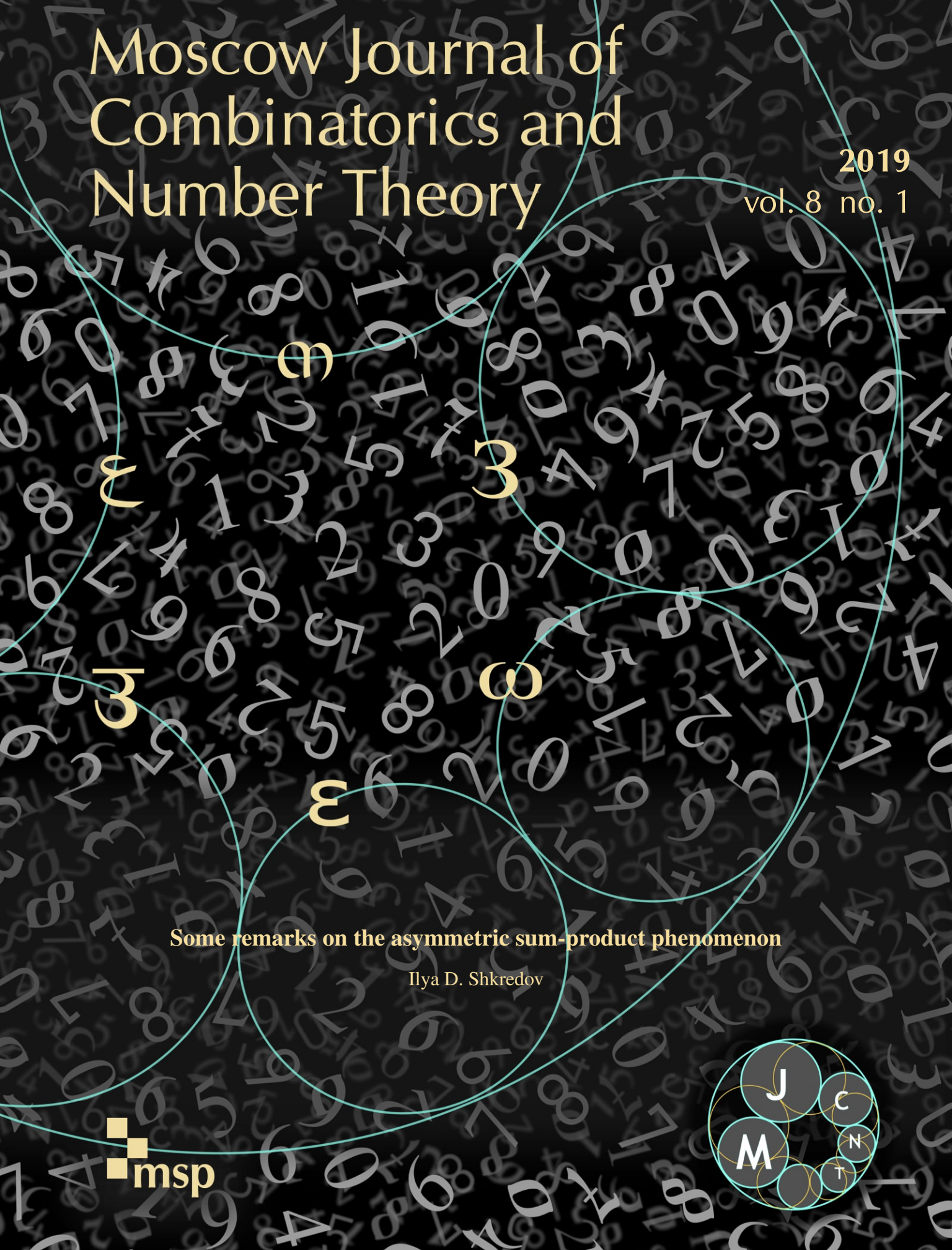
Moscow Journal of Combinatorics and Number Theory

2019
vol. 8 no. 1



# Some remarks on the asymmetric sum-product phenomenon

Ilya D. Shkredov

msp

msp

**Moscow Journal of Combinatorics and Number Theory**
Vol. 8, No. 1, 2019
dx.doi.org/10.2140/moscow.2019.8.15

# Some remarks on the asymmetric sum-product phenomenon

Ilya D. Shkredov

Using some new observations connected to higher energies, we obtain quantitative lower bounds on $\max\{|AB|, |A+C|\}$ and $\max\{|AB|, |(A+\alpha)C|\}$, where $\alpha \neq 0$, in the regime when the sizes of the finite subsets $A, B, C$ of a field differ significantly.

## 1. Introduction

Let $p$ be a prime number and $A, B \subset \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be finite sets. Define the *sum set*, the *difference set*, the *product set*, and the *quotient set* of $A$ and $B$ as

$$A+B := \{a+b : a \in A, b \in B\}, \quad A-B := \{a-b : a \in A, b \in B\},$$
$$AB := \{ab : a \in A, b \in B\}, \qquad A/B := \{a/b : a \in A, b \in B, b \neq 0\}.$$

One of the central problems in arithmetic combinatorics [Tao and Vu 2006] is the *sum-product problem*, which asks for estimates of the form

$$\max\{|A+A|, |AA|\} \geq |A|^{1+c} \tag{1}$$

for some positive $c$. This question was originally posed by Erdős and Szemerédi [1983] for finite sets of integers; they conjectured that (1) holds for all $c < 1$. The sum-product problem has since been studied over a variety of fields and rings; see, e.g., [Bourgain 2003; 2005b; 2007, Bush and Croot 2014; Bourgain et al. 2004; Erdős and Szemerédi 1983; Tao and Vu 2006]. We focus on the case of $\mathbb{F}_p$ (and sometimes consider $\mathbb{R}$), where the first estimate of the form (1) was proved by Bourgain, Katz, and Tao [Bourgain et al. 2004]. At the moment the best results in this direction are contained in [Roche-Newton et al. 2016; Konyagin and Shkredov 2016].

In this article we study an asymmetric variant of the sum-product question, in the spirit of the fundamental paper [Bourgain 2005c]: namely, sum-product theorems in $\mathbb{F}_p$ for sets of distinct sizes. We recall two results from that paper:

**Theorem 1.** *Given $0 < \varepsilon < \frac{1}{10}$, there is $\delta > 0$ such that the following holds. Let $A \subset \mathbb{F}_p$ be such that $p^{\varepsilon} < |A| < p^{1-\varepsilon}$. Then either*

$$|AB| > p^{\delta}|A| \quad \textit{for all } B \subset \mathbb{F}_p \textit{ with } |B| > p^{\varepsilon}$$

*or*

$$|A+C| > p^{\delta}|A| \quad \textit{for all } C \subset \mathbb{F}_p \textit{ with } |C| > p^{\varepsilon}.$$

*MSC2010:* 11B30, 11P70.
*Keywords:* sum-product, expanders, exponential sums.

**Theorem 2.** *Given $0 < \varepsilon < \frac{1}{10}$, there is $\delta > 0$ such that the following holds. Let $A \subset \mathbb{F}_p$ be such that $p^{\varepsilon} < |A| < p^{1-\varepsilon}$. Then for any $x \neq 0$ either*

$$|AB| > p^{\delta}|A| \quad \text{for all } B \subset \mathbb{F}_p \text{ with } |B| > p^{\varepsilon}$$

*or*

$$|(A+x)C| > p^{\delta}|A| \quad \text{for all } C \subset \mathbb{F}_p \text{ with } |C| > p^{\varepsilon}.$$

Theorems 1 and 2 were derived in [Bourgain 2005c] from the following result from [Bourgain 2005a]. Given a set $A \subseteq \mathbb{F}_p$ denote by $\mathsf{T}_k^+(A) := |\{(a_1,\dots,a_k,a_1',\dots,a_k') \in A^{2k} : a_1+\dots+a_k = a_1'+\dots+a_k'\}|$. We write $\mathsf{E}^+(A)$ for $\mathsf{T}_2^+(A)$.

**Theorem 3.** *For a positive integer $Q$, there are a positive integer $k$ and a real $\tau > 0$ such that if $H \subseteq \mathbb{F}_p^*$ and $|HH| < |H|^{1+\tau}$, then*

$$\mathsf{T}_k^+(H) < |H|^{2k}(p^{-1+1/Q} + c_Q|H|^{-Q}),$$

*where $c_Q > 0$ depends on $Q$ only.*

The aim of this paper is to obtain explicit bounds in the theorems above. Our arguments are different and more elementary than those of [Bourgain 2005c; Bourgain et al. 2006; Garaev 2010]. In the proof we almost do not use the Fourier approach and that is why we do not need lower bounds for sizes of $A, B, C$ in terms of the characteristic $p$, but, of course, these sets must be comparable somehow. Another difference between this article and [Bourgain 2005c] is that our arguments work in $\mathbb{R}$ as well.

We now formulate our variants of Theorems 1 and 2 (see also Corollary 33). One can show that Theorem 4 implies Theorems 1 and 2 if $|A| < p^{1/2-\varepsilon}$; see Remark 36.

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

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

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

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

*and for any $\alpha \neq 0$*

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

Actually, we prove that the lower bounds for $|A+C|$, $|(A+\alpha)C|$ in (3), (4) could be replaced by similar upper bounds for the energies $\mathsf{E}^+(A,C)$, $\mathsf{E}^{\times}(A+\alpha,C)$; see the second part of Corollary 33. We call Theorem 4 an asymmetric sum-product result because $A$ can be much larger than $B$ and $C$ (say, $|A| > (|B||C|)^{100}$) in contrast with the usual quadratic restrictions which follow from the classical Szemerédi–Trotter theorem; see [Szemerédi and Trotter 1983; Tao and Vu 2006] for the real setting and see [Bourgain et al. 2004; Garaev 2010; Rudnev 2017b] for prime fields. On the other hand, the roles of $B$, $C$ are not symmetric as well. The thing is that the method of the proof intensively uses the fact that if $|AB|$ is small comparable to $|A|$, then, roughly speaking, for any integer $k$, the size of $(kA)B$ is small comparable to $kA$, roughly speaking (rigorous formulation can be found in Section 5). Of course this observation is not true in any sense if we replace $\times$ to $+$ and vice versa.

Also, we obtain a "quantitative" version of Theorem 3.

**Theorem 5.** *Let $A, B \subseteq \mathbb{F}_p$ be sets, $M \geq 1$ be a real number and $|AB| \leq M|A|$. For any $k \geq 2$ such that $2^{16k} M^{2^{k+1}} C_*^2 \log^8 |A| \leq |B|$, one has*

$$\mathsf{T}^+_{2^k}(A) \leq$$
$$2^{4k+6} C_* \log^4 |A| \cdot \frac{M^{2^k} |A|^{2^{k+1}}}{p} + 16^{k^2} M^{2^{k+1}} C_*^{k-1} \log^{4(k-1)} |A| \cdot |A|^{2^{k+1}-4} |B|^{-\frac{k-1}{2}} \mathsf{E}^+(A). \quad (5)$$

*Here, $C_* > 0$ is an absolute constant.*

As a by-product, we obtain the best constants in the problem of estimating the exponential sums over multiplicative subgroups [Bourgain 2005a; Garaev 2010] (see Corollary 16 below) and relatively good bounds in the question of basis properties of multiplicative subgroups [Glibichuk and Konyagin 2007]. Also, we find a wide series of "superquadratic expanders in $\mathbb{R}$" [Balog et al. 2017] with four variables; see Corollary 35.

In contrast to [Bourgain 2005c], we prove Theorem 4 and Theorem 5 independently. We realize that Theorem 4 is equivalent to estimating energies of another sort, namely,

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

(see the definitions in Section 2). Thus, a new feature of this paper is an upper bound for $\mathsf{E}^+_k(A)$ for sets $A$ with $|AB| \ll |A|$ for some large $B$; see Theorem 27 below. Such an upper bound can be of independent interest. Let us formulate our result about $\mathsf{E}^+_k(A)$.

**Theorem 6.** *Let $A, B \subseteq \mathbb{F}_p$ be two sets, $k \geq 0$ be an integer, and put $M := |AB^{k+1}|/|A|$. Then for any $k \geq 0$ such that*

$$|B|^{k/8+1/2} \geq |A| \cdot M^{2^k+1} 2^{3k+1} C_*^{(k+4)/4} \log^k |AB^k|,$$

*where $C_* > 0$ is an absolute constant, we have*

$$\mathsf{E}^+_{2^{k+1}}(A) \leq 2|AB^k|^{2^{k+1}}. \quad (6)$$

Our approach develops the ideas from [Bourgain 2005c; Shkredov 2014] (see especially Section 4 there) and uses several sum-product observations of course. We avoid repeating Bourgain's combinatorial arguments (although we use a similar inductive proof strategy) but the method relies on recent geometrical sum-product bounds from [Rudnev 2017b] and further papers such as [Yazici et al. 2017; Murphy et al. 2017; Roche-Newton et al. 2016; Shkredov 2017]. In some sense we introduce a new approach of estimating moments $\mathrm{M}_k(f)$ (e.g., $\mathsf{T}^+_k(H)$ in Theorem 3 or $\mathsf{E}^+_k(A)$ in Theorem 6) of some specific functions $f$: instead of calculating $\mathrm{M}_k(f)$ in terms of suitable norms of $f$, we compare $\mathrm{M}_k(f)$ and $\mathrm{M}_{k/2}(f)$. If $\mathrm{M}_k(f)$ is much less than $\mathrm{M}_{k/2}(f)$, then we use induction, and if not, then thanks some special nature of the function $f$, we derive from this fact that the additive energy $\mathsf{E}^+$ of a level set of $f$ is huge and it gives a contradiction. Clearly, this process can be applied at most $O(\log k)$ number of times and that is why we usually have logarithmic savings (compare the index in $\mathsf{T}^+_{2^k}(A)$ and the gain $|B|^{-(k-1)/2}$ in estimate (5), say).

The paper is organized as follows. Section 2 contains all required definitions. In Section 3 we give a list of the results, which will be further used in the text. In Section 4, we consider a particular case

of multiplicative subgroups $\Gamma$ and obtain an upper estimate for $\mathsf{T}_k^+(\Gamma)$. This technique is developed in Section 5 although we avoid using the Fourier approach as was done in [Bourgain 2005c] and in the previous Section 4. Section 5 contains all main Theorems 4–6.

## 2. Notation

In this paper $p$ is an odd prime number, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. We denote the Fourier transform of a function $f : \mathbb{F}_p \to \mathbb{C}$ by $\hat{f}$,

$$\hat{f}(\xi) = \sum_{x\in\mathbb{F}_p} f(x)e(-\xi\cdot x), \tag{7}$$

where $e(x) = e^{2\pi i x/p}$. We rely on the following basic identities. The first one is called the Plancherel formula and its particular case $f = g$ is called the Parseval identity:

$$\sum_{x\in\mathbb{F}_p} f(x)\overline{g(x)} = \frac{1}{p}\sum_{\xi\in\mathbb{F}_p} \hat{f}(\xi)\overline{\hat{g}(\xi)}. \tag{8}$$

A particular case of (8) is

$$\sum_{y\in\mathbb{F}_p}\left|\sum_{x\in\mathbb{F}_p} f(x)g(y-x)\right|^2 = \frac{1}{p}\sum_{\xi\in\mathbb{F}_p} |\hat{f}(\xi)|^2|\hat{g}(\xi)|^2, \tag{9}$$

and the formula

$$f(x) = \frac{1}{p}\sum_{\xi\in\mathbb{F}_p} \hat{f}(\xi)e(\xi\cdot x) \tag{10}$$

is called the inversion formula. Further let $f, g : \mathbb{F}_p \to \mathbb{C}$ be two functions. Put

$$(f*g)(x) := \sum_{y\in\mathbb{F}_p} f(y)g(x-y) \quad \text{and} \quad (f\circ g)(x) := \sum_{y\in\mathbb{F}_p} \overline{f(y)}g(y+x). \tag{11}$$

Then

$$\widehat{f*g} = \hat{f}\hat{g} \quad \text{and} \quad \widehat{f\circ g} = \bar{\hat{f}}\hat{g}. \tag{12}$$

Put $\mathsf{E}^+(A, B)$ for the *common additive energy* of two sets $A, B \subseteq \mathbb{F}_p$ (see, e.g., [Tao and Vu 2006]); that is,

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

If $A = B$ we simply write $\mathsf{E}^+(A)$ instead of $\mathsf{E}^+(A, A)$ and $\mathsf{E}^+(A)$ is called the *additive energy* in this case. 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 (9),

$$\mathsf{E}(A, B) = \frac{1}{p}\sum_{\xi} |\hat{A}(\xi)|^2|\hat{B}(\xi)|^2. \tag{13}$$

Also, notice that

$$\mathsf{E}^+(A, B) \le \min\{|A|^2|B|, |B|^2|A|, |A|^{3/2}|B|^{3/2}\}. \tag{14}$$

Sometimes we write $\mathsf{E}^+(f_1, f_2, f_3, f_4)$ for the additive energy of four real functions, namely,

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

It can be shown using the Hölder inequality (see, e.g., [Tao and Vu 2006]) that

$$\mathsf{E}^+(f_1, f_2, f_3, f_4) \le (\mathsf{E}^+(f_1)\mathsf{E}^+(f_1)\mathsf{E}^+(f_1)\mathsf{E}^+(f_1))^{1/4}. \tag{15}$$

In the same way define the *common multiplicative energy* of two sets $A, B \subseteq \mathbb{F}_p$:

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

Certainly, the multiplicative energy $\mathsf{E}^\times(A, B)$ can be expressed in terms of multiplicative convolutions similar to (11).

Sometimes we use representation function notations like $r_{AB}(x)$ or $r_{A+B}(x)$, which counts the number of ways $x \in \mathbb{F}_p$ can be expressed as a product $ab$ or a sum $a + b$ with $a \in A$, $b \in B$, 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 this paper, we use the same letter to denote a set $A \subseteq \mathbb{F}_p$ and its characteristic function $A : \mathbb{F}_p \to \{0, 1\}$. Thus, $r_{A+B}(x) = (A * B)(x)$, say.

Now consider two families of higher energies. Firstly, let

$$\mathsf{T}^+_k(A) := \big|\{(a_1, \dots, a_k, a'_1, \dots, a'_k) \in A^{2k} : a_1 + \dots + a_k = a'_1 + \dots + a'_k\}\big| = \frac{1}{p} \sum_\xi |\hat{A}(\xi)|^{2k}. \tag{16}$$

It is useful to note that

$$\begin{aligned} \mathsf{T}^+_{2k}(A) = \big|\{(a_1, \dots, a_{2k}, a'_1, \dots, a'_{2k}) \in A^{4k} : (a_1 + \dots + a_k) + (a_{k+1} + \dots + a_{2k}) \\ = (a'_1 + \dots + a'_k) + (a'_{k+1} + \dots + a'_{2k})\}\big| \\ = \sum_{x,y,z} r_{kA}(x) r_{kA}(y) r_{kA}(x+z) r_{kA}(y+z), \end{aligned} \tag{17}$$

so one can rewrite $\mathsf{T}^+_{2k}(A)$ via the additive energy of the function $r_{kA}(x)$. Secondly, for $k \ge 2$, we put

$$\mathsf{E}^+_k(A) = \sum_{x \in \mathbb{F}_p} (A \circ A)(x)^k = \sum_{x \in \mathbb{F}_p} r^k_{A-A}(x) = \mathsf{E}^+(\Delta_k(A), A^k), \tag{18}$$

where

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

Thus, $\mathsf{E}^+_2(A) = \mathsf{T}^+_2(A) = \mathsf{E}^+(A)$. Also, notice that we always have $|A|^k \le \mathsf{E}^+_k(A) \le |A|^{k+1}$ and moreover

$$\mathsf{E}^+_k(A) \le |A|^{k-l} \mathsf{E}^+_l(A) \quad \text{for all } l \le k. \tag{19}$$

Finally, let us remark that by definition (18) one has $\mathsf{E}^+_1(A) = |A|^2$. Some results about the properties of the energies $\mathsf{E}^+_k$ can be found in [Schoen and Shkredov 2013]. Sometimes we use $\mathsf{T}^+_k(f)$ and $\mathsf{E}^+_k(f)$ for an arbitrary function $f$ and the first formula from (18) allows us to define $\mathsf{E}^+_k(A)$ for any positive $k$. It was proved in [Shkredov 2017, Proposition 16] that $(\mathsf{E}^+_k(f))^{1/2k}$ is a norm for even $k$ and a real

function $f$. The fact that $(\mathsf{T}_k^+(f))^{1/2k}$ is a norm is contained in [Tao and Vu 2006] and follows from a generalization of inequality (15).

Let $A$ be a set. Put

$$R[A] := \left\{ \frac{a_1 - a}{a_2 - a} : a, a_1, a_2 \in A, a_2 \neq a \right\}$$

and

$$Q[A] := \left\{ \frac{a_1 - a_2}{a_3 - a_4} : a_1, a_2, a_3, a_4 \in A, a_3 \neq a_4 \right\}.$$

All logarithms are base 2. The signs $\ll$ and $\gg$ are the usual Vinogradov symbols. When the constants in the signs depend on some parameter $M$, we write $\ll_M$ and $\gg_M$. For a positive integer $n$, we set $[n] = \{1, \dots, n\}$.

## 3. Preliminaries

We begin with a variation on the famous Plünnecke–Ruzsa inequality; see [Ruzsa 2009, Chapter 1].

**Lemma 7.** *Let $\boldsymbol{G}$ be a commutative group. Also, let $A, B_1, \dots, B_h \subseteq \boldsymbol{G}$, $|A + B_j| = \alpha_j |A|$, $j \in [h]$. Then there is a nonempty set $X \subseteq A$ such that*

$$|X + B_1 + \dots + B_h| \leq \alpha_1 \dots \alpha_h |X|. \tag{20}$$

*Further for any $0 < \delta < 1$ there is $X \subseteq A$ such that $|X| \geq (1-\delta)|A|$ and*

$$|X + B_1 + \dots + B_h| \leq \delta^{-h} \alpha_1 \dots \alpha_h |X|. \tag{21}$$

We need a result from [Rudnev 2017b] or see [Murphy et al. 2017, Theorem 8]. By the number of point-plane incidences $\mathcal{I}(\mathcal{P}, \Pi)$ between a set of points $\mathcal{P} \subseteq \mathbb{F}_p^3$ and a collection of planes $\Pi$ in $\mathbb{F}_p^3$ we mean

$$\mathcal{I}(\mathcal{P}, \Pi) := \big|\{(p, \pi) \in \mathcal{P} \times \Pi : p \in \pi\}\big|.$$

**Theorem 8.** *Let $p$ be an odd prime, $\mathcal{P} \subseteq \mathbb{F}_p^3$ be a set of points and $\Pi$ be a collection of planes in $\mathbb{F}_p^3$. Suppose that $|\mathcal{P}| = |\Pi|$ and that $k$ is the maximum number of collinear points in $\mathcal{P}$. Then the number of point-plane incidences satisfies*

$$\mathcal{I}(\mathcal{P}, \Pi) \ll \frac{|\mathcal{P}|^2}{p} + |\mathcal{P}|^{3/2} + k|\mathcal{P}|. \tag{22}$$

Notice that in $\mathbb{R}$ we do not need in the first term in estimate (22).

Let us derive a consequence of Theorem 8.

**Lemma 9.** *Let $A, Q \subseteq \mathbb{F}_p$ be two sets, $A, Q \neq \{0\}$, $M \geq 1$ be a real number, and $|QA| \leq M|Q|$. Then*

$$\mathsf{E}^+(Q) \leq C_* \left( \frac{M^2 |Q|^4}{p} + \frac{M^{3/2} |Q|^3}{|A|^{1/2}} \right), \tag{23}$$

*where $C_* \geq 1$ is an absolute constant.*

*Proof.* Put $A = A \setminus \{0\}$. We have

$$\begin{aligned}\mathsf{E}^+(Q) &= |\{q_1+q_2 = q_3+q_4 : q_1,q_2,q_3,q_4 \in Q\}| \\ &\le |A_*|^{-2}|\{q_1+\tilde{q}_2/a = q_3+\tilde{q}_4/a' : q_1,q_3 \in Q,\ \tilde{q}_2,\tilde{q}_4 \in QA,\ a,a' \in A_*\}|.\end{aligned}$$

The number of the solutions to the last equation can be interpreted as the number of incidences between the set of points $\mathcal{P} = Q \times QA \times A_*^{-1}$ and planes $\Pi$ with $|\mathcal{P}| = |\Pi| = |A_*||Q||QA|$. Here $k = |QA|$ because $A, Q \ne \{0\}$. Using Theorem 8 and a trivial inequality $|QA| \le |Q||A|$, we obtain

$$\mathsf{E}^+(Q) \ll |A|^{-2}\Big(\frac{|A|^2|Q|^2|QA|^2}{p} + |Q|^{3/2}|QA|^{3/2}|A|^{3/2}\Big) \ll \frac{M^2|Q|^4}{p} + \frac{M^{3/2}|Q|^3}{|A|^{1/2}},$$

as required. □

Finally, we need a purely combinatorial Lemma 10. It is a new (for $k > 2$) and simple tool which allows us to estimate the restricted higher energy $\sum_{x\in P} r^k_{A-A}(x)$ via some energies of $A$ and $P$; see (25), for example.

**Lemma 10.** *Let $\boldsymbol{G}$ be a finite abelian group and $A, P$ subsets of $\boldsymbol{G}$. For any $k \ge 1$ one has*

$$\Big(\sum_{x\in P} r^k_{A-A}(x)\Big)^2 \le |A|^k \sum_x r^k_{A-A}(x) r_{P-P}(x). \tag{24}$$

*In particular*,

$$\Big(\sum_{x\in P} r^k_{A-A}(x)\Big)^4 \le |A|^{2k}\mathsf{E}^+_{2k}(A)\mathsf{E}^+(P). \tag{25}$$

*Proof.* Clearly, inequality (25) follows from (24) by the Cauchy–Schwarz inequality. To prove estimate (24), we observe that

$$\begin{aligned}\Big(\sum_{x\in P} r^k_{A-A}(x)\Big)^2 &= \Big(\sum_{x_1,\dots,x_k\in A} |P\cap(A-x_1)\cap\dots\cap(A-x_k)|\Big)^2 \\ &\le |A|^k \sum_{x_1,\dots,x_k} |P\cap(A-x_1)\cap\dots\cap(A-x_k)|^2 = |A|^k \sum_x r_{P-P}(x) r^k_{A-A}(x),\end{aligned}$$

as required. □

Combining Theorem 8 and Lemma 10, we obtain a corollary.

**Corollary 11.** *Let $A \subseteq \mathbb{F}_p$, and $B, P \subseteq \mathbb{F}_p^*$ be sets. Then for any $k \ge 1$ one has*

$$\Big(\sum_{x\in P} r^k_{A-A}(x)\Big)^4 \le C_*|A|^{2k}\mathsf{E}^+_{2k}(AB)\Big(\frac{|P|^4}{p} + \frac{|P|^3}{|B|^{1/2}}\Big). \tag{26}$$

*Proof.* By Lemma 10, we have

$$\Big(\sum_{x\in P} r^k_{A-A}(x)\Big)^2 \le |A|^k \sum_x r^k_{A-A}(x) r_{P-P}(x).$$

Further, clearly for any $b \in B$ we have

$$r_{A-A}(x) \le r_{AB-AB}(xb).$$

Hence

$$\Big(\sum_{x\in P} r^k_{A-A}(x)\Big)^2 \le \frac{|A|^k}{|B|}\sum_x\sum_{b\in B} r^k_{AB-AB}(xb) r_{P-P}(x) = \frac{|A|^k}{|B|}\sum_x r^k_{AB-AB}(x) r_{B(P-P)}(x).$$

Using the Cauchy–Schwarz inequality, we obtain

$$\Big(\sum_{x\in P} r^k_{A-A}(x)\Big)^4 \le \frac{|A|^{2k}}{|B|^2}\mathsf{E}^+_{2k}(AB)\sum_x r^2_{B(P-P)}(x).$$

To estimate the sum $\sum_x r^2_{B(P-P)}(x)$, we use Theorem 8 similar to the proof of Lemma 9 (see [Yazici et al. 2017]). Indeed, taking $\mathcal{P} = (p_1, b'p_2, b')$, $\Pi = (b, p'_1, bp_2)$, where $(b, b', p_1, p_2, p'_1, p'_2) \in B^2 \times P^4$, we have

$$\begin{aligned}\sum_x r^2_{B(P-P)}(x) &= |\{(b, b', p_1, p_2, p'_1, p'_2) \in B^2 \times P^4 : b(p_1 - p_2) = b'(p'_1 - p'_2)\}| \\ &= |\{(x, y, z) \in \mathcal{P},\ (b, p'_1, bp_2) \in \Pi : bx + y - p'_1 z = bp_2\}| = \mathcal{I}(\mathcal{P}, \Pi) \\ &\le C_*\Big(\frac{|B|^2|P|^4}{p} + |B|^{3/2}|P|^3\Big).\end{aligned}$$

Thus,

$$\Big(\sum_{x\in P} r^k_{A-A}(x)\Big)^4 \le C_*|A|^{2k}\mathsf{E}^+_{2k}(AB)\Big(\frac{|P|^4}{p} + \frac{|P|^3}{|B|^{1/2}}\Big). \qquad \square$$

## 4. Multiplicative subgroups

In this section we obtain the best upper bounds for $\mathsf{T}^+_k(\Gamma)$, $\mathsf{E}^+_k(\Gamma)$ and for the exponential sums over multiplicative subgroups $\Gamma$. We begin with the quantity $\mathsf{T}^+_k(\Gamma)$.

**Theorem 12.** *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup. Then for any $k \ge 2$, $2^{64k}C_*^4 \le |\Gamma|$ one has*

$$\mathsf{T}^+_{2^k}(\Gamma) \le 2^{4k+6}C_*\log^4|\Gamma| \cdot \frac{|\Gamma|^{2^{k+1}}}{p} + 16^{k^2}C_*^{k-1}\log^{4(k-1)}|\Gamma| \cdot |\Gamma|^{2^{k+1}-\frac{k+7}{2}}\mathsf{E}^+(\Gamma), \qquad (27)$$

*where $C_*$ is the absolute constant from Lemma 9.*

*Proof.* Fix any $s \ge 2$. Our intermediate aim is to prove

$$\mathsf{T}^+_{2s}(\Gamma) \le 32C_*s^4\log^4|\Gamma| \cdot \Big(\frac{|\Gamma|^{4s}}{p} + |\Gamma|^{2s-1/2}\mathsf{T}^+_s(\Gamma)\Big). \qquad (28)$$

By (17), we have

$$\mathsf{T}^+_{2s}(\Gamma) = \sum_{x,y,z} r_{s\Gamma}(x) r_{s\Gamma}(y) r_{s\Gamma}(x+z) r_{s\Gamma}(y+z).$$

Put $\rho = \mathsf{T}^+_{2s}(\Gamma)/(16|\Gamma|^{3s})$. Since

$$\sum_{x,y,z:r_{s\Gamma}(x)\le\rho} r_{s\Gamma}(x)r_{s\Gamma}(y)r_{s\Gamma}(x+z)r_{s\Gamma}(y+z) \le \rho|\Gamma|^{3s} = \mathsf{T}^+_{2s}(\Gamma)/16$$

it follows that

$$\mathsf{T}^+_{2s}(\Gamma) \le \frac{4}{3}\sum\nolimits' k_{x,y,z} r_{s\Gamma}(x)r_{s\Gamma}(y)r_{s\Gamma}(x+z)r_{s\Gamma}(y+z) + \mathcal{E},$$

where the sum $\sum'$ is taken over nonzero variables $x, y, z$ with $r_{s\Gamma}(x), r_{s\Gamma}(y), r_{s\Gamma}(x+z), r_{s\Gamma}(y+z) > \rho$ and

$$\mathcal{E} \le 4r_{s\Gamma}(0)\sum_{y,z} r_{s\Gamma}(y)r_{s\Gamma}(z)r_{s\Gamma}(y+z) \le 4r_{s\Gamma}(0)|\Gamma|^s\mathsf{T}^+_s(\Gamma) \le 4|\Gamma|^{2s-1}\mathsf{T}^+_s(\Gamma). \qquad (29)$$

Put $P_j = \{x : \rho 2^{j-1} < r_{s\Gamma}(x) \le \rho 2^j\} \subseteq \mathbb{F}_p^*$. If (28) does not hold, then, in particular, $\mathsf{T}^+_{2s}(\Gamma) \ge 2^5|\Gamma|^{2s-1/2}\mathsf{T}^+_s(\Gamma) \ge 2^5|\Gamma|^{3s-1/2}$ and hence the possible number of sets $P_j$ does not exceed $L := s\log|\Gamma|$. Indeed, for any $x$ one has $r_{s\Gamma}(x) \le |\Gamma|^{s-1}$ and hence $\rho 2^{j-1} = 2^{j-5}\mathsf{T}^+_{2s}(\Gamma)|\Gamma|^{-3s}$ must be less than $|\Gamma|^{s-1}$ otherwise the correspondent set $P_j$ is empty. In other words,

$$2^{j-5} \le |\Gamma|^{4s-1}/\mathsf{T}^+_{2s}(\Gamma) \le |\Gamma|^{s-1/2}/2^5 \le |\Gamma|^s/2^5$$

as required. By the Dirichlet principle there is $\Delta = \rho 2^{j_0}$, and a set $P = P_{j_0}$ such that

$$\mathsf{T}^+_{2s}(\Gamma) \le \tfrac{4}{3}L^4(2\Delta)^4\mathsf{E}^+(P) + \mathcal{E} = \mathsf{T}'_{2s}(\Gamma) + \mathcal{E}.$$

Indeed, putting $f_i(x) = P_i(x)r_{s\Gamma}(x)$, and using (15), we get

$$\begin{aligned}\sum_{x,y,z}{}' r_{s\Gamma}(x)r_{s\Gamma}(y)r_{s\Gamma}(x+z)r_{s\Gamma}(y+z) &\le \sum_{i,j,k,l=1}^{L}\sum_{x,y,z} f_i(x)f_j(y)f_k(x+z)f_l(y+z)\\ &\le \sum_{i,j,k,l=1}^{L}(\mathsf{E}^+(f_i)\mathsf{E}^+(f_j)\mathsf{E}^+(f_k)\mathsf{E}^+(f_l))^{1/4}\\ &= \Big(\sum_{i=1}^{L}(\mathsf{E}^+(f_i))^{1/4}\Big)^4 \le L^3\sum_{i=1}^{L}\mathsf{E}^+(f_i) \le L^4\max_i \mathsf{E}^+(f_i).\end{aligned}$$

Moreover we always have $|P|\Delta^2 \le \mathsf{T}^+_s(\Gamma)$ and $|P|\Delta \le |\Gamma|^s$. Using Lemma 9, we obtain

$$\mathsf{E}^+(P) \le C_*\Big(\frac{|P|^4}{p} + \frac{|P|^3}{|\Gamma|^{1/2}}\Big).$$

Hence,

$$\mathsf{T}'_{2s}(\Gamma) \le \tfrac{4}{3}(16C_*)L^4\Delta^4\Big(\frac{|P|^4}{p} + \frac{|P|^3}{|\Gamma|^{1/2}}\Big) \le \tfrac{4}{3}(16C_*)L^4\Big(\frac{|\Gamma|^{4s}}{p} + \frac{|P|^3\Delta^4}{|\Gamma|^{1/2}}\Big). \qquad (30)$$

Let us consider the second term in (30). Then in view of $|P|\Delta^2 \le \mathsf{T}^+_s(\Gamma)$ and $|P|\Delta \le |\Gamma|^s$, we have

$$|P|^3\Delta^4 = (P\Delta)^2 P\Delta^2 \le |\Gamma|^{2s}\mathsf{T}^+_s(\Gamma).$$

In other words, by (29), we get

$$\mathsf{T}^+_{2s}(\Gamma) \le \tfrac{4}{3}(16C_*)L^4\left(\frac{|\Gamma|^{4s}}{p}+|\Gamma|^{2s-1/2}\mathsf{T}^+_s(\Gamma)\right)+4|\Gamma|^{2s-1}\mathsf{T}^+_s(\Gamma)$$
$$\le 32C_*s^4\log^4|\Gamma|\cdot\left(\frac{|\Gamma|^{4s}}{p}+|\Gamma|^{2s-1/2}\mathsf{T}^+_s(\Gamma)\right)$$

and inequality (28) is proved.

Now applying formula (28) successively $k-1$ times, we obtain

$$\mathsf{T}^+_{2^k}(\Gamma) \le 2^{4k+6}C_*\log^4|\Gamma|\cdot\frac{|\Gamma|^{2^{k+1}}}{p}+16^{k^2}C_*^{k-1}\log^{4(k-1)}|\Gamma|\cdot|\Gamma|^{2^k+\cdots+4-\frac{k-1}{2}}\mathsf{E}^+(\Gamma)$$
$$\le 2^{4k+6}C_*\log^4|\Gamma|\cdot\frac{|\Gamma|^{2^{k+1}}}{p}+16^{k^2}C_*^{k-1}\log^{4(k-1)}|\Gamma|\cdot|\Gamma|^{2^{k+1}-\frac{k+7}{2}}\mathsf{E}^+(\Gamma). \qquad (31)$$

To get the first term in the last formula we have used our condition $2^{64k}C_*^4 \le |\Gamma|$ to ensure that $|\Gamma|^{1/2} \ge 2^{4k+1}C_*\log^4|\Gamma|$. □

**Remark 13.** The condition $2^{64k}C_*^4 \le |\Gamma|$ can be dropped, but in that case we will have the factor $16^{k^2}(C_*\log|\Gamma|)^{k-1}$ in the first term of (27).

Splitting any $\Gamma$-invariant set onto cosets over $\Gamma$ and applying the norm property of $\mathsf{T}^+_l$, we obtain:

**Corollary 14.** *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, and $Q \subseteq \mathbb{F}_p^*$ be a set with $Q\Gamma = Q$. Then for any $k \ge 2$, $2^{64k}C_*^4 \le |\Gamma|$ one has*

$$\mathsf{T}^+_{2^k}(Q) \le 2^{4k+6}C_*\log^4|\Gamma|\cdot\frac{|Q|^{2^{k+1}}}{p}+16^{k^2}C_*^{k-1}\log^{4(k-1)}|\Gamma|\cdot|\Gamma|^{-\frac{k+7}{2}}\mathsf{E}^+(\Gamma)|Q|^{2^{k+1}}. \qquad (32)$$

Let $\Gamma$ be a subgroup of size less than $\sqrt{p}$. Considering the particular case $k=2$ of the formula in Theorem 12 and using $\mathsf{E}^+(\Gamma) \ll |\Gamma|^{5/2-c}$, where $c>0$ is an absolute constant (see [Shkredov 2013]), one has:

**Corollary 15.** *Let $\Gamma$ be a multiplicative subgroup, $|\Gamma| \le \sqrt{p}$. Then*

$$\mathsf{T}^+_4(\Gamma) \ll \frac{|\Gamma|^8\log^4|\Gamma|}{p}+|\Gamma|^{6-c}.$$

*In particular*, $|4\Gamma| \gg |\Gamma|^{2+c}$.

Previous results on $\mathsf{T}^+_k(\Gamma)$, $|\Gamma| \le \sqrt{p}$ with small $k$ had the form $\mathsf{T}^+_k(\Gamma) \ll |\Gamma|^{2k-2+c_k}$ with some $c_k>0$; see, e.g., [Konyagin and Shparlinski 1999]. The best upper bound for $\mathsf{T}^+_3(\Gamma)$ can be found in [Shteinikov 2015].

Now we prove a corollary about exponential sums over subgroups, which is parallel to results from [Bourgain and Garaev 2009; Bourgain et al. 2006; Garaev 2010]. The difference between the previous estimates and Corollary 16 is just a slightly better constant $C$ in (34).

**Corollary 16.** *Let $\Gamma$ be a multiplicative subgroup, $|\Gamma| \ge p^{\delta}$, $\delta > 0$. Then for all sufficiently large $p$ one has*

$$\max_{\xi \ne 0} |\hat{\Gamma}(\xi)| \ll |\Gamma| \cdot p^{-\delta/2^{7+2\delta^{-1}}}. \tag{33}$$

*Further we have a nontrivial upper bound $o(|\Gamma|)$ for the maximum in* (33) *if*

$$\log |\Gamma| \ge \frac{C \log p}{\log \log p}, \tag{34}$$

*where $C > 2$ is any constant.*

*Proof.* We can assume that $|\Gamma| < \sqrt{p}$, say, because otherwise the estimate (33) is known; see [Konyagin and Shparlinski 1999]. By $\rho$ denote the maximum in (33). Then by Theorem 12, a trivial bound $\mathsf{E}^+(\Gamma) \le |\Gamma|^3$ and (16), we obtain

$$|\Gamma|\rho^{2^{k+1}} \le p\mathsf{T}_{2^k}(\Gamma) \le 2^{4k+6} C_* \log^4 |\Gamma| \cdot |\Gamma|^{2^{k+1}} + 16^{k^2} C_*^{k-1} \log^{4(k-1)} |\Gamma| \cdot |\Gamma|^{2^{k+1}-(k+1)/2} p, \tag{35}$$

provided $2^{64k} C_*^4 \le |\Gamma|$. Put $k = \lceil 2 \log p / \log |\Gamma| + 4 \rceil \le 2/\delta + 5$. Also, notice that

$$\frac{p \log^{4(k-1)} |\Gamma|}{|\Gamma|^{k/2}} \le 1, \tag{36}$$

because $k \ge 2 \log p / \log |\Gamma| + 4$ and $p$ is a sufficiently large number depending on $\delta$ (the choice of $k$ is slightly larger than $2 \log p / \log |\Gamma|$ to "kill" $p$ by division by $|\Gamma|^{k/2}$ as well as logarithms $\log^{4(k-1)} |\Gamma|$). Also, since $|\Gamma| \ge p^{\delta}$, it follows that $2^{64k} C_*^4 \le |\Gamma|$ for sufficiently large $p$. Taking a power $1/2^{k+1}$ from both parts of (35), we see in view of (36) that

$$\rho \ll |\Gamma|(|\Gamma|^{-1/2^{k+2}} + |\Gamma|^{-1/2^{k+2}}) \ll |\Gamma|^{1-1/2^{k+2}} \ll |\Gamma| \cdot p^{-\frac{\delta}{2^{7+2\delta^{-1}}}}.$$

To prove the second part of our corollary just notice that the same choice of $k$ gives something nontrivial if $2^{k+2} \le \varepsilon \log |\Gamma|$ for any $\varepsilon > 0$. In other words, it is enough to have

$$k + 2 \le \frac{2 \log p}{\log |\Gamma|} + 7 \le \log \log |\Gamma| - \log(1/\varepsilon).$$

It means that the inequality $\log |\Gamma| \ge C \log p / (\log \log p)$ for any $C > 2$ is enough. □

**Remark 17.** One can improve some constants in the proof (but not the constant $C$ in (34)), probably, but we did not make such calculations.

Now we estimate a "dual" quantity $\mathsf{E}_s^+(Q)$ for $\Gamma$-invariant set $Q$ (about duality of $\mathsf{T}_{k/2}^+(A)$ and $\mathsf{E}_k^+(A)$; see [Schoen and Shkredov 2013] and (40)–(43)). We give even two bounds and both of them use the Fourier approach. Our first estimate (37) relatively quickly follows from Corollary 14 and the price for it is the appearance $p$ in the bounds. The second estimate (39) is more delicate but requires more work.

**Theorem 18.** *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, and $Q \subseteq \mathbb{F}_p^*$ be a set with $Q\Gamma = Q$ and $|Q|^2|\Gamma| \le p^2$. Then for $0 \le k$, $2^{64k} C_*^4 \le |\Gamma|$ one has*

$$\mathsf{E}^+_{2^{k+1}}(Q) \le 2^{2^{k+2}+3} (\log |Q|)^{2^{k+1}} |Q|^{2^{k+1}} \big(2^{4k+6} C_* \log^4 |Q| + 16^{k^2} C_*^{k-1} \log^{4(k-1)} |Q| \cdot |\Gamma|^{-\frac{k+1}{2}} p\big). \tag{37}$$

*Further let $k \ge 1$ be such that*

$$\Gamma|^{(k+2)/2} \ge |Q| \log^{4k} |Q|. \quad (38)$$

*Then*

$$\mathsf{E}^+_{2^{k+1}}(Q) \le (2^8 C_*)^{k+1} |Q|^{2^{k+1}} |\Gamma|^{1/2}. \quad (39)$$

*Proof.* We begin with (37) and we prove this inequality by induction. For $k = 0$ the result is trivial in view of our condition $|Q|^2|\Gamma| \le p^2$. Put $s = 2^k$, $k \ge 1$. By the Parseval identity and (12), we have

$$\mathsf{E}^+_{2s}(Q) = \frac{1}{p^{2s-1}} \sum_{x_1+\dots+x_{2s}=0} |\hat{Q}(x_1)|^2 \dots |\hat{Q}(x_{2s})|^2 \quad (40)$$

$$\le \frac{2s|Q|^2 \mathsf{E}^+_{2s-1}(Q)}{p} + \frac{1}{p^{2s-1}} \sum_{\substack{x_1+\dots+x_{2s}=0 \\ x_j \ne 0 \text{ for all } j}} |\hat{Q}(x_1)|^2 \dots |\hat{Q}(x_{2s})|^2 \quad (41)$$

$$= \frac{2s|Q|^2 \mathsf{E}^+_{2s-1}(Q)}{p} + \mathsf{E}'_{2s}(Q). \quad (42)$$

Put $L = \log |Q|$. By the Parseval identity

$$\frac{1}{p^{2s-1}} \sum_{\substack{x_1+\dots+x_{2s}=0 \\ x_j \ne 0 \text{ for all } j}} |\hat{Q}(x_1)|^2 \dots |\hat{Q}(x_{2s})|^2$$

$$\le \max_{x \ne 0} |\hat{Q}(x)|^2 \cdot \frac{1}{p^{2s-1}} \sum_{\substack{x_1+\dots+x_{2s}=0 \\ x_j \ne 0 \text{ for all } j}} |\hat{Q}(x_1)|^2 \dots |\hat{Q}(x_{2s-1})|^2 \le \max_{x \ne 0} |\hat{Q}(x)|^2 \cdot |Q|^{2s-1}.$$

Hence, as in the proof of Theorem 12, consider $\rho^2 = \mathsf{E}^+_{2s}(Q)/(4s|Q|^{2s-1})$ and the sets

$$P_j = \{x : \rho 2^{j-1} < |\hat{Q}(x)| \le \rho 2^j\} \subseteq \mathbb{F}_p^*.$$

Using the Dirichlet principle, we find $\Delta = \rho 2^{j_0} \ge \rho$ and $P = P_{j_0}$ such that

$$\mathsf{E}'_{2s}(Q) \le \frac{4L^{2s}(2\Delta)^{4s}}{p^{2s-1}} \mathsf{T}^+_s(P). \quad (43)$$

Here we bound the number of sets $P_j$ by the number $L$ because of

$$2^{2j-2} \le |Q|^2/\rho^2 \le 4s|Q|^{2s+1}/\mathsf{E}^+_{2s}(Q) \le |Q|/4$$

and the last inequality follows if (37) does not hold. Clearly, $P\Gamma = P$ (and this is the crucial point of the proof, actually). Applying Corollary 14, we get

$$\mathsf{E}'_{2s}(Q) \le$$

$$\frac{2^{4s+2}L^{2s}\Delta^{4s}}{p^{2s-1}} \left( 2^{4k+6} C_* \log^4 |\Gamma| \cdot \frac{|P|^{2s}}{p} + 16^{k^2} C_*^{k-1} \log^{4(k-1)} |\Gamma| \cdot |\Gamma|^{-\frac{k+7}{2}} \mathsf{E}^+(\Gamma) |P|^{2s} \right). \quad (44)$$

By the Parseval identity, we see that

$$\Delta^2 |P| \le |Q| p. \quad (45)$$

Hence

$$\mathsf{E}'_{2s}(Q) \le 2^{4s+2}L^{2s}|Q|^{2s}\cdot(2^{4k+6}C_*L^4+16^{k^2}C_*^{k-1}L^{4(k-1)}\cdot|\Gamma|^{-\frac{k+7}{2}}\mathsf{E}^+(\Gamma)p). \qquad (46)$$

Using a trivial bound $\mathsf{E}^+(\Gamma)\le|\Gamma|^3$, we get

$$\mathsf{E}'_{2s}(Q) \le 2^{4s+2}L^{2s}|Q|^{2s}\cdot(2^{4k+6}C_*L^4+16^{k^2}C_*^{k-1}L^{4(k-1)}\cdot|\Gamma|^{-\frac{k+1}{2}}p). \qquad (47)$$

Applying a crude bound (19), namely, $\mathsf{E}^+_{2s-1}(Q)\le|Q|^{s-1}\mathsf{E}^+_s(Q)$, the condition $|Q|^2|\Gamma|\le p^2$, and induction assumption, we get

$$\begin{aligned}\frac{2s|Q|^2\mathsf{E}^+_{2s-1}(Q)}{p} &\le \frac{2s|Q|^{s+1}\mathsf{E}^+_s(Q)}{p}\\ &\le \frac{2s|Q|^{s+1}}{p}\cdot L^s|Q|^s\cdot 2^{2s+3}(2^{4k+2}C_*L^4+16^{(k-1)^2}C_*^{k-2}L^{4(k-2)}\cdot|\Gamma|^{-k/2}p)\\ &\le 2^{4s+2}L^{2s}|Q|^{2s}\cdot(2^{4k+6}C_*L^4+16^{k^2}C_*^{k-1}L^{4(k-1)}\cdot|\Gamma|^{-\frac{k+1}{2}}p).\end{aligned}$$

Hence combining the last estimate with (47), we derive

$$\mathsf{E}^+_{2^{k+1}}(Q)\le 2^{2^{k+2}+3}L^{2^{k+1}}|Q|^{2^{k+1}}\cdot(2^{4k+6}C_*L^4+16^{k^2}C_*^{k-1}L^{4(k-1)}\cdot|\Gamma|^{-\frac{k+1}{2}}p)$$

and thus we have obtained (37).

To get (39), put $l=2^{k-1}$, $k\ge 1$ and consider $\mathsf{E}^+_{4l}(Q)$. Further define $g(x)=r^l_{Q-Q}(x)$ and notice that $\hat{g}(\xi)\ge 0$, $\hat{g}(0)=\mathsf{E}^+_l(Q)$. Moreover, taking the Fourier transform as in (40) and using the Dirichlet principle, we get

$$\begin{aligned}\mathsf{E}^+_{4l}(Q)=\sum_x(Q\circ Q)^{4l}(x)=\sum_x g^4(x)=\frac{\mathsf{E}^+(\hat{g})}{p^3}=\frac{1}{p^3}\sum_{x,y,z}\hat{g}(x)\hat{g}(y)\hat{g}(x+z)\hat{g}(y+z)\\ \le\frac{4\hat{g}(0)}{p^3}\sum_{y,z}\hat{g}(y)\hat{g}(z)\hat{g}(y+z)+\frac{1}{p^3}\sum_{x\ne 0,y\ne 0,z\ne 0}\hat{g}(x)\hat{g}(y)\hat{g}(x+z)\hat{g}(y+z)\\ \le\frac{4\mathsf{E}^+_l(Q)\mathsf{E}^+_{3l}(Q)}{p}+\frac{4L^4(2\omega)^4}{p^3}\mathsf{E}^+(G), \qquad (48)\end{aligned}$$

where $G=\{\xi:\omega<\hat{g}(\xi)\le 2\omega\}\subseteq\mathbb{F}_p^*$, and $\omega\ge 2^{-3}\mathsf{E}^+_{4l}(Q)|Q|^{-3l}:=\rho_*$ because the sum over $\hat{g}(\xi)<\rho_*$ by (10) does not exceed

$$\frac{4\rho_*}{p^3}\cdot\sum_{x,y,z}\hat{g}(y)\hat{g}(x+z)\hat{g}(y+z)=4\rho_*g^3(0)=4\rho_*|Q|^{3l}.$$

Further in view of the Parseval identity, we see that

$$\omega^2|G|\le\sum_{\xi\in G}\hat{g}(\xi)^2\le p\mathsf{E}^+_{2l}(Q), \qquad (49)$$

and by (10),

$$\omega|G|\le\sum_{\xi\in G}\hat{g}(\xi)=pg(0)=p|Q|^l. \qquad (50)$$

Clearly, $G$ is a $\Gamma$-invariant set (again, this is the crucial point of the proof). Further returning to (48) and applying Lemma 9, we see that

$$\mathsf{E}^+_{4l}(Q) \le \frac{4\mathsf{E}^+_l(Q)\mathsf{E}^+_{3l}(Q)}{p} + \frac{2^6L^4\omega^4}{p^3}\mathsf{E}^+(G) \le \frac{4\mathsf{E}^+_l(Q)\mathsf{E}^+_{3l}(Q)}{p} + \frac{2^6C_*L^4\omega^4}{p^3}\Bigl(\frac{|G|^4}{p} + \frac{|G|^3}{|\Gamma|^{1/2}}\Bigr)$$
$$= \frac{4\mathsf{E}^+_l(Q)\mathsf{E}^+_{3l}(Q)}{p} + \mathsf{E}'_{4l}(Q).$$

Applying (49) and (50), we get

$$\mathsf{E}'_{4l}(Q) \le 2^6C_*L^4|Q|^{4l} + \frac{2^6C_*L^4(\omega|G|)^2\omega^2|G|}{|\Gamma|^{1/2}p^3} \le 2^6C_*L^4|Q|^{4l} + 2^6C_*L^4|Q|^{2l}\mathsf{E}^+_{2l}(Q)|\Gamma|^{-1/2}.$$

It follows that

$$\mathsf{E}^+_{4l}(Q) \le \frac{4\mathsf{E}^+_l(Q)\mathsf{E}^+_{3l}(Q)}{p} + 2^6C_*L^4|Q|^{2l}\mathsf{E}^+_{2l}(Q)\Bigl(\frac{|Q|^{2l}}{\mathsf{E}^+_{2l}(Q)} + \frac{1}{|\Gamma|^{1/2}}\Bigr). \qquad (51)$$

Further estimating the first term of (51) very roughly as

$$\frac{\mathsf{E}^+_l(Q)\mathsf{E}^+_{3l}(Q)}{p} \le \frac{|Q|^{l+1}\mathsf{E}^+_{3l}(Q)}{p} \le \frac{|Q|^{2l+1}\mathsf{E}^+_{2l}(Q)}{p},$$

we get in view of our condition $|Q|^2|\Gamma| \le p^2$ that this term is less than $L^4|Q|^{2l}\mathsf{E}^+_{2l}(Q)|\Gamma|^{-1/2}$. Hence

$$\mathsf{E}^+_{4l}(Q) \le 2^7C_*L^4|Q|^{2l}\mathsf{E}^+_{2l}(Q)\Bigl(\frac{|Q|^{2l}}{\mathsf{E}^+_{2l}(Q)} + \frac{1}{|\Gamma|^{1/2}}\Bigr). \qquad (52)$$

Notice that the term $|Q|^{2l}/\mathsf{E}^+_{2l}(Q) + 1/|\Gamma|^{1/2} \le 2\cdot\max\{|Q|^{2l}/\mathsf{E}^+_{2l}(Q), 1/|\Gamma|^{1/2}\} \le 2$. Applying bound (52) exactly $0 \le s \le k$ times, where $s$ is the maximal number (if it exists) such that the second term $1/|\Gamma|^{1/2}$ in (52) dominates, we obtain

$$\mathsf{E}^+_{2^{k+1}}(Q) \le (2^8C_*)^sL^{4s}|\Gamma|^{-s/2}|Q|^{2^k+\ldots+2^{k-s+1}}\mathsf{E}^+_{2^{k-s+1}}(Q)\Bigl(\frac{|Q|^{2^{k-s+1}}}{\mathsf{E}^+_{2^{k-s+1}}(Q)} + \frac{1}{|\Gamma|^{1/2}}\Bigr). \qquad (53)$$

Now by the definition of $s$, we see that the first term in (53) dominates. Hence, using (51), (52) one more time (if $s < k$), we get

$$\mathsf{E}^+_{2^{k+1}}(Q) \le 2(2^8C_*)^sL^{4s}|\Gamma|^{-s/2}|Q|^{2^{k+1}-2^{k-s+1}}\cdot|Q|^{2^{k-s+1}} = 2(2^8C_*)^sL^{4s}|\Gamma|^{-s/2}|Q|^{2^{k+1}}. \qquad (54)$$

From the assumption $|\Gamma|^{(k+2)/2} \ge |Q|\log^{4k}|Q|$, it follows that $|\Gamma| \ge |Q|^{2/(k+2)}\log^{8k/(k+2)}|Q|$. Hence bound (54) is much better than (39) if $s < k$. If $s = k$, then by the same calculations, we derive

$$\mathsf{E}^+_{2^{k+1}}(Q) \le (2^8C_*)^kL^{4k}|\Gamma|^{-k/2}\mathsf{E}^+_2(Q)|Q|^{2^{k+1}-2}.$$

Since $|Q|^2|\Gamma| \le p^2$ by Lemma 9, it follows that $\mathsf{E}^+(Q) \le 2C_*|Q|^3/|\Gamma|^{1/2}$ and hence

$$\mathsf{E}^+_{2^{k+1}}(Q) \le (2^8C_*)^{k+1}L^{4k}|\Gamma|^{-(k+1)/2}|Q|^{2^{k+1}+1}.$$

Further by the choice of $k$, namely, $|\Gamma|^{(k+2)/2} \ge |Q|\log^{4k}|Q|$ we see that the last bound is better than (39). Finally, if $s=0$, then by definition $\mathsf{E}^+_{2^k}(Q) \le |Q|^{2^k}|\Gamma|^{1/2}$ and hence $\mathsf{E}^+_{2^{k+1}}(Q) \le |Q|^{2^{k+1}}|\Gamma|^{1/2}$. $\square$

**Remark 19.** From the second part of the arguments above one can derive explicit bounds for the energies $\mathsf{E}^+_s(Q)$ for small $s$. For example,

$$\mathsf{E}_4(Q) \ll \frac{|Q|^2\mathsf{E}_3(Q)}{p} + (\log|\Gamma|)^4|Q|^4 + (\log|\Gamma|)^4|Q|^2\mathsf{E}(Q)|\Gamma|^{-1/2}.$$

Now we obtain a uniform upper bound for the size of the intersection of an additive shift of any $\Gamma$-invariant set. Our bound (56) is especially effective if the sizes of $Q_1, Q_2$ are comparable with the size of $\Gamma$, namely, $|Q_1|, |Q_2| \ll |\Gamma|^C$, where $C$ is an absolute constant (which can be large). In this case the number $k$ below is a constant as well.

**Corollary 20.** *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| \ge p^\delta$, $\delta > 0$, and $Q_1, Q_2 \subseteq \mathbb{F}_p^*$ be two sets with $Q_1\Gamma = Q_1$, $Q_2\Gamma = Q_2$, $|Q_1|^2|\Gamma| \le p^2$, $|Q_2|^2|\Gamma| \le p^2$. Put $Q = \max\{|Q_1|, |Q_2|\}$. Then for any $x \ne 0$, one has*

$$|Q_1 \cap (Q_2 + x)| \ll \sqrt{|Q_1||Q_2|}\log Q \cdot p^{-\delta/2^{7+2\delta^{-1}}}. \qquad (55)$$

*Further choose $k \ge 1$ such that $|\Gamma|^{(k+2)/2} \ge Q\log^{4k} Q$. Then, for an arbitrary $x \ne 0$,*

$$|Q_1 \cap (Q_2 + x)| \ll \sqrt{|Q_1||Q_2|}\cdot|\Gamma|^{-1/4\cdot 2^{-k}}. \qquad (56)$$

*Proof.* From the conditions $|Q_1|^2|\Gamma| \le p^2$, $|Q_2|^2|\Gamma| \le p^2$, it follows that $|\Gamma| \le p^{2/3}$. Put $L = \log Q$. On the one hand, applying the Cauchy–Schwarz inequality, we obtain

$$\sum_y r^{2^{k+1}}_{Q_1-Q_2}(y) \le (\mathsf{E}^+_{2^{k+1}}(Q_1))^{1/2}(\mathsf{E}^+_{2^{k+1}}(Q_2))^{1/2}.$$

On the other hand, by formula (37) of Theorem 18 and $\Gamma$-invariance of $Q_1$, $Q_2$, we have

$$\begin{aligned}|\Gamma||Q_1 \cap (Q_2+x)|^{2^{k+1}} &\le \sum_y r^{2^{k+1}}_{Q_1-Q_2}(y)\\ &\le 2^{2^{k+2}+3}L^{2^{k+1}}(|Q_1||Q_2|)^{2^k}(2^{4k+6}L^4 + 16^{k^2}C_*^{k-1}L^{4(k-1)}\cdot|\Gamma|^{-\frac{k+1}{2}}p),\end{aligned}$$

provided $2^{64k}C_*^4 \le |\Gamma|$. As in Corollary 16 choosing $k = \lceil 2\log p/\log|\Gamma| + 4\rceil \le 2/\delta + 5$ and applying an analogue of (36) which holds for large $p$, namely,

$$\frac{pL^{4(k-1)}}{|\Gamma|^{k/2}} \ll 1$$

we obtain

$$\begin{aligned}|Q_1 \cap (Q_2+x)| &\ll L\sqrt{|Q_1||Q_2|}\cdot(|\Gamma|^{-1/2^{k+2}} + |\Gamma|^{-1/2^{k+2}})\\ &\ll L\sqrt{|Q_1||Q_2|}|\Gamma|^{-1/2^{k+2}} \ll L\sqrt{|Q_1||Q_2|}p^{-\delta/2^{7+2\delta^{-1}}},\end{aligned}$$

and it easy to ensure that inequality $2^{64k}C_*^4 \le |\Gamma|$ takes place for sufficiently large $p$.

To derive (56), we just use the second formula (39) of Theorem 18 and the previous calculations. $\square$

**Remark 21.** It is known (see, e.g., [Konyagin and Shparlinski 1999]) that if $\Gamma \subseteq \mathbb{F}_p^*$ is a multiplicative subgroup with $|\Gamma| < p^{3/4}$, then for any $x \neq 0$ one has $|\Gamma \cap (\Gamma + x)| \ll |\Gamma|^{2/3}$ and this bound is tight in some regimes. One can extend this to larger $\Gamma$-invariant sets and obtain a lower bound of a comparable quality. It gives a lower estimate in (55).

Indeed, let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup with $|\Gamma| < p^{1/2}$. Consider $R = R[\Gamma]$ and $Q = Q[\Gamma]$. It was proved in [Shkredov 2016b] that $|R| \gg |\Gamma|^2/\log|\Gamma|$ and one can check that $R = 1 - R$; see, e.g., [Murphy et al. 2017]. Finally, the set $Q$ is $\Gamma$-invariant and it is easy to check [Shkredov 2016a] that $|Q| \leq |\Gamma|^3$. Hence

$$|Q \cap (1-Q)| \geq |R| \gg \frac{|\Gamma|^2}{\log|\Gamma|} \gg \frac{|Q|^{2/3}}{\log|Q|}.$$

Also, notice that if $|\Gamma| < p^{1/2}$ and $|Q[\Gamma]|^2|\Gamma| \leq p^2$, then $|Q[\Gamma]| \gg |\Gamma|^{2+c}$ for some $c > 0$; see the first part of Corollary 35 from the next section.

Corollary 20 gives a nontrivial upper bound for the common additive energy of an arbitrary invariant set and *any* subset of $\mathbb{F}_p$.

**Corollary 22.** *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| \geq p^\delta$, $\delta > 0$, and $Q \subseteq \mathbb{F}_p^*$ be a set with $Q\Gamma = Q$, $|Q|^2|\Gamma| \leq p^2$. Then for any set $A \subseteq \mathbb{F}_p$, one has*

$$\mathsf{E}^+(A,Q) \ll |Q||A|^2 \cdot p^{-\delta/2^{7+2\delta^{-1}}} \log|Q| + |A||Q|. \tag{57}$$

*Further, for an arbitrary $\alpha \neq 0$,*

$$\mathsf{E}^\times(A,Q+\alpha) \ll |Q||A|^2 \cdot p^{-\delta/2^{7+2\delta^{-1}}} \log|Q| + |A||Q|. \tag{58}$$

*In particular,*

$$|A+Q| \gg |Q| \cdot \min\{|A|, p^{\frac{\delta}{2^{7+2\delta^{-1}}}} \log^{-1}|Q|\}, \tag{59}$$

*and*

$$|A(Q+\alpha)| \gg |Q| \cdot \min\{|A|, p^{\frac{\delta}{2^{7+2\delta^{-1}}}} \log^{-1}|Q|\}. \tag{60}$$

*If $k \geq 1$ is chosen as $|\Gamma|^{(k+2)/2} \geq |Q|\log^{4k}|Q|$, then one can replace the quantity $p^{\frac{\delta}{2^{7+2\delta^{-1}}}} \log^{-1}|Q|$ above by $|\Gamma|^{-1/4\cdot 2^{-k}}$.*

*Proof.* Inequalities (59), (60) follow from (57), (58) via the Cauchy–Schwarz inequality, so it is enough to obtain the required upper bound for the additive energy of $A$ and $Q$ and for the multiplicative energy of $A$ and $Q+\alpha$. By Corollary 20, we have

$$\mathsf{E}^+(A,Q) = \sum_x r_{A-A}(x) r_{Q-Q}(x) = |A||Q| + \sum_{x\neq 0} r_{A-A}(x) r_{Q-Q}(x)$$
$$\ll |A||Q| + |Q||A|^2 \cdot p^{-\delta/2^{7+2\delta^{-1}}} \log|Q|,$$

as required. Similarly

$$\mathsf{E}^\times(A,Q+\alpha) \ll |A||Q| + \sum_{x\neq 0,1} r_{A/A}(x) r_{(Q+\alpha)/(Q+\alpha)}(x) \ll |A||Q| + |Q||A|^2 \cdot p^{-\delta/2^{7+2\delta^{-1}}} \log|Q|,$$

because in view of Corollary 20 one has

$$r_{(Q+\alpha)/(Q+\alpha)}(x) = |Q \cap (xQ + \alpha(x-1))| \ll |Q| \cdot p^{-\delta/2^{7+2\delta^{-1}}} \log |Q|.$$

So, we have obtained bounds (57)–(60) with $p^{\frac{\delta}{2^{7+2\delta^{-1}}}} \log^{-1} |Q|$, and to replace it by $|\Gamma|^{-1/4\cdot 2^{-k}}$ one should use the second part of Corollary 20. □

From (59) one can obtain that for any multiplicative subgroup $\Gamma \subseteq \mathbb{F}_p^*$ there is $N$ such that $N\Gamma = \mathbb{F}_p$ and $N \ll \delta^{-1}4^{\delta^{-1}}$. The results of comparable quality were obtained in [Glibichuk and Konyagin 2007].

## 5. The proof of the main result

In this section we obtain an upper bound for $\mathsf{T}_k^+(A)$ (see Theorem 23) and an upper bound for $\mathsf{E}_k^+(A)$ (see Theorem 27) in the case when the size of the product set $AB$ is small comparable to $A$, where $B$ is a sufficiently large set. From the last result we derive our quantitative asymmetric sum-product Theorem 5 from the introduction. Let us begin with an upper bound for $\mathsf{T}_k^+(A)$.

**Theorem 23.** *Let $A, B \subseteq \mathbb{F}_p$ be sets, $M \geq 1$ be a real number, and $|AB| \leq M|A|$, $|A| > 1$. Then for any $k \geq 2$, $2^{16k} M^{2^{k+1}} C_*^2 \log^8 |A| \leq |B|$, one has*

$$\mathsf{T}_{2^k}^+(A) \leq 2^{4k+6} C_* \log^4 |A| \cdot \frac{M^{2^k} |A|^{2^{k+1}}}{p} + 16^{k^2} C_*^{k-1} M^{2^{k+1}} \log^{4(k-1)} |A| \cdot |A|^{2^{k+1}-4} |B|^{-\frac{k-1}{2}} \mathsf{E}^+(A). \tag{61}$$

*Proof.* We have $B \neq \{0\}$ by the condition $2^{16k} M^{2^{k+1}} C_*^2 \log^8 |A| \leq |B|$, for instance. We apply the arguments and the notation of the proof of Theorem 12. Fix any $s \geq 2$ and put $L := s \log |A|$. Our intermediate aim is to prove

$$\mathsf{T}_{2s}^+(A) \leq C s^4 M^{2s} \log^4 |A| \cdot \left( \frac{|A|^{4s}}{p} + \frac{|A|^{2s}}{\sqrt{|B|}} \mathsf{T}_s^+(A) \right), \tag{62}$$

where $C = 2^5 C_*$. As in the proof of Theorem 12, we get

$$\mathsf{T}_{2s}^+(A) \leq \tfrac{4}{3} L^4 (2\Delta)^4 \mathsf{E}^+(P) + \mathcal{E},$$

where

$$\mathcal{E} \leq 4|A|^{2s-1} \mathsf{T}_s^+(A). \tag{63}$$

Further, $\Delta > \mathsf{T}_{2s}^+(A)/(16|A|^{3s})$ is a real number and $P = \{x : \Delta < r_{sA}(x) \leq 2\Delta\} \subseteq \mathbb{F}_p^*$. Moreover, we always have $|P|\Delta^2 \leq \mathsf{T}_s^+(A)$. Notice also

$$|P|\Delta \leq \sum_{x \in P} r_{sA}(x) \leq \sum_x r_{sA}(x) \leq |A|^s.$$

To proceed as in the proof of Theorem 12, we need to estimate $|PB|$. Observe that for any $x \in PB$ one has $r_{sAB}(x) \geq \Delta$. Thus, we have

$$|PB|\Delta \leq \sum_{x \in PB} r_{sAB}(x) \leq |AB|^s \leq M^s |A|^s. \tag{64}$$

Hence using Lemma 9, we obtain

$$\mathsf{E}^+(P) \le C_*\Big(\frac{M^{2s}|A|^{2s}|P|^2}{\Delta^2 p} + \frac{M^{3s/2}|A|^{3s/2}|P|^{3/2}}{\Delta^{3/2}|B|^{1/2}}\Big).$$

Hence in view of estimate (63), combining with $|P|\Delta \le |A|^s$ and $|P|\Delta^2 \le \mathsf{T}_s^+(A)$, we get

$$\begin{aligned}\mathsf{T}_{2s}^+(A) &\le \tfrac{4}{3}(16C_*)L^4\Delta^4\Big(\frac{M^{2s}|A|^{2s}|P|^2}{\Delta^2 p} + \frac{M^{3s/2}|A|^{3s/2}|P|^{3/2}}{\Delta^{3/2}|B|^{1/2}}\Big) + 4|A|^{2s-1}\mathsf{T}_s^+(A)\\
&= \tfrac{4}{3}(16C_*)L^4\Big(\frac{M^{2s}|A|^{2s}|P|^2\Delta^2}{p} + \frac{M^{3s/2}|A|^{3s/2}|P|^{3/2}\Delta^{5/2}}{|B|^{1/2}}\Big) + 4|A|^{2s-1}\mathsf{T}_s^+(A)\\
&\le \tfrac{4}{3}(16C_*)L^4\Big(\frac{M^{2s}|A|^{4s}}{p} + \frac{M^{3s/2}|A|^{3s/2}(|P|\Delta^2)(|P|\Delta)^{1/2}}{|B|^{1/2}}\Big) + 4|A|^{2s-1}\mathsf{T}_s^+(A)\\
&\le 32C_*L^4\Big(\frac{M^{2s}|A|^{4s}}{p} + \frac{M^{3s/2}|A|^{2s}\mathsf{T}_s^+(A)}{|B|^{1/2}}\Big),\end{aligned}$$

and inequality (62) is proved. Here, we have used a trivial inequality $|B|^{1/2} \le |A|$ which follows from $|B| \le |AB| \le M|A| \le |B|^{1/2}|A|$ because $M^2 \le 2^{16k}M^{2^{k+1}}C_*^2\log^8|A| \le |B|$.

Now applying formula (62) successively $k-1$ times, we obtain

$$\begin{aligned}&\mathsf{T}_{2^k}(A)\\
&\le 2^{4k+6}C_*\log^4|A|\cdot\frac{M^{2^k}|A|^{2^{k+1}}}{p} + 16^{k^2}M^{2^{k+1}}C_*^{k-1}\log^{4(k-1)}|A|\cdot|A|^{2^{k+1}-4}|B|^{-\frac{k-1}{2}}\mathsf{E}^+(A), \quad (65)\end{aligned}$$

where the exponent $2^{k+1}-4$ comes from the sum $2^k+\dots+4$; to get the first term on the right-hand side of (65), we used $2^{16k}M^{2^{k+1}}C_*^2 \le |B|$ to ensure that $|B|^{1/2} \ge 2^{4k+1}C_*M^{2^k}\log^4|A|$. □

**Remark 24.** It is easy to see that instead of the assumption $|AB| \ll |A|$ we can assume a weaker condition $|A^s\cdot\Delta_s(B)| \ll |A|^s$, $1 < s \le 2^{k-1}$; see (64).

The same arguments work in the case of real numbers. In this situation we have no characteristic $p$ and hence we have no any restrictions on the parameter $k$.

**Theorem 25.** *Let $A, B \subset \mathbb{R}$ be finite sets, $M \ge 1$ be a real number, and $|AB| \le M|A|$. Then for any $k \ge 2$, one has*

$$\mathsf{T}_{2^k}^+(A) \le 16^{k^2}C_*^{k-1}M^{\frac{3}{2}(2^k-1)}\log^{4(k-1)}|A|\cdot|A|^{2^{k+1}-1}|B|^{-k/2}. \quad (66)$$

**Corollary 26.** *Let $A \subset \mathbb{R}$ be a finite set, $M \ge 1$ be a real number, and $|AA| \le M|A|$ or $|A/A| \le M|A|$. Then for any $k \ge 2$, one has*

$$|2^kA| \gg_k |A|^{1+k/2}M^{-3/2(2^k-1)}\cdot\log^{-4(k-1)}|A|. \quad (67)$$

Bounds of such a sort were obtained in [Konyagin 2014] by another method. The best results concerning lower bounds for multiple sum sets $kA$, $k \to \infty$ of sets $A$ with a small product/quotient set can be found in [Bush and Croot 2014].

To obtain an analogue of Theorem 18 for sets with $|AA| \ll |A|$, we cannot use the same arguments as in Section 4 because the spectrum is not an invariant set in this case. Moreover, in $\mathbb{R}$ there is an additional difficulty with using Fourier transform: the dual group of $\mathbb{R}$ does not coincide with $\mathbb{R}$ of course. That is why we suggest another method which works in "physical space" but not in the dual group.

To formulate our main result about $\mathsf{E}^+_k(Q)$ for sets $Q$ with small product $Q\Gamma$ for some relatively large set $\Gamma$ we need some notation. Let us write $Q^{(k)} = |Q\Gamma^{k-1}|$ for $k \ge 1$ and $Q^{(k)} = |Q|$ for $k = -1$.

**Theorem 27.** *Let $\Gamma, Q \subseteq \mathbb{F}_p$ be two sets, and $k \ge 0$ be an integer. Suppose that $|Q\Gamma^{k+1}||Q\Gamma^k||\Gamma| \le p^2$; further $Q^{(k)}|\Gamma| \le p$, and $M = |Q\Gamma^{k+1}|/|Q|$. Then either*

$$\mathsf{E}^+_{2^{k+1}}(Q) \le (M^{2^k+1}2^{3k+1}C_*^{(k+4)/4}\log^k Q^{(k)})\cdot|Q|^{2^{k+1}+1}|\Gamma|^{-k/8-1/2} \qquad (68)$$

*or*

$$\mathsf{E}^+_{2^{k+1}}(Q) \le 2(Q^{(k)})^{2^{k+1}}.$$

*In particular, if we choose $k$ such that $|\Gamma|^{k/8+1/2} \ge |Q|\cdot M^{2^k+1}2^{3k+1}C_*^{(k+4)/4}\log^k Q^{(k)}$, then*

$$\mathsf{E}^+_{2^{k+1}}(Q) \le 2(Q^{(k)})^{2^{k+1}}. \qquad (69)$$

*Proof.* Without loss of generality one can assume that $0 \notin \Gamma$. Fix an integer $l \ge 1$ and prove that either

$$\mathsf{E}^+_{5l/2}(Q) \le 8C_*^{1/4}\log|Q|\cdot|Q|^{l/2}\mathsf{E}^+_{2l}(Q\Gamma)|\Gamma|^{-1/8} \qquad (70)$$

or

$$\mathsf{E}^+_{5l/2}(Q) \le 2|Q|^{5l/2}. \qquad (71)$$

Put $g(x) = r^l_{Q-Q}(x)$, $L = \log|Q|$, and $\mathsf{E}'_{5l/2}(Q) = \mathsf{E}^+_{5l/2}(Q) - |Q|^{5l/2} \ge 0$. We will assume below that $\mathsf{E}'_{5l/2}(Q) \ge 2^{-1}\mathsf{E}^+_{5l/2}(Q)$ because otherwise we obtain (71) immediately. Using the Dirichlet principle, we find a set $P$ and a positive number $\Delta$ such that $P = \{x : \Delta < g(x) \le 2\Delta\} \subseteq \mathbb{F}_p^*$ and

$$\mathsf{E}'_{5l/2}(Q) \le L\sum_{x\in P} r^{5l/2}_{Q-Q}(x).$$

Applying Corollary 11, we obtain

$$\mathsf{E}'_{5l/2}(Q) \le L(2\Delta)^{3/2}\sum_{x\in P} r^l_{Q-Q}(x) \le 3C_*^{1/4}L\Delta^{3/2}|Q|^{l/2}(\mathsf{E}^+_{2l}(Q\Gamma))^{1/4}\left(\frac{|P|^4}{p}+\frac{|P|^3}{|\Gamma|^{1/2}}\right)^{1/4}$$
$$\le 3C_*^{1/4}L|Q|^{l/2}(\mathsf{E}^+_{2l}(Q\Gamma))^{1/4}\left(\frac{\Delta^6|P|^4}{p}+\frac{\Delta^6|P|^3}{|\Gamma|^{1/2}}\right)^{1/4}.$$

We have $\Delta|P| \le \mathsf{E}^+_l(Q)$, $\Delta^2|P| \le \mathsf{E}^+_{2l}(Q)$ and hence $\Delta^6|P|^4 \le (\mathsf{E}^+_{2l}(Q))^2(\mathsf{E}^+_l(Q))^2$. It follows that

$$\mathsf{E}'_{5l/2}(Q) \le 3C_*^{1/4}L|Q|^{l/2}(\mathsf{E}^+_{2l}(Q\Gamma))^{1/4}\left(\frac{(\mathsf{E}^+_{2l}(Q))^2(\mathsf{E}^+_l(Q))^2}{p}+\frac{(\mathsf{E}^+_{2l}(Q))^3}{|\Gamma|^{1/2}}\right)^{1/4}.$$

To prove that the first term $(\mathsf{E}^+_{2l}(Q))^2(\mathsf{E}^+_l(Q))^2/p$ is less than $(\mathsf{E}^+_{2l}(Q))^3/|\Gamma|^{1/2}$, we need to check that

$$(\mathsf{E}^+_l(Q))^2|\Gamma|^{1/2} \le \mathsf{E}^+_{2l}(Q)p.$$

But using the Hölder inequality, we see that the required estimate follows from

$$(\mathsf{E}^+_l(Q))^2|\Gamma|^{1/2} \le (\mathsf{E}^+_{2l}(Q))^{\frac{2(l-1)}{2l-1}}|Q|^{\frac{4l}{2l-1}}|\Gamma|^{1/2} \le \mathsf{E}^+_{2l}(Q)p$$

or, in other words, from

$$|Q|^{4l}|\Gamma|^{(2l-1)/2} \le \mathsf{E}^+_{2l}(Q)p^{2l-1}. \qquad (72)$$

Finally, we can suppose that for any $s \ge 2$ one has, say,

$$\mathsf{E}^+_s(Q) \ge |Q|^{s+1}|\Gamma|^{-1/8\log s - 1/2},$$

because otherwise estimate (68) follows easily. Our assumption $Q^{(k)}|\Gamma| \le p$ implies that $|Q||\Gamma| \le p$ and whence

$$|Q|^{2l-1}|\Gamma|^{\frac{1}{8}\log 2l + l} \le p^{2l-1}|\Gamma|^{1+1/8\log 2l - l} \le p^{2l-1},$$

and thus (72) takes place for $l \ge 2$. For $l = 1$, see the calculations below. Hence under this assumption and the inequality $\mathsf{E}'_{5l/2}(Q) \ge 2^{-1}\mathsf{E}^+_{5l/2}(Q)$, we have

$$\mathsf{E}^+_{5l/2}(Q) \le 8C_*^{1/4}\log|Q|\cdot|Q|^{l/2}\mathsf{E}^+_{2l}(Q\Gamma)|\Gamma|^{-1/8}$$

and we have proved (70). Trivially, it implies that

$$\mathsf{E}^+_{4l}(Q) \le 8C_*^{1/4}\log|Q|\cdot|Q|^{2l}\mathsf{E}^+_{2l}(Q\Gamma)|\Gamma|^{-1/8}$$

and subsequently using this bound, we obtain

$$\begin{aligned}\mathsf{E}^+_{2^k+1}(Q) &\le (2^{3k}C_*^{k/4}\log^k|Q\Gamma^{k-1}|)\cdot M^{2^{k-1}+\cdots+2}|Q|^{2^k+\cdots+2}\mathsf{E}^+(Q\Gamma^k)|\Gamma|^{-k/8}\\ &= (2^{3k}M^{2^k-2}C_*^{k/4}\log^k|Q\Gamma^{k-1}|)\cdot|Q|^{2^{k+1}-2}\mathsf{E}^+(Q\Gamma^k)|\Gamma|^{-k/8}.\end{aligned}$$

At the last step, we need to check $|Q\Gamma^{k-1}||\Gamma| \le p$, and it is guaranteed by our assumption $Q^{(k)}|\Gamma| \le p$ (for $k = -1$ we just need $|Q||\Gamma| \le p$). Now recalling the assumption $|Q\Gamma^{k+1}||Q\Gamma^k||\Gamma| \le p^2$ and applying Lemma 9, we get

$$\mathsf{E}^+_{2^k+1}(Q) \le (M^{2^k+1}2^{3k+1}C_*^{(k+4)/4}\log^k|Q\Gamma^{k-1}|)\cdot|Q|^{2^{k+1}+1}|\Gamma|^{-k/8-1/2}.$$

In particular, this final step covers the remaining case $l = 1$ above. □

**Remark 28.** Let $\Gamma$ be a multiplicative subgroup and $Q\Gamma = Q$. Then by Theorem 27 if $|Q||\Gamma| \le p$ and a number $k_1$ is chosen as $|\Gamma|^{k_1/8+1/2} \ge |Q|\log^{k_1}|Q|$, then $\mathsf{E}^+_{2^{k_1}+1}(Q) \ll_{k_1} |Q|^{2^{k_1}+1}$. Let us compare this with Theorem 18. By the second part of this result (see condition (38)), choosing $k_2$ such that $|\Gamma|^{(k_2+2)/2} \ge |Q|\log^{4k_2}|Q|$, we get $\mathsf{E}^+_{2^{k_2}+1}(Q) \ll_{k_2} |Q|^{2^{k_2}+1}|\Gamma|^{1/2}$. After that applying the second part of Corollary 20 $n := 2^{k_2+1}$ times, we obtain

$$\begin{aligned}\mathsf{E}^+_{2^{2k_2+2}}(Q) &\ll_{k_2} |Q|^{2^{2k_2+2}} + \mathsf{E}^+_{2^{k_2}+1}(Q)(|Q||\Gamma|^{-1/4\cdot 2^{-k_2}})^n\\ &\ll_{k_2} |Q|^{2^{2k_2+2}} + |Q|^{2^{k_2}+1}|\Gamma|^{1/2}|Q|^n|\Gamma|^{-1/2} \ll |Q|^{2^{2k_2+2}}.\end{aligned}$$

Thus, Theorem 18 gives a slightly better bound (in the case of multiplicative subgroups), but of the same form.

**Remark 29.** From formula (40), it follows that for any $l$ one has $\mathsf{E}^+_l(Q) \geq |Q|^{2l}/p^{l-1}$. Hence the upper bound (69) has a place just for small sets $Q$. For example, taking the smallest possible $l = 2$ and comparing $|Q|^2$ with $|Q|^4/p$ we see that the condition $|Q| < \sqrt{p}$ is enough. If $Q = Q\Gamma$, where $\Gamma$ is a multiplicative subgroup, then it is possible to refine this condition because in the proof of Theorem 18 another method (the Fourier approach) was used. We did not make such calculations.

Now we can obtain analogues of Corollaries 20 and 22.

**Corollary 30.** *Let $\Gamma, Q_1, Q_2 \subseteq \mathbb{F}_p$ be sets. Take $k \geq 0$ such that for $j = 1, 2$, one has*

$$|Q_j\Gamma^{k+2}||Q_j\Gamma^{k+1}||\Gamma| \leq p^2, \quad |Q_j\Gamma^k||\Gamma| \leq p, \quad |Q_j\Gamma| \leq M_*|Q_j|, \quad |Q_j\Gamma^{k+2}| \leq M|Q_j|,$$

*and*

$$|\Gamma|^{k/8+1/2} \geq |Q_j| \cdot M_* M^{2^k+1} 2^{3k+1} C_*^{(k+4)/4} \log^k |Q_j\Gamma^k|. \tag{73}$$

*Then, for any $x \neq 0$,*

$$|Q_1 \cap (Q_2 + x)| \leq 2M_* M \sqrt{|Q_1||Q_2|} \cdot |\Gamma|^{-1/2\,(2^{-k})}. \tag{74}$$

*Proof.* Denote by $\rho$ the quantity $|Q_1 \cap (Q_2 + x)|$. On the one hand, applying the Cauchy–Schwarz inequality and the second part of Theorem 27 for sets $\Gamma Q_1$ and $\Gamma Q_2$, we obtain

$$\begin{aligned}\sum_y r^{2^k+1}_{\Gamma Q_1 - \Gamma Q_2}(y) &\leq (\mathsf{E}^+_{2^k+1}(\Gamma Q_1))^{1/2} (\mathsf{E}^+_{2^k+1}(\Gamma Q_2))^{1/2} \\ &\leq 2^{3k+2} M^{2^k+1} (|Q_1\Gamma||Q_2\Gamma|)^{2^k} \leq 2^{3k+2} M^{2^k+1} M_*^{2^k+1} (|Q_1||Q_2|)^{2^k}.\end{aligned}$$

On the other hand, it is easy to see that for any $y \in \Gamma x$ one has $r_{\Gamma Q_1 - \Gamma Q_2}(y) \geq \rho$. Thus,

$$\rho^{2^k+1} |\Gamma| \leq 2^{3k+2} M^{2^k+1} M_*^{2^k+1} (|Q_1||Q_2|)^{2^k},$$

and hence

$$\rho \leq 2M_* M \sqrt{|Q_1||Q_2|} \cdot |\Gamma|^{-1/2(2^{-k})}.$$

Here we have used the inequality $k \geq 5$, which easily follows from $|\Gamma| \leq |Q_j\Gamma| \leq M|Q_j|$ and (73). $\square$

In the next two corollaries we show how to replace the condition $|Q\Gamma^k| \ll |Q|$ with a condition with a single multiplication, namely, $|Q\Gamma| \ll |Q|$.

**Corollary 31.** *Let $\Gamma, Q$ be subsets of $\mathbb{F}_p$, $M \geq 1$ be a real number, $|Q\Gamma| \leq M|Q|$. Suppose that for $k \geq 1$ one has $(2M)^{k+1}|Q||\Gamma| \leq p$, and*

$$|\Gamma|^{k/8+1/2} \geq |Q| \cdot (2M)^{(k+3)2^k} C_*^{(k+4)/4} \log^k((2M)^k |Q|). \tag{75}$$

*Then, for any $A \subseteq \mathbb{F}_p$,*

$$|A + Q| \geq 2^{-3}|Q| \cdot \min\{|A|, 2^{-(4+k)} M^{-(k+3)} |\Gamma|^{\frac{1}{2}2^{-k}}\}, \tag{76}$$

*and for any $\alpha \neq 0$,*

$$|A(Q + \alpha)| \geq 2^{-3}|Q| \cdot \min\{|A|, 2^{-(4+k)} M^{-(k+3)} |\Gamma|^{\frac{1}{2}2^{-k}}\}. \tag{77}$$

*Proof.* Using Lemma 7, find a set $X \subseteq Q$, $|X| \geq |Q|/2$ such that, for any $l$,

$$|X\Gamma^l| \leq (2M)^l |X|. \qquad (78)$$

Also, notice that $|X\Gamma| \leq |Q\Gamma| \leq 2M|X|$. We apply Corollary 30 with $M$ replacing by $(2M)^{k+2}$, $M_* = 2M$ and see that, for any $x \neq 0$,

$$|Q_1 \cap (Q_2 + x)| \leq 2^{k+4} M^{k+3} \sqrt{|Q_1||Q_2|} \cdot |\Gamma|^{-1/2\,(2^{-k})}.$$

Here, $Q_1 = X$ and $Q_2 = X$ or $Q_2 = \alpha X$. We will check the condition $|Q_j\Gamma^{k+2}||Q_j\Gamma^{k+1}||\Gamma| \leq p^2$ of Corollary 30 later and notice that the assumptions $|Q_j\Gamma^k||\Gamma| \leq p$, $|Q_j\Gamma| \leq M_*|Q_j|$, $|Q_j\Gamma^{k+2}| \leq M|Q_j|$ easily follow from (78) and our condition $(2M)^{k+1}|Q||\Gamma| \leq p$. Now using the arguments from Corollary 22, we estimate the energies $\mathsf{E}^+(A, X)$, $\mathsf{E}^\times(A, X+\alpha)$. In particular, we obtain lower bounds for the sum set from (76) and the product set from (77). It remains to check condition $(2M)^{2k+3}|Q|^2|\Gamma| \leq p^2$. But it follows from $(2M)^{k+1}|Q||\Gamma| \leq p$ if $M \leq |\Gamma|/2$. The last inequality is a simple consequence of (75). $\square$

Now we prove an analogue of Corollary 30 where we require that $|Q_j\Gamma|$, $j = 1, 2$ are small comparable to $|Q_j|$. For simplicity, we formulate the next corollary in the situation $|Q'| = |Q|$, but of course the general bound takes place as well.

**Corollary 32.** *Let $\Gamma, Q, Q'$ be subsets of $\mathbb{F}_p$, $|Q'| = |Q|$, $M \geq 1$ be a real number, $|Q\Gamma|, |Q'\Gamma| \leq M|Q|$. Suppose that for $k \geq 1$ one has $(2M)^{k+1}|Q||\Gamma| \leq p$, and*

$$|\Gamma|^{\frac{k}{8} + \frac{1}{2(k+4)}} \geq |Q| \cdot M^{(k+3)2^k} C_*^{(k+4)/4} \log^k(|\Gamma|^{\frac{k}{2(k+4)} 2^{-k}} |Q|)$$

*Then for any $x \neq 0$ one has*

$$|Q \cap (Q' + x)| \leq 4M|Q| \cdot |\Gamma|^{-\frac{1}{2(k+4)} 2^{-k}}. \qquad (79)$$

*Proof.* Let $\tilde{Q} = Q \cap (Q' + x)$. Then $|\tilde{Q}\Gamma| \leq |Q\Gamma| \leq M|Q| = M|Q|/|\tilde{Q}| \cdot |\tilde{Q}| := \tilde{M}|\tilde{Q}|$. Similarly, $|(\tilde{Q} - x)\Gamma| \leq |Q'\Gamma| \leq M|Q|$. Applying the second part of Corollary 31 with $\alpha = x$, $Q = \tilde{Q}$, $A = \Gamma$, and $M = \tilde{M}$, we get

$$M|Q| \geq |(\tilde{Q} - x)\Gamma| \geq 2^{-(7+k)} |\tilde{Q}| \tilde{M}^{-(k+3)} |\Gamma|^{\frac{1}{2} 2^{-k}} = 2^{-(7+k)} M^{-(k+3)} |\tilde{Q}|^{k+4} |Q|^{-(k+3)} |\Gamma|^{\frac{1}{2} 2^{-k}}$$

provided

$$\begin{aligned} |\Gamma|^{k/8 + 1/2} &\geq |Q| \cdot (2\tilde{M})^{(k+3)2^k} C_*^{(k+4)/4} \log^k((2\tilde{M})^k |Q|) \\ &\geq |\tilde{Q}| \cdot (2\tilde{M})^{(k+3)2^k} C_*^{(k+4)/4} \log^k((2\tilde{M})^k |\tilde{Q}|). \end{aligned}$$

This gives us

$$|\tilde{Q}| \leq 4M|Q| \cdot |\Gamma|^{-\frac{1}{2(k+4)} 2^{-k}}. \qquad (80)$$

Now if the last inequality does not hold, then

$$M|Q|/\tilde{M} = |\tilde{Q}| \geq 4M|Q| \cdot |\Gamma|^{-\frac{1}{2(k+4)} 2^{-k}}$$

and thus $\tilde{M} \leq |\Gamma|^{\frac{1}{2(k+4)}2^{-k}}/4$. Hence the condition

$$|\Gamma|^{\frac{k}{8}+\frac{1}{2(k+4)}} \geq |Q| \cdot M^{(k+3)2^k} C_*^{(k+4)/4} \log^k (|\Gamma|^{\frac{k}{2(k+4)}2^{-k}}|Q|)$$

is enough. □

Now we are ready to prove the main asymmetric sum-product result of this section.

**Corollary 33.** *Let $A, B, C \subseteq \mathbb{F}_p$ be arbitrary sets, and $k \geq 1$ be such that $|A||B|^{1+\frac{k+1}{2(k+4)}2^{-k}} \leq p$ and*

$$|B|^{\frac{k}{8}+\frac{1}{2(k+4)}} \geq |A| \cdot C_*^{(k+4)/4} \log^k (|A||B|). \tag{81}$$

*Then*

$$\max\{|AB|, |A+C|\} \geq 2^{-3}|A| \cdot \min\{|C|, |B|^{\frac{1}{2(k+4)}2^{-k}}\}, \tag{82}$$

*and for any $\alpha \neq 0$,*

$$\max\{|AB|, |(A+\alpha)C|\} \geq 2^{-3}|A| \cdot \min\{|C|, |B|^{\frac{1}{2(k+4)}2^{-k}}\}. \tag{83}$$

*Moreover,*

$$|AB| + \frac{|A|^2|C|^2}{\mathsf{E}^+(A,C)} \geq 2^{-4}|A| \cdot \min\{|C|, |B|^{\frac{1}{4(k+4)}2^{-k}}\}, \tag{84}$$

*and, for any $\alpha \neq 0$, we have*

$$|AB| + \frac{|A|^2|C|^2}{\mathsf{E}^\times(A+\alpha,C)} \geq 2^{-4}|A| \cdot \min\{|C|, |B|^{\frac{1}{4(k+4)}2^{-k}}\}, \tag{85}$$

*provided*

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

*Proof.* We will prove just (82) because the same arguments hold for (83). Put $|AB| = M|A|$, $M \geq 1$, and apply Corollary 31 with $Q = A$, $\Gamma = B$, $A = C$. Supposing that

$$|B|^{k/8+1/2} \geq |A| \cdot 2^{(k+3)2^k} M^{(k+3)2^k} C_*^{(k+4)/4} \log^k ((2M)^k|A|), \tag{86}$$

we obtain

$$|A+C| \geq 2^{-3}|A| \cdot \min\{|C|, 2^{-(k+4)}M^{-(k+3)}|B|^{\frac{1}{2}2^{-k}}\}. \tag{87}$$

Put $M_0 = 2^{-2}|B|^{\frac{1}{2(k+4)}2^{-k}}$ and consider two cases: $M \geq M_0$ and $M < M_0$. If $M \geq M_0$, then there is nothing to prove. If not, then we apply (87) and obtain the same. In other words,

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

To check (86), we use $M < M_0$ and see that the inequality

$$|B|^{k/8+1/2} \geq |A| \cdot 2^{(k+3)2^k} M_0^{(k+3)2^k} C_*^{(k+4)/4} \log^k ((2M_0)^k|A|)$$

follows from our condition (81). The condition $(2M)^{k+1}|A||B| \leq p$ gives us $|A||B|^{1+\frac{k+1}{2(k+4)}2^{-k}} \leq p$.

To prove (84), (85), we use Corollary 32 instead of Corollary 31 and apply the arguments of the proof of Corollary 22. We obtain $\mathsf{E}^+(A,C), \mathsf{E}^\times(A+\alpha,C) \leq 2|A||C| + 4|A||C|^2 \cdot M \cdot |B|^{-\frac{1}{2(k+4)}2^{-k}}$. After that it remains to compare $M$ with the optimal value $M_0 = 2^{-1}|B|^{\frac{1}{4(k+4)}2^{-k}}$. □

Notice that one cannot obtain any nontrivial bounds for $\min\{\mathsf{E}^{\times}(A,B), \mathsf{E}^{+}(A,C)\}$. Just take $B$ equals a geometric progression, $C$ equals an arithmetic progression, $|B| = |C|$, and $A = B \cup C$.

**Remark 34.** The results of this section take place in $\mathbb{R}$. In this case we do not need in any conditions containing the characteristic $p$.

Corollary 33 gives us a series of examples of "superquadratic expanders" [Balog et al. 2017] with four variables, i.e., functions $f(x_1,\dots,x_n)$ such that for any finite $A \subset \mathbb{R}$ one has

$$\left|\{f(x_1,\dots,x_n) : (x_1,\dots,x_n) \in A^n\}\right| \gg |A|^{2+c},$$

where $c > 0$ is an absolute constant. The first example of such an expander with four variables was given in [Rudnev 2017a], namely the cross-ratio function

$$f(x,y,z,w) = \frac{(y-x)(w-z)}{(z-x)(w-y)}$$

(see also [Rudnev 2017b]). It would be is interesting to find an example of a rational superquadratic expander with three variables.

**Corollary 35.** *Let $\varphi : \mathbb{R} \to \mathbb{R}$ be an injective function. Then for any $\kappa < \frac{1}{40}2^{-16}$ and an arbitrary finite set $A \subset \mathbb{R}$, one has $|R[A]\varphi(A)| \gg |A|^{2+\kappa}$. In particular,*

$$R[A]A = \left\{\frac{(y-x)w}{z-x} : x,y,z,w \in A,\ x \neq z\right\}$$

*is a superquadratic expander with four variables.*

*Moreover, for any finite sets $A, B, C, D$ of equal sizes one has*

$$\left|\left\{\frac{(y-x)w}{z-x} : x \in A,\ y \in B,\ z \in C,\ w \in D,\ x \neq z\right\}\right| \gg |A|^{2+\kappa}. \tag{88}$$

*Proof.* By a result from [Jones 2013; Roche-Newton 2015], we have $|R[A]| \gg |A|^2/\log|A|$. Further $R[A] = 1 - R[A]$ and $R^{-1}[A] = R[A]$; see Remark 21. Hence applying estimate (83) of Corollary 33 with $A = R[A]$, $B = C = \varphi(A)$, and $\alpha = -1$, we obtain

$$|R[A]\varphi(A)| \gg |R[A]| \cdot |A|^{\frac{1}{2(k+4)}2^{-k}},$$

provided

$$|A|^{\frac{k}{8}+\frac{1}{2(k+4)}} \geq |R[A]| \cdot 2^{2k} C_*^{(k+4)/4} \log^k |A| \geq |R[A]| \cdot C_*^{(k+4)/4} \log^k |R[A]\varphi(A)|. \tag{89}$$

Put $|R[A]| = C|A|^{2+c}/\log|A|$, $c \geq 0$, and $C > 0$ is an absolute constant. Then taking $k = 16 + 8c$, say, we satisfy (89) for large $A$. It follows that

$$|R[A]\varphi(A)| \gg |A|^{2+c+\frac{1}{2(20+8c)}2^{-16-8c}} \log^{-1}|A|.$$

One can check that the optimal choice of $c$ is $c = 0$. Finally, to prove (88) just notice that from the method of [Jones 2013; Roche-Newton 2015] it follows that

$$\left|\left\{\frac{b-a}{c-a} : a \in A,\ b \in B,\ c \in C,\ c \neq a\right\}\right| \gg |A|^2/\log|A|$$

for any sets $A, B, C$ of equal cardinality. After that, repeat the arguments above. □

**Remark 36.** Let us show quickly how Corollary 33 implies both Theorems 1, 2 for sets $A$ with $|A| < p^{1/2-\varepsilon}$ (the appearance $\sqrt{p}$ bound was discussed in Remark 29).

Let $B, C$ be sets of sizes greater than $p^{\varepsilon}$ such that $\max\{|AB|, |A+C|\} \le p^{\delta}|A|$ or $\max\{|(A+\alpha)B|, |A+C|\} \le p^{\delta}|A|$ for some $\alpha \neq 0$. We can find sufficiently large $k = k(\varepsilon)$ such that condition (81) takes place for $B$ because $|A| < p^{1/2-\varepsilon} \le p$ and $|B| \ge p^{\varepsilon}$. Applying Corollary 33 for $A, B, C$, we arrive to a contradiction. Finally, to ensure that $|A||B|^{1+\frac{k+1}{2(k+4)}2^{-k}} \le p$ just use the assumption $|A| < p^{1/2-\varepsilon}$, inequality $|B| \le |AB| \le p^{\delta}|A|$, and take sufficiently small $\delta = \delta(\varepsilon)$ and sufficiently large $k = k(\varepsilon)$.

Let $A \subset \mathbb{R}$ be a finite set. We consider a characteristic of $A$ (see, e.g., [Shkredov 2016a]) that generalizes the notion of small multiplicative doubling of $A$. Namely, put

$$d^{+}(A) := \inf_{f} \min_{B \neq \varnothing} \frac{|f(A)+B|^2}{|A||B|},$$

where the infimum is taken over convex/concave functions $f$.

**Problem.** Suppose that $d^{+}(A) \le |A|^{\varepsilon}$ and $\varepsilon > 0$ is a small number. Is it true that there is $k = k(\varepsilon)$ such that $\mathsf{E}^{+}_{k}(A) \ll |A|^{k}$?

Notice that one cannot obtain a similar bound for $\mathsf{T}^{+}_{k}(A)$. Indeed, let $A = \{1^2, 2^2, \dots, n^2\}$. Then one can show that for such $A$, the quantity $d^{+}(A)$ is $O(1)$ (see, e.g., [Shkredov 2016a]) but, clearly, $|kA| \ll_k |A|^2$. This means that it is not possible to obtain any upper bound for $\mathsf{T}^{+}_{k}(A)$ of the form $\mathsf{T}^{+}_{k}(A) \ll |A|^{2k-2-c}$, $c > 0$, and hence any analogues of Theorems 23, 25 for sets $A$ with small $d^{+}(A)$.

## Acknowledgements

The author thanks Misha Rudnev and Sophie Stevens for careful reading of the first draft of this paper and for useful discussions. Also he thanks the referee for valuable suggestions, remarks and careful reading of our article. This work is supported by the Russian Science Foundation under grant 14-11-00433.

## References

[Balog et al. 2017] A. Balog, O. Roche-Newton, and D. Zhelezov, "Expanders with superquadratic growth", *Electron. J. Combin.* **24**:3 (2017), art. id. 3.14. MR Zbl

[Bourgain 2003] J. Bourgain, "On the Erdős–Volkmann and Katz–Tao ring conjectures", *Geom. Funct. Anal.* **13**:2 (2003), 334–365. MR Zbl

[Bourgain 2005a] J. Bourgain, "Estimates on exponential sums related to the Diffie–Hellman distributions", *Geom. Funct. Anal.* **15**:1 (2005), 1–34. MR Zbl

[Bourgain 2005b] J. Bourgain, "Exponential sum estimates over subgroups of $\mathcal{Z}_q^*$, $q$ arbitrary", *J. Anal. Math.* **97** (2005), 317–355. MR

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

[Bourgain 2007] J. Bourgain, "Exponential sum estimates in finite commutative rings and applications", *J. Anal. Math.* **101** (2007), 325–355. MR Zbl

[Bourgain and Garaev 2009] J. Bourgain and M. Z. Garaev, "On a variant of sum-product estimates and explicit exponential sum bounds in prime fields", *Math. Proc. Cambridge Philos. Soc.* **146**:1 (2009), 1–21. MR Zbl

[Bourgain et al. 2004] J. Bourgain, N. Katz, and T. Tao, "A sum-product estimate in finite fields, and applications", *Geom. Funct. Anal.* **14**:1 (2004), 27–57. MR Zbl

[Bourgain et al. 2006] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin, "Estimates for the number of sums and products and for exponential sums in fields of prime order", *J. London Math. Soc.* (2) **73**:2 (2006), 380–398. MR Zbl

[Bush and Croot 2014] A. Bush and E. Croot, "Few products, many $h$-fold sums", preprint, 2014. arXiv

[Erdős and Szemerédi 1983] P. Erdős and E. Szemerédi, "On sums and products of integers", pp. 213–218 in *Studies in pure mathematics*, edited by P. Erdős, Birkhäuser, Basel, 1983. MR

[Garaev 2010] M. Z. Garaev, "Sums and products of sets and estimates for rational trigonometric sums in fields of prime order", *Uspekhi Mat. Nauk* **65**:4 (2010), 599–658. In Russian; translated in *Russian Math. Surveys* **65**:4 (2010), 599–658. MR Zbl

[Glibichuk and Konyagin 2007] A. A. Glibichuk and S. V. Konyagin, "Additive properties of product sets in fields of prime order", pp. 279–286 in *Additive combinatorics*, edited by A. Granville et al., CRM Proc. Lecture Notes **43**, Amer. Math. Soc., Providence, RI, 2007. MR Zbl

[Jones 2013] T. G. F. Jones, "New quantitative estimates on the incidence geometry and growth of finite sets", preprint, 2013. arXiv

[Konyagin 2014] S. Konyagin, "$h$-fold sums from a set with few products", *Mosc. J. Comb. Number Theory* **4**:3 (2014), 14–20. MR Zbl

[Konyagin and Shkredov 2016] S. V. Konyagin and I. D. Shkredov, "New results on sums and products in $\mathcal{R}$", *Tr. Mat. Inst. Steklova* **294** (2016), 87–98. In Russian. MR Zbl

[Konyagin and Shparlinski 1999] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Tracts in Mathematics **136**, Cambridge University Press, 1999. MR Zbl

[Murphy et al. 2017] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev, and I. D. Shkredov, "New results on sum-product type growth over fields", preprint, 2017. arXiv

[Roche-Newton 2015] O. Roche-Newton, "A short proof of a near-optimal cardinality estimate for the product of a sum set", pp. 74–80 in *31st International Symposium on Computational Geometry*, vol. 34, edited by L. Arge, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, Germany, 2015. MR Zbl

[Roche-Newton et al. 2016] O. Roche-Newton, M. Rudnev, and I. D. Shkredov, "New sum-product type estimates over finite fields", *Adv. Math.* **293** (2016), 589–605. MR

[Rudnev 2017a] M. Rudnev, "On distinct cross-ratios and related growth problems", preprint, 2017. arXiv

[Rudnev 2017b] M. Rudnev, "On the number of incidences between points and planes in three dimensions", *Combinatorica* (2017).

[Ruzsa 2009] I. Z. Ruzsa, "Sumsets and structure", pp. 87–210 in *Combinatorial number theory and additive group theory*, edited by M. Castellet, Birkhäuser, Basel, Switzerland, 2009. MR Zbl

[Schoen and Shkredov 2013] T. Schoen and I. D. Shkredov, "Higher moments of convolutions", *J. Number Theory* **133**:5 (2013), 1693–1737. MR Zbl

[Shkredov 2013] I. D. Shkredov, "Some new inequalities in additive combinatorics", *Mosc. J. Comb. Number Theory* **3**:3-4 (2013), 189–239. MR Zbl

[Shkredov 2014] I. Shkredov, "Energies and structure of additive sets", *Electron. J. Combin.* **21**:3 (2014), art. id. 3.44. MR Zbl

[Shkredov 2016a] I. D. Shkredov, "Difference sets are not multiplicatively closed", *Discrete Anal.* (2016), art. id. 17. MR Zbl

[Shkredov 2016b] I. D. Shkredov, "On tripling constant of multiplicative subgroups", *Integers* **16** (2016), art. id. A75. MR Zbl

[Shkredov 2017] I. Shkredov, "Some remarks on the Balog–Wooley decomposition theorem and quantities $D^+$, $D^x$", *Proc. Steklov Inst. Math.* **298** (2017), 74–90.

[Shteinikov 2015] Y. N. Shteinikov, "Estimates of trigonometric sums over subgroups and some of their applications", *Math. Notes* **98**:3-4 (2015), 606–625. MR

[Szemerédi and Trotter 1983] E. Szemerédi and W. T. Trotter, Jr., "Extremal problems in discrete geometry", *Combinatorica* **3**:3-4 (1983), 381–392. MR Zbl

[Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, 2006. MR Zbl

[Yazici et al. 2017] E. A. Yazici, B. Murphy, M. Rudnev, and I. Shkredov, "Growth estimates in positive characteristic via collisions", *Int. Math. Res. Not.* **2017**:23 (2017), 7148–7189.

Received 1 Dec 2017.

ILYA D. SHKREDOV:

ilya.shkredov@gmail.com
Steklov Mathematical Institute, ul. Gubkina, 9, Moscow, Russia, 119991

and

IITP RAS, Bolshoy Karetny per. 19, Moscow, Russia, 127994

and

MIPT, Institutskii per. 9, Dolgoprudnii, Russia, 141701

# Moscow Journal of Combinatorics and Number Theory

msp.org/moscow




See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2019 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2220-5438 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

**mathematical sciences publishers**

**nonprofit scientific publishing**

http://msp.org/

Moscow Journal of Combinatorics and Number Theory
vol. 8 no. 1 2019