Journal of Number Theory 217 (2020) 278–291

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Small doubling in prime-order groups: From 2.4 to 2.6

Vsevolod F. Lev [a,*], Ilya D. Shkredov [b,1]

[a] *Department of mathematics, the University of Haifa at Oranim, Tivon 36006, Israel*
[b] *Steklov Mathematical Institute, ul. Gubkina, 8, Moscow, 119991, Russia*

ARTICLE INFO

Article history:
Received 24 December 2019
Received in revised form 6 May 2020
Accepted 9 May 2020
Available online 25 June 2020
Communicated by L. Smajlovic

Keywords:
Sumset
Additive combinatorics
Small doubling

ABSTRACT

Improving upon the results of Freiman and Candela-Serra-Spiegel, we show that for a non-empty subset $A \subseteq \mathbb{F}_p$ with p prime and $|A| < 0.0045p$, (i) if $|A + A| < 2.59|A| - 3$ and $|A| > 100$, then A is contained in an arithmetic progression of size $|A+A|-|A|+1$, and (ii) if $|A-A| < 2.6|A|-3$, then A is contained in an arithmetic progression of size $|A-A|-|A|+1$. The improvement comes from using the properties of higher energies.

1. Introduction. Summary of results

The *sumset* and the *difference set* of the subsets A and B of an additively written group are defined by

$$A + B = \{a + b \colon a \in A,\, b \in B\}$$

* Corresponding author.
E-mail addresses: seva@math.haifa.ac.il (V.F. Lev), ilya.shkredov@gmail.com (I.D. Shkredov).

[1] The second author is supported by the Russian Science Foundation grant 19–11–00001.

https://doi.org/10.1016/j.jnt.2020.05.009

and

$$A - B = \{a - b \colon a \in A,\, b \in B\},$$

respectively. We are mostly concerned with the groups of prime order which are identified with the additive group of the corresponding field and, accordingly, denoted $\mathbb{F}_p$; here p is the order of the group.

The Cauchy-Davenport theorem asserts that if $A, B \subseteq \mathbb{F}_p$ are nonempty, then

$$|A + B| \geq \min\{|A| + |B| - 1, p\}.$$

This basic theorem, proved by Cauchy [C13] and independently rediscovered by Davenport [D35,D47], is arguably the earliest result in the area of additive combinatorics.

The case of equality in the Cauchy-Davenport theorem was investigated by Vosper.

Theorem 1 *(Vosper [V56a,V56b]). Let p be a prime. If $A, B \subseteq \mathbb{F}_p$ satisfy $|A|, |B| \geq 2$ and $|A+B| \leq p-2$, then $|A+B| \geq |A|+|B|$ unless A and B are arithmetic progressions sharing the same common difference.*

A far-reaching extension of Vosper's theorem, due to Freiman, establishes the structure of sets $A \subseteq \mathbb{F}_p$ with the doubling coefficient $|A + A|/|A|$ up to 2.4.

Theorem 2 *(Freiman [F61]). Let p be a prime. If $A \subseteq \mathbb{F}_p$ satisfies $|A+A| < 2.4|A|-3$ and $|A| < p/35$, then A is contained in an arithmetic progression with at most $|A+A|-|A|+1$ terms.*

Theorem 2 is commonly referred to as *Freiman's* 2.4*-theorem.*

While the expression $|A + A| - |A| + 1$ in Theorem 2 is sharp, the assumptions $|A + A| < 2.4|A| - 3$ and $|A| < p/35$ are certainly not and, conjecturally, can be substantially relaxed. Indeed, some improvements along these lines have been obtained. For instance, as it follows from a general result by Green and Ruzsa [GR06], the conclusion of Theorem 2 holds true provided that $|A + A| < 3|A| - 3$ (which is the best possible bound), and that A is very small as compared to p: namely, $|A| < 96^{-108}p$. Two more results to mention are due to Rodseth [R06] (relaxing the density assumption in Theorem 2 to $|A| < p/10.7$), and Candela-Serra-Spiegel [CSS] (replacing the assumptions with $|A + A| < 2.48|A| - 7$ and $|A| < 10^{-10}p$).

We recommend the interested reader to check [CSS] for further discussion and historical comments.

In this paper we make yet another step in the indicated direction, improving the constants further and establishing a similar result for the difference set $A - A$.

Theorem 3. *Let p be a prime, and suppose that $A \subseteq \mathbb{F}_p$ satisfies $|A| < 0.0045p$. If $|A - A| < 2.6|A| - 3$, then A is contained in an arithmetic progression with at most $|A - A| - |A| + 1$ terms.*

Theorem 4. *Let p be a prime, and suppose that $A \subseteq \mathbb{F}_p$ satisfies $100 < |A| < 0.0045p$. If $|A+A| < 2.59|A| - 3$, then A is contained in an arithmetic progression with at most $|A+A| - |A| + 1$ terms.*

Our method allows for further slight improvements, but we tried to keep a reasonable balance to obtain good constants while avoiding excessively technical computations.

The proofs of Theorems 3 and 4 presented in Section 3 follow, from some point on, the familiar path involving Fourier bias and partial rectification. The major novelty is that we use an argument of combinatorial nature, based on the properties of higher energies, to obtain a bias larger than that obtained by the standard reasoning. Our contribution is therefore two-fold, including both an improvement in the constants and a new sort of the argument introduced, of potential use elsewhere.

In the appendix we apply our approach to obtain large Fourier bias for the indicator function of a small-difference set in the general settings of an arbitrary finite abelian group.

2. Notation and the toolbox

In this section we gather the notation and results used in Section 3 to prove Theorems 3 and 4.

We will occasionally identify sets with their indicator functions; thus, for instance, for a subset A of a finite abelian group G, we have $\sum_{x\in G} A(x) = |A|$. The non-normalized Fourier coefficients of A are denoted $\widehat{A}$; that is,

$$\widehat{A}(\chi) = \sum_{a\in A} \chi(a), \quad \chi \in \widehat{G}.$$

Hence, $\widehat{A}(1) = |A|$ (where 1 denotes the principal character), and the Parseval identity reads

$$\sum_{\chi\in\widehat{G}} |\widehat{A}(\chi)|^2 = |A||G|.$$

For a finite subset A and an element x of an abelian group, we let $A_x := A \cap (A+x)$; therefore, $|A_x|$ is the number of representations of x as a difference of two elements of A, and in particular $|A_x| = 0$ if $x \notin A - A$. We have

$$\sum_{x\in A-A} |A_x| = |A|^2$$

and

$$A_x - A \subseteq (A-A)_x.$$

The latter relation, often called the *Katz-Koester observation* [KK10], can be proved as follows:

$$A_x - A = (A \cap (A+x)) - A \subseteq (A-A) \cap ((A+x)-A)$$
$$= (A-A) \cap ((A-A)+x) = (A-A)_x.$$

The sum version of the Katz-Koester observation is

$$A_x + A \subseteq (A+A)_x.$$

The *common energy* $\mathsf{E}(A,B)$ of finite subsets A and B of an abelian group G is the number of quadruples $(a_1,a_2,b_1,b_2) \in A^2 \times B^2$ such that $a_1 - a_2 = b_1 - b_2$; equivalently,

$$\mathsf{E}(A,B) = \sum_{x \in G} |A_x||B_x|.$$

Also, if G is finite, then

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

We write $\mathsf{E}(A)$ as a commonly used abbreviation of $\mathsf{E}(A,A)$. For $k > 0$ we set

$$\mathsf{E}_k(A) := \sum_{x \in A-A} |A_x|^k;$$

thus, $\mathsf{E}_2(A) = \mathsf{E}(A)$, and if k is an integer, then

$$\mathsf{E}_k(A) = |\{(a_1,\dots,a_k,b_1,\dots,b_k) \in A^{2k} \colon a_1 - b_1 = \dots = a_k - b_k\}|.$$

For real $u \le v$, by $[u,v]$ we denote the set of all integers $u \le n \le v$, and also the "canonical" image of this set in $\mathbb{F}_p$.

The following theorem follows easily from the results of [F62a].

Theorem 5 *(Freiman [F62a]). Suppose that A is a finite set of integers. If $|A+A| \le 3|A|-4$, then A is contained in an arithmetic progression with at most $|A+A|-|A|+1$ terms. Similarly, if $|A-A| \le 3|A|-4$, then A is contained in an arithmetic progression with at most $|A-A|-|A|+1$ terms.*

We need two more lemmas due to Freiman; the former originates from [F62b], while the latter is implicit in [F61] and in fact in any exposition of the proof of Theorem 2, such as [N96, Section 2.8].

Lemma 1 *(Freiman [F62b]). Suppose that Z is a finite subset of the unit circle on the complex plane. If*

$$\Big|\sum_{z\in Z} z\Big| = \eta|Z|, \quad \eta\in[0,1],$$

then there is an open arc of the circle of the angle measure π containing at least $\frac{1}{2}(1+\eta)|Z|$ elements of Z.

Lemma 2 *(Freiman [F61]). Suppose that p is a prime, and that a subset $A\subseteq\mathbb{F}_p$ satisfies $|A|<p/12$ and $|A+A|<K|A|-3$ with a real K. If there is an arithmetic progression in $\mathbb{F}_p$ with $(p+1)/2$ terms, containing at least $\frac{1}{3}K|A|$ elements of A, then, indeed, the whole set A is contained in an arithmetic progression with at most $|A+A|-|A|+1$ terms.*

An essentially identical statement holds true for the subsets $A\subseteq\mathbb{F}_p$ with the difference set satisfying $|A-A|<K|A|-3$. For self-completeness, we provide a very brief sketch of the proof, addressing both the sum and the difference versions together.

Proof of Lemma 2. Scaling and translating A appropriately, we assume without loss of generality that, with an appropriate choice of $0\le l\le(p-1)/2$, the set $A':=A\cap[0,l]$ satisfies $|A'|\ge\frac{1}{3}K|A|$. Moreover, we can assume that A' is not contained in an arithmetic progression with l or fewer terms.

Let A'' be the inverse image of A' in $[0,l]$ under the canonical homomorphism; thus, $|A''|=|A'|$.

The set A' of residues modulo p and the set of integers A'' behave identically under addition. As a result,

$$|A''\pm A''|=|A'\pm A'|\le|A\pm A|<K|A|-3\le 3|A''|-3,$$

and by Theorem 5, the set A'' is contained in an arithmetic progression with at most $|A''\pm A''|-|A''|+1$ terms. Hence, so is the set A', and it follows that

$$l\le|A''\pm A''|-|A''|\le|A\pm A|-\frac{1}{3}K|A|<\frac{2}{3}K|A|-3<p/6$$

(for the last inequality notice that the assumptions of the lemma imply $K\le 3$).

Therefore, $A'\subseteq[0,l]$ with $l<p/6$, and it follows that $A'+A'-A'\subseteq[-l,2l]$, showing that for any element $x\in[2l+1,p-l-1]\subseteq\mathbb{F}_p$, the sets $x+A'$ and $A'+A'$ are disjoint. If we had $x\in A$, then, in view of the Cauchy-Davenport theorem, we would get

$$|A\pm A|\ge|A'\pm A'|+|x+A'|\ge 3|A'|-1\ge K|A|-1,$$

a contradiction. Thus, $A\subseteq[-l,2l]$, showing that A is contained in an arithmetic progression with at most $(p+1)/2$ terms. Considering now the inverse image of A in the

interval $[-l, 2l]$, we conclude, as above, that this image, and therefore the set A itself, are in fact contained in arithmetic progressions with at most $|A \pm A| - |A| + 1$ terms, as wanted. $\square$

Combining Lemmas 1 and 2 we obtain

Corollary 1. *Let p be a prime, and suppose that $A \subseteq \mathbb{F}_p$ is a set such that $|A| < p/12$ and $|A \pm A| < K|A| - 3$ with a real K. If there exists a nonprincipal character $\chi \in \widehat{\mathbb{F}_p}$ such that $|\widehat{A}(\chi)| \geq \eta|A|$, where $\eta \in [0,1]$ satisfies $\frac{1}{2}(1+\eta) \geq \frac{1}{3}K$, then A is contained in an arithmetic progression with at most $|A \pm A| - |A| + 1$ terms.*

Finally, we state and prove a lemma which bounds the number of *Schur triples* contained in a subset of $\mathbb{F}_p$.

Lemma 3. *Let p be a prime. For any set $D \subset \mathbb{F}_p$ with $|D|$ odd and $|D| \leq (2p+1)/3$, we have*

$$\sum_{x,y \in D} D(x-y) \leq \frac{3}{4}|D|^2 + \frac{1}{4}.$$

Proof. Let $n := (|D| - 1)/2$. The sum in the left-hand side counts triples $(x, y, z) \in D^3$ with $x - y - z = 0$. By [L01, Theorem 1], the number of such triples can only increase if D is replaced with the interval $[-n, n] \subseteq \mathbb{F}_p$. Therefore, the sum in question does not exceed

$$\begin{aligned}
&|\{(x,y,z) \in [-n,n]^3 \colon x - y - z = 0\}| \\
&\qquad = |\{(x,y) \in [-n,n]^2 \colon y - x \in [-n,n]\}| \\
&\qquad = \sum_{x \in [-n,n]} |[x-n, x+n] \cap [-n,n]| \\
&\qquad = (2n+1) + 2\sum_{x=1}^{n} |[x-n, n]| \\
&\qquad = (2n+1) + 2\sum_{x=1}^{n} (2n+1-x) \\
&\qquad = \frac{3}{4}(2n+1)^2 + \frac{1}{4};
\end{aligned}$$

here all intervals are subsets of $\mathbb{F}_p$, and the assumption $2n+1 = |D| \leq (2p+1)/3$ ensures that $[x-n, x+n] \cap [-n,n] = [x-n, n]$ whenever $x \in [1, n]$. $\square$

3. Proofs of Theorems 3 and 4

For a subset $A \subseteq \mathbb{F}_p$ with $|A - A| = K|A|$, as an immediate application of the Cauchy-Schwarz inequality we have $\mathsf{E}(A) \geq K^{-1}|A|^3$. We start with a lemma improving this trivial bound; this lemma will be used in the proof of Theorem 3.

Lemma 4. *Let p be a prime, and suppose that $A \subset \mathbb{F}_p$ is a nonempty subaset satisfying $|A - A| = K|A| < p/2$. Then*

$$\mathsf{E}(A) \geq \left(\frac{1}{K} + \frac{1}{3K(K+2)}\left(1 - |A|^{-2}\right)\right)|A|^3.$$

Proof. Write $D := A - A$ and $\lambda := |A|^2/|D|$, and let

$$F(x) := |A_x| - \lambda D(x), \quad x \in \mathbb{F}_p$$

and

$$\sigma_k := \sum_{x \in \mathbb{F}_p} F^k(x),$$

where k is a positive integer. We have

$$\sigma_1 = \sum_{x \in \mathbb{F}_p} F(x) = 0,$$

$$\sigma_2 = \sum_{x \in \mathbb{F}_p} F^2(x) = \mathsf{E}(A) - 2\lambda|A|^2 + \lambda^2|D| = \mathsf{E}(A) - \frac{|A|^4}{|D|}, \tag{1}$$

and

$$\begin{aligned}\sigma_3 &= \sum_{x \in \mathbb{F}_p} F^3(x) \\ &= \mathsf{E}_3(A) - 3\lambda\mathsf{E}(A) + 3\lambda^2|A|^2 - \lambda^3|D| \\ &= \mathsf{E}_3(A) - 3\lambda\left(\mathsf{E}(A) - \frac{|A|^4}{|D|}\right) - \frac{|A|^6}{|D|^2} \\ &= \mathsf{E}_3(A) - 3\frac{|A|^2}{|D|}\sigma_2 - \frac{|A|^6}{|D|^2}. \end{aligned} \tag{2}$$

Also, from $F(x) \leq |A| - \lambda = |A| - |A|^2/|D| = (1 - |A|/|D|)|A|$ we get

$$\sigma_3 \leq \left(1 - \frac{|A|}{|D|}\right)|A|\sigma_2. \tag{3}$$

From (1)–(3),

$$\mathsf{E}_3(A) = \sigma_3 + 3\,\frac{|A|^2}{|D|}\,\sigma_2 + \frac{|A|^6}{|D|^2} \le \Big(1 + 2\,\frac{|A|}{|D|}\Big)|A|\sigma_2 + \frac{|A|^6}{|D|^2}$$
$$= \Big(1 + 2\,\frac{|A|}{|D|}\Big)\Big(\mathsf{E}(A) - \frac{|A|^4}{|D|}\Big)|A| + \frac{|A|^6}{|D|^2}. \quad (4)$$

We now use the basic properties of higher energies from [SS13] to estimate $\mathsf{E}_3(A)$ from below. To this end, we observe that

$$\begin{aligned}\sum_{x,y\in\mathbb{F}_p} |A\cap(A+x)\cap(A+y)| &= \sum_{x,y\in\mathbb{F}_p} |\{a\in A\colon a-x, a-y\in A\}|\\ &= \sum_{a\in A} |\{(x,y)\in\mathbb{F}_p^2\colon a-x, a-y\in A\}|\\ &= \sum_{a\in A} |A|^2\\ &= |A|^3.\end{aligned}$$

In a similar way, considering pairs $(a,b)\in A^2$ with $a-x, a-y, b-x, b-y\in A$, we get

$$\sum_{x,y\in\mathbb{F}_p} |A\cap(A+x)\cap(A+y)|^2 = \mathsf{E}_3(A).$$

Furthermore, the number of non-zero summands in these sums is the number of pairs (x,y) such that there exist $a,b,c\in A$ with $x=a-b$ and $y=a-c$; that is, the number of pairs representable in the form $(a-b, a-c)$, where $a,b,c\in A$. Consequently, using the Cauchy–Schwarz inequality we obtain

$$\begin{aligned}|A|^6 &= \Big(\sum_{x,y\in\mathbb{F}_p} |A\cap(A+x)\cap(A+y)|\Big)^2\\ &\le \sum_{x,y\in\mathbb{F}_p} |A\cap(A+x)\cap(A+y)|^2\cdot|\{(b-a,c-a)\colon a,b,c\in A\}|\\ &\le \mathsf{E}_3(A)\sum_{x,y\in D} D(x-y).\end{aligned}$$

Applying Lemma 3, we conclude that

$$\mathsf{E}_3(A)\cdot\Big(\frac{3}{4}\,|D|^2 + \frac{1}{4}\Big) \ge |A|^6.$$

Since $\mathsf{E}_3(A)\le|A|^4$, this leads to

$$\mathsf{E}_3(A) \ge \frac{4}{3}\frac{|A|^6}{|D|^2} - \frac{1}{3}\frac{|A|^4}{|D|^2}.$$

From this inequality and (4),

$$\frac{4}{3}\frac{|A|^6}{|D|^2} - \frac{1}{3}\frac{|A|^4}{|D|^2} \le \Big(1 + 2\frac{|A|}{|D|}\Big)\Big(\mathsf{E}(A) - \frac{|A|^4}{|D|}\Big)|A| + \frac{|A|^6}{|D|^2},$$

and a short computation gives

$$\begin{aligned}\mathsf{E}(A) &\ge \frac{|A|^4}{|D|} + \frac{1}{3}\frac{|A|^5 - |A|^3}{(|D| + 2|A|)|D|} \\ &= \Big(\frac{1}{K} + \frac{1}{3K(K+2)} - \frac{1}{3K(K+2)|A|^2}\Big)|A|^3. \quad \square\end{aligned}$$

We are now ready to prove Theorems 3 and 4.

Proof of Theorem 3. Using the Cauchy-Davenport and Vosper theorems, it is easy to verify the assertion for $|A| \le 4$; we therefore assume throughout that $|A| \ge 5$. We set $D := A - A$ and $K := |D|/|A|$; thus, $K < 2.6$.

Let η be defined by $\max\{|\widehat{A}(\chi)|\colon \chi \in \widehat{\mathbb{F}_p} \setminus \{1\}\} = \eta|A|$, and let $\alpha := |A|/p$ be the density of A. In view of

$$\mathsf{E}(A) = p^{-1} \sum_{\chi \in \widehat{\mathbb{F}_p}} |\widehat{A}(\chi)|^4 \le \alpha|A|^3 + \eta^2|A|^3, \tag{5}$$

from Lemma 4 we obtain

$$\eta^2 \ge \frac{1}{K} + \frac{1}{3K(K+2)} - \frac{1}{3K(K+2)|A|^2} - \alpha. \tag{6}$$

With some extra effort, we now prove a slightly better bound, in the spirit of [SS13] where a short proof of a Katz-Koester energy result [KK10] is presented.

Consider the sum

$$\sum_{x \in D} |A_x||A - A_x|. \tag{7}$$

The term corresponding to $x = 0$ is $|A||D|$, while for every element $x \in D \setminus \{0\}$ we have $|A - A_x| \ge |A| + |A_x| - 1$ by the Cauchy-Davenport theorem. Therefore

$$\begin{aligned}\sum_{x \in D} |A_x||A - A_x| &\ge |A||D| + \sum_{x \in D \setminus \{0\}} |A_x|(|A| + |A_x| - 1) \\ &= |A||D| + (|A|^2 - |A|)|A| + (\mathsf{E}(A) - |A|^2) - (|D| - 1) \\ &> |A|^3 + \mathsf{E}(A) + (K-2)|A|^2 - K|A|. \end{aligned} \tag{8}$$

Combining this estimate with the estimate of Lemma 4 and the Katz-Koester observation $|A - A_x| \le |D_x|$, we get

$$\begin{aligned}
p^{-1}|A|^2|D|^2 + & p^{-1}\eta^2|A|^2(p-|D|)|D| \\
&\geq p^{-1}\sum_{\chi\in\widehat{\mathbb{F}_p}}|\widehat{A}(\chi)|^2|\widehat{D}(\chi)|^2 \\
&= \sum_{x\in\mathbb{F}_p}|A_x||D_x| \\
&= \sum_{x\in D}|A_x||D_x| \\
&> |A|^3 + \mathsf{E}(A) + (K-2)|A|^2 - K|A| \\
&\geq \left(1+\frac{1}{K}+\frac{1}{3K(K+2)}-\frac{1}{3K(K+2)|A|^2}+\frac{K-2}{|A|}-\frac{K}{|A|^2}\right)|A|^3.
\end{aligned}$$

Asymptotically, in the regime where $|A|$ grows, but $\alpha K^2 = o(1)$, this yields

$$\eta^2 \geq \frac{1}{K}+\frac{1}{K^2}+\frac{1}{3K^2(K+2)}+o(1)$$

(which is worth comparing against (6)).

To obtain an explicit version of this estimate suitable for our present purposes, we let $\eta_0 := \frac{2}{3}\cdot 2.6 - 1$ and notice that if $\eta < \eta_0$, then the last computation gives

$$\alpha K^2 + K(1-\alpha K)\eta_0^2 \geq 1+\frac{1}{K}+\frac{1}{3K(K+2)}-\frac{1}{3K(K+2)|A|^2}+\frac{K-2}{|A|}-\frac{K}{|A|^2};$$

equivalently,

$$(1-\eta_0^2)\alpha K^2 + \left(\eta_0^2-\frac{1}{|A|}\right)K+\frac{2}{|A|} \geq 1+\frac{1}{K}+\frac{1}{3K(K+2)}-\frac{1}{3K(K+2)|A|^2}-\frac{K}{|A|^2}.$$

Since the left-hand side is an increasing function of K, while the right-hand side is decreasing, the inequality remains valid with K substituted by 2.6; making the substitution, dividing through by $(1-\eta_0^2)K^2$, and computing numerically, we obtain

$$\alpha > 0.0045 + \frac{0.1920}{|A|} - \frac{0.8410}{|A|^2} > 0.0045,$$

contrary to the assumptions. Thus, $\eta \geq \eta_0$, and an application of Corollary 1 completes the proof. □

The proof of Theorem 4 is in fact a simplified version of that of Theorem 3, due to the fact that some components of the proof specific for the differences cannot be reproduced for the sums, and are thus omitted. As a result, the argument is somewhat shorter, but the eventual estimate is slightly less precise.

Proof of Theorem 4. As in the proof of Theorem 3, we write $D := A - A$ and $\alpha := |A|/p$, and define η by $\max\{|\widehat{A}(\chi)|\colon \chi \in \widehat{\mathbb{F}_p} \setminus \{1\}\} = \eta|A|$. We also let $S := A + A$ and $K := |S|/|A|$.

Instead of Lemma 4, our starting point is the estimate $\mathsf{E}(A) \ge |A|^4/|S|$ following by interpreting $\mathsf{E}(A)$ as a number of quadruples $(a_1, a_2, a_3, a_4) \in A^4$ with $a_1 + a_2 = a_3 + a_4$ and concluding that $\mathsf{E}(A) = \sum_{s\in S} r^2(s)$, where $r(s)$ is the number of representations of the element $s \in S$ as a sum of two elements of A. Instead of (7), we now consider the sum $\sum_{x\in D} |A_x||A + A_x|$ for which, applying the Cauchy-Davenport theorem, we get

$$\begin{aligned}\sum_{x\in D} |A_x||A + A_x| &\ge \sum_{x\in D} |A_x|(|A| + |A_x| - 1) - |A|(2|A| - 1) + |A||S| \\ &= |A|^3 + \mathsf{E}(A) + |A||S| - 3|A|^2 + |A|,\end{aligned}$$

cf. (8). Using, on the other hand, the estimate $|A + A_x| \le |S_x|$, we obtain

$$\begin{aligned}p^{-1}|A|^2|S|^2 &+ p^{-1}\eta^2|A|^2(p - |S|)|S| \\ &\ge p^{-1} \sum_{\chi\in\widehat{\mathbb{F}_p}} |\widehat{A}(\chi)|^2|\widehat{S}(\chi)|^2 \\ &= \sum_{x\in D} |A_x||S_x| \\ &\ge \sum_{x\in D} |A_x||A + A_x| \\ &\ge |A|^3 + \mathsf{E}(A) + |A||S| - 3|A|^2 + |A| \\ &\ge \left(1 + \frac{1}{K} - \frac{3 - K}{|A|}\right) |A|^3.\end{aligned}$$

As a result,

$$\eta^2 \ge \frac{1}{K(1 - \alpha K)} \left(1 + \frac{1}{K} - \frac{3 - K}{|A|} - \alpha K^2\right).$$

Let $\eta_0 := \frac{2}{3} \cdot 2.59 - 1$. If we had $\eta < \eta_0$, this would imply

$$K(1 - \alpha K)\eta_0^2 > 1 + \frac{1}{K} - \frac{3 - K}{|A|} - \alpha K^2;$$

that is,

$$(1 - \eta_0^2)\alpha K^2 + \left(\eta_0^2 - \frac{1}{|A|}\right)K + \frac{3}{|A|} > 1 + \frac{1}{K}.$$

Since the left-hand side is an increasing function of K, while the right-hand side is decreasing, in view of $K < 2.59$ we would conclude that the last inequality stays true

if K gets substituted by 2.59; substituting, normalizing, and computing numerically, we obtain

$$\alpha + \frac{0.1296}{|A|} > 0.0058,$$

contradicting the assumptions $\alpha < 0.0045$ and $|A| > 100$.

Thus, $\eta \geq \eta_0$, and we invoke Corollary 1 to complete the proof. □

Acknowledgment

We are grateful to the referee for a careful reading of the manuscript and the remarks.

Appendix A. Arbitrary groups

The standard argument shows that for a subset A of an arbitrary finite abelian group G, keeping the notation K for the doubling coefficient $|A+A|/|A|$, and $\eta|A|$ for the largest absolute value of a non-trivial Fourier coefficient of the indicator function of A, one has

$$\eta \geq \frac{1}{\sqrt{K}} \sqrt{\frac{1-\gamma}{1-\alpha}},$$

where $\alpha := |A|/|G|$ and $\gamma := |A+A|/|G|$ are the densities of A and $A+A$, respectively.

The same estimate holds true for the difference set $A-A$. In any case, assuming $\gamma = o(1)$, we get

$$\eta \geq \frac{1+o(1)}{\sqrt{K}}. \tag{9}$$

In the case of difference sets we have the following slight improvement which basically replaces the term $o(1)$ in (9) with a positive constant.

Theorem 6. *Let A be a non-empty subset of a finite abelian group G of density $\alpha = |A|/|G|$. If $|A-A| = K|A|$, then*

$$\eta \geq \left(\frac{1+\sqrt{5}}{2}\right)^{1/2} \frac{1+O(K^3\alpha)}{\sqrt{K+1}},$$

where η is defined by $\max\{|\widehat{A}(\chi)| \colon \chi \in \widehat{G} \setminus \{1\}\} = \eta|A|$.

Proof. From (4) and (5) (which are valid in any finite abelian group, not necessarily of prime order),

$$\mathsf{E}_3(A) \leq \left(1+\frac{2}{K}\right)\left(\eta^2 - \frac{1}{K} + \alpha\right)|A|^4 + \frac{|A|^4}{K^2}. \tag{10}$$

On the other hand, letting $D := A - A$, by Hölder's inequality,

$$|A|^2 = \sum_{x\in D} |A_x| \le |D|^{1/3}\Big(\sum_x |A_x|^{3/2}\Big)^{2/3} = |D|^{1/3}(\mathsf{E}_{3/2}(A))^{2/3};$$

that is,

$$\mathsf{E}_{3/2}(A) \ge K^{-1/2}|A|^{5/2}.$$

Combining this with the estimate

$$|A|^2\,\mathsf{E}_{3/2}^2(A) \le \mathsf{E}_3(A)\mathsf{E}(A,D)$$

established in [S13, Corollary 4.3], and then with (10) and

$$\mathsf{E}(A,D) = p^{-1}\sum_\chi |\widehat{A}(\chi)|^2|\widehat{D}(\chi)|^2 \le \alpha K^2|A|^3 + \eta^2 K(1-\alpha K)|A|^3,$$

we obtain

$$K^{-1}|A|^7 \le \mathsf{E}_3(A)\mathsf{E}(A,D) \le \left(\left(1+\frac{2}{K}\right)\left(\eta^2 - \frac{1}{K} + \alpha\right)|A|^4 + \frac{|A|^4}{K^2}\right) \cdot \big(\alpha K^2|A|^3 + \eta^2 K(1-\alpha K)|A|^3\big).$$

This gives

$$1 \le \big((K+2)(\eta^2 K - 1) + 1\big)\cdot\eta^2 + O(K^3\alpha),$$

and after rearranging the terms,

$$\eta^4 K(K+2) - (K+1)\eta^2 - (1 + O(K^3\alpha)) \ge 0.$$

It follows that

$$\left((K+1)\eta^2 - \frac{1}{2}\right)^2 \ge \frac{5}{4} + O(K^3\alpha) = \frac{5}{4}\,(1 + O(K^3\alpha)),$$

whence

$$(K+1)\eta^2 \ge \frac{1}{2} + \sqrt{\frac{5}{4}\,(1+O(K^3\alpha))} = \frac{1+\sqrt{5}}{2}\,(1+O(K^3\alpha)),$$

resulting in

$$\eta \ge \left(\frac{1+\sqrt{5}}{2}\right)^{1/2}\frac{1}{\sqrt{K+1}}\,(1+O(K^3\alpha)). \quad \square$$

If something is known about subgroups of the group G (as, for instance, in the case where $G = \mathbb{F}_p$), then Fournier–type results [Fou77] can be applied (see [S11, Lemma 7.2] for a modern exposition), allowing one to estimate $\mathsf{E}_3(A)$ from below nontrivially, and hence improving Theorem 6 in this situation.

References

[CSS] P. Candela, O. Serra, C. Spiegel, A step beyond Freiman's theorem for set addition modulo a prime, arXiv preprint, arXiv:1805.12374, 2018.

[C13] A.L. Cauchy, Recherches sur les nombers, J. Éc. Polytech. 9 (1813) 99–123.

[D35] H. Davenport, On the addition of residue classes, J. Lond. Math. Soc. 10 (1935) 30–32.

[D47] H. Davenport, A historical note, J. Lond. Math. Soc. 22 (1947) 100–101.

[Fou77] J.J.F. Fournier, Sharpness in Young's inequality for convolution, Pac. J. Math. 72 (2) (1977) 383–397.

[F61] G.A. Freiman, Inverse problems in additive number theory. Addition of sets of residues modulo a prime, Dokl. Akad. Nauk SSSR 141 (1961) 571–573.

[F62a] G.A. Freiman, Inverse problems in additive number theory, VI. On the addition of finite sets, III, Izv. Vysš. Učebn. Zaved., Mat. 3 (1962) 151–157 (in Russian).

[F62b] G.A. Freiman, Inverse problems of additive number theory, VII. On addition of finite sets, IV, Izv. Vysš. Učebn. Zaved., Mat. 31 (6) (1962) 131–144.

[GR06] B. Green, I.Z. Ruzsa, Sets with small sumset and rectification, Bull. Lond. Math. Soc. 38 (1) (2006) 43–52.

[KK10] N.H. Katz, P. Koester, On additive doubling and energy, SIAM J. Discrete Math. 24 (2010) 1684–1693.

[L01] V. Lev, Linear equations over $\mathbb{F}_p$ and moments of exponential sums, Duke Math. J. 107 (2) (2001) 239–263.

[N96] M. Nathanson, Additive Number Theory. Inverse Problems and the Geometry of Sumsets, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, New York, 1996.

[R06] Ø.J. Rødseth, On Freiman's 2.4-theorem, Skr. - K. Nor. Vidensk. Selsk. 4 (2006) 11–18.

[S11] T. Sanders, A quantitative version of the non–abelian idempotent theorem, Geom. Funct. Anal. 21 (1) (2011) 141–221.

[SS13] T. Schoen, I.D. Shkredov, Higher moments of convolutions, J. Number Theory 133 (5) (2013) 1693–1737.

[S13] I.D. Shkredov, Some new results on higher energies, Trans. Mosc. Math. Soc. 74 (1) (2013) 35–73.

[V56a] A.G. Vosper, The critical pairs of subsets of a group of prime order, J. Lond. Math. Soc. 31 (1956) 200–205.

[V56b] A.G. Vosper, Addendum to "The critical pairs of subsets of a group of prime order", J. Lond. Math. Soc. 31 (1956) 280–282.