ISSN 0001-4346, Mathematical Notes, 2020, Vol. 108, No. 4, pp. 557–565. © Pleiades Publishing, Ltd., 2020.
Russian Text © The Author(s), 2020, published in Matematicheskie Zametki, 2020, Vol. 108, No. 4, pp. 561–571.

On Popular Sums and Differences for Sets with Small Multiplicative Doubling

K. I. Ol'mezov[1]*, A. S. Semchenkov[1], and I. D. Shkredov[1]*****

[1] *Steklov Mathematical Institute of Russian Academy of Sciences, Moscow, 119991 Russia*

Received December 18, 2019; in final form, May 8, 2020; accepted May 15, 2020

Abstract—We improve an estimate for the additive energy of sets A with small product AA. The proof uses some properties of level sets of convolutions of the indicator function of A, namely, their almost invariance under multiplication by elements of A.

DOI: 10.1134/S000143462009028X

Keywords: *arithmetic combinatorics, small multiplicative doubling, additive energy, sumset, sum-product theorem.*

1. INTRODUCTION

For a prime p and the residue field $\mathbb{F}_p$ modulo p, consider a multiplicative subgroup $\Gamma \subseteq \mathbb{F}_p \setminus \{0\}$. The classical question about the structure of Γ with respect to addition was studied in [1]–[4] and many other papers. This question is closely related to the sum-product theorem (see [5], [6]). When studying the structure of Γ, it is often useful to note that the difference set of Γ is Γ-invariant (see, e.g., [1], [7], [8]). Some functions well reflecting the additive structure, such as the convolutions of Γ, and their level sets have the same property. The present paper generalizes these ideas to the field of real numbers. The counterpart of a subgroup is a set A such that $|AA|$ is small compared with $|A|$. In particular, we show that, for any $A \subseteq \mathbb{R}$ with this property, each level set P (on which the convolutions of A take values in a narrow interval) is almost invariant under multiplication by elements of A. (See Sec. 4 for more precise statements.) Earlier results of this kind can be found in [9], [10], and [8]. Using assertions about P, one can obtain new estimates for the additive energy of A. The most recent result in this direction was obtained in [9, Theorem 3] via a development of methods in [11] and [12].

Theorem 1. *Let $A \subset \mathbb{R}$ be a finite set such that $|AA| \le M|A|$. Then*

$$\mathsf{E}^+(A) := |\{(a,b,c,d) \in A^4 : a+b=c+d\}| \lesssim M^{8/5}|A|^{49/20}. \tag{1.1}$$

Combining combinatorial ideas with the operator method, we improve this result for small M. (Only the simplest case of $M \ll 1$ is presented here; see the general statement in Theorem 5.)

Theorem 2. *Let $A \subset \mathbb{R}$ be a finite set such that $|AA| \ll M|A|$. Then*

$$\mathsf{E}^+(A) \lesssim |A|^{22/9}. \tag{1.2}$$

We see that the exponent $22/9$ here is better than the exponent $49/20$ in Theorem 1 for sets with the same condition $|AA| \ll |A|$.

Using the same operator method, we re-prove the following theorem in [10] and [9, Theorems 2, 10] on sum sets and difference sets. (A similar result for multiplicative subgroups in $\mathbb{F}_p^*$ can be found in [13].)

Theorem 3. *Let $A \subset \mathbb{R}$ be a finite set such that $|AA| \ll M|A|$. Then*

$$|A-A| \gtrsim |A|^{5/3} \qquad \text{and} \qquad |A+A| \gtrsim |A|^{8/5}. \tag{1.3}$$

Finally, we discuss other results on sums and products in Sec. 6.

*E-mail: olmezov.ki@gmail.com
**E-mail: aliaksei.semchankau@gmail.com
***E-mail: ilya.shkredov@gmail.com

2. NOTATION AND DEFINITIONS

Let $\mathbf{G}$ be an Abelian group. The characteristic function of a set $S \subseteq \mathbf{G}$ will sometimes be denoted by the same letter:

$$S(g) = \begin{cases} 1, & g \in S, \\ 0, & g \notin S. \end{cases}$$

The cardinality of a set S is denoted by $|S|$. We define the *product* of sets $A, B \subseteq \mathbf{G}$ as

$$AB := \{ab : a \in A,\ b \in B\}.$$

In a similar way, we define the sum $A + B$ and products with a larger number of factors, say, AAA. We will use the Plünnecke–Ruzsa inequality [14]

$$|nA - mA| \le \left(\frac{|A + A|}{|A|}\right)^{n+m} \cdot |A|.$$

Given two functions $f, g\colon \mathbf{G} \to \mathbb{C}$, their *convolutions* are defined by

$$(f * g)(x) := \sum_{y \in \mathbf{G}} f(y)g(x - y) \qquad \text{and} \qquad (f \circ g)(x) := \sum_{y \in \mathbf{G}} f(y)g(y + x). \tag{2.1}$$

Accordingly, the functions $(A * A)$ and $(A \circ A)$ are the *convolutions of a set* A. By $\mathsf{E}^+(A, B)$ we denote the *additive energy* of two sets $A, B \subseteq \mathbf{G}$ (see [14]), which is defined by

$$\mathsf{E}^+(A, B) = |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : a_1 + b_1 = a_2 + b_2\}|.$$

If $A = B$, then we just write $\mathsf{E}^+(A)$ instead of $\mathsf{E}^+(A, A)$. Clearly,

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

For $k \ge 2$, we also define the *higher energies* ([11], [15])

$$\mathsf{E}^+_k(A) = |\{(a_1, \dots, a_k, a'_1, \dots, a'_k) \in A^{2k} : a_1 - a'_1 = a_2 - a'_2 = \dots = a_k - a'_k\}|.$$

Thus, $\mathsf{E}^+(A) = \mathsf{E}^+_2(A)$. For convenience, we set $\mathsf{E}^+_1(A) = |A|^2$. For two sets $A, P \subseteq \mathbf{G}$, let $\sigma_P(A) := \sum_{x \in P}(A \circ A)(x)$. In the same way, we define the *multiplicative energy*

$$\mathsf{E}^\times(A, B) = |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : a_1 b_1 = a_2 b_2\}|$$

of two sets $A, B \subseteq \mathbf{G}$ and, in a similar way, $\mathsf{E}^\times_k(A)$. It is clear that the multiplicative energy $\mathsf{E}^\times(A, B)$ can be expressed via multiplicative convolutions by analogy with (2.1). We shall also use partition functions, such as, for example, $r_{AB}(x)$, $r_{A+B}(x)$, or $r_{AB^{-1}}(x)$, which count the number of ways in which $x \in \mathbf{G}$ can be represented as the product ab, the sum $a + b$, or the quotient ab^{-1}, respectively, where $a \in A$ and $b \in B$. For example,

$$|A| = r_{AA^{-1}}(1), \qquad \mathsf{E}(A, B) = r_{AA^{-1}BB^{-1}}(1) = \sum_x r^2_{A^{-1}B}(x).$$

All logarithms are to the base 2. The symbols $\ll$ and $\gg$ are the usual Vinogradov symbols; i.e., $a \ll b$ means $a = O(b)$ and $a \gg b$ means $b = O(a)$. If K is a parameter, then we write $\ll_K$ and $\gg_K$ to indicate the polynomial dependence on K of the constants hidden in $\ll$ and $\gg$. Given a set A, we write $a \lesssim b$, or $b \gtrsim a$, if $a = O(b \cdot \log^c |A|)$, where $c > 0$ is some absolute constant. For any prime p, the finite prime field of characteristic p is denoted by $\mathbb{F}_p$, and by $\mathbb{F}$ we denote any field, regardless of whether it is finite or not.

3. PRELIMINARY REMARKS

We need a fairly well-known corollary of the Szemerédi–Trotter theorem, which can be found, e.g., in [11, Corollary 28]. It claims that the higher additive energies of a set A that has small multiplicative doubling can be estimated almost optimally.

Lemma 1. *Let $A \subset \mathbb{R}$ be a finite set such that $|AA| \le M|A|$. Then*

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

We shall also use the lemma obtained by the operator method in [12, Theorem 5.1, inequality (5.7)]. (Formulas (3.2) and (3.3) have simple combinatorial proofs as well.)

Lemma 2. *Let $\mathbf{G}$ be an Abelian group, and let $A \subset \mathbf{G}$ be a finite set. Assume that a set $P \subseteq A - A := D$ has the following property: $\Delta < (A \circ A)(x) \le 2\Delta$ for some Δ and for any $x \in P$. Then*

$$\left(\frac{\sigma_P^2(A)\,\mathsf{E}(A)}{|A|^3}\right)^2 \lesssim \mathsf{E}_3(A) \cdot \sum_{x,y} (A \circ A)^2(x-y)P(x)P(y). \tag{3.1}$$

In a similar way, it is true for any $P \subseteq D$ that

$$\left(\frac{\sigma_P^2(A)}{|A|}\right)^2 \le \mathsf{E}_3(A) \cdot \sum_{x,y} D(x-y)P(x)P(y). \tag{3.2}$$

In particular,

$$|A|^6 \le \mathsf{E}_3(A) \cdot \sum_{x,y} D(x-y)D(x)D(y). \tag{3.3}$$

The following lemma is a slight generalization of Exercise 1.1.8 in [14]. For example, it can be obtained by the probabilistic method with the use of the Plünnecke–Ruzsa inequality.

Lemma 3. *Let $A, B \subseteq \mathbf{G}$ be finite sets. Then there exists a set $X \subseteq A + B - B$ with*

$$|X| \ll \frac{|A+B-B|}{|B|} \cdot \log|A+B|$$

such that $A + B \subseteq X + B$. In particular, if $B = A$, then $A + A \subseteq X + A$ and

$$|X| \ll \frac{|A+A|^3}{|A|^3} \cdot \log|A|.$$

Indeed, take a random subset $X \subseteq A + BB$, each of its elements being chosen independently with probability $p = c\log|A+B|/|B|$, where $c > 0$ is a sufficiently small constant. Then the probability that a given $z \in A + B$ does not lie in $X + B$ is $(1-p)^{|B|}$. Hence the probability that $A + B \nsubseteq X + B$ is at most $|A+B|(1-p)^{|B|}$, which can be made strictly less than 1 in view of our choice of the constant c. It remains to note that the expectation of the cardinality of X is

$$p|A+B-B| \ll \frac{|A+B-B|}{|B|} \cdot \log|A+B|.$$

Further, we need the already mentioned Szemerëdi–Trotter theorem itself [16] on incidences between sets of points and lines on the plane. Recall the notation used in that theorem. Let $\mathcal{L}$ be a finite set of lines and $\mathcal{P}$ a finite set of points on the plane. The *number $\mathcal{I}(\mathcal{P},\mathcal{L})$ of incidences* is determined by the formula $\mathcal{I}(\mathcal{P},\mathcal{L}) = |\{(p,l) \in \mathcal{P} \times \mathcal{L} : p \in l\}|$.

Theorem 4. *Let $\mathcal{P}$ be a finite set of points, and let $\mathcal{L}$ be a finite set of lines. Then*

$$\mathcal{I}(\mathcal{P},\mathcal{L}) \ll |\mathcal{P}|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{P}| + |\mathcal{L}|.$$

4. ON THE SUMS AND DIFFERENCES OF SETS WITH SMALL MULTIPLICATIVE DOUBLING

First, let us discuss the following simple question about sets A in an arbitrary field $\mathbb{F}$: is it true that if $|AA| \lesssim |A|$, then $|A(A+A)| \lesssim |A+A|$ and $|A(A-A)| \lesssim |A-A|$? This is undoubtedly the case for a multiplicative subgroup in $\mathbb{F}_p$, but what happens with sets in infinite fields, for example, in $\mathbb{R}$, where a finite set cannot be a subgroup in the strict sense of the word? Below we give a partial answer to this question in terms of popular subsets of $A+A$ and $A-A$. For now, note that the dual conjecture stating that $|A+A| \lesssim |A|$ implies $|AA+A| \lesssim |AA|$ and $|A/A+A| \lesssim |A/A|$ is obviously wrong. (It suffices to consider intervals shifted by sufficiently large numbers.)

For a set A, we write $D = A-A$ and $\Pi = AA$. Take a $\Delta > 0$ and consider a set $P \subseteq D$ such that $r_{A-A}(x) \geq \Delta$ for every $x \in P$. Then the inequality $r_{\Pi-\Pi}(xa) \geq \Delta$ holds for $xa \in PA$, because distinct representations $xa = (a_1 - a_2)a = a_1 a - a_2 a \in \Pi - \Pi$ are generated by distinct representations $x = a_1 - a_2$. Hence

$$\Delta|PA| \leq \sum_{x \in PA} r_{\Pi-\Pi}(x) \leq \sum_x r_{\Pi-\Pi}(x) = |AA|^2 = M^2|A|^2.$$

It follows that

$$|PA| \leq \frac{|AA|^2}{\Delta} = \frac{M^2|A|^2}{\Delta}. \tag{4.1}$$

A similar argument is valid for A/A instead of AA and even for more general products AB.

Now let us obtain a different estimate. Assume that not only $\Delta \leq r_{AA}(x)$, but also $r_{AA}(x) \leq 2\Delta$ for $x \in P$ and also that the inequality

$$\sum_{x \in P} r^k_{A-A}(x) \gtrsim \mathsf{E}^+_k(A)$$

holds for some $k \geq 1$. By analogy with the preceding argument, formula (4.1) can be generalized to

$$|PA|\Delta^k \leq \sum_{x \in PA} r^k_{\Pi-\Pi}(x) \leq \mathsf{E}^+_k(AA).$$

Furthermore, $AA \subset XA$ for some set X with $|X| \lesssim M^3$ by Lemma 6. The following lemma was proved in [15, Sec. 4].

Lemma 4. *Let* $\mathbf{G}$ *be an Abelian group, and let* $A_1, \dots, A_l \subset \mathbf{G}$ *be its arbitrary subsets. Then*

$$\mathsf{E}^{1/2k}_k\Big(\bigcup_{j=1}^l A_j\Big) \leq \sum_{j=1}^l \mathsf{E}^{1/2k}_k(A_j).$$

Using this lemma and the definition of the set P, we obtain

$$|PA|\Delta^k \leq \mathsf{E}^+_k(AA) \leq \Big(\sum_{x \in X} (\mathsf{E}^+_k(xA))^{1/(2k)}\Big)^{2k} = |X|^{2k}\,\mathsf{E}^+_k(A) \lesssim_k M^{6k}\,\mathsf{E}^+_k(A) \tag{4.2}$$

$$\lesssim M^{6k} \sum_{x \in P} r^k_{A-A}(x) \leq 2^k M^{6k}|P|\Delta^k. \tag{4.3}$$

This means that

$$|PA| \lesssim_{2^k} M^{6k}|P|. \tag{4.4}$$

It is of interest to note that it is not possible to swap addition and multiplication in formulas (4.2) and (4.3).

For $k = 1$, it is easily seen that there is a stronger estimate (see (4.1)) for any sets P with $\Delta|P| \gg |A|^2$; namely,

$$|PA| \ll M^2|P|. \tag{4.5}$$

Finally, note that a similar argument is true for AA instead of $A+A$ and for T_k^+, $\mathsf{E}_{k,l}^+$, or other energies having the property of being a norm in the sense of Lemma 4 above (see also [11], [15]). In a similar way, the condition $|A/A| \le M|A|$ can be considered instead of $|AA| \le M|A|$, but the dependence of the estimate (4.4) on M in this case will be slightly worse.

The above reasoning allows us to show that the set P of popular sums or differences of the set A with small multiplicative doubling are so-called Szemerëdi–Trotter sets. For details on such sets, see [17].

Corollary 1. *Let $A \subset \mathbb{R} \setminus \{0\}$ be a finite set with $|AA| \le M|A|$, and let P be defined in the same way as above in this subsection. Then*

$$\mathsf{E}_3^+(P) \lesssim_{2^k} \frac{M^{12k}|P|^4}{|A|} + |P|^3, \tag{4.6}$$

and it is true for any set $B \subset \mathbb{R}$ that

$$\mathsf{E}^+(P,B) \lesssim_{2^k} \frac{M^{6k}|P|^{3/2}|B|^{3/2}}{|A|^{1/2}} + |P||B|. \tag{4.7}$$

Proof. If $P = \{0\}$, then the statement is trivial. We shall only consider the case $\tau \gg 1$. Then it suffices to prove the estimate

$$|\{s : |\{p - b = s : p \in P,\, b \in B\}| \ge \tau\}| \lesssim_{2^k} \frac{M^{12k}|B|^2|P|^2}{|A|\tau^3}, \tag{4.8}$$

because inequalities (4.6) and (4.7) can be obtained from it by straightforward summation. Indeed,

$$\mathsf{E}_3^+(P) \lesssim_{2^k} \sum_{j=0}^{\log|P|} \frac{2^{3j}M^{12k}|P|^4}{|A|2^{3j}} + |P|^3 \lesssim_{2^k} \frac{M^{12k}|P|^4}{|A|} + |P|^3,$$

as desired. Next, we denote the set on the left-hand side in inequality (4.8) by S_τ. Our task is to estimate the cardinality of S_τ. By definition,

$$\tau|S_\tau||A| \le |\{\pi a^{-1} - b = s : \pi \in PA,\, b \in B,\, s \in S_\tau,\, a \in A\}|.$$

The equation on the right-hand side can be interpreted as a condition for the presence of an incidence between a point and a line provided that $\mathcal{P} = A^{-1} \times S_\tau$ and the lines in $\mathcal{L}$ are indexed by pairs $(\alpha, \beta) \in PA \times B$. Therefore, it follows from Theorem 4 that

$$\tau|S_\tau||A| \ll (|A||S_\tau||PA||B|)^{2/3} + |S_\tau||A| + |B||PA|.$$

If the first term is maximal in the sum on the right, then the estimate (4.4) follows directly from inequality (4.8). The second term dominates only for $\tau \ll 1$, and we do not consider this case. Finally, if the third term exceeds the others, then it suffices to note that $\tau \le \min\{|P|, |B|\}$, which gives

$$|S_\tau| \ll \frac{|B||PA|}{\tau|A|} = \frac{|B|^2|PA||P|}{\tau^3|A|},$$

and again use inequality (4.8). □

5. PROOF OF THE MAIN RESULT

Now we are in a position to prove Theorem 2 from the introduction.

Theorem 5. *Let $A \subset \mathbb{R}$ be a finite set such that $|AA| \le M|A|$. Then*

$$\mathsf{E}^+(A) \lesssim M^{7/3}|A|^{22/9}. \tag{5.1}$$

Proof. Since $r_{A-A}(x) \le |A|$, it follows by the Dirichlet principle that $\Delta \ge 1$ and $P \subseteq A-A$ can be chosen to satisfy

$$\sum_{x\in P} r^2_{A-A}(x) \gg \frac{\mathsf{E}^+(A)}{\log|A|}$$

and $\Delta < r_{A-A}(x) \le 2\Delta$ for all $x \in P$. Up to logarithms (in Lemma 1) or even without them,

$$\Delta \ll \frac{M^2|A|^3}{\mathsf{E}^+(A)}; \tag{5.2}$$

see [12], Lemma 3.7 or the proofs of Theorems 5.1 and 5.4. Applying lemma 2 and the definition of the set P, we obtain

$$\begin{aligned}\left(\frac{\Delta^2|P|^2\,\mathsf{E}^+(A)}{|A|^3}\right)^2 &\le \left(\frac{\sigma_P^2(A)\,\mathsf{E}^+(A)}{|A|^3}\right)^2 \lesssim \mathsf{E}_3^+(A)\cdot\sum_{x,y} r^2_{A-A}(x-y)P(x)P(y)\\ &= \mathsf{E}_3^+(A)\cdot\sum_{z} r^2_{A-A}(z)r_{P-P}(z).\end{aligned}$$

By Hölder's inequality,

$$\left(\frac{\Delta^2|P|^2\,\mathsf{E}^+(A)}{|A|^3}\right)^6 \lesssim (\mathsf{E}_3^+(A))^5\,\mathsf{E}_3^+(P).$$

To estimate the higher energies, we apply Lemma 1 and Corollary 1 (for $k=2$) and find that

$$\left(\frac{\Delta^2|P|^2\,\mathsf{E}^+(A)}{|A|^3}\right)^6 \lesssim |A|^{14}M^{34}|P|^4.$$

Thus, using inequality (5.2) and the fact that $\mathsf{E}^+(A) \lesssim \Delta^2|P|$, we readily obtain

$$(\mathsf{E}^+(A))^{14} \lesssim M^{34}|A|^{32}\Delta^4 \ll M^{34}|A|^{32}\left(\frac{M^2|A|^3}{\mathsf{E}^+(A)}\right)^4,$$

whence

$$\mathsf{E}^+(A) \lesssim M^{7/3}|A|^{22/9}. \quad \square$$

Arguing in a similar way, we prove Theorem 3. We set $D = A-A$ and $S = A+A$. Take a $\Delta \ge 1$ and a set $P \subseteq D$ such that $\sigma_P(A) \gtrsim |A|^2$ and $\Delta < r_{AA}(x) \le 2\Delta$ for all $x \in P$. It follows from inequality (3.2) in Lemma 2 that

$$|A|^6 \lesssim \mathsf{E}_3^+(A)\sum_{z\in D} r_{P-P}(z),$$

and therefore, by Hölder's inequality,

$$|A|^{18} \lesssim (\mathsf{E}_3^+(A))^3\,\mathsf{E}_3^+(P)|D|^2.$$

We again apply Lemma 1 and Corollary 1 and arrive at the inequality

$$|A|^{10} \lesssim M^{10}|D|^6, \tag{5.3}$$

as desired. It is of interest to note that our estimate (5.3) coincides with the classical estimate for Elekes' sum-products [18] (if we ignore the logarithms).

Following the proof of [17, Theorem 11, inequality (4.9)], we have

$$|A|^{10} \lesssim |S|^2\,\mathsf{E}_3^+(A)\sum_{z} r^2_{A-A}(z)r_{S'-S'}(z),$$

where $S' \subseteq \{x : r_{A+A}(x) \geq |A|^2/(2|S|)\}$ and $\Delta < r_{A+A}(x) \leq 2\Delta$ for $x \in S'$. Applying Hölder's inequality, we see that

$$|A|^{30} \lesssim |S|^6 (\mathsf{E}_3^+(A))^5\, \mathsf{E}_3^+(S').$$

Applying Lemma 1 and Corollary 1, we obtain

$$|A|^{16} \lesssim M^{14}|S|^{10},$$

which completes the proof of Theorem 3. □

6. GENERAL PROBLEM

For sets $A \subseteq \mathbb{F}$, one can pose the problem of finding good estimates for fractional-rational expressions $R(A)$ in terms of sums and products of the set A. In other words, let $K = |A+A|/|A|$ and $M = |AA|/|A|$. Then we are interested in estimates of the form $|R(A)| \ll_{K,M} |A|$ for $R(A)$. The first results of this kind were obtained in [19]. For $R(A) = nA - mA$ and $R(A) = A^n/A^m$, where n and m are positive integers, the corresponding estimate is called the Plünnecke–Ruzsa inequality, which we have already mentioned in Sec. 2. Moreover, the theory of sum-products (see [19], [14]) implies that the inequality $KM \gg |A|^c$, $c > 0$, holds in many fields $\mathbb{F}$. This obviously gives the estimate $|R(A)| \ll_{K,M} |A|$ (for sufficiently large exponents K and M), and the only question may be to find the optimal dependence on K and M. We can assume that $R(A)$ simultaneously includes summation (or subtraction) and multiplication (or division), which means that the exponents K and M in the precise "optimal" estimate will be at least 1. Thus, we can start studying the problem from the simplest polynomial $R(x,y,z) = x(y+z)$.

Question. Assume that A is a finite subset of $\mathbb{R}$ or a sufficiently small subset of $\mathbb{F}_p$. Also suppose that $K = |A+A|/|A|$, and let $M = |AA|/|A|$. Is it true that

$$|A(A+A)| \ll_M K|A|? \tag{6.1}$$

As we have seen in Sec. 4, the answer to the "dual" question as to whether $|AA+A| \ll_K M|A|$ is obviously negative. Further, if inequality (6.1) holds, then, by the Cauchy–Schwarz inequality,

$$\sum_x r^2_{A(A+A)}(x) \gg_M \frac{|A|^5}{K}. \tag{6.2}$$

However, it can readily be seen that the stronger form (6.2) of the inequality follows from (4.4) and (4.5).

Proposition 1. *Let $A \subseteq \mathbb{F}$ and $\varepsilon \in \{-1,1\}$. Then*

$$\sum_x r^2_{A^\varepsilon(A\pm A)}(x) \gtrsim \frac{|A|^8}{|AA^\varepsilon|^2|A \pm A|}, \tag{6.3}$$

$$\sum_x r^2_{A^\varepsilon(A\pm A)}(x) \gtrsim_{|AA^\varepsilon|/|A|} (\mathsf{E}^+_{3/2}(A))^2. \tag{6.4}$$

Proof. We put $\Delta_* = |A|^2/(2|A \pm A|)$. By the Dirichlet principle, there exists a $\Delta \geq \Delta_*$ and a set $P = \{x : \Delta < r_{A\pm A}(x) \leq 2\Delta\}$ such that

$$\sum_{x\in P} r_{A\pm A}(x) \gtrsim |A|^2.$$

According to the estimate (4.5), $|PA^\varepsilon| \lesssim M^2|P|$, where $M = |AA^\varepsilon|/|A|$. Therefore, using the Cauchy–Schwarz inequality, we obtain

$$\mathsf{E}^\times(P, A^\varepsilon) \geq \frac{|A|^2|P|^2}{|PA^\varepsilon|} \gtrsim \frac{|A|^2|P|}{M^2}.$$

Then we multiply the last estimate by Δ^2 and arrive at

$$\sum_x r^2_{A^\varepsilon(A+A)}(x) \ge \Delta^2\,\mathsf{E}^\times(P,A^\varepsilon) \ge \frac{|A|^2\Delta^2|P|}{M^2} \gtrsim \frac{|A|^4\Delta_*}{M^2} \ge \frac{|A|^6}{2M^2|A\pm A|}, \tag{6.5}$$

as desired. To obtain (6.4), it suffices to apply the estimate (6.5) and inequality (4.4) with $k=3/2$. This completes the proof. □

Remark 1. It is possible to get rid of the logarithms in the estimate (6.3) by using the same proof scheme and resorting to more precise but voluminous calculations. We leave this to the interested reader and give a shorter proof with slightly weaker results.

The estimates (6.3) and (6.4) are sharp provided that A has small product AA. Now let us obtain another lower bound for $\sum_x r^2_{A(A+A)}(x)$, which is, on the contrary, sharp, provided that A has small sum $A+A$.

Proposition 2. *Let $A,B\subseteq\mathbb{F}$ be finite sets. Then*

$$|A/B|\cdot\sum_s r^2_{(A\pm B)/B}(s) \ge \mathsf{E}^+(A,B)^2.$$

Proof. Consider $s\in A\pm B$ and let $n(s)$ denote the number of pairs $(a_i,b_i)\in A\times B$ such that $s=a_i\pm b_i$, $i\in\{1,\dots,n(s)\}$. It is clear that

$$\sum_s n^2(s) = \mathsf{E}^+(A,B).$$

Consider the mapping $\varphi\colon A\pm B\to 2^{A\times B\times B}$ defined as $\varphi(s)=\{(a_i,b_i,b_j): i,j\in\{1,\dots,n(s)\}\}$, for which, obviously, $|\varphi(s)|=n^2(s)$ and if $\varphi(s)=\varphi(s')$, then $s=s'$, $i=i'$, and $j=j'$. Therefore, there are at least $\mathsf{E}^+(A,B)$ distinct triples of the form (a_i,b_i,b_j). Further,

$$\frac{a_i\pm b_i}{b_j} = \frac{s}{b_j} = \frac{a_j\pm b_j}{b_j} = \frac{a_j}{b_j}\pm 1 \in \frac{A}{B}\pm 1,$$

and hence the image of the function $f(x,y,z)=(x\pm y)/z$ on the set of our triples has cardinality at least $|A/B|$. By the Cauchy–Schwarz inequality,

$$\sum_s r^2_{(A\pm B)/B}(s) \ge \sum_{\alpha\in\mathbb{F}} |\{x\in A,\, y,z\in B : f(x,y,z)=\alpha\}|^2 \ge \frac{\mathsf{E}^+(A,B)^2}{|A/B|},$$

which completes the proof. □

Finally, let us make one more remark. As we have already seen in Sec. 4, if

$$P=\{s\in A\pm A : r_{A\pm A}(s)\ge\Delta\},$$

then $\Delta|AP|\le M^2|A|^2$. In other words, the sets of "popular sums" (of those s for which $r_{A\pm A}(s)$ is bounded below by the mean value) have small product with the set A. However, if we take

$$\widetilde{P}=\left\{s\in A\pm A : \exists\, x,y\in A,\, x+y=s,\, r_{A/A}\left(\frac{x}{y}\right)\ge\Delta\right\},$$

i.e., if $\widetilde{P}$ is popular in terms of "division," then a similar estimate holds for $\widetilde{P}$. Indeed, let $\widetilde{\Lambda}=\{\lambda\in A/A : r_{A/A}(\lambda)\ge\Delta\}$. Then $a(b\pm c)=ab(1\pm c/b)$, whence $|A\widetilde{P}|\le|AA(1\pm\widetilde{\Lambda})|$. It is clear, however, that the mapping $\varphi\colon AA(1\pm\widetilde{\Lambda})\to AA/A\times(A\pm A)$ defined as

$$\varphi(x)=(\pi(x)/c(x), b(x)\pm c(x)),$$

where $\pi(x)\in AA$ and $b(x)/c(x)=\lambda(x)\in\widetilde{\Lambda}$ for $x\in AA(1\pm\widetilde{\Lambda})$, is injective (which can be verified by considering the product of elements of the image). By the Plünnecke–Ruzsa inequality,

$$\Delta|A\widetilde{P}|\le\Delta|AA(1+\widetilde{\Lambda})|\le|AA/A||A\pm A|\le\frac{|AA|^3|A\pm A|}{|A|^2}.$$ □

ACKNOWLEDGMENTS

The authors wish to express gratitude to T. Schoen for valuable remarks.

FUNDING

This work was supported by the Russian Science Foundation under grant 19-11-00001.

REFERENCES

1. J. Bourgain, "More on the sum-product phenomenon in prime fields and its applications," Int. J. Number Theory **1** (1), 1–32 (2005).
2. J. Bourgain, "Estimates on exponential sums related to the Diffie–Hellman distributions," Geom. Funct. Anal. **15** (1), 1–34 (2005).
3. S. V. Konyagin, "Estimates for trigonometric sums over subgroups and for Gauss sums," in *IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems*, Pt. III (Moskov. Gos. Univ., Moscow, 2002), pp. 86–114 [in Russian].
4. J. B. Friedlander, J. Hansen, and I. E. Shparlinski, "Character sums with exponential functions," Mathematika **47** (1–2), 75–85 (2000).
5. J. B. Friedlander, J. Hansen, and I. E. Shparlinski, "Stronger sum-product inequalities for small sets," Proc. Amer. Math. Soc. **148** (4), 1467–1479 (2020).
6. G. Shakan, *On Higher Energy Decomposition and the Sum-Product Phenomenon*, `arXiv:1803.04637` (2018).
7. J. Bourgain and M.-Ch. Chang, "On the size of k-fold sum and product sets of integers," J. Amer. Math. Soc. **17** (2), 473–497 (2004).
8. I. D. Shkredov, "Some remarks on the asymmetric sum-product phenomenon," Mosc. J. Comb. Number Theory **8** (1), 15–41 (2019).
9. B. Murphy, M. Rudnev, I. D. Shkredov, and Yu. N. Shteinikov, "On the few products, many sums problem," J. Theor. Nombres Bordeaux **31** (3), 573–603 (2019).
10. I. D. Shkredov, "Some remarks on sets with small quotient set," Sb. Math. **208** (12), 1854–1868 (2017).
11. T. Schoen and I. D. Shkredov, "Higher moments of convolutions," J. Number Theory **133** (5), 1693–1737 (2013).
12. I. D. Shkredov, "Some new results on higher energies," in *Trans. Moscow Math. Soc.* (2013), Vol. 74, pp. 31–63.
13. I. V. Vyugin and I. D. Shkredov, "On additive shifts of multiplicative subgroups," Sb. Math. **203** (6), 844–863 (2012).
14. T. Tao and V. Vu, *Additive Combinatorics*, in *Cambridge Stud. Adv. Math.* (Cambridge Univ. Press, Cambridge, 2006), Vol. 105.
15. I. D. Shkredov, "Some remarks on the Balog–Wooley decomposition theorem and quantities D^+, $D^\times$," Proc. Steklov Inst. Math. **298** (suppl. 1), 74–90 (2017).
16. E. Szemerédi and W. T. Trotter, "Extremal problems in discrete geometry," Combinatorica **3** (3–4), 381–392 (1983).
17. I. D. Shkredov, "On sums of Szemerédi–Trotter sets," Proc. Steklov Inst. Math. **289**, 300–309 (2015).
18. G. Elekes, "On the number of sums and products," Acta Arith. **81** (4), 365–367 (1997).
19. J. Bourgain, N. Katz, and T. Tao, "A sum-product estimate in finite fields, and applications," Geom. Funct. Anal. **14** (1), 27–57 (2004).