ll c^{-1/2(k-1)} \log^{3/2} |A| \quad \text{and} \quad \sigma \sim |A| d^{-2}.$$

Then the conditions (7.5) are satisfied. Thus, there exists a set $A' \subseteq A$ of dimension at most d such that

$$|A'| \geqslant \sigma d \gg |A| c^{1/2(k-1)} \log^{-3/2} |A|.$$

This completes the proof. □

8. Further remarks

We finish the paper with some remarks on other possible variants of additive dimension, which we considered here. Recall that

$$d(A) = \min\{|S| : S \subseteq A,\ A \subseteq \operatorname{Span} S\}, \quad d_*(A) = \min\{|S| : A \subseteq \operatorname{Span} S\}$$

and

$$\tilde{d}(A) = \min\{|\Lambda| : \Lambda \subseteq A, \Lambda \text{ is a maximal (by inclusion) dissociated subset of } A\}.$$

Example 8.1. Let $x \neq y$ be integers and let $A_1 = \{x, y, x+y, 2x+y\}$, $A_2 = \{y, x+y, 2x+y\}$. Clearly, $A_2 \subsetneq A_1$ and $\dim(A_1) = 3$, $d(A) = d_*(A_1) = 2$, $\dim(A_2) = d(A_2) = 3$ and $d_*(A_2) = 2$. Thus, every kind of dimension can differ from another one. Note also that $d(A_2) > d(A_1)$ and $\tilde{d}(A_2) > \tilde{d}(A_1)$, but $A_2 \subsetneq A_1$.

Observe that

$$d_*(A) \leqslant d(A) \leqslant \tilde{d}(A) \leqslant \dim(A).$$

On the other hand,

$$\dim(A) \ll d_*(A) \log d_*(A) \leqslant d(A) \log d(A)$$

(see [10]). Indeed, let $\Lambda \subseteq A$ be a maximal dissociated subset of A, $|\Lambda| = \dim(A)$ and let $|S| = d_*(A)$. There are $2^{|\Lambda|}$ different subset sums of Λ and any element of A and hence any element of Λ belongs to $\operatorname{Span} S$, so that

$$2^{|\Lambda|} \leqslant (2|\Lambda| + 1)^{|S|}$$

and the result follows.

Each of the dimensions has useful properties: $\dim(A)$, $d_*(A)$ are monotone (but $d(A)$ is not, as Example 8.1 shows); furthermore, all dimensions are subadditive:

$$\dim(C_1 \cup \cdots \cup C_n) \leqslant \sum_{j=1}^{n} \dim(C_j)$$

and the same holds for $d_*(A)$, $d(A)$ and the dimension $d(A)$ is 'subadditive' in the following sense:

$$d(C_1 + \cdots + C_n) \leqslant \sum_{j=1}^{n} d(C_j)$$

for any disjoint sets C_j.

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press

Acknowledgement

I. D. S. is grateful to S. Konyagin for very fruitful discussions. Both authors are grateful to the referee for plenty of useful comments which allowed us to improve several results of the paper.

References

[1] M. Bateman and N. Katz, 'Structure in additively nonsmoothing sets', Preprint, 2011, arXiv:1104.2862v1.
[2] M. Bateman and N. Katz, 'New bounds on cap sets', *J. Amer. Math. Soc.* **25**(2) (2012), 585–613.
[3] J. Bourgain, 'On arithmetic progressions in sums of sets of integers', in: *A Tribute of Paul Erdös* (Cambridge University Press, Cambridge, 1990), 105–109.
[4] J. Bourgain, 'On triples in arithmetic progression', *Geom. Funct. Anal.* **9** (1999), 968–984.
[5] J. Bourgain, 'Roth's theorem on progressions revisited', *J. Anal. Math.* **104** (2008), 155–206.
[6] B. Bukh, 'Sums of dilates', *Combin. Probab. Comput.* **17**(5) (2008), 627–639.
[7] P. Candela and H. A. Helfgott, 'On the dimension of additive sets', *Acta Arith.* **167**(1) (2015), 91–100.
[8] M.-C. Chang, 'A polynomial bound in Freiman's theorem', *Duke Math. J.* **113**(3) (2002), 399–419.
[9] B. Green and T. Tao, 'An equivalence between inverse sumset theorems and inverse conjectures for the U^3-norms', *Math. Proc. Cambridge Philos. Soc.* **149**(1) (2010), 1–19.
[10] V. F. Lev and R. Yuster, 'On the size of dissociated bases', *Electron. J. Combin.* **18**(1) (2011), #P117.
[11] T. Łuczak and T. Schoen, 'On a problem of Konyagin', *Acta Arith.* **134**(2) (2008), 101–109.
[12] W. Rudin, *Fourier Analysis on Groups* (John Wiley & Sons Inc., New York, 1990), (reprint of the 1962 original).
[13] I. Z. Ruzsa, 'Solving linear equations in sets of integers. I', *Acta Arith.* **65** (1993), 259–282.
[14] I. Z. Ruzsa, 'Cardinality questions about sumsets', in: *Additive Combinatorics*, CRM Proceedings & Lecture Notes, 43 (American Mathematical Society, Providence, RI, 2007), 195–205.
[15] I. Z. Ruzsa, 'Sumsets and structure', in: *Combinatorial Number Theory and Additive Group Theory* (Birkhäuser, Basel, 2009), 87–210.
[16] T. Sanders, 'On a theorem of Shkredov', *Online J. Anal. Combin.* (5) (2010), Art. 5, 4 pp.
[17] T. Sanders, 'On Roth's theorem on progressions', *Ann. of Math.* (2) **174** (2011), 619–636.
[18] T. Sanders, 'On the Bogolubov–Ruzsa lemma', *Anal. PDE* **5** (2012), 627–655.
[19] T. Sanders, 'On certain other sets of integers', *J. Anal. Math.* **116** (2012), 53–82.
[20] T. Sanders, 'Structure in sets with logarithmic doubling', *Canad. Math. Bull.* **56**(2) (2013), 412–423.
[21] T. Sanders, 'The structure theory of set addition revisited', *Bull. Amer. Math. Soc. (N.S.)* **50**(1) (2013), 93–127.
[22] T. Schoen, 'Near optimal bounds in Freiman's theorem', *Duke Math. J.* **158** (2011), 1–12.
[23] T. Schoen and I. D. Shkredov, 'Higher moments of convolutions', *J. Number Theory* **133** (2013), 1693–1737.
[24] I. D. Shkredov, 'On sets with small doubling', *Mat. Zametki* **84**(6) (2008), 927–947.
[25] I. D. Shkredov, 'Some new results on higher energies', *Trans. Moscow Math. Soc.* **74**(1) (2013), 35–73.
[26] I. D. Shkredov and I. V. V'ugin, 'On additive shifts of multiplicative subgroups', *Mat. Sb.* **203**(6) (2012), 81–100.
[27] I. D. Shkredov and S. Yekhanin, 'Sets with large additive energy and symmetric sets', *J. Combin. Theory Ser. A* **118** (2011), 1086–1093.
[28] T. Tao and V. Vu, *Additive Combinatorics* (Cambridge University Press, Cambridge, 2006).

TOMASZ SCHOEN, Faculty of Mathematics and Computer Science,
Adam Mickiewicz University, Umultowska 87, 61-614 Poznań, Poland
e-mail: schoen@amu.edu.pl

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

https://doi.org/10.1017/S1446788715000324 Published online by Cambridge University Press