Journal Pre-proof

On some applications of GCD sums to Arithmetic Combinatorics

Ilya D. Shkredov

PII: S0022-314X(21)00190-6
DOI: https://doi.org/10.1016/j.jnt.2021.05.011
Reference: YJNTH 6799

To appear in: *Journal of Number Theory*

Received date: 3 November 2020
Revised date: 1 May 2021
Accepted date: 5 May 2021

Please cite this article as: I.D. Shkredov, On some applications of GCD sums to Arithmetic Combinatorics, *J. Number Theory* (2021), doi: https://doi.org/10.1016/j.jnt.2021.05.011.

On some applications of GCD sums to Arithmetic Combinatorics

Ilya D. Shkredov*

Abstract

Using GCD sums, we show that the set of the primes has small common multiplicative energy with an arbitrary exponentially large integer set S. This implies that if S is a set of small multiplicative doubling then the size of any arithmetic progression in S, beginning at zero, is at most $O(\log |S| \cdot \log\log |S|)$. This result can be considered as an integer analogue of Vinogradov's question about the least quadratic non–residue. The proof rests on a certain repulsion property of the function $f(x) = \log x$. Also, we consider the case of general k–convex functions f and obtain a new incidence result for collections of the curves $y = f(x) + c$.

1 Introduction

Having a ring R with two operations $+$ and $\cdot$ one can define the *sumset* of sets $A, B \subseteq R$ as

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

and, similarly, the *product* set

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

The *sum–product phenomenon* (see, e.g., [21]) predicts that additive and multiplicative structure cannot coexist up to some natural algebraic constraints. This can be expressed in many different ways see, e.g., [6] and in our paper we consider just one of them. Let us formulate a particular case of the main result, which is contained in Theorem 12 from section 3.

Theorem 1 *Let $S \subset \mathbb{Z}$ be a finite set, l be an integer number, and let $\mathcal{P}^{(l)}$ be the set of primes in the segment $\{1, \dots, l\}$. Then the condition*

$$\log |S| = o\left(\frac{l}{\log l}\right) \qquad (1)$$

implies

$$|\{(p, p', s, s') \in \mathcal{P}^{(l)} \times \mathcal{P}^{(l)} \times S \times S \ : \ ps = p's'\}| = o(|\mathcal{P}^{(l)}|^2 |S|)\,. \qquad (2)$$

*This work is supported by the Russian Science Foundation under grant 19–11–00001.

In particular, if $|SS| \ll |S|$, then size of any arithmetic progression A with the beginning at zero in S does not exceed
$$|A| \ll \log |S| \cdot \log\log |S| \,. \tag{3}$$

The result above can be considered as an integer analogue of Vinogradov's question about the least quadratic non–residue. Namely, having a number p one can take the subgroup of squares $\mathcal{R} \subseteq \mathbb{Z}/p\mathbb{Z}$ with the product set $\mathcal{R}\mathcal{R}$ equals $\mathcal{R}$ and ask the question about the maximal length of the arithmetic progression with the beginning at zero, belonging to $\mathcal{R}$. The size of this arithmetic progression is usually denoted as n_p and it is known see [14] that under the Generalized Riemann Hypothesis (a weaker unconditional result can be found in [9]) there are infinitely many primes such that
$$n_p \gg \log p \cdot \log\log p \,.$$
On the other hand, the Generalized Riemann Hypothesis implies [2] that $n_p = O(\log^2 p)$ (the best unconditional bound belongs to Burgess [8] who proved $n_p \ll p^{\frac{1}{4\sqrt{e}}+o(1)}$). Thus in the integer case our Theorem 1 gives upper bound (3) of a comparable quality. The author does not know the right answer to the integer variant of this problem (the obvious lower bound is $|A| \gg \log |S|$).

Another result of ours is Theorem 9 from section 3.

Theorem 2 *Let $A, S \subset \mathbb{Z}$ be finite sets and $0 \leqslant \alpha < 1/6$ be any number. Suppose that $|A+A| \leqslant K|A|$ with*
$$K \ll \exp(\log^\alpha |A|) \tag{4}$$
and
$$|S| \leqslant \exp\left(\frac{\log^{2-6\alpha} |A|}{\log\log |A|} \right) \,. \tag{5}$$
Then for an absolute constant $C > 0$ and a certain $a \in A$ one has
$$|(A-a)S| \gg |S| \cdot \exp(C \log^{1-3\alpha} |A|) \,. \tag{6}$$
In particular, $|(A-A)S| \gg |S| \cdot \exp(C \log^{1-3\alpha} |A|)$.

The result above can be considered as the first step towards the main conjecture from [3] where authors do not assume that the additional condition (4) takes place (also, see papers [11], [12] in this direction).

The method of the proofs of Theorems 1, 2 uses so–called GCD sums (see, e.g., [1], [5], [4], [13]), which are connected with a series of questions of the Uniform Distribution, as well as Number Theory in particular, with large values of the zeta function. In our paper we follow the beautiful exposition of random zeta functions approach from [13]. Thus our method extensively uses the arithmetic of the integers. It is interesting to obtain some analogues of Theorems 1, 2 for subsets of $\mathbb{R}$ or $\mathbb{C}$.

If one takes the function $f(x) = \log x$, then Theorem 2 can be considered as a repulsion result concerning the logarithmic function. Namely, estimate (6) says that $|f(A-a)+\log S|$ must be significantly larger than $|S|$ for rather big sets S as in (5). The first results in the direction were obtained in [10] for general k–convex functions (that is having strictly monotone the first k derivatives). Recall [10, Theorem 1.4] (also, see very recent paper [7]).

Theorem 3 *Let A be a finite set of real numbers contained in an interval I and let f be a function which is k–convex on I for some $k \geq 1$. Suppose that $|A| > 10k$. Then if $|A + A - A| \leq K|A|$, then we have*

$$\left|2^k f(A) - (2^k - 1)f(A)\right| \geq \frac{|A|^{k+1}}{(CK)^{2^{k+1}-k-2}(\log|A|)^{2^{k+2}-k-4}}$$

for some absolute constant $C > 0$.

In this direction we obtain a result on common energy of an arbitrary set S and the image of a k–convex function (the required definitions can be found in section 2). Of course general Theorem 4 below gives weaker bounds than Theorem 1 in the particular case $f(x) = \log x$.

Theorem 4 *Let f be a function which is k–convex on a set I for some $k \geq 1$. Suppose that $|I + I - I| \leqslant |I|^{1+\kappa}$. Then for any finite set $S \subset \mathbb{R}$ with $|I| \geqslant |S|^{\varepsilon}$, $\varepsilon \gg 1/k$, $\kappa \leqslant \exp(-1/(c\varepsilon))$ there is $\delta(\varepsilon) > 0$ such that*

$$\mathsf{E}^{+}(f(I), S) \ll |I|^2 |S|^{1-\delta(\varepsilon)}. \tag{7}$$

In particular, $|f(I) + S| \gg |S|^{1+\delta(\varepsilon)}$.

The method of the proofs of Theorems 3 and 4 are combinatorial and do not use such delicate tools as GCD sums. On the other hand, our Theorem 4 takes place for the real numbers and for rather general functions f. Further, using the Plünnecke inequality (see estimate (11) below) one can show that to have growth as in (6) under the assumptions as in (4) Theorem 3 requires the condition

$$|S| \leqslant \exp(O(\log|A| \cdot \log\log|A|)) \tag{8}$$

and our restriction (5) is wider. Theorem 12, as well as Proposition 11 below require much weaker restrictions on $|S|$ but provide a smaller growth.

Finally, recall the main result from [19], which can be considered as a quantitative version of some results from [6].

Theorem 5 *Let p be a prime number, $A, B, C \subseteq \mathbb{F}_p$ be arbitrary sets, and $k \geq 1$ be such that $|A||B|^{1+\frac{(k+1)}{2(k+4)}2^{-k}} \leq p$ and*

$$|B|^{\frac{k}{8}+\frac{1}{2(k+4)}} \geq |A| \cdot C_*^{(k+4)/4} \log^k(|A||B|),$$

where $C_* > 0$ is an absolute constant. Then

$$\max\{|AB|, |A+C|\} \geq 2^{-3}|A| \cdot \min\left\{|C|, |B|^{\frac{1}{2(k+4)}2^{-k}}\right\},$$

and for any $\alpha \neq 0$

$$\max\{|AB|, |(A+\alpha)C|\} \geq 2^{-3}|A| \cdot \min\left\{|C|, |B|^{\frac{1}{2(k+4)}2^{-k}}\right\}.$$

The result above takes the form in $\mathbb{R}$ as well. In this case we do not need any conditions containing the characteristic p. The main difference between Theorems 2, 4 and Theorem 5 is that A is large and B is small in Theorem 5 but the opposite situation takes place in Theorem 4 (here $|A| = |I| = |f(I)|$) and similar in Theorem 2.

The author thanks Christoph Aistleitner and Sergei Konyagin for useful discussions. Also, we are grateful to the reviewer for valuable suggestions and remarks.

2 Definitions and preliminaries

Let $\mathbf{G}$ be an abelian group. Put $\mathsf{E}^+(A,B)$ for the *common additive energy* of two sets $A, B \subseteq \mathbf{G}$ (see, e.g., [21]), that is,

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

If $A = B$, then we simply write $\mathsf{E}^+(A)$ instead of $\mathsf{E}^+(A,A)$ and the quantity $\mathsf{E}^+(A)$ is called the *additive energy* in this case. Sometimes we write $\mathsf{E}^+(f_1,f_2,f_3,f_4)$ for the additive energy of four real functions, namely,

$$\mathsf{E}^+(f_1,f_2,f_3,f_4) = \sum_{x,y,z} f_1(x) f_2(y) f_3(x+z) f_4(y+z) \,.$$

Thus $\mathsf{E}^+(f_1,f_2,f_3,f_4)$ pertains to additive quadruples, weighted by the values of f_1, f_2, f_3, f_4. It can be shown using the Hölder inequality (see, e.g., [21]) that

$$\mathsf{E}^+(f_1,f_2,f_3,f_4) \leqslant (\mathsf{E}^+(f_1)\mathsf{E}^+(f_1)\mathsf{E}^+(f_1)\mathsf{E}^+(f_1))^{1/4} \,. \tag{9}$$

More generally, we deal with a higher energy

$$\mathsf{T}^+_k(A) := |\{(a_1,\dots,a_k,a'_1,\dots,a'_k) \in A^{2k} \ :\ a_1+\dots+a_k = a'_1+\dots+a'_k\}| \tag{10}$$

and similar $\mathsf{T}^+_k(f)$ for a general function f. Sometimes we use representation function notations like $r_{A+B}(x)$ or r_{A+A-B}, which counts the number of ways $x \in \mathbf{G}$ can be expressed as a sum $a+b$ or as a sum $a+a'-b$ with $a, a' \in A$, $b \in B$, respectively. For example, $|A| = r_{A-A}(0)$ and $\mathsf{E}^+(A) = r_{A+A-A-A}(0) = \sum_x r^2_{A+A}(x) = \sum_x r^2_{A-A}(x)$. In the same way define the *common multiplicative energy* of two sets A, B

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

further $\mathsf{T}^\times_k(A)$, $\mathsf{T}^\times_k(f)$ and so on.

If $\mathbf{G}$ is an abelian group, then the Plünnecke–Ruzsa inequality (see, e.g., [21]) takes place

$$|nA - mA| \leqslant \left(\frac{|A+A|}{|A|} \right)^{n+m} \cdot |A| \,, \tag{11}$$

and

$$|nA| \leqslant \left(\frac{|A+A|}{|A|}\right)^n \cdot |A|\,. \tag{12}$$

Now recall our current knowledge about the Polynomial Freiman–Ruzsa Conjecture, see [16], [17] and [21]. We need a simple consequence of [17, Proposition 2.5, Theorem 2.7]. Recall that if $P_1, \dots, P_d \subset \mathbb{Z}$ are arithmetic progressions, then $Q := P_1 + \dots + P_d$ is a *generalized arithmetic progression* (GAP) of *dimension* d. A generalized arithmetic progression, Q, is called to be *proper* if $|Q| = \prod_{j=1}^d |P_j|$. For properties of generalized arithmetic progressions consult, e.g., [21].

Theorem 6 *Let $A \subset \mathbb{Z}$ be a finite set, $|A+A| \leqslant K|A|$ and $\kappa > 3$ be any constant. Then there is a proper GAP H of size at most $|A| \exp(O(\log^\kappa K))$ and dimension $O(\log^\kappa K)$ such that for a set of shifts X, $|X| \leqslant \exp(O(\log^\kappa K))$ one has $A \subseteq H + X$.*

All logarithms are to base 2. The signs $\ll$ and $\gg$ are the usual Vinogradov symbols. For a positive integer n, let $[n] = \{1, \dots, n\}$.

3 The proof of the main result

Now we obtain Theorem 2 from the introduction. Following the method from [13] we recall some required definitions.

For each prime $p \in \mathcal{P}$ take a random variable X_p, which is uniformly distributed on S^1 and let all X_p be independent. For every $n \in \mathbb{N}$, $n = p_1^{\omega_1} \dots p_s^{\omega_s}$, where $p_j \in \mathcal{P}$, $j \in [s]$ are different primes put $X_n := \prod_{j=1}^s X_{p_j}^{\omega_j}$. Then define the random zeta function by the formula (let α be a real number, $\alpha > \frac{1}{2}$, say)

$$\zeta_X(\alpha) := \sum_{n\in\mathbb{N}} \frac{X_n}{n^\alpha} = \prod_{p\in\mathcal{P}} \left(1 - \frac{X_p}{p^\alpha}\right)^{-1}. \tag{13}$$

Using the product formula (13) one can compute the moments of the random zeta function (13), see [13, Lemma 6] (or just similar calculations in our Lemma 10 below).

Lemma 7 *Let l be a positive integer. Then*

$$\log \mathbb{E}\, |\zeta_X(\alpha)|^{2l} \ll \begin{cases} l \log\log l, & \alpha = 1\,, l \geqslant 3 \\ C(\alpha) l^{1/\alpha} (\log l)^{-1}, & 1/2 < \alpha < 1\,, l \geqslant 3 \\ l^2 \log\left(\frac{1}{2\alpha-1}\right), & 1/2 < \alpha\,, l \geqslant 1\,, \end{cases}$$

where $C(\alpha) = \frac{\alpha}{1-\alpha} + \frac{\alpha}{2\alpha-1}$.

Also, for any function $g : \mathbb{Z} \to \mathbb{C}$ consider the following random analogue of its "multiplicative" Fourier transform

$$\widehat{g}(X) = \sum_{n\in\mathbb{N}} g(n) X_n\,. \tag{14}$$

Clearly, we have an analogue of the Parseval identity

$$\mathbb{E}|\widehat{g}(X)|^2 = \|g\|_2^2 \,, \tag{15}$$

and, moreover, for $k \geqslant 1$ one has

$$\mathbb{E}|\widehat{g}(X)|^{2k} = \mathsf{T}^{\times}_k(g) \,. \tag{16}$$

Further one can compute

$$\mathbb{E}|\widehat{g}(X)\zeta_X(\alpha)|^2 = \sum_{n_1,n_2,m_1,m_2 \,:\, n_1m_1=n_2m_2} \frac{g(m_1)\overline{g}(m_2)}{(n_1n_2)^{\alpha}} =$$

$$= \zeta(2\alpha) \sum_{m_1,m_2} g(m_1)\overline{g}(m_2) \cdot \frac{\mathrm{gcd}(m_1,m_2)^{2\alpha}}{(m_1m_2)^{\alpha}} \tag{17}$$

and hence GCD sum (17) can be interpreted as the multiplicative energy (see the definition of Fourier transform (14)) of our weight g with the random zeta function $\zeta_X(\alpha)$. It is easy to see (consult estimate (20) below) that it can be converted further to the ordinary multiplicative energy of the function g and the interval $[N]$.

We follow the method from [13], [4], [1] to give the proof of Lemma 8 below. Generally speaking, our bound (19) is close to the optimal one, see [5].

Lemma 8 *Let $w : \mathbb{Z} \setminus \{0\} \to \mathbb{R}^+$ be a non–negative function and N be a positive integer. Then for any positive integer s one has*

$$\mathsf{E}^{\times}([N], w) \ll N\|w\|_2^2 \exp\left(C\left(\sqrt{s^{-1}\log\log N \cdot \log(\mathsf{T}^{\times}_{s+1}(w)\|w\|_2^{-2(s+1)})} + \log\log N\right)\right) \ll \tag{18}$$

$$\ll N\|w\|_2^2 \exp\left(C\left(\sqrt{\log\log N \cdot \log(\|w\|_1\|w\|_2^{-1})} + \log\log N\right)\right)\,, \tag{19}$$

where $C > 0$ is an absolute constant.

P r o o f. Let $L = \log N$ and $\alpha \in (1/2, 1)$. Using the Dirichlet principle, as well as the multiplicative analogue of estimate (9), we find a positive number $U \leqslant N$ such that

$$\mathsf{E}^{\times}([N], w) \ll L^2 \sum_{U<n_1,n_2\leqslant 2U,\, m_1,m_2 \,:\, n_1m_1=n_2m_2} w(m_1)w(m_2) \ll$$

$$\ll L^2U^{2\alpha} \sum_{U<n_1,n_2\leqslant 2U,\, m_1,m_2 \,:\, n_1m_1=n_2m_2} \frac{w(m_1)w(m_2)}{(n_1n_2)^{\alpha}} \,.$$

In terms of the random zeta function (13), we see that the last sum clearly does not exceed

$$\sum_{n_1,n_2,m_1,m_2 \,:\, n_1m_1=n_2m_2} \frac{w(m_1)w(m_2)}{(n_1n_2)^{\alpha}} = \mathbb{E}|\widehat{w}(X)\zeta_X(\alpha)|^2 \,.$$

Thus

$$\mathsf{E}^{\times}([N],w) \ll L^2 U^{2\alpha} \mathbb{E}|\widehat{w}(X)\zeta_X(\alpha)|^2 \tag{20}$$

and our task is to estimate the last expectation. Let $l \geqslant 3$ be an integer parameter, which we will choose later. Also, let $\mathsf{T}_{s+1} = \mathsf{T}^{\times}_{s+1}(w)$. Thanks to identities (15), (16) and the Hölder inequality, we have

$$\mathbb{E}|\widehat{w}(X)\zeta_X(\alpha)|^2 \leqslant (\mathbb{E}|\widehat{w}(X)|^{2+2/(l-1)})^{1-1/l} \cdot (\mathbb{E}|\zeta_X(\alpha)|^{2l})^{1/l} \leqslant \tag{21}$$

$$\leqslant \left(\mathbb{E}|\widehat{w}(X)|^2\right)^{\frac{s(l-1)-1}{sl}} \left(\mathbb{E}|\widehat{w}(X)|^{2s+2}\right)^{\frac{1}{sl}} \cdot \mathbb{E}^{1/l}|\zeta_X(\alpha)|^{2l} = \|w\|_2^2 \mathsf{T}_{s+1}^{\frac{1}{sl}} \|w\|_2^{-\frac{2s+2}{sl}} \cdot (\mathbb{E}|\zeta_X(\alpha)|^{2l})^{1/l} . \tag{22}$$

Applying Lemma 7, we get

$$\mathbb{E}|\widehat{w}(X)\zeta_X(\alpha)|^2 \ll$$

$$\ll \|w\|_2^2 \exp\left(\frac{1}{ls}\log(\mathsf{T}_{s+1}\|w\|_2^{-2(s+1)}) + \min\left\{\frac{C(\alpha)l^{1/\alpha}}{l\log l}, O\left(l\log\frac{1}{2\alpha-1}\right)\right\}\right) . \tag{23}$$

Put $Y = s^{-1}\log(\mathsf{T}_{s+1}\|w\|_2^{-2(s+1)}) \geqslant 0$. First of all, take the second term in the minimum in (23). In this case we see that the optimal choice of $l = \lfloor Y^{1/2}\log^{-1/2}(1/(2\alpha-1))\rfloor$. Hence

$$\mathbb{E}|\widehat{w}(X)\zeta_X(\alpha)|^2 \ll \|w\|_2^2 \exp\left(O\left(Y^{1/2}\log^{1/2}\frac{1}{2\alpha-1}\right)\right) .$$

Now we take $\alpha = \frac{1}{2} + \frac{1}{\log N}$. We can assume that $l \geqslant 3$ because otherwise $Y \ll \log\log N$ and the desired bound (19) follows from (20) and (23). Using $U \leqslant N$, we get in view of (20) that

$$\mathsf{E}^{\times}([N],w) \ll L^2 N \|w\|_2^2 \exp\left(O\left(\sqrt{s^{-1}\log\log N \cdot \log(\mathsf{T}_{s+1}\|w\|_2^{-2(s+1)})}\right)\right) .$$

To obtain (19) just notice that $\mathsf{T}_{s+1} \leqslant \|w\|_1^{2s}\|w\|_2^2$. This completes the proof. □

Using lemma above we obtain in particular, Theorem 2 from the introduction.

Theorem 9 *Let $A, S \subset \mathbb{Z}$ be finite sets and $0 \leqslant \alpha < 1/6$ be any number. Suppose that $|A+A| \leqslant K|A|$ with*

$$K \ll \exp(\log^{\alpha}|A|) \tag{24}$$

and

$$|S| \leqslant \exp\left(\frac{\log^{2-6\alpha}|A|}{\log\log|A|}\right) . \tag{25}$$

Then there are at least $\exp(O(\log^{1-3\alpha}|A|))$ elements $a \in A$ such that

$$|(A-a)S| \gg |S| \cdot \exp(O(\log^{1-3\alpha}|A|)) . \tag{26}$$

In addition, if $|S+S| \leqslant K_*|S|$, then (26) takes place provided

$$K_* \log|S| \leqslant \exp\left(\frac{\log^{2-6\alpha}|A|}{\log\log|A|}\right) . \tag{27}$$

Proof. Using Theorem 6 we find a proper GAP H of size at most $|A|\exp(O(\log^\kappa K))$ and dimension $d = O(\log^\kappa K)$ such that for a set of shifts X, $|X| \leqslant \exp(O(\log^\kappa K))$ one has $A \subseteq H + X$. Here $\kappa > 3$ is any number. We have $H = P_1 + \dots + P_d$, where the sum is direct and all P_j are arithmetic progressions. Without loss of generality we can assume that for $P = P_1$ one has $|P| \geqslant |H|^{1/d}$. Also, there is $x \in X$ such that $|A \cap (H + x)| \geqslant |A|/|X|$ and hence

$$|A| \cdot \exp(-O(\log^\kappa K)) \leqslant |A|/|X| \leqslant |A \cap (H+x)| \leqslant \sum_{y \in P_2 + \dots + P_d} |A \cap (P + y + x)| .$$

Thus there exists $y \in P_2 + \dots + P_d + x$ such that

$$|P| \cdot \exp(-O(\log^\kappa K)) \leqslant |P||A|/|H| \cdot \exp(-O(\log^\kappa K)) =$$
$$= |A| \cdot \exp(-O(\log^\kappa K))(|P_2| \dots |P_d|)^{-1} \leqslant |A \cap (P+y)| . \tag{28}$$

For any $a \in A \cap (P+y)$, we have $D_* := A \cap (P+y) - a \subseteq (A-A) \cap (P-P)$. Applying Lemma 8, the lower bound $|P| \geqslant |H|^{1/d}$ and using the Holder inequality several times, as well as estimate (28), we obtain

$$|D_* S| \geqslant \frac{|D_*|^2|S|^2}{\mathsf{E}^\times(P-P,S)} \gg \frac{|A \cap (P+y)|^2|S|^2}{\mathsf{E}^\times(P,S)} \gg$$
$$\gg |S||P| \cdot \exp(-O(\log^\kappa K + \sqrt{\log\log|P| \cdot \log|S|} - \log\log|P|)) \gg \tag{29}$$
$$\gg |S| \cdot \exp\left(O\left(\frac{\log|A|}{\log^\kappa K} - \log^\kappa K - \sqrt{\log\log|A| \cdot \log|S|}\right)\right) .$$

Here we have ignored the term $\log\log|P|$ from (29) because $|S| \gg \log|A| \gg \log|P|$. Indeed, if $|S| \ll \log|A|$, then inequality (26) is trivial. Thanks to our conditions (24), (25), we obtain

$$|D_* S| \gg |S| \cdot \exp\left(O\left(\frac{\log|A|}{\log^\kappa K} - \sqrt{\log\log|A| \cdot \log|S|}\right)\right) \gg |S| \cdot \exp\left(O\left(\frac{\log|A|}{\log^\kappa K}\right)\right) \gg \tag{30}$$
$$\gg |S| \cdot \exp(O(\log^{1-3\alpha}|A|)) \tag{31}$$

as required. In a similar way, we have the following lower bound for and number of $a \in A \cap (P+y)$, namely,

$$|A \cap (P+y)| \geqslant |P| \cdot \exp(-O(\log^\kappa K)) \geqslant |H|^{1/d} \cdot \exp(-O(\log^\kappa K)) \gg \exp\left(-O\left(\frac{\log|A|}{\log^\kappa K} + \log^\kappa K\right)\right)$$
$$\gg \exp(O(\log^{1-3\alpha}|A|)) .$$

Now to obtain (27) just repeat the previous calculations and use Lemma 8 with the parameter $s = 1$. By Solymosi's result [20] we know that $\mathsf{E}^\times(S) \ll |S+S|^2 \log|S| \ll K_*^2|S|^2 \log|S|$ and we arrive to an analogue of (30), (31)

$$|D_* S| \gg |S| \cdot \exp\left(O\left(\frac{\log|A|}{\log^\kappa K} - \sqrt{\log\log|A| \cdot \log(K_*^2 \log|S|)}\right)\right) .$$

This completes the proof. $\square$

Now consider another zeta function, which allows to make calculations above better and even simpler. Let $\alpha > 0$ be a real number and z be a positive integer. Then

$$\mathcal{Z}_X(\alpha) := \prod_{z \leqslant p < 2z} \left(1 + \frac{X_p}{p^\alpha}\right) . \tag{32}$$

Denote by $\mathcal{P}_z$ the set of all primes in $[z, 2z)$ and let g be any non–negative function. Since the support of $\mathcal{Z}_X(\alpha)$ coincides with all possible products of primes from $\mathcal{P}_z$ and 1, we see that the function $\mathcal{Z}_X(\alpha)$ can be used to calculate the common energy of the set $\mathcal{P}_z$ with any function g, namely,

$$\mathsf{E}^\times(g, \mathcal{P}_z) < 4^\alpha z^{2\alpha} \cdot \mathbb{E}|\widehat{g}(X)\mathcal{Z}_X(\alpha)|^2 . \tag{33}$$

Thus to compute $\mathsf{E}^\times(g, \mathcal{P}_z)$ we need to estimate all moments of the function $\mathcal{Z}_X(\alpha)$ similar to Lemma 7.

Lemma 10 *Let $\alpha > 0$ be any real number, l be a positive integer and $l \leqslant z^\alpha$. Then*

$$\log \mathbb{E}|\mathcal{Z}_X(\alpha)|^{2l} \ll \frac{l^2 z^{1-2\alpha}}{\log z} .$$

P r o o f. In view of the fact that all the variables X_p, $p \in \mathcal{P}_z$ are independent, we have

$$\mathbb{E}|\mathcal{Z}_X(\alpha)|^{2l} = \prod_{z \leqslant p < 2z} \mathbb{E}\left(1 + \frac{X_p}{p^\alpha}\right)^l \left(1 + \frac{\overline{X}_p}{p^\alpha}\right)^l := \prod_{z \leqslant p < 2z} E_l(p) ,$$

and

$$E_l(p) = \frac{1}{2\pi} \int_0^{2\pi} \left(1 + \frac{e^{i\theta}}{p^\alpha}\right)^l \left(1 + \frac{e^{-i\theta}}{p^\alpha}\right)^l d\theta = \sum_{n=0}^{l} \binom{l}{n}^2 \frac{1}{p^{2\alpha n}} .$$

Using the condition $l \leqslant z^\alpha$, we obtain $\log E_l(p) \leqslant 2l^2/p^{2\alpha}$. Hence

$$\log \mathbb{E}|\mathcal{Z}_X(\alpha)|^{2l} \leqslant 2l^2 \sum_{z \leqslant p < 2z} p^{-2\alpha} \ll \frac{l^2 z^{1-2\alpha}}{\log z} .$$

This completes the proof. $\square$

Now we formulate an analogue of Lemma 8 allowing to calculate the common energy of the set $\mathcal{P}_z$ with a general weight w.

Proposition 11 *Let $w : \mathbb{Z} \setminus \{0\} \to \mathbb{R}^+$ be a non–negative function and s, z be positive integers. Suppose that*

$$\log(\mathsf{T}^\times_{s+1}(w)\|w\|_2^{-2(s+1)}) \leqslant \frac{sz}{\log z} . \tag{34}$$

Then for any $\alpha > 0$ the following holds

$$\mathsf{E}^\times(\mathcal{P}_z, w) \ll z^{2\alpha}\|w\|_2^2 \exp\left(C z^{1/2-\alpha}\sqrt{s^{-1}\log^{-1} z \cdot \log(\mathsf{T}^\times_{s+1}(w)\|w\|_2^{-2(s+1)})}\right) . \tag{35}$$

In particular, for any $\varepsilon > 0$ and $z > 1/\varepsilon$ one has

$$\mathsf{E}^\times(\mathcal{P}_z, w) \ll (\varepsilon z)^2 \|w\|_2^2 \exp\left(C\varepsilon^{-1} z^{-1/2} \sqrt{s^{-1} \log^{-1} z \cdot \log(\mathsf{T}^\times_{s+1}(w) \|w\|_2^{-2(s+1)})} \right) . \qquad (36)$$

P r o o f. Let $X = s^{-1} \log(\mathsf{T}^\times_{s+1}(w)\|w\|_2^{-2(s+1)})$. Choose $l = (X \log z/z)^{1/2} z^\alpha$. Thanks to our assumption (34), we have $l \leqslant z^\alpha$. Using Lemma 10 as in lines (21)—(23), combining with bound (33), we get

$$\mathsf{E}^\times(\mathcal{P}_z, w) \ll z^{2\alpha} \|w\|_2^2 \exp\left(\frac{1}{ls} \log(\mathsf{T}^\times_{s+1}(w)\|w\|_2^{-2(s+1)}) + \frac{l z^{1-2\alpha}}{\log z} \right) \ll$$

$$\ll z^{2\alpha} \|w\|_2^2 \exp\left(C z^{1/2-\alpha} \sqrt{s^{-1} \log^{-1} z \cdot \log(\mathsf{T}^\times_{s+1}(w)\|w\|_2^{-2(s+1)})} \right) . \qquad (37)$$

Taking $\alpha = 1 - \frac{\log(1/\varepsilon)}{\log z}$, we obtain

$$\mathsf{E}^\times(\mathcal{P}_z, w) \ll (\varepsilon z)^2 \|w\|_2^2 \exp\left(C\varepsilon^{-1} z^{-1/2} \sqrt{s^{-1} \log^{-1} z \cdot \log(\mathsf{T}^\times_{s+1}(w)\|w\|_2^{-2(s+1)})} \right) \qquad (38)$$

as required. $\square$

Now we derive an upper bound for the common energy of the set of the primes in a segment and an arbitrary set. It shows that in a sense the primes "repulse" the other sets.

Theorem 12 *Let $S \subset \mathbb{Z}$ be a set, l be an integer number, and $\mathcal{P}^{(l)} := [l] \cap \mathcal{P}$. Then for any $d \neq 0$ the conditions*

$$\log |S| \ll \frac{\varepsilon l}{\log l} , \qquad \varepsilon \gg \frac{\log l}{l} \qquad (39)$$

imply

$$\mathsf{E}^\times(d \cdot \mathcal{P}^{(l)}, S) \leqslant \varepsilon |\mathcal{P}_l|^2 |S| . \qquad (40)$$

P r o o f. Take any $z \leqslant [l/2]$. By estimate (35) of Proposition 11, we get for any $\varepsilon_* > 0$

$$\mathsf{E}^\times(\mathcal{P}_z, S) \ll (\varepsilon_* z)^2 |S| \exp\left(C\varepsilon_*^{-1} z^{-1/2} \sqrt{\log^{-1} z \cdot \log |S|} \right) .$$

Summing over $z > \frac{\log l}{\sqrt{\varepsilon}} := z_0$ of the form $2^j \leqslant l/2$ and using the prime number theorem, we obtain

$$\mathsf{E}^\times(d \cdot \mathcal{P}^{(l)}, S) \ll \varepsilon_*^2 l^2 |S| \exp\left(C\varepsilon_*^{-1} l^{-1/2} \sqrt{\log^{-1} l \cdot \log |S|} \right) + \frac{z_0^2 |S|}{\log^2 z_0} .$$

Notice that the second condition from (39) gives us $z_0 \ll \sqrt{l \log l}$. Now put $\varepsilon_*^2 = \frac{\varepsilon}{\log^2 l}$. Then thanks to our assumption (39) and $z_0 \ll \sqrt{l \log l}$, we have (40). This completes the proof. $\square$

Theorem 12 implies Theorem 1 from the introduction. Indeed, in the notation of Theorem 1, we have $A \subseteq S$, where A is an arithmetic progression and $|SS| \ll |S|$. Take $P = \mathcal{P}^{(|A|)}$. Applying the Cauchy–Schwarz inequality, we derive

$$|P|^2|S|^2 \leqslant \mathsf{E}^{\times}(P,S)|PS| \leqslant \varepsilon|P|^2|S||SS| \ll \varepsilon|P|^2|S|^2$$

and taking ε to be a sufficiently small constant, we obtain a contradiction. Hence the first condition from (39) does not hold and we have

$$\log|S| \gg \frac{|A|}{\log|A|}$$

which implies $|A| \ll \log|S| \cdot \log\log|S|$ as required.

Of course in Theorem 12 one can consider more general arithmetic progressions as well but in this case one should control the beginning and the step of such progression, simultaneously.

4 On general k–convex functions

In [10, Theorem 1.3] authors obtained the following growth result for sequences of the form $A = f([N])$, where f is an arbitrary k–convex function.

Theorem 13 *Let $k \geqslant 2$ be an integer and let A be a k–convex sequence. Then*

$$|2^k A - (2^k - 1)A| \gg \frac{|A|^{k+1}}{2^{k^2}}\,.$$

Thus Theorem 3 from the introduction can be considered as a "statistical" version of Theorem 13. Also, notice that the dependence on k in Theorem 13 is better.

In this section we show how Theorem 3 implies an upper bound for the higher energy of any k–convex function. Basically, we repeat the combination of the arguments from [15, Theorem 13] and [18, Theorem 23].

Theorem 14 *Let f be a function which is k–convex on a set I for some $k \geq 1$. Suppose that $|I+I-I| \leqslant |I|^{1+\epsilon}$. Then for all $l \leqslant 2^k$, $\epsilon \leqslant \frac{\log l}{l}$ one has*

$$\mathsf{T}^{+}_{2^l}(f(I)) \ll |I|^{2^{l+1}-c\log l}\,. \tag{41}$$

for a certain absolute constant $c > 0$.

P r o o f. Put $A = f(I)$. Let $\mathsf{T}_{2^j} := \mathsf{T}^{+}_{2^j}(A)$ and $\mathsf{T}_1 = |A|^2$. Our task is to prove for any $j \in [l]$ that

$$\mathsf{T}_{2^j} \leqslant \frac{\mathsf{T}_{2^{j-1}}|A|^{2^j}}{Q}\,, \tag{42}$$

where $Q=|A|^{\frac{c\log j}{j}}$ because it clearly implies (41). Suppose not. Put $L=O(k\log|A|)$. By the dyadic Dirichlet principle and the Hölder inequality in the form (9) there is a number $\Delta>0$ and a set $P=\{x\in\mathbb{Z}\ :\ \Delta<r_{2^{j-1}A}(x)\leqslant 2\Delta\}$ such that

$$L^4\Delta^4\mathsf{E}^+(P)\gg \mathsf{T}_{2^j}\geqslant \frac{|A|^{2^j}\mathsf{T}_{2^{j-1}}}{Q}\geqslant \frac{(\Delta|P|)^2\Delta^2|P|}{Q}\,. \tag{43}$$

Indeed, we can assume that (41) does not hold (otherwise there is nothing to prove) and thus by our condition $j\leqslant l\leqslant 2^k$ one has

$$|A|^{2^{j-1}-1}\geqslant\Delta\gg|A|^{2^{j-1}-c\log j}$$

and hence we do indeed have the upper bound (43) with the quantity L. Also, we have used the trivial bounds

$$\Delta|P|\leqslant|A|^{2^{j-1}}\qquad\text{and}\qquad\Delta^2|P|\leqslant\mathsf{T}_{2^{j-1}}\,. \tag{44}$$

Further from (43), we obtain $\Delta\gg L^{-4}\mathsf{T}_{2^j}|A|^{-3\cdot 2^{j-1}}$ because by (44)

$$L^4\Delta|A|^{3\cdot 2^{j-1}}\geqslant L^4\Delta^4|P|^3\geqslant L^4\Delta^4\mathsf{E}^+(P)\gg\mathsf{T}_{2^j}$$

and

$$\mathsf{E}^+(P)\gg L^{-4}\frac{|P|^3}{Q}:=\frac{|P|^3}{Q_1}\,.$$

Also notice that $\Delta^4\mathsf{E}^+(P)\leqslant\Delta^2|P|(\Delta|P|)^2\leqslant\mathsf{T}_{2^{j-1}}(\Delta|P|)^2$ and hence from (43), we get

$$\Delta|P|\geqslant\frac{|A|^{2^{j-1}}}{L^2Q^{1/2}}\,. \tag{45}$$

Similarly, by (44), we have $\Delta^4\mathsf{E}^+(P)\leqslant(\Delta^2|P|)|A|^{2^j-2}|P|^2\leqslant\mathsf{T}_{2^{j-1}}|A|^{2^j-2}|P|^2$ and thus from (43), we derive

$$|P|\geqslant\frac{|A|}{L^2Q^{1/2}}\,. \tag{46}$$

By the Balog–Szemerédi–Gowers Theorem (see, e.g., [21]), we find $P_*\subseteq P$ such that $|P_*|\gg|P|Q_1^{-C_*}$, and $|P_*+P_*|\ll Q_1^{C_*}|P_*|$. Here $C_*>1$ is an absolute constant, which may change from line to line. By the definition of the set P, we have

$$\Delta|P_*|\leqslant\sum_{x\in P_*}r_{2^{j-1}A}(x)=\sum_{x_1,\dots,x_{2^{j-1}-1}\in A}r_{P_*-A}(x_1+\dots+x_{2^{j-1}-1})\,.$$

Hence there is a shift x and a set $A_*\subseteq A\cap(P_*-x)$ such that

$$|A_*|\geqslant\Delta|P_*|/|A|^{2^{j-1}-1}\gg|A|(LQ)^{-C_*}\,. \tag{47}$$

Here we have used bound (45). The set A_* has the form $A_*=f(S)$, where $S\subseteq I$ is a set of the same size. Clearly,

$$|S+S-S|\leqslant|I+I-I|\leqslant|I|^{1+\epsilon}=|A|^{1+\epsilon}/|A_*|\cdot|S|:=K|S|\,.$$

Applying Theorem 3 with a parameter $t = t(j) \leqslant k$, which we will choose later, combining with inequality (11), we obtain

$$\frac{|A_*|^{t+1}}{(CK)^{2^{t+1}-t-2}(\log|A_*|)^{2^{t+2}-t-4}} \leqslant |2^t A_* - (2^t-1)A_*| \leqslant |2^t P_* - (2^t-1)P_*| \ll$$

$$\ll Q_1^{(2^{t+1}-1)C_*}|P_*|\,. \tag{48}$$

Thanks to estimate (47), we know that $K \ll (LQ)^{C_*}|A|^\epsilon$. By the assumption $\epsilon \leqslant \frac{\log l}{l}$ and hence $K \ll (LQ)^{C_*}$ (with another constant C_* of course) by our choice of Q. Using this estimate, as well as both inequalities from (47), combining with (45) and the lower bound $|P_*| \gg |P|Q_1^{-C_*}$, we derive from (48)

$$\Delta|P_*| \cdot |A|^{t+1-2^{j-1}} Q_1^{-C_* 2^t} \leqslant \left(\frac{\Delta|P_*|}{|A|^{2^{j-1}-1}}\right)^{t+1} \ll Q_1^{C_* 2^t}|P_*|\,.$$

Hence

$$\Delta|A|^{t+1-2^{j-1}} \ll Q_1^{C_* 2^t}$$

and in view of (43), we get

$$|A|^{2^{j-1}-(t+1)} Q_1^{C_* 2^t} |A|^{3\cdot 2^{j-1}} \geqslant \mathsf{T}_{2^j} \geqslant |A|^{2^{j+1}-c\log j}\,.$$

Now take the parameter t as $t(j) = \log j$. It follows that for sufficiently large constant C' we get $Q \gg |A|^{\frac{\log j}{C' j}}$. This completes the proof. $\square$

Remark 15 *In a very recent paper [7] the authors obtain better bounds (using another and more direct method) in a result which is parallel to Theorem 14.*

Theorem 14 can be used to obtain a series of lower bounds for various combinations of *different* sets see, e.g., [10, Corollary 1.5]. We restrict ourself by just one consequence. Much more stronger results for subsets of $\mathbb{Z}$ were obtained in [11], [12].

Corollary 16 *Let m be a positive integer, $A_1, \dots, A_{2^m} \subset \mathbb{R}$ be sets of the same size $|A_1|$, $|A_j A_j| \ll |A_j|$, $j \in [2^m]$. Then for any non–zero shifts $z_1, \dots, z_{2^m}$ one has*

$$|(A_1+z_1)\dots(A_{2^m}+z_{2^m})| \gg |A_1|^{c\log m}\,.$$

Proof. For any $z \neq 0$ consider the function $f_z(x) = \log(z + e^x)$. Then f_z is k–convex for any k. Also, for $I = \log A$, where A is any of the sets A_j, $j \in [2^m]$ one has in view of (11) that $|I + I - I| \ll |I|$. Applying Theorem 14 for $f = f_z$, and $l = m$, we see that $\mathsf{T}^{\times}_{2^m}(A+z) \ll |A|^{2^{m+1}-c\log m}$. Hence by the Hölder inequality

$$|A_1|^{2^{m+1}} \leqslant |(A_1+z_1)\dots(A_{2^m}+z_{2^m})| \cdot \sum_x r^2_{(A_1+z_1)\dots(A_{2^m}+z_{2^m})}(x) \leqslant$$

$$\leqslant |(A_1+z_1)\dots(A_{2^m}+z_{2^m})|\cdot\left(\prod_{j=1}^{2^m} \mathsf{T}^{\times}_{2^m}(A_j+z_j)\right)^{1/2^m} \ll |(A_1+z_1)\dots(A_{2^m}+z_{2^m})|\cdot|A_1|^{2^{m+1}-c\log m}$$

as required. □

Now we obtain a new incidence result for one–parametric curves.

Theorem 17 *Let f be a function which is k–convex on a set I for some $k \geq 1$. Suppose that $|I+I-I| \leqslant |I|^{1+\kappa}$ and $\kappa \leqslant \frac{\log k}{k}$. Then for any finite sets $B, C \subset \mathbb{R}$ with $|I| \geqslant |B|^{\varepsilon}$, $\varepsilon \gg 1/k$ and $\kappa \leqslant \exp(-1/(c\varepsilon))$ there is $\delta(\varepsilon) \geqslant \exp(-\exp(O(1/\varepsilon))) > 0$ such that*

$$|\{(i,b,c) \in I\times B\times C \ : \ f(i)+b=c\}| \ll \sqrt{|B||C|}|I|\cdot|B|^{-\delta(\varepsilon)}\,. \tag{49}$$

P r o o f. Put $A = f(I)\cup(-f(I))$ and let σ be cardinality of the set on the left–hand side of (49). Using the Cauchy–Schwarz inequality several times, we obtain for any j

$$\sigma^{2^j} \leqslant |C|^{2^{j-1}}|B|^{2^{j-1}-1}\sum_x r_{2^jA}(x) r_{B-B}(x)\,.$$

Applying the Cauchy–Schwarz inequality one more time, we get

$$\sigma^{2^{j+1}} \leqslant |C|^{2^j}|B|^{2^j-2}\mathsf{E}^+(B)\mathsf{T}_{2^j}(A)\,.$$

Now suppose that $j \leqslant 2^k$. Then by Theorem 14 and the trivial bound $\mathsf{E}^+(B) \leqslant |B|^3$, we obtain

$$\sigma^{2^{j+1}} \ll |C|^{2^j}|B|^{2^j}\cdot|B||I|^{2^{j+1}-c\log j}\,.$$

It gives us

$$\sigma \ll \sqrt{|B||C|}|I|\cdot\left(\frac{|B|}{|I|^{c\log j}}\right)^{2^{-(j+1)}}$$

By our assumption $|I| \geqslant |B|^{\varepsilon}$ and hence taking $j \gg \exp(1/(c\varepsilon))$, we derive

$$\sigma \ll \sqrt{|B||C|}|I|\cdot|B|^{-2^{-(j+1)}}$$

as required. Here $\delta(\varepsilon) \sim \exp(-\exp(1/c\varepsilon))$. This completes the proof. □

Notice that Lemma 8 alllows us to estimate the common mulplicative energy of $[N]$ and an arbitrary set. It gives an analogue of the incidence bound (49) with $f(x) = \log x$ by a single application of the Cauchy–Schwarz inequality.

The incidence result above implies Theorem 4 from the introduction.

Corollary 18 *Let f be a function which is k–convex on a set I for some $k \geq 1$. Suppose that $|I+I-I| \leqslant |I|^{1+\kappa}$. Then for any finite set $B \subset \mathbb{R}$ with $|I| \geqslant |B|^{\varepsilon}$, $\varepsilon \gg 1/k$, $\kappa \leqslant \exp(-1/(c\varepsilon))$ there is $\delta(\varepsilon) > 0$ such that*

$$\mathsf{E}^+(f(I), B) \ll |I|^2|B|^{1-\delta(\varepsilon)}\,. \tag{50}$$

In particular, $|f(I)+B| \gg |B|^{1+\delta(\varepsilon)}$.

Proof. Let $\tau > 0$ be a real number and

$$S_\tau = \{s \in \mathbb{R} \ : \ |\{(i,b) \in I \times B \ : \ f(i) + b = s\}| \geqslant \tau\}\,.$$

Using Theorem 14, we have

$$\tau |S_\tau| \leqslant |\{(i,b,s) \in I \times B \times S_\tau \ : \ f(i) + b = s\}| \ll \sqrt{|B||S_\tau|}|I||B|^{-\delta(\varepsilon)}\,.$$

By summation we obtain (50) and the bound $|f(I) + B| \gg |B|^{1+\delta(\varepsilon)}$ follows from the Cauchy–Schwarz inequality. This completes the proof. □

References

[1] C. Aistleitner, D. El–Baz, M. Munsch, *A pair correlation problem, and counting lattice points with the zeta function,* arXiv:2009.08184 (2020).

[2] N. C. Ankeny, *The least quadratic non residue,* Ann. of Math. (2) **55** (1952), 65–72.

[3] A. Balog, O. Roche-Newton, D. Zhelezov, *Expanders with Superquadratic Growth,* The Electronic Journal of Combinatorics (2017): P3–14.

[4] T.F. Bloom, A. Walker, *GCD sums and sum–product estimates,* Israel J. Math., 235(1):1–11, 2020.

[5] A. Bondarenko, K. Seip, *Large greatest common divisor sums and extreme values of the Riemann zeta function,* Duke Math. J., 166(9):1685–1701, 2017.

[6] J. Bourgain, *More on the sum–product phenomenon in prime fields and its applications,* Int. J. Number Theory **1**:1 (2005), 1–32.

[7] P.J. Bradshaw, B. Hanson, M. Rudnev, *Higher Convexity and Iterated Second Moment Estimates,* preprint, arXiv:2104.11330v1 [math.NT]

[8] D.A. Burgess, *On character sums and primitive roots,* Proc. LMS **12**:3 (1962), 179–192.

[9] S. Graham, C. Ringrose, *Lower bounds for least quadratic non-residues,* Analytic Number Theory (Allterton Park, IL, 1989), 269–309.

[10] B. Hanson, O. Roche–Newton, M. Rudnev, *Higher convexity and iterated sum sets,* arXiv:2005.00125 (2020).

[11] B. Hanson, O. Roche–Newton, D. Zhelezov, *On iterated product sets with shifts,* Mathematika 65.4 (2019): 831–850.

[12] B. Hanson, O. Roche–Newton, D. Zhelezov, *On iterated product sets with shifts, II,* Algebra & Number Theory 14.8 (2020): 2239–2260.

[13] M. Lewko, M. Radziwill, *Refinements of Gál's theorem and applications,* Adv. Math., 305:280–297, 2017.

[14] H.L. Montgomery, *Topics in Multiplicative Number Theory,* Lecture Notes in Math. 227, Springer-Verlag, New York, 1971.

[15] M. Rudnev, I. D. Shkredov, *On growth rate in $SL_2(\mathbb{F}_p)$, the affine group and sum-product type implications,* arXiv preprint arXiv:1812.01671 (2018).

[16] T. Sanders, *On the Bogolyubov–Ruzsa lemma,* Analysis & PDE, **5**:3 (2012), 627–655.

[17] T. Sanders, *The structure theory of set addition revisited,* Bulletin of the American Mathematical Society **50**:1 (2013), 93–127.

[18] I. D. Shkredov, *Energies and structure of additive sets,* Electronic Journal of Combinatorics, **21**:3 (2014), #P3.44, 1–53.

[19] I. D. Shkredov, *Some remarks on the asymmetric sum–product phenomenon,* Moscow J. Combin. Number Theory, 8:1 (2019), 15–41.

[20] J. Solymosi, *Bounding multiplicative energy by the sumset,* Advances in Mathematics Volume **222**:2 (2009), 402–408.

[21] T. Tao, V. Vu, *Additive combinatorics,* Cambridge University Press 2006.

Steklov Mathematical Institute,
ul. Gubkina, 8, Moscow, Russia, 119991
ilya.shkredov@gmail.com