Труды Москов. Матем. Общ.
Том 79 (2018), вып. 2

Trans. Moscow Math. Soc.
2018, Pages 231–281
https://doi.org/10.1090/mosc/283
Article electronically published on November 29, 2018

ON ASYMPTOTIC FORMULAE IN SOME SUM–PRODUCT QUESTIONS

I. D. SHKREDOV

Abstract. In this paper we obtain a series of asymptotic formulae in the sum–product phenomena over the prime field $\mathbb{F}_p$. In the proofs we use the usual incidence theorems in $\mathbb{F}_p$, as well as the growth result in $\mathrm{SL}_2(\mathbb{F}_p)$ due to Helfgott. Here are some of our applications:

- a new bound for the number of the solutions to the equation $(a_1 - a_2)(a_3 - a_4) = (a'_1 - a'_2)(a'_3 - a'_4)$, $a_i, a'_i \in A$, A is an arbitrary subset of $\mathbb{F}_p$,
- a new effective bound for multilinear exponential sums of Bourgain,
- an asymptotic analogue of the Balog–Wooley decomposition theorem,
- growth of $p_1(b)+1/(a+p_2(b))$, where a, b runs over two subsets of $\mathbb{F}_p$, $p_1, p_2 \in \mathbb{F}_p[x]$ are two non–constant polynomials,
- new bounds for some exponential sums with multiplicative and additive characters.

1. Introduction

Let p be an odd prime number, and let $\mathbb{F}_p$ be the finite field. Having two sets $A, B \subset \mathbb{F}_p$, we define the *sumset*, the *product set* and the *quotient set* of A and B as

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

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

and

$$A/B := \{a/b \ : \ a \in A,\, b \in B,\, b \neq 0\}\,,$$

correspondingly. Our paper is devoted to the so–called *sum–product phenomenon* in $\mathbb{F}_p$ which was developed in papers [1]–[17], [27]–[44], [49]–[54], [58], [59], and in many others. This is an extensively growing area of mathematics with plenty of applications to number theory, additive combinatorics, computer science, and dynamical systems. It seems like at the moment there is "the second wave" of results and applications in this field, see, e.g., [2], [34]–[40], [44], and this wave is connected with a fundamental incidence result of Rudnev [43] (see a simple proof of his theorem in [60] and also the famous Guth–Katz [19] solution of the Erdős distinct distance problem which contains the required technique for such incidence results), as well as with more applicable *energy* versions of the sum–product phenomenon [2], [10], [29], [34], [37], and [44]. The sum–product phenomenon asserts that either the sumset or the product set of a set must be large up to some natural algebraic constraints. One of the strongest forms of this principle is the Erdős–Szemerédi conjecture [14] which says that for any sufficiently large set A of reals and an arbitrary $\epsilon > 0$ one has

$$\max\{|A + A|, |AA|\} \gg |A|^{2-\epsilon}\,.$$

2010 *Mathematics Subject Classification.* Primary 11B75.

Key words and phrases. Sum-product phenomenon, asymptotic formulae, incidence geometry, exponantial sums.

This work was supported by grant Russian Scientific Foundation RSF 14–11–00433.

At the moment the best results in the direction can be found in [53], [28], [29], [44], and in [1], [42] for $\mathbb{R}$ and $\mathbb{F}_p$, respectively. For example, let us recall the main results from [1], [42].

Theorem 1. *Let $A \subseteq \mathbb{F}_p$ be an arbitrary set and $|A| < p^{5/8}$. Then*

$$\max\{|A+A|, |AA|\} \gg |A|^{1+1/5} . \tag{1}$$

As one can see the bound above works for small sets only and this is a usual thing for the results in this area. On the other hand, the exact behaviour of the maximum in (1) and other sum–product quantities are known just for very large sets having its sizes comparable to the characteristic p; see, e.g., [15], [16], [58], [59]. Even in the strong recent paper [54] containing an optimal estimate for the number of point/line incidences in the case of Cartesian products we have just an upper bound for such incidences but not an asymptotic. The first result in the sum–product theory which gives us an asymptotic formula for a sum–product quantity and which works for sets of any size was proved in [37, Theorem 10] (on $\mathsf{T}(A)$; see [31]).

Theorem 2. *Let $A \subseteq \mathbb{F}_p$ be a set and let $\mathsf{Q}(A)$ be the number of collinear quadruples in $A \times A$. Then*

$$\mathsf{Q}(A) = \frac{|A|^8}{p^2} + O(|A|^5 \log |A|) . \tag{2}$$

Further, for the number $\mathsf{T}(A)$ of collinear triples in $A \times A$ one has

$$\mathsf{T}(A) = \frac{|A|^6}{p} + O(p^{1/2}|A|^{7/2}) . \tag{3}$$

It is known that formula (2) is sharp up to logarithmic factors but (3) is probably not; see [37].

One of the aims of our paper is to prove a series of new asymptotic formulae in the considered area. In the proofs we use the usual incidence theorems in $\mathbb{F}_p$, see [43], [54] and other papers, as well as the growth result in $\mathrm{SL}_2(\mathbb{F}_p)$ due to Helfgott [22]. So, another of our aims is to obtain some new applications (also, see the recent papers [33], [32] where other applications were found) of classical graph (group) expansion phenomena; see [9], [21], [18], [22], [45], and others.

Our first asymptotic formula concerns the quantity

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

(similarly one can define its multiplicative analogue $\mathsf{T}^\times_k(A)$) in the case when A is a multiplicative subgroup of $\mathbb{F}^*_p$ (see Theorem 25 below). In papers [4], [5], [12], [51] just upper bounds for $\mathsf{T}^+_k(A)$ can be found but not an asymptotic formula.

Theorem 3. *Let $\Gamma \subseteq \mathbb{F}^*_p$ be a multiplicative subgroup. Then for any $k \geq 1$ one has*

$$0 \leq \mathsf{T}^+_{2^k}(\Gamma) - \frac{|\Gamma|^{2^{k+1}}}{p} \leq 2^{3k^2}(C_* \log^4 p)^{k-1} \cdot |\Gamma|^{2^{k+1} - \frac{(k+7)}{2}} \mathsf{T}^+_2(\Gamma) , \tag{4}$$

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

In Section 5 we obtain new asymptotic formulae and bounds for the quantities

$$|\{(a_1 - a_2) \dots (a_{2k-1} - a_{2k}) = (a'_1 - a'_2) \dots (a'_{2k-1} - a'_{2k}) \ : \ a_i,\, a'_i \in A\}| \tag{5}$$

as well as for

$$|\{a_1 a_2 + \dots + a_{2k-1} a_{2k} = a'_1 a'_2 + \dots + a'_{2k-1} a'_{2k} \ : \ a_i,\, a'_i \in A\}|. \tag{6}$$

It allows us to improve estimates for exponential sums of Petridis and Shparlinski [40] as well as Macourt [31]; see Corollary 45 below.

Corollary 4. *Given three sets $X, Y, Z \subseteq \mathbb{F}_p$, $|X| \ge |Y| \ge |Z|$ and three complex weights $\rho = (\rho_{x,y})$, $\sigma = (\sigma_{x,z})$, $\tau = (\tau_{y,z})$ all bounded by one, we have*

$$\sum_{x \in X,\, y \in Y,\, z \in Z} \rho_{x,y} \sigma_{x,z} \tau_{y,z} e(xyz) \ll p^{1/8} |X|^{7/8} |Y|^{29/32} |Z|^{29/32} (|Y||Z|)^{-1/3072} ,$$

provided $|Y|, |Z| < p^{48/97}$.

Moreover we obtain a new effective bound for such sums in an optimal range $|X||Y||Z| \ge p^{1+\delta}$ (and for higher sums). Previously, Bourgain [6, Theorem 1] obtained $(\delta/10)^{10^4}$ instead of $\frac{\delta}{8\log(8/\delta)+4}$; see formula (8) below. In general, our saving has the form $p^{-\delta/(C_1 \log(C_2 r/\delta))^r}$ for r sets instead of $p^{-(\delta/r)^{Cr}}$ from [6, Theorem A]. Here $C, C_1, C_2 > 0$ are some absolute constants.

Theorem 5. *Let $X, Y, Z \subseteq \mathbb{F}_p$ be arbitrary sets such that for some $\delta > 0$ the following holds:*

$$|X||Y||Z| \ge p^{1+\delta} . \tag{7}$$

Then

$$\sum_{x \in X,\, y \in Y,\, z \in Z} e(xyz) \ll |X||Y||Z| \cdot p^{-\frac{\delta}{8\log(8/\delta)+4}} . \tag{8}$$

Our next result is an asymptotic version of the Balog–Wooley [2] decomposition theorem; also, see [29], [42], [49] (consult Theorem 48 and Corollary 49 below). In particular, it gives us an asymptotic variant of Theorem 1 (signs $\lesssim, \gtrsim$ suppress powers of the logarithm of $|A|$).

Theorem 6. *Let $A \subseteq \mathbb{F}_p$ be a set and let $1 \le M \le p/(2|A|)$ be a parameter. There exist two disjoint subsets B and C of A such that $A = B \sqcup C$ and*

$$0 \le \mathsf{T}^{+}_2(B) - \frac{|B|^4}{p} \le \frac{|A|^{2/3}|B|^{7/3}}{M} , \tag{9}$$

and for any set $X \subseteq \mathbb{F}_p$ one has

$$\mathsf{T}^{\times}_2(C, X) \lesssim \frac{M^2 |X|^2 |A|^2}{p} + M^{3/2} |A| |X|^{3/2} . \tag{10}$$

In particular, for any set $A \subseteq \mathbb{F}_p$ either

$$|A + A| \ge 5^{-1} \min\{|A|^{6/5}, p/2\}$$

or

$$|AA| \gtrsim \min\{p|A|^{-2/5}, |A|^{6/5}\} .$$

In Section 8 we consider the expansion in $\mathrm{SL}_2(\mathbb{F}_p)$ and obtain some combinatorial applications of the celebrated Helfgott's growth result. Our first theorem concerns the intersection of the inverses of additively rich sets A; see Corollary 55.

Theorem 7. *Let $A, B \subseteq \mathbb{F}_p$, $|B| \ge p^{\varepsilon}$, $\varepsilon > 0$, and $|A + B| \le K|A|$. Then for any $\lambda \ne 0$ one has*

$$\left| \left\{ \frac{1}{a_1} - \frac{1}{a_2} = \lambda \ :\ a_1, a_2 \in A \right\} \right| \le \frac{K^2 |A|^2}{p} + 2K|A|p^{-1/2^{k+2}} ,$$

where $k = k(\varepsilon)$. Also,

$$\mathsf{T}^{+}_2(1/A, 1/B) - \frac{K^2|A|^2|B|^2}{p} \ll K^{5/4} |A|^{5/4} |B|^{3/2} + K^2 |A|^2 .$$

The theorem above can be extended to general polynomial maps (and even to rational functions); see Corollary 61.

Theorem 8. *Let $p_1, p_2 \in \mathbb{F}_p[x]$ be any non–constant polynomial. Then for any $A, B \subseteq \mathbb{F}_p$, $|B| \ge p^\varepsilon$, $\varepsilon > 0$ one has*

$$0 \le \left| \left\{ p_1(b) + \frac{1}{a+p_2(b)} = p_1(b') + \frac{1}{a'+p_2(b')} ~:~ a,a' \in A,\, b,b' \in B \right\} \right| - \frac{|A|^2|B|^2}{p}$$

$$\le 2|A||B|^2 p^{-1/2^{k+2}}\,, \tag{11}$$

where $k = k(\varepsilon, \deg p_1, \deg p_2)$. In particular,

$$\left| \left\{ p_1(b) + \frac{1}{a+p_2(b)} ~:~ a \in A,\, b \in B \right\} \right| \gg \min\{p, |A|p^{1/2^{k+2}}\}\,.$$

We write the saving $p^{-1/2^{k+2}}$ with $k = k(\varepsilon, \deg p_1, \deg p_2)$ in the form to specify the dependence on parameters ε, $\deg p_1$, $\deg p_2$ below. Also, we break the square root barrier for exponential sums of the form (and many other exponential sums)

$$e\left(y\left(\frac{1}{x+b_1}+b_2\right)\right)\,, \qquad e\left(y\left(p_1(b)+\frac{1}{x+p_2(b)}\right)\right)\,,$$

$$\chi\left(y+b_2+\frac{1}{x+b_1}\right)\,, \qquad \chi\left(y+p_1(b)+\frac{1}{x+p_2(b)}\right)\,;$$

see Corollaries 56, 62 below. Here the variables x, y belong to some sets X, Y; further $b_1, b_2 \in B$, $|B| > p^\varepsilon$, e and χ are any non–principal additive/multiplicative characters and $p_1, p_2 \in \mathbb{F}_p[x]$ are non–constant polynomials.

Finally, we obtain an expansion result of another sort (see Corollary 67 from Section 9).

Corollary 9. *Let $A \subseteq \mathbb{F}_p$, $B_1, B_2, B_3 \subseteq \mathbb{F}_p$, $B := |B_1| = |B_2| = |B_3| > p^\varepsilon$. Suppose that $|B_3 - B_1B_2| \le B^2 p^{-\varepsilon}$. Then there is $\delta = \delta(\varepsilon) > 0$ such that*

$$\left| \left\{ \frac{a+b_1}{ab_2+b_3} ~:~ a \in A\,, b_j \in B_j \right\} \right| \gg \min\{p, |A|p^\delta\}\,. \tag{12}$$

The paper is organized as follows. Section 2 contains the required notation. In Section 3 we give a list of the results, which will be used further in the text. Here we discuss the "design" bound for the incidences, namely, estimate (31) and a much deeper result of Rudnev, namely, Theorem 10. These two bounds are foundations of our paper and its combination allows us to obtain many asymptotic results of this section and of further sections. We finish this section by discussing some asymptotic sum–product results from $\mathrm{SL}_2(\mathbb{F}_p)$, see, e.g., [7], [9], which counterintuitively appeared before any asymptotic sum–product theorem in $\mathbb{F}_p$. In the next section we prove, among other results, Theorem 3, which can be considered as an analogue of the discussed asymptotic result from [9]. In Sections 5, 6 we study the quantities from (5), (6) and obtain new bounds for multilinear exponential sums. It allows us to improve some results of papers [6], [40], [31] while our scheme of the proof is different. Section 7 is devoted to an asymptotic version of the Balog–Wooley [2] decomposition theorem. In Sections 8, 9 we give a new application of the celebrated Helfgott result [22] on the growth in $\mathrm{SL}_2(\mathbb{F}_p)$ to sum–product questions in $\mathbb{F}_p$. The main advantage of $\mathrm{SL}_2(\mathbb{F}_p)$–actions is that they give non–linear results (because $\mathrm{SL}_2(\mathbb{F}_p)$ is naturally connected to points on hyperbolas) contrary to classical linear incidences of Section 3. The first application of such sort was obtained in [32]. A reader who is not interested in $\mathrm{SL}_2(\mathbb{F}_p)$ can skip these sections as well as the last one. In the appendix we give our proof of Bougain–Gamburd Theorem 50 as well as a consequence of the famous Frobenius Theorem on representations of $\mathrm{SL}_2(\mathbb{F}_p)$ for convolutions.

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 $\widehat{f}$,

$$\widehat{f}(\xi) = \sum_{x \in \mathbb{F}_p} f(x) e(-\xi \cdot x)\,, \tag{13}$$

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

$$\sum_{x \in \mathbb{F}_p} f(x)\overline{g(x)} = \frac{1}{p} \sum_{\xi \in \mathbb{F}_p} \widehat{f}(\xi)\overline{\widehat{g}(\xi)}\,. \tag{14}$$

Another particular case of (14) is

$$\sum_{y \in \mathbb{F}_p} \Big| \sum_{x \in \mathbb{F}_p} f(x) g(y-x) \Big|^2 = \frac{1}{p} \sum_{\xi \in \mathbb{F}_p} \big|\widehat{f}(\xi)\big|^2 \big|\widehat{g}(\xi)\big|^2\,, \tag{15}$$

and the identity

$$f(x) = \frac{1}{p} \sum_{\xi \in \mathbb{F}_p} \widehat{f}(\xi) e(\xi \cdot x) \tag{16}$$

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

$$(f * g)(x) := \sum_{y \in \mathbb{F}_p} f(y) g(x-y) \quad \text{and} \quad (f \circ g)(x) := \sum_{y \in \mathbb{F}_p} \overline{f(y)} g(y+x)\,. \tag{17}$$

Then

$$\widehat{f * g} = \widehat{f}\widehat{g} \quad \text{and} \quad \widehat{f \circ g} = \overline{\widehat{f}}\widehat{g}\,. \tag{18}$$

Put $\mathsf{E}^+(A,B)$ for the *common additive energy* of two sets $A, B \subseteq \mathbb{F}_p$ (see, e.g., [57]), 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. 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 (15),

$$\mathsf{E}(A,B) = \frac{1}{p} \sum_{\xi} |\widehat{A}(\xi)|^2 |\widehat{B}(\xi)|^2\,. \tag{19}$$

Also, notice that

$$\mathsf{E}^+(A,B) \le \min\{|A|^2|B|, |B|^2|A|, |A|^{3/2}|B|^{3/2}\}\,. \tag{20}$$

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, weighed by the values of f_1, f_2, f_3, f_4. It can be shown using the Hölder inequality (see, e.g., [57]) that

$$\mathsf{E}^+(f_1,f_2,f_3,f_4) \le (\mathsf{E}^+(f_1)\mathsf{E}^+(f_2)\mathsf{E}^+(f_3)\mathsf{E}^+(f_4))^{1/4}\,. \tag{21}$$

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

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

Certainly, the multiplicative energy $\mathsf{E}^{\times}(A,B)$ can be expressed in terms of multiplicative convolutions similar to (17). Further, the definitions and the formulae above take place in an arbitrary abelian group $\mathbf{G}$. If there is no difference between E^{+} and $\mathsf{E}^{\times}$ or this is the only operation on the considered group $\mathbf{G}$, then we write just E.

Sometimes we use representation function notation 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. Having $P \subseteq A - A$ we write $\sigma_P(A) := \sum_{x \in P} r_{A-A}(x)$. Also, we write $f_A(x)$ for the balanced function of a set $A \subseteq \mathbb{F}_p$, namely, $f_A(x) = A(x) - |A|/p$.

Now consider two families of higher energies. First, let

(22)
$$\mathsf{T}^{+}_k(A) := |\{(a_1,\dots,a_k,a'_1,\dots,a'_k) \in A^{2k} \ : \ a_1+\dots+a_k = a'_1+\dots+a'_k\}| = \frac{1}{p}\sum_{\xi} |\widehat{A}(\xi)|^{2k} \,.$$

It is useful to note that

$$\mathsf{T}^{+}_{2k}(A) = |\{(a_1,\dots,a_{2k},a'_1,\dots,a'_{2k}) \in A^{4k} \ : \ (a_1+\dots+a_k)+(a_{k+1}+\dots+a_{2k})$$
$$= (a'_1+\dots+a'_k)+(a'_{k+1}+\dots+a'_{2k})\}|$$
$$= \sum_{x,y,z} r_{kA}(x) r_{kA}(y) r_{kA}(x+z) r_{kA}(y+z) \,, \tag{23}$$

so one can rewrite $\mathsf{T}^{+}_{2k}(A)$ via the additive energy of the function $r_{kA}(x)$. Sometimes we use $\mathsf{T}^{+}_k(f)$ for an arbitrary function f, again $\mathsf{T}^{+}_k(f)$ pertains to additive $2k$–tuples, weighed by the $2k$ values of f. It is easy to check that

$$\mathsf{T}^{+}_k(f) \le \|f\|_1^2 \mathsf{T}^{+}_{k-1}(f) \,, \tag{24}$$

and hence by the Parseval identity

$$\mathsf{T}^{+}_k(f) \le \|f\|_1^{2k-2} \|f\|_2^2 \,. \tag{25}$$

Further, counting the trivial solutions $a_j = a'_j$ to equation (22), we have

$$\mathsf{T}^{+}_k(f) \ge \|f\|_2^{2k} \tag{26}$$

(another way to see that the last equality takes place is to apply the Hölder inequality to (22) starting with $\mathsf{T}_1(f) = \|f\|_2^2$ and apply the Parseval identity). Second, for $k \ge 2$, we put

$$\mathsf{E}^{+}_k(A) = \sum_{x \in \mathbb{F}_p} (A \circ A)(x)^k = \sum_{x \in \mathbb{F}_p} r^k_{A-A}(x) = \mathsf{E}^{+}(\Delta_k(A), A^k) \,, \tag{27}$$

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

$$\mathsf{E}^{+}_k(A) \le |A|^{k-l} \mathsf{E}^{+}_l(A) \qquad \forall l \le k \,. \tag{28}$$

Finally, let us remark that by definition (27) one has $\mathsf{E}^+_1(A) = |A|^2$. Similarly, one can define $\mathsf{E}^+(f)$ for an arbitrary function f. From the inversion formula and the Parseval identity, it follows that

$$\mathsf{E}^+_k(f) = p^{1-k} \sum_{x_1+\dots+x_k=0} |\widehat{f}(x_1)|^2 \dots |\widehat{f}(x_k)|^2 \ge 0\,. \tag{29}$$

Some further results about the properties of the energies E^+_k can be found in [46]. Again, sometimes we use $\mathsf{E}^+_k(f)$ for an arbitrary function f and the first formula from (27) allows us to define $\mathsf{E}^+_k(A)$ for any positive k. It was proved in [49, 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 [57] and follows from a generalization of inequality (21).

We write $\delta\{x\} = 1$ if $x = 0$ and $\delta\{x\} = 0$ otherwise.

All logarithms are to base 2. The signs $\ll$ and $\gg$ are the usual Vinogradov symbols. If we have a set A, then we will write $a \lesssim b$ or $b \gtrsim a$ if $a = O(b \cdot \log^c |A|)$, $c > 0$. When the constants in the signs depend on a parameter M, we write $\ll_M$ and $\gg_M$. For a positive integer n, we set $[n] = \{1, \dots, n\}$. We do not normalize L_p–norms of functions. So, $\|f\|_p = (\sum_x |f(x)|^p)^{1/p}$ for any complex function f.

3. Preliminaries

First of all, we need a general design bound for the number of incidences. Let $\mathcal{P} \subseteq \mathbb{F}_q^3$ be a set of points and Π be a collection of planes in $\mathbb{F}_q^3$. Having $r \in \mathcal{P}$ and $\pi \in \Pi$, we write

$$\mathcal{I}(r,\pi) = \begin{cases} 1 & \text{if } q \in \pi, \\ 0 & \text{otherwise.} \end{cases}$$

So, $\mathcal{I}$ is the $|\mathcal{P}| \times |\Pi|$ matrix. If $\mathcal{P} = \mathbb{F}_q^3$ and Π is the family of all planes in $\mathbb{F}_q^3$, then we obtain the matrix $\overline{\mathcal{I}}$ and $\mathcal{I}$ is a submatrix of $\overline{\mathcal{I}}$. One can easily calculate $\overline{\mathcal{I}}^* \overline{\mathcal{I}}$ and $\overline{\mathcal{I}}\,\overline{\mathcal{I}}^*$ embedding $\mathbb{F}_q^3$ into the projective plane $\mathbb{PF}_q^3$ and check that both of these matrices are of the form $a\mathbf{Id} + b\mathbf{1}$, where a, b are some scalar coefficients, $\mathbf{Id}$ and $\mathbf{1}$ are an identity matrix and all-ones matrices of corresponding dimensions; see, for example, [58, 59]. Moreover, one can check that in our case of points and planes the following holds: $a = p^2$ and $b = p + 1$ (see [58, 59]). In view of these facts and using the singular decomposition (see, e.g., [23]), we have

$$\overline{\mathcal{I}}(r,\pi) = \sum_{j=1}^{\min\{|\mathcal{P}|,|\Pi|\}} \mu_j u_j(r) v_j(\pi)\,,$$

where $\mu_j \ge 0$ are square roots of the eigenvalues of $\overline{\mathcal{I}\mathcal{I}}^t$ (which coincide with square roots of non-zero eigenvalues of $\overline{\mathcal{I}}^t\overline{\mathcal{I}})$ and u_j and v_j, are the eigenfunctions of $\overline{\mathcal{I}\mathcal{I}}^t$ and $\overline{\mathcal{I}}^t\overline{\mathcal{I}}$, respectively, $j = 1, \dots, \min\{|\mathcal{P}|, |\Pi|\}$. Put $Q := \min\{|\mathcal{P}|, |\Pi|\}$. From $\overline{\mathcal{I}\mathcal{I}}^t = p^2\mathbf{Id} + (p + 1)\mathbf{1}$, we obtain

$$\mu_1^2 = p^2 + (p+1)Q \qquad \text{and} \qquad \mu_2 = \ldots = \mu_Q = p$$

and

$$u_1(r) = (1, \dots, 1) \in \mathbb{R}^Q \qquad \text{and} \qquad v_1(\pi) = (1, \dots, 1) \in \mathbb{R}^{\max\{|\mathcal{P}|,|\Pi|\}}\,.$$

Hence we derive that for any functions $f : \mathcal{P} \to \mathbb{C}$ and $g : \Pi \to \mathbb{C}$, supported by only $\mathcal{P}$ and Π, respectively, one has

$$\left|\sum_{r\in\mathcal{P}}\sum_{\pi\in\Pi}\mathcal{I}(r,\pi)f(r)g(\pi)\right| = \left|\sum_{r\in\mathcal{P}}\sum_{\pi\in\Pi}\overline{\mathcal{I}}(r,\pi)f(r)g(\pi)\right| = \left|\sum_{j=2}^{Q}\mu_j\langle f,u_j\rangle\langle g,v_j\rangle\right|$$
$$\le p\sum_{j=2}^{Q}|\langle f,u_j\rangle\langle g,v_j\rangle|\,,$$

provided that

$$\sum_{q\in\mathcal{P}} f(r) = 0 \quad \text{or} \quad \sum_{\pi\in\Pi} g(\pi) = 0\,. \tag{30}$$

Using the Cauchy–Schwarz inequality we now see that under the condition (30) we have

$$\left|\sum_{r\in\mathcal{P}}\sum_{\pi\in\Pi}\mathcal{I}(r,\pi)f(r)g(\pi)\right| \le p\|f\|_2\|g\|_2\,, \tag{31}$$

where, as usual $\|f\|_2$ and $\|g\|_2$ are the L^2-norms of functions f and g, respectively. Of course, similar arguments work not just for point/plane incidences but, e.g., point/line incidences and so on.

A much deeper result on incidences is contained in [43] (or see [37, Theorem 8] and the proof of Corollary 2 from [34]). In the proof of formula (33) one should use an incidence bound from [36, Section 3].

Theorem 10. *Let p be an odd prime, let $\mathcal{P}\subseteq\mathbb{F}_p^3$ be a set of points, and let Π be a collection of planes in $\mathbb{F}_p^3$. Suppose that $|\mathcal{P}|\le|\Pi|$ and that k is the maximum number of collinear points in $\mathcal{P}$. Then the number of point/plane incidences satisfies*

$$\mathcal{I}(\mathcal{P},\Pi) \ll \frac{|\mathcal{P}||\Pi|}{p} + |\mathcal{P}|^{1/2}|\Pi| + k|\Pi|\,. \tag{32}$$

More precisely,

$$\mathcal{I}(\mathcal{P},\Pi) - \frac{|\mathcal{P}||\Pi|}{p} \ll |\mathcal{P}|^{1/2}|\Pi| + k|\Pi|\,. \tag{33}$$

Corollary 11. *Let α,β be non–negative functions, let $C\subseteq\mathbb{F}_p$ be a set. Suppose that*

$$\max\{\|\alpha\|_1\|\beta\|_1^{-1}\|\alpha\|_2^{-1}\|\beta\|_2,\|\alpha\|_1^{-1}\|\beta\|_1\|\alpha\|_2\|\beta\|_2^{-1}\} \le |C|^{1/2} \le \frac{\|\alpha\|_1\|\beta\|_1}{\|\alpha\|_2\|\beta\|_2} \tag{34}$$

and put $L=\log(\|\alpha\|_1\|\beta\|_1|C|/(\|\alpha\|_2\|\beta\|_2))$. Then

$$\sum_x r^2_{\alpha\beta+C}(x) - \frac{(\|\alpha\|_1\|\beta\|_1|C|)^2}{p} \ll L^4\|\alpha\|_1\|\beta\|_1\|\alpha\|_2\|\beta\|_2|C|^{3/2} \tag{35}$$

and

$$\sum_x r^2_{\alpha(\beta+C)}(x) - \frac{(\|\alpha\|_1\|\beta\|_1|C|)^2}{p} \ll L^4\|\alpha\|_1\|\beta\|_1\|\alpha\|_2\|\beta\|_2|C|^{3/2}\,. \tag{36}$$

Proof. We obtain (35) because the proof of (36) is similar. Let $f(x)=C(x)-|C|/p$. Then

$$\sum_x r^2_{\alpha\beta+\gamma}(x) = \frac{(\|\alpha\|_1\|\beta\|_1|C|)^2}{p} + \sum_x r^2_{\alpha\beta+f}(x)\,.$$

Split the level set of α,β into level sets $P_j(\alpha)$, $P_j(\beta)$ where the functions α, β differ at most twice, correspondingly. Clearly, there are at most L such sets because if, say, $\alpha(x)\le\varepsilon:=2^{-2}|C|^{-1/2}\|\beta\|_1^{-1}\|\alpha\|_2\|\beta\|_2$, then

$$\varepsilon\|\alpha\|_1|C|^2\|\beta\|_1^2 \le 2^{-2}|C|^{3/2}\|\alpha\|_1\|\beta\|_1\|\alpha\|_2\|\beta\|_2\,,$$

so it is negligible and hence the inequality $2^j\varepsilon \le \|\alpha\|_1$ gives the required bound. Using the pigeonhole principle and positivity of the operator $r_{f-f}(x-y)$, we find some Δ_A, Δ_B and $A \subseteq P_j(\alpha)$, $B \subseteq P_j(\beta)$ such that

$$\sigma := \sum_x r^2_{\alpha\beta+f}(x) \ll L^4 \Delta_A^2 \Delta_B^2 \sum_x r^2_{AB+f}(x)\,.$$

On the one hand, in view of (31) the last sum is bounded by

$$\sigma \le L^4 \Delta_A^2 \Delta_B^2 p \|f\|_2^2 |A||B| \le L^4 \Delta_A^2 \Delta_B^2 p |A||B||C|\,. \tag{37}$$

On the other hand, using Theorem 10 (one can consult paper [1])

$$\sum_x r^2_{AB+f}(x) = \frac{|A|^2|B|^2|C|^2}{p} + \sum_x r^2_{AB+C}(x)$$

$$\ll \frac{|A|^2|B|^2|C|^2}{p} + (|A||B||C|)^{3/2} + |A||B||C| \max\{|A|,|B|,|C|\}\,.$$

If the second term in the last formula dominates, then we are done. If the first term is the largest one, then $p \le (|A||B||C|)^{1/2}$ and (37) gives us

$$\sigma \le L^4 \Delta_A^2 \Delta_B^2 p |A||B||C| \le L^4 \Delta_A^2 \Delta_B^2 (|A||B||C|)^{3/2} \le L^4 \|\alpha\|_1 \|\beta\|_1 \|\alpha\|_2 \|\beta\|_2 |C|^{3/2},$$

as required. Finally, condition (34) implies that the third term is negligible. This completes the proof. □

Now we obtain a simple asymptotic formula for the number of point/line incidences in the case when the set of points form a Cartesian product.

Lemma 12. *Let $A, B \subseteq \mathbb{F}_p$ be sets, $|A| \le |B|$, $\mathcal{P} = A \times B$, and let $\mathcal{L}$ be a collection of lines in $\mathbb{F}_p^2$. Then*

$$\mathcal{I}(\mathcal{P},\mathcal{L}) - \frac{|A||B||\mathcal{L}|}{p} \ll |A|^{3/4}|B|^{1/2}|\mathcal{L}|^{3/4} + |\mathcal{L}| + |A||B|\,. \tag{38}$$

Proof. Let $f(x) = B(x) - |B|/p$ be the balanced function of the set B. Then, using the natural notation, we get

$$\mathcal{I}(\mathcal{P},\mathcal{L}) = \frac{|A||B||\mathcal{L}|}{p} + \mathcal{I}(f \otimes A, \mathcal{L})\,,$$

where we count the number of incidences with the weight $f(x)A(a)$ or, in other words,

$$\mathcal{I}(f \otimes A, \mathcal{L}) := \sum_{l \in \mathcal{L}} \sum_{r=(x,a)} f(x)A(a)\mathcal{I}(r,l)\,.$$

Using the design bound for point/line incidences, we obtain

$$\mathcal{I}(f \otimes A, \mathcal{L}) \le \|f\|_2 (p|A||\mathcal{L}|)^{1/2} \le (p|A||B||\mathcal{L}|)^{1/2}\,. \tag{39}$$

By an analogue of the Szemerédi–Trotter theorem in $\mathbb{F}_p$, see [54] (or [34, Theorem 7], [37, Theorem 9]), we have

$$\mathcal{I}(f \otimes A, \mathcal{L}) \ll |A|^{3/4}|B|^{1/2}|\mathcal{L}|^{3/4} + |\mathcal{L}| + |A||B|\,, \tag{40}$$

provided $|A||\mathcal{L}| \le p^2$. But if $|A||\mathcal{L}| > p^2$, then by (39), we see that

$$\mathcal{I}(f \otimes A, \mathcal{L}) \le (p|A||B||\mathcal{L}|)^{1/2} \le |A|^{3/4}|B|^{1/2}|\mathcal{L}|^{3/4}$$

and the last bound is even better than (40). This completes the proof. □

We need a lemma from [51, Lemma 9] which is a consequences of the main result from [43] or Theorem 10.

Lemma 13. *Let $A, Q \subseteq \mathbb{F}_p$ be two sets, $A, Q \neq \{0\}$, let $M \geq 1$ be a real number, and $|QA| \leq M|Q|$. Then*

$$\mathsf{E}^+(Q) \leq C_* \left(\frac{M^2|Q|^4}{p} + \frac{M^{3/2}|Q|^3}{|A|^{1/2}} \right) , \tag{41}$$

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

The second lemma can be obtained in the same vein.

Lemma 14. *Let $A, B \subseteq \mathbb{F}_p$, and $|A+B| \leq K|A|$. Then*

$$\mathsf{E}^+(1/A, 1/B) - \frac{K^2|A|^2|B|^2}{p} \ll K^{5/4}|A|^{5/4}|B|^{3/2} + K^2|A|^2 . \tag{42}$$

Proof. Indeed, for any α, β the following holds:

$$\left(\frac{1}{\alpha} + \frac{1}{\beta} \right)^{-1} = \frac{\alpha\beta}{\alpha+\beta} = \beta - \beta^2 \cdot \frac{1}{\alpha+\beta} .$$

Hence

$$\mathsf{E}^+(1/A, 1/B) \leq \left| \{ b_1 - b_1^2 x = b_2 - b_2^2 y \ : \ b_1, b_2 \in B,\ x, y \in (A+B)^{-1} \} \right| = \mathcal{I}(\mathcal{P}, \mathcal{L}) ,$$

where $\mathcal{P} = (A+B) \times (A+B)$, $\mathcal{L} = \{l_{b_1,b_2}\}$, and line l_{b_1,b_2} is defined by the equation $b_1 - b_1^2 x = b_2 - b_2^2 y$. Applying Lemma 12, we get

$$\mathcal{I}(\mathcal{P}, \mathcal{L}) - \frac{|A+B|^2|B|^2}{p} \ll |A+B|^{5/4}|B|^{3/2} + |B|^2 + |A+B|^2 .$$

Clearly, $|B| \leq |A+B| \leq K|A|$ and hence

$$\mathsf{E}^+(1/A, 1/B) - \frac{K^2|A|^2|B|^2}{p} \ll K^{5/4}|A|^{5/4}|B|^{3/2} + K^2|A|^2,$$

as required. □

The next result is a slight generalization of [51, Lemma 10].

Lemma 15. *Let f be a real function and let $P \subseteq \mathbb{F}_p^*$ be a set. Then for any $k \geq 1$ one has*

$$\left(\sum_{x \in P} r^k_{f-f}(x) \right)^4 \leq \|f\|_2^{4k} \mathsf{E}^+_{2k}(f) \mathsf{E}^+(P) . \tag{43}$$

Proof. We have

$$\left(\sum_{x \in P} r^k_{f-f}(x) \right)^2 = \left(\sum_{x_1, \dots, x_k} \prod_{j=1}^k f(x_j) \sum_y P(y) f(y+x_1) \dots f(y+x_k) \right)^2$$

$$\leq \|f\|_2^{2k} \sum_{x_1, \dots, x_k} | \sum_y P(y) f(y+x_1) \dots f(y+x_k)|^2 = \|f\|_2^{2k} \sum_x r_{P-P}(x) r^k_{f-f}(x) .$$

Hence by the Cauchy–Schwarz inequality, we obtain

$$\left(\sum_{x \in X} r^k_{f-f}(x) \right)^4 \leq \|f\|_2^{4k} \mathsf{E}^+_{2k}(f) \mathsf{E}^+(P),$$

as required. □

Let $A, B, C, D \subseteq \mathbb{F}_p$ be four sets. By $\mathsf{Q}(A, B, C, D)$ we denote the number of *collinear quadruples* in $A \times A$, $B \times B$, $C \times C$, $D \times D$, that is, the number of quadruples of points from the plane $\mathbb{F}_p^2$ lying on a line such that the first point belongs to $A \times A$, the second point belongs to $B \times B$, and so on. If $A = B = C = D$, then we write $\mathsf{Q}(A)$ for $\mathsf{Q}(A, A, A, A)$. Recent results on the quantity $\mathsf{Q}(A)$ can be found in [39] and [37]. It is easy to see (or consult [37]) that

(44)
$$\mathsf{Q}(A,B,C,D)=\left|\left\{\frac{b'-a'}{b-a}=\frac{c'-a'}{c-a}=\frac{d'-a'}{d-a} \ : \ a,a'\in A,\ b,b'\in B,\ c,c'\in C,\ d,d'\in D\right\}\right|$$

$$(45) \qquad = \sum_{a,a'\in A} \sum_{x} r_{(B-a)/(B-a')}(x) r_{(C-a)/(C-a')}(x) r_{(D-a)/(D-a')}(x)\,.$$

Notice that in (44), we mean that the condition, say, $b = a$ implies $c = d = b = a$ or, in other words, that all four points $(a, a'), (b, b'), (c, c'), (d, d')$ have the same abscissa. More rigorously, the summation in (45) should be taken over $\mathbb{F}_p \cup \{+\infty\}$, where $x = +\infty$ means that the denominator in any fraction $x = \frac{b'-a'}{b-a}$ from, say, $r_{(B-a)/(B-a')}(x)$ equals zero. Anyway, it is easy to see that the contribution of the point $+\infty$ is at most $O(M^5)$, where $M = \max\{|A|, |B|, |C|, |D|\}$, and hence it is negligible (see, say, Theorem 2 above). Further, defining a function $q_{A,B,C,D}(x, y)$ (see [37]) as

$$(46) \qquad q_{A,B,C,D}(x,y) := \left|\left\{\frac{b-a}{c-a}=x,\ \frac{d-a}{c-a}=y \ : \ a\in A,\ b\in B,\ c\in C,\ d\in D\right\}\right|,$$

we obtain another formula for the quantity $\mathsf{Q}(A, B, C, D)$, namely,

$$\mathsf{Q}(A,B,C,D) = \sum_{x,y} q^2_{A,B,C,D}(x,y)$$

because

$$\sum_{x,y} q^2_{A,B,C,D}(x,y)$$

$$= \sum_{x,y} \left|\left\{\frac{b-a}{c-a}=x=\frac{b'-a'}{c'-a'},\ \frac{d-a}{c-a}=y = \frac{d'-a'}{c'-a'} \ : \ a,a'\in A,\ b,b'\in B,\ c,c'\in C,\ d,d'\in D\right\}\right|$$

$$= \left|\left\{\frac{b-a}{c-a}=\frac{b'-a'}{c'-a'},\ \frac{d-a}{c-a}=\frac{d'-a'}{c'-a'} \ : \ a,a'\in A,\ b,b'\in B,\ c,c'\in C,\ d,d'\in D\right\}\right|$$

$$= \left|\left\{\frac{b'-a'}{b-a}=\frac{c'-a'}{c-a}=\frac{d'-a'}{d-a} \ : \ a,a'\in A,\ b,b'\in B,\ c,c'\in C,\ d,d'\in D\right\}\right|$$

$$= \mathsf{Q}(A,B,C,D)\,.$$

An optimal (up to logarithmic factors) upper bound for $\mathsf{Q}(A)$ was obtained in [37], [39]; see Theorem 2 from the introduction. We need a simple lemma about the same bound for a generalization of the quantity $\mathsf{Q}(A)$. The proof is analogous to the proof [52, Lemma 6] and [50, Lemma 5].

Lemma 16. *Let $A, B \subseteq \mathbb{F}_p$ be two sets, $|B| \le |A| \le \sqrt{p}$. Then*

$$(47) \qquad \mathsf{Q}(B,A,A,A) \ll |A|^{15/4}|B|^{5/4}\log^2|A| + \mathsf{T}(A)\,.$$

It is known [1, Proposition 2.5] that $\mathsf{T}(A) \ll |A|^{9/2}$, provided $|A| \le p^{2/3}$ (also, see Theorem 2 from the introduction). So, the term $\mathsf{T}(A)$ in (47) is negligible if A and B have comparable sizes, say.

Proposition 16 from [44] contains a combinatorial lemma; see Lemma 17 below.

Lemma 17. *Let $(\mathbf{G}, +)$ be an abelian group. Also, let $A \subseteq \mathbf{G}$ be a set, $P \subseteq A - A$, $P = -P$. Then there is $A_* \subseteq A$ and a number q, $q \lesssim |A_*|$ such that for any $x \in A_*$ one has $r_{A+P}(x) \ge q$, and $\sum_{x\in P} r_{A-A}(x) \sim |A_*|q$.*

Another combinatorial result is [44, Theorem 13].

Theorem 18. *Let $(\mathbf{G}, +)$ be an abelian group. Also, let $A \subseteq \mathbf{G}$ be a set, let $K \ge 1$ be a real number, and let $k \ge 2$ be an integer. Suppose that $\mathsf{E}^+(A) \ge |A|^3/K$. Then there are sets $A_* \subseteq A$, $P \subseteq A - A$ such that $|A_*| \ge |A|/(8kK)$, $|P| \le 8kK|A|$ and for any $a_1, \dots, a_k \in A_*$ one has*

$$|A \cap (P + a_1) \cap \dots \cap (P + a_k)| \ge \frac{|A|}{4K}\,. \tag{48}$$

We need a result on the energy of a set which is obtained using the eigenvalues method; see [47], [48], [37], [38]. In this form an analogue of the result above appeared for the first time in [37, Theorem 28]. One can decrease the number of logarithmic factors slightly but it is not our aim.

Theorem 19. *Let A be a finite subset of an abelian group $(\mathbf{G}, +)$. Suppose there are parameters D_1 and D_2 such that*

$$\mathsf{E}^+_3(A) \le D_1|A|^3$$

and for any finite set $B \subset \mathbf{G}$

$$\mathsf{E}^+(A, B) \le D_2|A||B|^{3/2}.$$

Then

$$\mathsf{E}^+(A) \ll D_1^{6/13} D_2^{2/13} |A|^{32/13} \log^{12/13} |A|\,.$$

It is implicit in the proof of Theorem 19 that the bound for $\mathsf{E}(A, B)$ only needs to hold for $|B| \le 4|A|^4/\mathsf{E}^+(A)$.

Theorem 19 implies the following bound for the multiplicative energy of a subset of $\mathbb{F}_p$ with large additive energy.

Corollary 20. *Let $A \subseteq \mathbb{F}_p$ and $\mathsf{E}^+(A) \ge |A|^3/K$. Then there is $A_* \subseteq A$, $|A_*| \ge |A|/(16K)$ such that for any $B \subseteq \mathbb{F}_p$ the following holds:*

$$\mathsf{E}^\times(A_*, B) \ll \frac{K^4|A|^2|B|^2}{p} + K^{7/2}|B|^{3/2}|A|\,, \tag{49}$$

and if $|A|K \le \sqrt{p}$, then

$$\mathsf{E}^\times_3(A_*) \ll K^{23/4}|A|^3 \log^2 |A|\,. \tag{50}$$

In particular, if $|A|K \le \sqrt{p}$, then

$$\mathsf{E}^\times(A_*) \lesssim K^{83/26}|A|^{32/13}\,. \tag{51}$$

Proof. Applying Theorem 18 with $k = 3$, we find two sets $A_* \subseteq A$, $P \subseteq A - A$, $|A_*| \ge |A|/(24K)$, $|P| \le 24K|A|$ such that for any $a_1, a_2, a_3 \in A_*$ one has

$$|A \cap (P + a_1) \cap (P + a_2) \cap (P + a_3)| \ge \frac{|A|}{4K}\,. \tag{52}$$

Then
(53)

$$\mathsf{E}^{\times}(A_*, B) \le (|A|/4K)^{-2} \left|\{(a-p)b = (a'-p')b' \ : \ a, a' \in A,\, b, b' \in B,\, p, p' \in P\}\right| .$$

Clearly, the number of the solutions to equation (53) can be interpreted as point/plane incidences. Hence applying Theorem 10, we obtain
(54)

$$\mathsf{E}^{\times}(A_*, B) \ll (|A|/K)^{-2} \left(\frac{|A|^2|B|^2|P|^2}{p} + (|A||B||P|)^{3/2} + |A||B||P| \max\{|A|, |B|, |P|\} \right) .$$

In view of the desired bound (49) one can assume that $|B| \ge K^7$, $|A| \ge |B|^{1/2} K^{7/2}$ (otherwise trivial bounds (20), namely, $\mathsf{E}^{\times}(A_*, B) \le \min\{|A||B|^2, |A|^2|B|\}$ work better). Also, (52) implies, trivially, $|P| \ge |A|/(4K)$ and we can assume that $|B| \le 4|A|^4/\mathsf{E}^{+}(A) \ll K|A|$. Thus it is easy to check that the third term in (54) is negligible and using $|P| \ll K|A|$, we obtain (49).

To prove (50) we notice that in view of (52) and (44) one has

$$\mathsf{E}^{\times}_3(A_*) = |\{\alpha/\alpha' = \beta/\beta' = \gamma/\gamma' \ : \ \alpha, \alpha', \beta, \beta', \gamma, \gamma' \in A_*\}|$$

$$(|A|/4K)^{-2} \left| \left\{ \frac{b-a}{b'-a'} = \frac{c-a}{c'-a'} = \frac{d-a}{d'-a'} \ : \ a, a' \in A,\, b, b', c, c', d, d' \in P \right\} \right|$$

$$\ll (|A|/K)^{-2} \mathsf{Q}(A, P, P, P) .$$

Suppose that $|A| \le |P| \le \sqrt{p}$. One can assume that $K \le |A|^{4/23}$ because otherwise there is nothing to prove. It remains to estimate $\mathsf{Q}(A, P, P, P)$ and we have by Lemma 16 that

$$\mathsf{Q}(A, P, P, P) \ll |P|^{15/4} |A|^{5/4} \log^2 |A| + \mathsf{T}(P) . \tag{55}$$

Thus in view of $\mathsf{T}(P) \ll |P|^{9/2}$, see [1, Proposition 2.5], the second term in (55) is negligible. Then applying Lemma 16 and the bound $|P| \le 24K|A|$, we obtain (50). If $|A| > |P|$, then we get an even better estimate for $\mathsf{E}^{\times}_3(A_*)$. Finally, using Theorem 19, we derive from (49), (50) the desired bound (51) (because $|B| \le 4|A|^4/\mathsf{E}^{+}(A)$ and $|A|K \le \sqrt{p}$ we see that the second term in (49) dominates). This completes the proof. □

In [38] some better bounds for the energy were obtained (for the reals and the case of multiplicative subgroups) but they work in a situation which is opposite to Corollary 20, namely, when the product set (not the sumset) is small.

Now consider the group $\mathrm{SL}_2(\mathbb{F}_p)$ of matrices

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} , \qquad a, b, c, d \in \mathbb{F}_p , \qquad ad - bc = 1 ,$$

which acts on $\mathbb{F}_p$ (actually on the projective line) by

$$gz := \frac{az+b}{cz+d} , \qquad z \in \mathbb{F}_p .$$

There are two important subgroups in $\mathrm{SL}_2(\mathbb{F}_p)$. Let B be the standard Borel subgroup of upper–triangular matrices, namely, elements of B are

$$b = b_{r,q} = \begin{pmatrix} r & q \\ 0 & r^{-1} \end{pmatrix} , \qquad q \in \mathbb{F}_p , \quad r \in \mathbb{F}_p \setminus \{0\} .$$

Also, let $U \subseteq B$ be the standard unipotent subgroup. In other words, elements of U are

$$u = u_q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} , \qquad q \in \mathbb{F}_p .$$

Having a group which is acting as a set, one can define a convolution which slightly generalizes the ordinary convolution.

Definition 21. Let $F : \mathrm{SL}_2(\mathbb{F}_p) \to \mathbb{C}$ and $f : \mathbb{F}_p \to \mathbb{C}$ be two functions. Define the convolution of $F * f : \mathbb{F}_p \to \mathbb{C}$ as

$$(F * f)(x) := \sum_{g \in \mathrm{SL}_2(\mathbb{F}_p)} F(g) f(g^{-1}x) \,.$$

Let us mention a well–known lemma (see [9], [21], [45], and other papers) on convolutions in $\mathrm{SL}_2(\mathbb{F}_p)$ which follows from the well–known Frobenius Theorem [20] on representations of $\mathrm{SL}_2(\mathbb{F}_p)$. For the sake of completeness we add the proof of this lemma in the appendix.

Lemma 22. *Let $f : \mathbb{F}_p \to \mathbb{C}$ be a function such that $\sum_x f(x) = 0$. Then for any function $F : \mathrm{SL}_2(\mathbb{F}_p) \to \mathbb{C}$ and $\varphi : \mathbb{F}_p \to \mathbb{C}$ one has*

$$\sum_{x \in \mathbb{F}_p} (F * f)(x) \varphi(x) \le 2p \|F\|_2 \|\varphi\|_2 \|f\|_2 \,. \tag{56}$$

Finally, we need the classification of subgroups of $\mathrm{SL}_2(\mathbb{F}_p)$; see [55].

Theorem 23. *Let p be a prime and $p \ge 5$. Then any subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ is isomorphic to one of the following subgroups:*
(1) *finite groups A_4, S_4, A_5,*
(2) *the dihedral groups of order $4\left(\frac{p\pm1}{2}\right)$ and their subgroups,*
(3) *a Borel subgroup of order $p(p-1)$ and its subgroups.*

We finish this section recalling the celebrated result of Helfgott [22] on the growth in $\mathrm{SL}_2(\mathbb{F}_p)$.

Theorem 24. *Let $A \subseteq \mathrm{SL}_2(\mathbb{F}_p)$. Assume that $|A| < p^{3-\delta}$ for $\delta > 0$ and A is not contained in any proper subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$. Then there is a positive function $\kappa(\delta) > 0$ such that*

$$|AAA| \gg_\delta |A|^{1+\kappa(\delta)} \,.$$

4. First results

Throughout this section Γ is a multiplicative subgroup of $\mathbb{F}_p^*$. Such subgroups were studied by various authors and many deep results about subgroups were obtained, e.g., [5], [8], [12], [30], [51], and others. In this section we find upper bounds for $\mathsf{T}^+_k(f)$, $\mathsf{E}^+_k(f)$, and for the exponential sums over f, where f is an arbitrary Γ–invariant function, that is, $f(x\gamma) = f(x)$ for all $\gamma \in \Gamma$ (so the value of $f(0)$ can be arbitrary). Recall that for a function f, we put

$$\mathsf{T}^+_k(f) := \sum_{x_1 + \dots + x_k = x'_1 + \dots + x'_k} f(x_1) \dots f(x_k) f(x'_1) \dots f(x'_k) \,.$$

The main difference between our new theorems and results from [51] is, first, that we consider general functions f and, second, the absence of any restrictions on size of support of f (but not on size of Γ, of course) similar to $\mathbb{R}$ where we have no such restrictions; see our previous paper [51].

We begin with the quantity $\mathsf{T}^+_k(f)$ and we use $\mathsf{T}^+_2(f)$ in bounds below to make our results sharper. Of course, one can replace this quantity to $\|f\|_1^2 \|f\|_2^2$ (see formula (25)) or by something even smaller using Lemma 13.

Theorem 25. *Let f be a Γ–invariant complex function with $\sum_x f(x) = 0$. Then for any $k \ge 1$ one has*

$$\mathsf{T}^+_{2^k}(f) \le 2^{3k^2} (C_* \log^4 p)^{k-1} \cdot \|f\|_1^{2^{k+1}-4} |\Gamma|^{\frac{(1-k)}{2}} \mathsf{T}^+_2(f) \,, \tag{57}$$

where C_* is the absolute constant from Lemma 13.

Proof. For $k=1$ bound (57) is trivial, so below we will assume that $k\ge 2$. Fix any $s\ge 2$ and put $L=L_s:=s\log p$. Our aim is to prove

$$\mathsf{T}^+_{2s}(f)\le 128C_*L_s^4\|f\|_1^{2s}\mathsf{T}^+_s(f)|\Gamma|^{-1/2}\,. \tag{58}$$

After that we use induction and obtain

$$\mathsf{T}^+_{2^k}(f)\le (128C_*)^{k-1}\log^{4(k-1)}p\cdot 2^{4((k-1)+(k-2)+\dots+2)}\|f\|_1^{2^k+\dots+4}|\Gamma|^{\frac{-(k-1)}{2}}\mathsf{T}^+_2(f)$$

$$2^{2k^2+5k-11}(C_*\log^4 p)^{k-1}\cdot\|f\|_1^{2^{k+1}-4}|\Gamma|^{\frac{(1-k)}{2}}\mathsf{T}^+_2(f)$$
$$\le 2^{3k^2}(C_*\log^4 p)^{k-1}\cdot\|f\|_1^{2^{k+1}-4}|\Gamma|^{\frac{(1-k)}{2}}\mathsf{T}^+_2(f)$$

and this coincides with (57).

To prove (58) we notice that by formula (23) one has

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

Here as usual we have denoted by $r_{sf}(x)$ the function $r_{f+\dots+f}(x)$, where the number of f's in the sum is s. We give two upper bounds for $\mathsf{T}^+_{2s}(f)$ and first of all, notice that from the last formula, it follows that $\mathsf{T}^+_{2s}(f)$ equals

$$\sigma:=|\Gamma|^{-2}\sum_{\gamma_1,\gamma_2\in\Gamma}\sum_{a,b,c,d}r_{sf}(a)r_{sf}(b)r_{sf}(c)r_{sf}(d)\cdot\delta\{a+\gamma_1 b=c+\gamma_2 d\}$$

plus the term $\mathcal{E}$ which corresponds to a,b,c,d equals zero (see below). Consider the set of points $\mathcal{P}\subseteq\mathbb{F}_p^3$, each point p indexed by (γ_1,c,d) and the set of planes $\Pi\subseteq\mathbb{F}_p^3$ indexed by (a,b,γ_2) and each $\pi=\pi_{a,b,\gamma_2}\in\Pi$ has the form $\pi: a+xb=y+\gamma_2 z$. Then in terms of formula (31) one has $\delta\{a+\gamma_1 b=c+\gamma_2 d\}=\mathcal{I}(p,\pi)$ for $p=(\gamma_1,c,d)$ and $\pi=\pi_{a,b,\gamma_2}$. By the assumption $\sum_x f(x)=0$. It follows that $\sum_x r_{sf}(x)=0$ and hence

$$\sigma=|\Gamma|^{-2}\sum_{\gamma_1,\gamma_2}f_\Gamma(\gamma_1)f_\Gamma(\gamma_2)\sum_{a,b,c,d}r_{sf}(a)r_{sf}(b)r_{sf}(c)r_{sf}(d)\cdot\delta\{a+\gamma_1 b=c+\gamma_2 d\}\,, \tag{59}$$

where $f_\Gamma(x)=\Gamma(x)-|\Gamma|/p$ is the balanced function of Γ. In a similar way, considering for all non-zero x the function $R(x)=|\Gamma|^{-1}\sum_y f_\Gamma(y)r_{sf}(xy^{-1})$, we obtain

$$\sigma=|\Gamma|^{-4}\sum_{\gamma_1,\gamma_2,\gamma_3,\gamma_4}f_\Gamma(\gamma_1)f_\Gamma(\gamma_2)f_\Gamma(\gamma_3)f_\Gamma(\gamma_4)\sum_{a,b,c,d}r_{sf}(a)r_{sf}(b)r_{sf}(c)r_{sf}(d)\cdot\delta\{\gamma_1 a+\gamma_2 b$$
$$=\gamma_3 c+\gamma_4 d\}$$
$$=\sum_{x,y,z}R(x)R(y)R(x+z)R(y+z)\,. \tag{60}$$

Clearly, $R(0)=0$; further $R(x)=r_{sf}(x)$, $x\ne 0$, and $\|R\|_\infty=\|r_{sf}\|_\infty$ if one considers the function r_{sf} as a function on $\mathbb{F}_p^*$ only. Also, notice that $\|f_\Gamma\|_1<2|\Gamma|$ and hence

$$\|R\|_1\le|\Gamma|^{-1}\|r_{sf}\|_1\|f_\Gamma\|_1<2\|r_{sf}\|_1\le 2\|f\|_1^s\,.$$

Now put $\rho=\mathsf{T}^+_{2s}(f)/(64\|f\|_1^{3s})$. Since

$$\left|\sum_{x,y,z\,:\,|R(x)|\le\rho}R(x)R(y)R(x+z)R(y+z)\right|\le 8\rho\|f\|_1^{3s}=\mathsf{T}^+_{2s}(f)/8\,,$$

it follows that

$$\mathsf{T}^+_{2s}(f)\le\frac{3}{2}\sum_{x,y,z}{}'\,R(x)R(y)R(x+z)R(y+z)+\frac{3}{2}\mathcal{E}\,,$$

where the sum $\sum'$ above (we denote it as $\mathsf{T}'_{2s}(f)$) is taken over non-zero variables $x, y, x+z, y+z$ with $|R(x)|, |R(y)|, |R(x+z)|, |R(y+z)| > \rho$ and by (24)

$$\mathcal{E} \le 4|r_{sf}(0)| \left| \sum_{y,z} r_{sf}(y) r_{sf}(z) r_{sf}(y+z) \right| \le 4 r_{s|f|}(0) \|f\|_1^s \mathsf{T}^+_s(f) \le 4\|f\|_2^2 \|f\|_1^{2s-2} \mathsf{T}^+_s(f)$$

(notice that $\mathcal{E}$ can be non-zero even if $f(0) = 0$). Let us compare the obtained estimate for $\mathcal{E}$ with the upper bound in (58). By the assumption f is a Γ–invariant function and hence $\|f\|_1 = |\Gamma| \sum_{\xi \in \mathbb{F}_p^*/\Gamma} |f(\xi)|$, as well as

$$\|f\|_2^2 = |\Gamma| \sum_{\xi \in \mathbb{F}_p^*/\Gamma} |f(\xi)|^2 \le |\Gamma|^{-1} \|f\|_1^2 \,. \tag{61}$$

In particular,

$$\mathcal{E} \le 4\|f\|_1^{2s} \mathsf{T}^+_s(f) |\Gamma|^{-1} \le 4\|f\|_1^{2s} \mathsf{T}^+_s(f) |\Gamma|^{-1/2} \,. \tag{62}$$

Thus the obtained estimate for $\mathcal{E}$ is much smaller than the upper bound for $\mathsf{T}^+_{2s}(f)$ in (58). Hence if (58) holds, then there is nothing to prove and in the opposite case, we get

$$\mathcal{E} \le \mathsf{T}^+_{2s}(f)/(32 C_* L^4) \,, \tag{63}$$

so it is negligible. Also, we can assume that $\mathsf{T}'_{2s}(f) > 0$ because otherwise there is nothing to prove.

Put $P_j = \{x \,:\, \rho 2^{j-1} < |r_{sf}(x)| \le \rho 2^j\} \subseteq \mathbb{F}_p^*$, $j \in \mathbb{N}$. By (26), we have $\mathsf{T}^+_s(f) \ge \|f\|_2^{2s}$. If (58) does not hold, then, in particular,

$$\mathsf{T}^+_{2s}(f) \ge 2^7 \|f\|_1^{2s} \mathsf{T}^+_s(f) |\Gamma|^{-1/2} \ge 2^7 \|f\|_1^{2s} \|f\|_2^{2s} |\Gamma|^{-1/2} \tag{64}$$

and hence the possible number of the sets P_j does not exceed L. Indeed, for any x one has $|r_{s\Gamma}(x)| \le \|f\|_1^{s-2} \|f\|_2^2$ and hence $\rho 2^{j-1} = 2^{j-7} \mathsf{T}^+_{2s}(f) \|f\|_1^{-3s}$ must be less than $\|f\|_1^{s-2} \|f\|_2^2$ otherwise the correspondent set P_j is empty. In other words, using the Hölder inequality one more time, as well as bound (64), we obtain

$$\begin{aligned} 2^{j-7} \le \|f\|_1^{4s-2} \|f\|_2^2 / \mathsf{T}^+_{2s}(f) &\le \|f\|_1^{2s-2} \|f\|_2^{-(2s-2)} |\Gamma|^{1/2} / 2^7 \\ &\le p^{s-1} |\Gamma|^{1/2} / 2^7 < p^s / 2^7, \end{aligned}$$

as required. By the Dirichlet principle there is $\Delta = \rho 2^{j_0 - 1}$, and a set $P = P_{j_0}$ such that

$$\mathsf{T}^+_{2s}(f) \le \frac{3}{2} L^4 (2\Delta)^4 \mathsf{E}^+(P) + \frac{3}{2}\mathcal{E} = \mathsf{T}'_{2s}(f) + \frac{3}{2}\mathcal{E} \,. \tag{65}$$

Indeed, putting $g_i(x) = P_i(x) r_{sf}(x)$, and using (21), we get

$$\begin{aligned} \sum_{x,y,z}' r_{sf}(x) r_{sf}(y) r_{sf}(x+z) r_{sf}(y+z) &\le \sum_{i,j,k,l=1}^{L} \sum_{x,y,z} g_i(x) g_j(y) g_k(x+z) g_l(y+z) \\ \le \sum_{i,j,k,l=1}^{L} (\mathsf{E}^+(g_i)\mathsf{E}^+(g_j)\mathsf{E}^+(g_k)\mathsf{E}^+(g_l))^{1/4} &= \left(\sum_{i=1}^{L} (\mathsf{E}^+(g_i))^{1/4} \right)^4 \\ &\le L^3 \sum_{i=1}^{L} \mathsf{E}^+(g_i) \le L^4 \max_i \mathsf{E}^+(g_i) \,. \end{aligned}$$

Certainly, the sum $\sum'_{x,y,z} R(x)R(y)R(x+z)R(y+z)$ can be estimated in a similar way and one can check that all functions $R_i(x) = |\Gamma|^{-1} \sum_y f_\Gamma(y) r_i(xy^{-1})$ have zero mean and $\|R_i\|_\infty \le \|r_i\|_\infty$. Moreover we always have $|P|\Delta^2 \le \mathsf{T}^+_s(f)$ and

$$|P|\Delta \le \sum_{x \in P} |r_{sf}(x)| \le \sum_x |r_{sf}(x)| \le \sum_x r_{s|f|}(x) = \|f\|_1^s \,. \tag{66}$$

Using Lemma 13, we obtain

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

Hence

$$\mathsf{T}'_{2s}(f) \le 3(16C_*)L^4 \left(\frac{\Delta^4|P|^4}{p} + \frac{\Delta^4|P|^3}{|\Gamma|^{1/2}} \right) . \tag{67}$$

Suppose that the second term in (67) dominates. Then in view of $|P|\Delta^2 \le \mathsf{T}^{+}_s(f)$ and $|P|\Delta \le \|f\|_1^s$, we have

$$|P|^3\Delta^4 = (P\Delta)^2 P\Delta^2 \le \|f\|_1^{2s}\mathsf{T}^{+}_s(f) .$$

In other words, the second term in (67) does not exceed

$$3(16C_*)L^4\|f\|_1^{2s}\mathsf{T}^{+}_s(f)|\Gamma|^{-1/2} , \tag{68}$$

and inequality (58) (also, recall bound (62)) is proved.

If the first term in (67) dominates, then we notice that $|P||\Gamma|^{1/2} \ge p$ and use another bound. By $\sum_x f_\Gamma(x) = 0$, formulae (59), (65), and (31), as well as the last estimate, we have

$$\mathsf{T}^{'}_{2s}(f) \le 3\cdot 8L^4 p(4|P|\Delta^2)^2|\Gamma|^{-1} = 3\cdot 2^7 L^4|P|^3\Delta^4|\Gamma|^{-1} \le 3\cdot 16L^4|P|^3\Delta^4|\Gamma|^{-1/2} \tag{69}$$

for $|\Gamma| \ge 2^6$. Of course quantity (69) is less than the second term in (67). If $|\Gamma| < 2^6$, then it is easy to check that (57) takes place. Combining the obtained bound (69) with (68), we see that in any case

$$\mathsf{T}'_{2s}(f) \le 6(16C_*)L^4\|f\|_1^{2s}\mathsf{T}^{+}_s(f)|\Gamma|^{-1/2} .$$

Finally, using (62), we have

$$\mathsf{T}^{+}_{2s}(f) \le 128C_* L^4\|f\|_1^{2s}\mathsf{T}^{+}_s(f)|\Gamma|^{-1/2}.$$

This completes the proof. □

Now we are ready to obtain an upper bound for the exponential sums over any Γ–invariant function f.

Corollary 26. *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| \ge p^\delta$, $\delta > 0$, and let f be a Γ–invariant complex function with $\sum_x f(x) = 0$. Then for all sufficiently large p one has*

$$\max_{\xi} |\widehat{f}(\xi)| \ll \|f\|_1 \cdot p^{-\frac{5\delta}{2^{7+2\delta^{-1}}}} . \tag{70}$$

Further we have a non-trivial upper bound $o(\|f\|_1)$ for the maximum in (70) if

$$\log|\Gamma| \ge \frac{C\log p}{\log\log p} , \tag{71}$$

where $C > 2$ is any constant.

Proof. By ρ denote the maximum in (70). It is attained at some non-zero ξ because $\sum_x f(x) = 0$. Then by Theorem 25, a trivial bound which follows from (25), namely, $\mathsf{T}^{+}_2(f) \le \|f\|_1^2\|f\|_2^2$ and formula (22), we obtain

$$|\Gamma|\rho^{2^{k+1}} \le p\mathsf{T}^{+}_{2^k}(f) \le p2^{3k^2}(C_*\log^4 p)^{k-1}\cdot\|f\|_1^{2^{k+1}-2}\|f\|_2^2|\Gamma|^{\frac{(1-k)}{2}} . \tag{72}$$

Using formula (61), we get

$$|\Gamma|\rho^{2^{k+1}} \le p2^{3k^2}(C_*\log^4 p)^{k-1}\cdot\|f\|_1^{2^{k+1}}|\Gamma|^{-\frac{(k+3)}{2}} .$$

Put $k = \lceil 2\log p/\log|\Gamma| + 4\rceil \le 2/\delta + 5$, say. Also, notice that

$$\frac{p\log^{4(k-1)} p}{|\Gamma|^{k/2}} \le 1 \tag{73}$$

because $k \ge 2\log p/\log|\Gamma| + 4$ and p is a sufficiently large number depending on δ (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 $\log^{4(k-1)} p$). Taking a power $1/2^{k+1}$ from both parts of (72), we see in view of (73) that

$$\rho \ll \|f\|_1 \cdot |\Gamma|^{-\frac{5}{2^{k+2}}} \ll \|f\|_1 \cdot p^{-\frac{5\delta}{2^{7+2\delta^{-1}}}} \,.$$

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

$$k \le \frac{2\log p}{\log|\Gamma|} + 5 \le \log\log|\Gamma| - \log(1/\varepsilon)\,.$$

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

Let us obtain a new general bound for $\mathsf{E}^+_k(f)$.

Theorem 27. *Let f be a Γ–invariant function real function with $\sum_x f(x) = 0$. Then for positive integer $k \ge 2$ either*

$$\mathsf{E}^+_{2^{k+1}}(f) \le 32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1}))\|f\|_2^{2^{k+1}}\mathsf{E}^+_{2^k}(f)|\Gamma|^{-1/8}$$

or

$$\mathsf{E}^+_{2^{k+1}}(f) \le 2\|f\|_2^{2^{k+2}}\,.$$

Here C_* is the absolute constant from Lemma 13. *In particular, if k is chosen as*

$$|\Gamma|^{\frac{k-1}{8}} \ge (32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1})))^{k-1}\|f\|_1^2\|f\|_2^{-2}\,, \tag{74}$$

then $\mathsf{E}^+_{2^{k+1}}(f) \le 2\|f\|_2^{2^{k+2}}$.

Proof. Fix an even integer $l \ge 1$ and prove that either

$$\mathsf{E}^+_{4l}(f) \le 32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1}))\|f\|_2^{4l}\mathsf{E}^+_{2l}(f)|\Gamma|^{-1/8} \tag{75}$$

or

$$\mathsf{E}^+_{4l}(f) \le 2\|f\|_2^{8l}\,. \tag{76}$$

After that it requires the use of induction to see

$$\mathsf{E}^+_{2^{k+1}}(f) \le (32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1}))^{k-1}\|f\|_2^{2^{k+1}+\dots+2^3}\mathsf{E}^+_4(f)|\Gamma|^{-(k-1)/8}$$
$$\le (32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1}))^{k-1}\|f\|_2^{2^{k+2}-8}\mathsf{E}^+_4(f)|\Gamma|^{-(k-1)/8}\,.$$

Trivially, $\mathsf{E}^+_4(f) \le \|f\|_2^6\|f\|_1^2$ and hence

$$\|f\|_2^{2^{k+2}} \le \mathsf{E}^+_{2^{k+1}}(f) \le (32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1}))^{k-1}\|f\|_2^{2^{k+2}-2}\|f\|_1^2|\Gamma|^{-(k-1)/8}\,.$$

Thus if

$$|\Gamma|^{\frac{k-1}{8}} \ge (32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1}))^{k-1}\|f\|_1^2\|f\|_2^{-2}\,,$$

then, clearly, $\mathsf{E}^+_{2^{k+1}}(f) \le 2\|f\|_2^{2^{k+2}}$.

We give two upper bounds for $\mathsf{E}^+_{4l}(f)$. First, let us remark that for any positive integer n there exists a function F such that

$$r^n_{f-f}(x) = r_{F-F}(x)\,. \tag{77}$$

Indeed, from the definition of the required function F and formula (29) one has

$$|\widehat{F}(x)|^2 = p^{1-n} \sum_{y_1+\dots+y_n=x} |\widehat{f}(y_1)|^2 \dots |\widehat{f}(y_n)|^2 \geq 0$$

and we can choose the Fourier transform of F taking, say, a positive square root of the left–hand side of the previous formula. It defines our function F (but not uniquely, even in the case $n=1$ one can take $F(x) = f(x)$ or $F(x) = f(-x)$, say). In particular, by the Parseval identity, we get

$$\|F\|_2^2 = p^{-1}\|\widehat{F}\|_2^2 = p^{-n} \sum_x \sum_{y_1+\dots+y_n=x} |\widehat{f}(y_1)|^2 \dots |\widehat{f}(y_n)|^2 = \|f\|_2^{2n} . \tag{78}$$

To obtain another proof of the last equality just substitute $x=0$ into (77) and notice that $(F \circ F)(0) = \|F\|_2^2 = r^n_{f-f}(0) = (f \circ f)^n(0) = \|f\|_2^{2n}$. Applying these arguments for $n = 4l-1$, we obtain

$$\mathsf{E}^+_{4l}(f) = \sum_x r_{f-f}(x) r^{4l-1}_{f-f}(x) = \sum_x r_{f-f}(x) r_{F-F}(x) .$$

By the assumption the function f is Γ–invariant. Thus

$$\mathsf{E}^+_{4l}(f) = |\Gamma|^{-2} \sum_{\gamma_1,\gamma_2\in\Gamma} \sum_{a,b,c,d} F(a)f(b)F(c)f(d) \cdot \delta\{a+\gamma_1 b = c+\gamma_2 d\} .$$

Consider the set of points $\mathcal{P} \subseteq \mathbb{F}_p^3$, each point p indexed by (γ_1, c, d) and the set of planes $\Pi \subseteq \mathbb{F}_p^3$ indexed by (a, b, γ_2) and each $\pi \in \Pi$ has the form $\pi : a + xb = y + \gamma_2 z$. Then we have as in Theorem 25 that $\delta\{a+\gamma_1 b = c+\gamma_2 d\} = \mathcal{I}(p,\pi)$. By the assumption $\sum_x f(x) = 0$. Besides $\|F\|_2^2 = \|f\|_2^{8l-2}$. Hence by (31), we have

$$\mathsf{E}^+_{4l}(f) \leq p\|f\|_2^{8l}|\Gamma|^{-1} . \tag{79}$$

Now let us give another bound for $\mathsf{E}^+_{4l}(f)$. Put $g(x) = r^l_{f-f}(x)$, $L = 2+2\log(\|f\|_1\|f\|_2^{-1})$ and $\mathsf{E}'_{4l}(f) = \mathsf{E}^+_{4l}(f) - \|f\|_2^{8l}$. We will assume below that $\mathsf{E}'_{4l}(f) \geq 2^{-1}\mathsf{E}^+_{4l}(f) > 0$ because otherwise the required inequality (76) follows immediately. Similarly, we can assume that $\mathsf{E}'_{4l}(f) \geq \|f\|_2^{8l}$ because otherwise $\mathsf{E}^+_{4l}(f) \leq 2\|f\|_2^{8l}$ and we are done. Further, put $\rho^{4-1/l} = 2^{-1}\|f\|_2^{8l}\|f\|_1^{-2}$ and $P_j = \{x \ : \ \rho 2^{j-1} < g(x) \leq \rho 2^j\}$. Clearly,

$$\sum_{x \ : \ g(x)<\rho} g^4(x) < \rho^{4-1/l}\|f\|_1^2 = 2^{-1}\|f\|_2^{8l} .$$

Thus the number of the sets P_j does not exceed L. Indeed, for any x one has $g(x) \leq \|f\|_2^{2l}$ and hence $2^{j-1}\rho$ must be less than $\|f\|_2^{2l}$ because otherwise P_j is empty. Whence for $j \geq 3$

$$2^{j-2}\|f\|_2^{8l}\|f\|_1^{-2} \leq 2^{(j-1)(4-1/l)-1}\|f\|_2^{8l}\|f\|_1^{-2} = 2^{(j-1)(4-1/l)}\rho^{4-1/l} \leq \|f\|_2^{8l-2}$$

and $j \leq 2+2\log(\|f\|_1\|f\|_2^{-1}) := L$ (if $j<3$, then the last bound holds trivially). Notice that $\log(\|f\|_1\|f\|_2^{-1}) \geq 0$. Using the Dirichlet principle, we find a set $P = P_{j_0}$ and a positive number $\Delta = \rho 2^{j_0-1}$ such that $P = \{x \ : \ \Delta < g(x) \leq 2\Delta\} \subseteq \mathbb{F}_p^*$ and

$$\mathsf{E}'_{4l}(f) \leq 2L \sum_{x\in P} r^{4l}_{f-f}(x) \leq 2L\|f\|_2^{3l} \sum_{x\in P} r^{5l/2}_{f-f}(x) := \|f\|_2^{3l}\sigma . \tag{80}$$

Applying Lemma 15, combining with Lemma 13, we obtain

$$\sigma \le 2L(2\Delta)^{3/2} \sum_{x\in P} r^l_{f-f}(x) \le 2^{5/2} C_*^{1/4} L \Delta^{3/2} \|f\|_2^l (\mathsf{E}^+_{2l}(f))^{1/4} \left(\frac{|P|^4}{p} + \frac{|P|^3}{|\Gamma|^{1/2}} \right)^{1/4}$$

$$\le 2^{5/2} C_*^{1/4} L \|f\|_2^l (\mathsf{E}^+_{2l}(f))^{1/4} \left(\frac{\Delta^6 |P|^4}{p} + \frac{\Delta^6 |P|^3}{|\Gamma|^{1/2}} \right)^{1/4} . \qquad (81)$$

Suppose that the second term in (4) dominates. Since l is an even number, we have $\Delta|P| \le \mathsf{E}^+_l(f)$, $\Delta^2|P| \le \mathsf{E}^+_{2l}(f)$ and hence $\Delta^6|P|^3 \le (\mathsf{E}^+_{2l}(f))^3$. It follows that

$$2^{-1}\mathsf{E}^+_{4l}(f) \le \mathsf{E}'_{4l}(f) \le 8C_*^{1/4} L \|f\|_2^{4l} \mathsf{E}^+_{2l}(f) |\Gamma|^{-1/8}$$

and we obtain (75). Now if the first term in (4) dominates, then $|P||\Gamma|^{1/2} \ge p$ and returning to (80), we have

$$\mathsf{E}'_{4l}(f) \le 32 L \Delta^4 |P| .$$

Multiplying this inequality by $|P|$ and using $\Delta^2|P| \le \mathsf{E}^+_{2l}(f)$, we get

$$|P|\mathsf{E}'_{4l}(f) \le 32L(\mathsf{E}^+_{2l}(f))^2 .$$

Recalling (79), applying the inequality $|P||\Gamma|^{1/2} \ge p$ and the last bound, we obtain

$$\mathsf{E}^+_{4l}(f) \le p\|f\|_2^{8l} |\Gamma|^{-1} \le |P| \|f\|_2^{8l} |\Gamma|^{-1/2} \le 32L \|f\|_2^{8l} (\mathsf{E}^+_{2l}(f))^2 |\Gamma|^{-1/2} (\mathsf{E}'_{4l}(f))^{-1} .$$

Whence in view of the inequality $2^{-1}\mathsf{E}^+_{4l}(f) \le \mathsf{E}'_{4l}(f)$, we have

$$\mathsf{E}^+_{4l}(f) \le 8L^{1/2} \|f\|_2^{4l} \mathsf{E}^+_{2l}(f) |\Gamma|^{-1/4} .$$

Thus we see that the required inequality (75) takes place in any case. This completes the proof. □

Remark 28. The upper bound in Theorem 27 is optimal. Indeed, let $\chi(x)$ be the Legendre symbol. In other words, if R is the set of quadratic residues and $\chi_0(x)$ is the trivial character, then $\chi(x) = 2R(x) - \chi_0(x)$. Let $\Gamma \subseteq R$ be a multiplicative subgroup. Then $\chi(x)$ is a real Γ–invariant function and $\sum_x \chi(x) = 0$. By standard formulas for characters, see, e.g., [3], one has for any $k \ge 2$ that $\mathsf{E}^+_k(\chi) = \sum_x (\chi\circ\chi)^k(x) = (p-1)^k + (p-1)(-1)^k \sim p^k \sim \|\chi\|_2^{2k}$.

Remark 29. Let f be a real Γ–invariant function with zero mean and let $T = \|f\|_1/\|f\|_2$. By (61) we have $T \ge |\Gamma|^{1/2}$. Choosing an integer $k = C\log T/\log|\Gamma|$ with sufficiently large constant $C > 0$, we satisfy condition (74), provided $\log T \ll |\Gamma|$. Under this condition, we get

$$|\Gamma| \left(\max_{x\neq 0} |(f\circ f)(x)| \right)^{2^{k+1}} \le 2\|f\|^{2^{k+2}} .$$

It follows that

$$\max_{x\neq 0} |(f\circ f)(x)| \le \|f\|_2^2 \cdot (2|\Gamma|^{-1})^{1/2^{k+1}} . \qquad (82)$$

Thus we have obtained a non–trivial upper bound for the quantity $\max_{x\neq 0} |(f\circ f)(x)|$ if the condition

$$\log|\Gamma| \gg \frac{\log T}{\log\log T}$$

holds. Of course, the last bound implies $\log T \ll |\Gamma|$. Some applications of such sort of bounds can be found in papers [4], [51].

Corollary 30. *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| \ge p^\delta$, and let f be a Γ–invariant real function with $\sum_x f(x) = 0$. Also, let k be chosen as*

$$|\Gamma|^{\frac{k-1}{8}} \ge (32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1})))^{k-1}\|f\|_1^2\|f\|_2^{-2}\,, \tag{83}$$

and $s = \lceil 2\log\|f\|_1/\log(|\Gamma|/2)\rceil$. Then

$$\mathsf{E}^{\times}_{2^{k+s+1}+1}(f+1) \le 3\|f\|_2^{2^{k+s+2}+2}\,.$$

Proof. For any integer l, we have

$$\mathsf{E}^{\times}_{l}(f+1) = \|f\|_2^{2l} + |f^{2l}(-1)| + \sum_{x\neq 0,1} r^l_{(f+1)/(f+1)}(x)$$

$$\le 2\|f\|_2^{2l} + \sum_{x\neq 0,1} r^l_{(f+1)/(f+1)}(x)\,.$$

Here we have used that $\sum_x f(x) = 0$. Further, for any $\alpha \neq 0,1$ put $f^\alpha(x) = f(\alpha^{-1}x)$. Then

$$r_{(f+1)/(f+1)}(x) = r_{f-f^x}(x-1)\,.$$

Take k such that

$$|\Gamma|^{\frac{k-1}{8}} \ge (32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1})))^{k-1}\|f\|_1^2\|f\|_2^{-2}\,.$$

As in Remark 29, we have for any $x \neq 0,1$

$$|\Gamma|\left(\max_{y\neq 0}|(f^x\circ f)(y)|\right)^{2^{k+1}} \le \sum_y r^{2^{k+1}}_{f-f^x}(y) \le (\mathsf{E}^+_{2^{k+1}}(f^x)\mathsf{E}^+_{2^{k+1}}(f))^{1/2} = \mathsf{E}^+_{2^{k+1}}(f)\,.$$

Here we have used the Cauchy–Schwarz inequality. Applying Theorem 27, we obtain

$$\max_{y\neq 0}|(f^x\circ f)(y)| \le \|f\|_2^2\cdot(2|\Gamma|^{-1})^{1/2^{k+1}}\,.$$

Thus for any s, we have

$$\mathsf{E}^{\times}_{2^{k+1+s}+1}(f+1) \le 2\|f\|_2^{2^{k+2+s}+2} + \|f\|_2^{2^{k+2+s}}\|f\|_1^2(2/|\Gamma|)^s = \|f\|_2^{2^{k+2+s}+2}(2+\|f\|_1^2(2/|\Gamma|)^s)\,.$$

Taking s such that

$$(|\Gamma|/2)^s \ge \|f\|_1^2\,,$$

or, in other words, $s \ge 2\log\|f\|_1/\log(|\Gamma|/2)$, we obtain the required result. This completes the proof. □

For example, let $f(x) = Q(x) - |Q|/p$, where Q is any Γ–invariant set, $\log|Q| \ll |\Gamma|$. Then $k \sim \log|Q|/\log|\Gamma|$ and $s \sim \log|Q|/\log|\Gamma|$, so we have the same bound as in Theorem 27 for more or less the same order $l \sim k, s$ of the energy $\mathsf{E}_l(f)$.

The next result shows that smallness of the energy E^+_k allows us to obtain upper bounds for sums of types (85) and (86). The arguments of the proof are rather general. Estimate (86) allows us to give an alternative proof of formula (82). Also, putting $s = 2^k$ and $B = P$ in formula (86) one can derive Lemma 15.

Corollary 31. *Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup and let f be a Γ–invariant function real function with $\sum_x f(x) = 0$. If k is chosen as*

$$|\Gamma|^{\frac{k-1}{8}} \ge (32C_*^{1/4}(1+\log(\|f\|_1\|f\|_2^{-1})))^{k-1}\|f\|_1^2\|f\|_2^{-2}\,, \tag{84}$$

then for any set $B \subseteq \mathbb{F}_p$ one has

$$p^{-1}\sum_x |\widehat{f}(x)|^2 r_{B-B}(x) \le \|f\|_2^2|B|\left(\frac{2\mathsf{E}^+(B)}{p|B|^2}\right)^{1/2^{k+1}} \tag{85}$$

and for any function $g : \mathbb{F}_p \to \mathbb{C}$ and a positive integer $s \le 2^k$ the following holds:

$$\left| \sum_{x \in B} (g \circ f)^s(x) \right| \le |B| \|g\|_2^s \|f\|_2^s \left(\frac{2\mathsf{E}^+(B)}{|B|^4} \right)^{s/2^{k+2}} . \tag{86}$$

Proof. Denote by σ the sum from (85) and put $\mu(x) = p^{-1} |\widehat{f}(x)|^2$. Clearly,

$$\sigma := \sum_{x \in B} (\mu * B)(x) .$$

Then using the Cauchy–Schwarz inequality k times, we obtain

$$\sigma^{2^k} \le |B|^{2^k - 1} \sum_{x \in B} (\mu *_{2^k} \mu * B)(x) = |B|^{2^k - 1} \sum_x (\mu *_{2^k} \mu)(x) (B \circ B)(x) .$$

Applying the Cauchy–Schwarz inequality one more time, as well as formula (29), we get

$$\sigma^{2^{k+1}} \le |B|^{2^{k+1} - 2} \mathsf{E}^+(B) \mathsf{T}^+_{2^k}(\mu) = p^{-1} |B|^{2^{k+1} - 2} \mathsf{E}^+(B) \mathsf{E}^+_{2^{k+1}}(f) .$$

By our choice of the parameter k and Theorem 27, we have $\mathsf{E}^+_{2^{k+1}}(f) \le 2 \|f\|_2^{2^{k+2}}$ and hence

$$\sigma \le |B| \|f\|_2^2 \left(\frac{2\mathsf{E}^+(B)}{p|B|^2} \right)^{1/2^{k+1}} .$$

It remains to prove (86). Using the Hölder inequality twice, one has

$$\left(\sum_{x \in B} (g \circ f)^s(x) \right)^{2^{k+2}/s} \le |B|^{2^{k+2}/s - 4} \left(\sum_{x \in B} (g \circ f)^{2^k}(x) \right)^4$$

$$= |B|^{2^{k+2}/s - 4} \left(\sum_{y_1, \dots, y_{2^k}} g(y_1) \dots g(y_{2^k}) \sum_{x \in B} f(y_1 + x) \dots f(y_{2^k} + x) \right)^4$$

$$\le |B|^{2^{k+2}/s - 4} \|g\|_2^{2^{k+2}} \left(\sum_x (f \circ f)^{2^k}(x) (B \circ B)(x) \right)^2 \le |B|^{2^{k+2}/s - 4} \|g\|_2^{2^{k+2}} \mathsf{E}_{2^{k+1}}(f) \mathsf{E}^+(B).$$

By our choice of the parameter k and Theorem 27, we have $\mathsf{E}^+_{2^{k+1}}(f) \le 2 \|f\|_2^{2^{k+2}}$. Hence

$$\left| \sum_{x \in B} (g \circ f)^s(x) \right| \le \|g\|_2^s \|f\|_2^s |B| \left(\frac{2\mathsf{E}^+(B)}{|B|^4} \right)^{s/2^{k+2}} ,$$

as required. □

Estimate (86) shows that the smallness of $\mathsf{E}_k(A)$ energy implies that the sums from this inequality are small. It is easy to see that the reverse direction takes place as well. Indeed, suppose to the contrary that $\mathsf{E}_n(A) \ge M|A|^n$ for a parameter $M \ge 1$ and for all positive integers n. Also, let l be a positive integer and let $P = P_l$ be a set as in the proof of Theorem 27 such that $\mathsf{E}_{l+1}(A) \sim |P| \Delta^{l+1}$ and $\Delta < r_{A-A}(x) \le 2\Delta$ on P. Then $|P| \gtrsim M$, and using our assumption (let $s = 1$ for simplicity)

$$\mathsf{E}_{l+1}(A) \lesssim \Delta^l \sigma_P(A) \ll \Delta^l |A| |P| |P|^{-\varepsilon} \lesssim |A| \mathsf{E}_l(A) M^{-\varepsilon} ,$$

where $\varepsilon > 0$ is a constant from our assumption. So, after t applications of this argument, we get

$$M|A|^{l+t} \le \mathsf{E}_{l+t}(A) \lesssim |A|^t \mathsf{E}_l(A) M^{-\varepsilon t} \le |A|^{t+l+1} M^{-\varepsilon t}$$

and hence after t steps such that $M^{\varepsilon t+1} \gtrsim |A|$ we obtain a contradiction and it means that, in particular, $\mathsf{E}_{t+1}(A) \le M|A|^t$. For example, if $M = |A|^\delta$, then $\mathsf{E}_{t+1}(A) \le |A|^{t+\delta}$ for $t \gg \frac{1}{\varepsilon\delta}$, say.

5. On some sum–product quantities with six and eight variables

For any set $A \subseteq \mathbb{F}_p$ let

$$\mathsf{D}^\times(A) = \mathsf{D}^\times_2(A) := |\{(a_1-a_2)(a_3-a_4) = (a'_1-a'_2)(a'_3-a'_4) \ : \ a_i,\, a'_i \in A\}|\,, \tag{87}$$

and more generally for $k \ge 1$

$$\mathsf{D}^\times_k(A) := |\{(a_1-a_2)\dots(a_{2k-1}-a_{2k}) = (a'_1-a'_2)\dots(a'_{2k-1}-a'_{2k}) \ : \ a_i,\, a'_i \in A\}|\,.$$

Clearly, $\mathsf{D}^\times_1(A) = \mathsf{E}^+(A)$. Sometimes, we need $\mathsf{D}^\times_k(A,B)$ for two sets A, B and even more generally $\mathsf{D}^\times_k(\alpha,\beta)$ for two functions α,β.

Our task is to estimate the quantities $\mathsf{D}^\times(A)$, $\mathsf{D}^\times_k(A)$. The quantity $\mathsf{D}^\times(A)$ (and similar $\mathsf{D}^\times_k(A)$) can be interpreted as the number of incidences between points and planes (see details in [1])

$$(a_1-a_2)\lambda = (a'_1-a'_2)\mu\,, \tag{88}$$

counting with the weights $|\{a_3-a_4=\lambda \ : \ a_3,a_4\in A\}|$ and $|\{a'_3-a'_4=\mu \ : \ a'_3,a'_4\in A\}|$.

Theorem 32. *Let $A \subseteq \mathbb{F}_p$ be a set. Then*

$$\mathsf{D}^\times(A) - \frac{|A|^8}{p} \ll (\log|A|)^2 |A|^5 (\mathsf{E}^+(A))^{1/2}\,. \tag{89}$$

Moreover, for all $k \ge 2$ one has

$$\mathsf{D}^\times_k(A) - \frac{|A|^{4k}}{p} \ll (\log|A|)^4 |A|^{4k-2-2^{-k+2}} \mathsf{E}^+(A)^{1/2^{k-1}}\,. \tag{90}$$

Generally, for any non–negative function α and $\beta(x) = A(x)$, the following holds:

$$\mathsf{D}^\times_k(\alpha,\beta) - \frac{\|\alpha\|_1^{2k}\|\beta\|_1^{2k}}{p} \ll L^8(\|\alpha\|_1\|\beta\|_1)^{2k-2}(\|\alpha\|_2\|\beta\|_2)^{2-2^{-k+2}}\mathsf{E}^+(\alpha,\beta)^{1/2^{k-1}}\,, \tag{91}$$

where $L := \log(\|\alpha\|_1\|\beta\|_1|A|/(\|\alpha\|_2\|\beta\|_2))$.

Proof. We have

$$\mathsf{D}^\times(A) = \sum_{\lambda,\mu} r_{A-A}(\lambda) r_{A-A}(\mu) n(\lambda,\mu)\,,$$

where $n_{A,A}(\lambda,\mu) = \sum_x r_{(A-A)\lambda}(x) r_{(A-A)\mu}(x)$. Consider the balanced function $f(x) = f_A(x) = A(x) - |A|/p$. Then we have

$$\mathsf{D}^\times(A) = \frac{|A|^8}{p} + \sum_{\lambda,\mu} r_{A-A}(\lambda) r_{A-A}(\mu) n_{f,f}(\lambda,\mu) := \frac{|A|^8}{p} + \sigma\,.$$

Our task is to estimate the error term σ. Put $L = \log|A|$. Splitting the sum, we get

$$\sigma \ll \sum_{i,j=1}^{L} \sum_{\lambda,\mu} n_{f,f}(\lambda,\mu) r^{(i)}_{A-A}(\lambda) r^{(j)}_{A-A}(\mu)\,,$$

where by $r^{(j)}_{A-A}(\mu)$ we have denoted the restriction of the function r_{A-A} on some set P_j with $\Delta_j < r^{(j)}_{A-A}(\mu) \le 2\Delta_j$, $\mu \in P_j$ and $\Delta_j > 0$ is some number. Clearly, the operator $n_{f,f}(\lambda,\mu)$ is non–negatively defined and hence

$$\sigma \ll L \sum_{j=1}^{L} \sum_{\lambda,\mu} n_{f,f}(\lambda,\mu) r^{(j)}_{A-A}(\lambda) r^{(j)}_{A-A}(\mu)\,.$$

By the pigeonhole principle there is some $\Delta = \Delta_j$ and $P = P_j$ such that

$$\sigma \ll L^2 \Delta^2 \sum_{\lambda,\mu} n_{f,f}(\lambda,\mu) P(\lambda) P(\mu)\,. \tag{92}$$

Since $\sum_x f(x) = 0$, we derive from (88) and (31) that

$$\sigma \ll L^2 p |A|^2 |P| \Delta^2\,. \tag{93}$$

Now we obtain another bound for σ. Using Theorem 10, we get

$$\sigma \ll L^2 \Delta^2 \left(\frac{|A|^4 |P|^2}{p} + |A|^3 |P|^{3/2} + |A|^2 |P| \max\{|A|,|P|\} \right)\,. \tag{94}$$

Since $P \subseteq A - A$ it is easy to see that the term $|A|^2|P|\max\{|A|,|P|\}$ is negligible comparable to $|A|^3|P|^{3/2}$. Suppose that the second term in the last formula dominates. Then

$$\sigma \ll L^2 |A|^3 (\Delta |P|) \cdot (\Delta^2 |P|)^{1/2}\,.$$

Clearly,

$$\Delta |P| \le \sum_x r^{(j)}_{A-A}(x) \le \sum_x r_{A-A}(x) \le |A|^2 \tag{95}$$

and

$$\Delta^2 |P| \le \sum_x (r^{(j)}_{A-A}(x))^2 \le \mathsf{E}^+(A)\,.$$

Hence

$$\sigma \ll L^2 |A|^5 (\mathsf{E}^+(A))^{1/2}$$

and we are done. If the first term in formula (94) is the largest one, then $p \le |A||P|^{1/2}$ and inequality (93) gives us

$$\sigma \le L^2 p |A|^2 \Delta^2 |P| \ll L^2 |A|^3 \Delta^2 |P|^{3/2}\,.$$

We see that it is smaller than the second term in (94) and hence we have proved (89). Another way to bound (92) is just to use estimate (33) of Theorem 10.

To obtain (90) we first, notice that

$$\begin{aligned}\mathsf{D}^\times(A) &= \frac{|A|^8}{p} + \sum_{\lambda,\mu} r_{A-A}(\lambda) r_{A-A}(\mu) n_{f,f}(\lambda,\mu)\\ &= \frac{|A|^8}{p} + \sum_{\lambda,\mu} r_{f-f}(\lambda) r_{f-f}(\mu) n_{f,f}(\lambda,\mu) := \frac{|A|^8}{p} + \sigma\end{aligned}$$

and using the Dirichlet principle as above, we can find a set P and a number Δ such that $\Delta < |r_{f-f}(\mu)| \le 2\Delta$ on P and

$$\sigma \ll L^2 \Delta^2 \sum_{\lambda,\mu} n_{f,f}(\lambda,\mu) P(\lambda) P(\mu)$$

(from the Fourier transform, say, it is easy to see that $n_{f,f}(\lambda,\mu) \ge 0$ for any function f but actually one can avoid this step of the proof). Second, we have

$$\Delta |P| \le \sum_{x \in P} |r_{f-f}(x)| \le \sum_x (r_{A-A}(x) + |A|^2/p) \le 2|A|^2$$

and

$$\Delta^2 |P| \le \sum_{x\in P} (r_{f-f}(x))^2 \le \mathsf{E}^+(f)\,.$$

Thus one can refine the upper bound for σ, namely,

$$\sigma = \mathsf{D}^\times(f) \ll L^2 |A|^5 (\mathsf{E}^+(f))^{1/2}\,.$$

Similarly as above, we get for any $k \ge 2$

$$\mathsf{D}^\times_k(f) \ll L^2 |A|^{2k+1} (\mathsf{D}^\times_{k-1}(f))^{1/2} .$$

Hence by induction

$$\mathsf{D}^\times_k(f) \ll L^4 |A|^{4k-2-2^{-k+2}} \mathsf{E}^+(f)^{1/2^{k-1}} \le L^4 |A|^{4k-2-2^{-k+2}} \mathsf{E}^+(A)^{1/2^{k-1}} . \tag{96}$$

If the third term in (94) dominates (we are considering the quantity $\mathsf{D}^\times_k(f)$ now), then the term $|A|^{4k-2}$ appears but it is easy to check that it does not exceed the last estimate in (96) because $\mathsf{E}^+(A) \ge |A|^2$. Finally, to obtain (91) use Corollary 11 to estimate the required number of incidences with weights α, β. Using

$$\mathsf{E}^+(\alpha,\beta) \le \min\{ \|\alpha\|_2 \|\beta\|_2 \|\alpha\|_1 \|\beta\|_1, \|\alpha\|^2_2 \|\beta\|^2_1, \|\alpha\|^2_1 \|\beta\|^2_2 \} \tag{97}$$

as well as $\mathsf{E}^+(\alpha,\beta) \ge \|\alpha\|^2_2 \|\beta\|^2_2$ (at other steps of our iterative procedure similar bounds work) and $\|\alpha\|_1 \ge \|\alpha\|_2$ for $\alpha(x) \ge 0$, one can check that all conditions (34) are satisfied. This completes the proof. □

Remark 33. Similarly, one can obtain an upper bound for the quantity

$$\mathsf{D}'(A) = |\{ a_1 a_2 + a_3 a_4 = a'_1 a'_2 + a'_3 a'_4 \ : \ a_i, \, a'_i \in A \}| ,$$

as well as for higher energies $\mathsf{D}'_k(A) = \mathsf{T}^+_k(r_{AA})$, $\mathsf{D}'_k(A,B)$, and even $\mathsf{D}'_k(\alpha,\beta)$ for an arbitrary non–negative function α and $\beta = A(x)$. In this case E^+ in (89)–(91) should be changed to $\mathsf{E}^\times$. Notice that our bound for $\mathsf{D}'_k(A)$ is better than the correspondent bound in [6, Theorem 2]. Some additional conditions on A and k are required in [6].

Is is easy to see that our error term for $\mathsf{D}'_k(A)$ cannot be significantly improved for large k. Indeed, considering A to be a small interval $[n]$, we get $|AA| \ge |A|^{2-\varepsilon}$ and $|kAA| \ll_k |A|^2$. Hence one cannot obtain something better than a quadratic saving for the error term.

Remark 34. The same method works for convex sets [25] in the real setting where one obtains

$$\mathsf{T}^+_k(A) \ll (\log|A|)^4 |A|^{2k-2-2^{-k+3}} \mathsf{E}^+(A)^{1/2^{k-2}} \ll (\log|A|)^4 |A|^{2k-2+2^{-k+1}}$$

for any convex set A, and we have used that $\mathsf{E}^+(A) \ll |A|^{5/2}$. This coincides with the main result of [25] up to logarithmic factors. Applying the best known bound for the additive energy of a convex set (see [48]), namely, $\mathsf{E}^+(A) \lesssim |A|^{32/13}$, we obtain an improvement.

The theorem above immediately implies a consequence on the growth of the products of the differences (here we use a trivial upper bound for the energy $\mathsf{E}^+(A) \le |A|^3$).

Corollary 35. *Let $A \subseteq \mathbb{F}_p$ be a set. Then for any $\varepsilon > 0$ and an arbitrary integer $k \ge 1$ one has*

$$|(A-A)^k| \gg \min\{p, |A|^{2-2^{1-k}-\varepsilon}\} .$$

Another quick consequence of Theorem 32 is (also, see Section 4 from [37]) the following.

Corollary 36. *Let $A \subseteq \mathbb{F}_p$ be a set, $|A| \le p^{9/16}$. Then*

$$|(A-A)(A-A)| \gg \min\{p, |A|^{3/2+c}\} ,$$

where $c > 0$ is an absolute constant.

Proof. By Theorem 32 and the Cauchy–Schwarz inequality, we obtain

$$|A|^8 \ll Q\left(\frac{|A|^8}{p} + |A|^5(\mathsf{E}^+(A))^{1/2}\log^2|A|\right)\,, \tag{98}$$

where $Q = |(A-A)(A-A)|$. Thus if the first term in (98) dominates, then we are done. Further, if $\mathsf{E}^+(A) \le |A|^{3-\varepsilon}$, where $\varepsilon > 0$ is some small constant, then we are done. If not, then put $M = |A|^\varepsilon$ and apply the Balog–Szemerédi–Gowers Theorem [57], finding $A' \subseteq A$, $|A'| \gg_M |A|$ and $|A'+A'| \ll_M |A'|$. Using Theorem 4 from [37], we have for any $a \in A$ that

$$|(A-A)(A-A)| \ge |(A-a)(A-a)| \gtrsim_M |A|^{14/9}\,,$$

provided $|A| \le p^{9/16}$. This completes the proof. □

The same argument works for the set $\frac{A-A}{A-A}$ but in this situation much better bounds are known; see [41], [56]. A lower bound for the sets of the form $(A-A)(A-A)$, $(A-A)/(A-A)$ in general fields $\mathbb{F}_q$ can be found in paper [35].

Similar arguments allow us to formulate the second part of Theorem 2 as the following.

Theorem 37. *Let $A \subseteq \mathbb{F}_p$ be a set and let $\mathsf{T}(A)$ be of collinear triples in $A \times A$. Then*

$$0 \le \mathsf{T}(A) - \frac{|A|^6}{p} \ll \min\left\{p^{1/2}|A|^{7/2}, |A|^{9/2}\right\}\,.$$

Proof. We use the arguments from [54]. Put $f(x) = A(x) - |A|/p$. It is easy to see that the quantity $\mathsf{T}(A)$ equals the number of incidences between

$$\text{the planes } \frac{x}{a''-a'} - \frac{a'}{a''-a'} - \alpha y + z = 0 \text{ and the points } \left(a, \frac{1}{\alpha''-\alpha'}, \frac{\alpha'}{\alpha''-\alpha'}\right)\,. \tag{99}$$

Hence as in the proof of Theorem 32, we have

$$\mathsf{T}(A) := \frac{|A|^6}{p} + \sigma\,,$$

where the sum σ counts the number of incidences (99) with the weight $f(a)f(\alpha)$. Hence by (31), we get $\sigma \le p|A|^3$ and by Theorem 10, we have $\sigma \ll \frac{|A|^6}{p} + |A|^{9/2}$. If $|A|^{3/2} \ge p$, then $\sigma \le p|A|^3 \le |A|^{9/2}$. If $|A|^{3/2} < p$, then $\sigma \ll \frac{|A|^6}{p} + |A|^{9/2} \ll |A|^{9/2}$. In any case $\sigma \ll |A|^{9/2}$. Combining this with the bound from Theorem 2, we obtain the required result. This completes the proof. □

For any sets $A, B, C \subseteq \mathbb{F}_p$ put

$$\mathsf{N}(A,B,C) = |\{a(b-c) = a'(b'-c') \;:\; a,a' \in A,\, b,b' \in B,\, c,c' \in C\}|\,.$$

We write $\mathsf{N}(A)$ if $A = B = C$. Now we prove an upper bound for the quantity $\mathsf{N}(A)$ which is better than $O(|A|^{9/2})$ for sets A with small energies $\mathsf{E}^\times(A)$ and $\mathsf{E}^+(A)$, namely, when $(\mathsf{E}^\times(A))^2\mathsf{E}^+(A) \ll |A|^{8-\varepsilon}$, $\varepsilon > 0$.

Corollary 38. *Let $A, B \subseteq \mathbb{F}_p$ be sets. Then*

$$\mathsf{N}(B,A,A) - \frac{|A|^4|B|^2}{p} \ll (\mathsf{E}^\times(B))^{1/2}(\mathsf{E}^+(A))^{1/4}|A|^{5/2}\log|A|\,.$$

Proof. Put $f(x) = A(x) - |A|/p$. We have

$$\begin{aligned}\mathsf{N}(B,B,A) &= \sum_\lambda r_{B/B}(\lambda) r_{(A-A)/(A-A)}(\lambda)\\ &= \frac{|A|^4|B|^2}{p} + \sum_\lambda r_{B/B}(\lambda) r_{(f-f)/(A-A)}(\lambda) := \frac{|A|^4|B|^2}{p} + \sigma\,.\end{aligned}$$

By the Cauchy–Schwarz inequality, we get

$$\sigma^2 = \left(\sum_\lambda r_{B/B}(\lambda) r_{(f-f)/(A-A)}(\lambda) \right)^2 \le \sum_\lambda r^2_{B/B}(\lambda) \cdot \sum_\lambda r^2_{(f-f)/(A-A)}(\lambda)$$

$$\le \mathsf{E}^\times(B) \left(\mathsf{D}^\times(A) - \frac{|A|^8}{p} \right) .$$

Using Theorem 32, we obtain the required result. □

Similarly to $\mathsf{N}(A)$, put

$$\mathsf{N}'(A) = |\{a_1a_2 + a_3 = a'_1a'_2 + a'_3 \ : \ a_i, \, a'_i \in A\}| . \tag{100}$$

Corollary 39. *Let $A \subseteq \mathbb{F}_p$ be a set. Then*

$$\mathsf{N}'(A) - \frac{|A|^6}{p} \ll |A|^{5/2} \mathsf{E}^+(A)^{1/2} \mathsf{E}^\times(A)^{1/4} \log |A| .$$

Proof. Put $f(x) = A(x) - |A|/p$. As in the proof of Theorem 32, we have

$$\mathsf{N}'(A) := \frac{|A|^6}{p} + \sigma ,$$

where the sum σ counts the number of the solutions to equation (100) with the weights $f(a_j)$, $f(a'_j)$. Thus by Theorem 10, the Dirichlet principle, and the Hölder inequality, we get

$$\sigma = \mathsf{E}^+(f, r_{ff}) \le (\mathsf{E}^+(f))^2 (\mathsf{E}^+(r_{ff}))^{1/2} \ll \log |A| \cdot \Delta \mathsf{E}^+(A)^{1/2} \mathsf{E}^+(r_{ff}, P)^{1/2}$$

$$\ll \log |A| \cdot \Delta \mathsf{E}^+(A)^{1/2} \left(\frac{|A|^4 |P|^2}{p} + |A|^3 |P|^{3/2} \right)^{1/2} , \tag{101}$$

where $\Delta < |r_{ff}(x)| \le 2\Delta$ on the set P. Here we have used the definition of $\mathsf{E}^+(r_{ff}, P)$, namely,

$$\mathsf{E}^+(r_{ff}, P) = |\{p + a_1a_2 = p' + a'_1a'_2 \ : \ p, p' \in P\}| ,$$

counting with the weights $f(a_1)f(a_2)$, $f(a'_1)f(a'_2)$. Again one can assume that the second term in (101) dominates. Hence using $\Delta|P| \ll |A|^2$, $\Delta^2|P| \le \mathsf{E}^\times(f) \le \mathsf{E}^\times(A)$, we obtain

$$\sigma \ll \log |A| \cdot \mathsf{E}^+(A)^{1/2} |A|^{5/2} \mathsf{E}^\times(A)^{1/4},$$

as required. □

The results above imply an estimate for some average sums of the energies (other results on such quantities can be found in [44]).

Corollary 40. *Let $A \subseteq \mathbb{F}_p$ be a set. Then*

$$\sum_{x\in X} \mathsf{E}^+(A, xA) - \frac{|X||A|^4}{p} \ll |A|^{5/4} \mathsf{E}^+(A)^{3/4} \mathsf{E}^\times(X)^{1/4} \log^{1/2} |A| .$$

Proof. Indeed, putting $f(x) = A(x) - |A|/p$, we have

$$\sigma := \sum_{x\in X} \mathsf{E}^+(A, xA) = \sum_\lambda r_{A-A}(\lambda) r_{(A-A)X}(\lambda) = \frac{|X||A|^4}{p} + \sum_\lambda r_{A-A}(\lambda) r_{(f-f)X}(\lambda) .$$

Hence by the Hölder inequality, we get

$$\sigma - \frac{|X||A|^4}{p} \ll \mathsf{E}^+(A)^{1/2} \left(\sum_\lambda r^2_{(f-f)X}(\lambda) \right)^{1/2} .$$

Using the Hölder inequality one more time, we obtain

$$\sum_\lambda r^2_{(f-f)X}(\lambda) \le \mathsf{E}^\times(X)^{1/2} \left(\mathsf{D}^\times(A) - \frac{|A|^8}{p} \right)^{1/2} .$$

Applying Theorem 32, we have finally

$$\sigma \ll |A|^{5/4} \mathsf{E}^+(A)^{3/4} \mathsf{E}^\times(X)^{1/4} \log^{1/2}|A|,$$

as required. □

Notice that it was proved in [44, Corollary 8] that for any $A \subseteq \mathbb{F}_p$, $|A| \le p^{3/5}$ there exist two disjoint sets B and C of A, each of cardinality $\ge |A|/3$, such that $\mathsf{E}^\times(B)^3 \mathsf{E}^+(C)^2 \lesssim |A|^{14}$.

6. Unconditional upper bounds for $\mathsf{D}^\times(A)$, $\mathsf{D}'(A)$ and multilinear exponential sums

The aim of this section is to prove the following.

Theorem 41. *Let $A \subseteq \mathbb{F}_p$ be a set, $|A| \le p^{2846/4991}$. Then for any $c < \frac{1}{434}$ one has*

$$\mathsf{D}^\times(A) \ll |A|^{13/2-c} .$$

Further, if $|A| \le p^{48/97}$, then for any $c_1 < \frac{1}{192}$ the following holds:

$$\mathsf{D}^\times(A) \ll |A|^{13/2-c_1} .$$

We need two lemmas from [37, Section 4.5].

Lemma 42. *Let $A \subseteq \mathbb{F}_p$ be a set and $|A+A| = M|A|$, $|A| \le p^{13/23} M^{25/92}$. Then for any $\alpha \in \mathbb{F}_p$ one has*

$$\mathsf{E}^\times(A+\alpha) \lesssim M^{51/26} |A|^{32/13} .$$

Lemma 43. *Let $A \subseteq \mathbb{F}_p$ be a set and $|AA| = M|A|$, $|A| \le p^{13/23} M^{10/23}$. Then for any $\alpha \in \mathbb{F}_p^*$ one has*

$$\mathsf{E}^\times(A+\alpha) \lesssim M^{33/13} |A|^{32/13} .$$

We have a connection between the quantities $\mathsf{E}^\times(A-\alpha)$ and $\mathsf{D}^\times(A)$, namely

$$\mathsf{D}^\times(A) \le |A|^4 \max_{\alpha \in A} \mathsf{E}^\times(A-\alpha) . \tag{102}$$

Indeed, just fix four variables a_2, a_2', a_4, a_4' in (87).

Now we are ready to prove Theorem 41.

Proof. Let K be a parameter and $D = \mathsf{D}^\times(A) - \frac{|A|^8}{p}$. Our proof is a sort of an algorithm. If $D \lesssim |A|^{13/2}/K^{1/2}$, then we are done. If not, then $\mathsf{E}^+(A) \gtrsim |A|^3/K$ because otherwise by Theorem 32 we have $D \lesssim |A|^{13/2}/K^{1/2}$. So, we suppose that $\mathsf{E}^+(A) \gtrsim |A|^3/K$. Applying the Balog–Szemerédi–Gowers Theorem (see the required form of this result in [10]), we find $A' \subseteq A$, $|A'| \gtrsim |A|/K$ such that $|A'+A'| \lesssim K^4 |A'|^3 |A|^{-2}$. By Lemma 42 and estimate (102), we have

$$\mathsf{D}^\times(A') \lesssim |A|^4 |A'|^{5/2-1/26} K^{102/13} M^{51/13} ,$$

where $M = |A'|/|A|$. The condition of the lemma takes place if

$$|A'| \le p^{13/23} (K^4 (|A'|/|A|)^2)^{25/92} \tag{103}$$

and we will check (103) later. After that consider $A\setminus A'$ and continue our algorithm with this set. We obtain disjoint sets $A_1 = A'$, $A_2, \dots$ and, clearly, $\sum_j |A_j| \le |A|$. Finally, in view of (102) and the norm property of $\mathsf{E}^\times(\cdot)$, we get an upper bound for D, namely,

$$D \lesssim |A|^{13/2}K^{-1/2} + K^{102/13}|A|^4 \left(\sum_j (|A_j|^{5/2-1/26}(|A_j|/|A|)^{51/13})^{1/4} \right)^4$$
$$\lesssim |A|^{13/2}K^{-1/2} + K^{102/13}|A|^4|A|^{5/2-1/26} .$$

Optimizing over K, that is, taking $K = |A|^{1/217}$ we obtain the required bound because condition (103) follows from

$$|A'|^{42}|A|^{50} \le |A|^{92} \le p^{52}K^{100}$$

or, in other words, from $|A| \le p^{(52+100/217)/92} = p^{2846/4991}$. Also, in view of the condition $|A| \le p^{2846/4991}$ the term $|A|^8/p$ is negligible.

Similarly, using bound (51) of Corollary 20 and the same calculations, we see that

$$D \lesssim |A|^{13/2}K^{-1/2} + K^{83/26}|A|^4|A|^{5/2-1/26} + K^{83/26} \left(\sum_j |A_j|(|A|^{5/2-1/26})^{1/4} \right)^4$$
$$\lesssim |A|^{13/2}K^{-1/2} + K^{83/26}|A|^4|A|^{5/2-1/26} .$$

Optimizing over K, that is, taking $K = |A|^{1/96}$ we obtain the required bound because the condition $|A|K \le \sqrt{p}$ follows from $|A| \le p^{48/97}$. This completes the proof. □

Remark 44. The same arguments, combining with Lemma 43 (or its refinement from [38]) allow us to prove that either $\mathsf{D}'(A) \ll |A|^{13/2-c}$ or $\mathsf{D}'(A+\alpha) \ll |A|^{13/2-c}$ for any $\alpha \neq 0$ and all sufficiently small sets A (also, see Remark 33). Here $c > 0$ is an absolute constant.

Given three sets $X, Y, Z \subseteq \mathbb{F}_p$ and three complex weights $\alpha = (\alpha_x)_{x\in X}$, $\beta = (\beta_y)_{y \in Y}$, $\gamma = (\gamma_x)_{x \in Z}$ all bounded by one, put

$$S(X,Y,Z;\alpha,\beta,\gamma) = \sum_{x\in X,\, y \in Y,\, z\in Z} \alpha_x \beta_y \gamma_z e(xyz) .$$

Similarly, for some complex weights $\rho = (\rho_{x,y})$, $\sigma = (\sigma_{x,z})$, $\tau = (\tau_{y,z})$ all bounded by one, we define

$$T(X,Y,Z;\rho,\sigma,\tau) = \sum_{x\in X,\, y \in Y,\, z\in Z} \rho_{x,y}\sigma_{x,z}\tau_{y,z} e(xyz) .$$

Such sums were studied in [40], [31]. Using Corollary 38 and Theorem 41, we improve [40, Theorems 1.3] and refine [40, Theorems 1.1] for sets with small energies (a similar bound can be obtained for a correspondent sum with four variables; see [40, Theorem 1.2, 1.4] for large range). The proof follows the arguments from [40], [31] almost literally.

Corollary 45. *Let $|X| \ge |Y| \ge |Z|$. Then*

$$S(X,Y,Z;\alpha,\beta,\gamma)$$
$$\ll \log^{1/4}|Y| \cdot p^{1/4}|X|^{3/4}|Y|^{5/8}|Z|^{1/2}(\mathsf{E}^\times(Z))^{1/8}(\mathsf{E}^+(Y))^{1/16} + |X|^{3/4}|Y||Z| ,$$

and if $|Y| < p^{48/97}$, then

$$T(X,Y,Z;\rho,\sigma,\tau) \ll p^{1/8}|X|^{7/8}|Y|^{29/32}|Z|^{29/32}(|Y||Z|)^{-1/3072} .$$

A series of applications of upper bounds for $S(X,Y,Z;\alpha,\beta,\gamma)$, $T(X,Y,Z;\rho,\sigma,\tau)$ can be found in the same papers [40], [31]. Now we obtain a quantitative form of the main result of [6].

Theorem 46. *Let $X,Y,Z \subseteq \mathbb{F}_p$ be arbitrary sets. Then for any $k \ge 2$ one has*

$$\sum_{x\in X,\, y\in Y,\, z\in Z} e(xyz) \ll |X||Y||Z| \left(|Z|^{-2^{-(k+1)}} + \left(\frac{p}{|X||Y||Z|}\right)^{2^{-(k+1)}} (|X||Y|)^{2^{-2^k}} \right) . \tag{104}$$

More generally, for any non–negative functions $\alpha(x)$, $\beta(y)$, $\gamma(z)$ the following holds:

$$\sum_{x,y,z} \alpha(x)\beta(y)\gamma(z)e(xyz) \ll p^{o(1)} \|\alpha\|_1\|\beta\|_1\|\gamma\|_1$$

$$\times \left(\left(\frac{\|\gamma\|_2^2}{\|\gamma\|_1^2}\right)^{-2^{-(k+1)}} + \left(\frac{p\|\alpha\|_2^2\|\beta\|_2^2\|\gamma\|_2^2}{\|\alpha\|_1^2\|\beta\|_1^2\|\gamma\|_1^2}\right)^{2^{-(k+1)}} \left(\frac{\|\alpha\|_1\|\beta\|_1}{\|\alpha\|_2\|\beta\|_2}\right)^{2^{-2^k}} \right) . \tag{105}$$

Proof. Let S be the sum from (104). Using the Cauchy–Schwarz inequality several times, we get for any k

$$|S|^{2^k} \le |Z|^{2^k-1} \sum_{\lambda,z} (r_{XY} *_{2^k} r_{XY})(\lambda) Z(z) e(\lambda z) .$$

Applying the Cauchy–Schwarz inequality one more time, combining with the Parseval identity, we obtain

$$|S|^{2^{k+1}} \le |Z|^{2^{k+1}-2} \mathsf{D}'_{2^k}(X,Y) p|Z| . \tag{106}$$

Put $l = 2^k$. By an analogue of Theorem 32 for $\mathsf{D}'_k(X,Y)$, see Remark 33, and bound (20), we have

$$|S|^{2^{k+1}} \ll p|Z|^{2^{k+1}-1} \left(\frac{(|X||Y|)^{2^{k+1}}}{p} + (\log|X||Y|)^8 \left(\frac{\mathsf{E}^\times(X,Y)}{|X||Y|}\right)^{2^{-l+1}} (|X||Y|)^{2^{k+1}-1} \right)$$

$$\le p|Z|^{2^{k+1}-1} \left(\frac{(|X||Y|)^{2^{k+1}}}{p} + (\log|X||Y|)^8 (|X||Y|)^{2^{-l}} (|X||Y|)^{2^{k+1}-1} \right) ,$$

as required. Similarly, to obtain (105) just use Corollary 11 (actually, in this case we do not need sharp asymptotic formulae but just the incidence results as in Theorem 10) to estimate the required number of incidences with weights α, namely,

$$\mathsf{D}'_{2^k}(\alpha,\beta) \ll L^8 \cdot \frac{(\|\alpha\|_1\|\beta\|_1)^{2^{k+1}}}{p} + L^8 \cdot (\|\alpha\|_1\|\beta\|_1)^{2^{k+1}-2} (\|\alpha\|_2\|\beta\|_2)^{2-2^{-l+2}} (\mathsf{E}^\times(\alpha,\beta))^{2^{-l+1}}$$

$$\ll L^8 \cdot (\|\alpha\|_1\|\beta\|_1)^{2^{k+1}} \left(\frac{1}{p} + \frac{\|\alpha\|_2^2\|\beta\|_2^2}{\|\alpha\|_1^2\|\beta\|_1^2} \left(\frac{\|\alpha\|_1\|\beta\|_1}{\|\alpha\|_2\|\beta\|_2}\right)^{2^{-l+1}} \right)$$

and apply the previous arguments. Here we have put

$$L = \log(\|\alpha\|_1\|\beta\|_1\|\gamma\|_1(\|\alpha\|_2\|\beta\|_2\|\gamma\|_2)^{-1}) \ll \log p$$

and also we have used the bound $\mathsf{E}^\times(\alpha,\beta) \le \|\alpha\|_2\|\beta\|_2\|\alpha\|_1\|\beta\|_1$ as in (97). This completes the proof. □

One can obtain Theorem 46 for general weights like in [6]. Also, it is known that an analogue of our result (and un upper bound for the multilinear exponential sums as well) for more than three sets follows from the case of three sets; see [6, Section 8]. We demonstrate this just for exponential sums with three and four sets; see explicit bounds (108), (109) below. In general, one can use a simple inequality which takes place for any even k_j and non–negative functions α_j

$$\left| \sum_{a_1,\dots,a_r} \alpha_1(a_1)\dots\alpha_r(a_r) e(a_1\dots a_r) \right|^{k_1\dots k_r}$$

$$\le \frac{(\prod_{j=1}^r \|\alpha_j\|_1)^{k_1\dots k_r}}{\prod_{j=1}^r \|\alpha_j\|_1^{k_j}} \sum_{a_1,\dots,a_r} (\alpha_1 *_{k_1} \alpha_1)(a_1)\dots(\alpha_r *_{k_r} \alpha_r)(a_r) e(a_1\dots a_r)$$

and ensure that the dependence on r in the saving has the form $p^{-\delta/(C_1\log(C_2 r/\delta))^r}$, where $C_1, C_2 > 0$ are absolute constants. In this case we do not need sharp asymptotic formulae but just the incidence results as in Theorem 10. The dependence in [6, Theorem A] was $p^{-(\delta/r)^{Cr}}$, where $C > 0$ is another absolute constant, so our result is better.

Corollary 47. *Let $X, Y, Z \subseteq \mathbb{F}_p$ be arbitrary sets such that for some $\delta > 0$ the following holds:*

$$|X||Y||Z| \ge p^{1+\delta} \,. \tag{107}$$

Then

$$\sum_{x\in X,\, y\in Y,\, z\in Z} e(xyz) \ll |X||Y||Z| \cdot p^{-\frac{\delta}{8\log(8/\delta)+4}} \,. \tag{108}$$

Finally, let $r = 4$; then for any sets $A_1, \dots, A_r \subseteq \mathbb{F}_p$ with $\prod_{j=1}^r |A_j| \ge p^{1+\delta}$ one has

$$\sum_{a_1\in A_1,\, \dots,\, a_r\in A_r} e(a_1\dots a_r) \ll \prod_{j=1}^r |A_j| \cdot p^{-\frac{\delta}{16\lceil 0.5\log(200/\delta)\rceil^2}} \,. \tag{109}$$

Proof. To obtain (108) we want to use Theorem 46. Put $l = 2^k$. Then using crude bounds $|X|, |Y| \le p$, we get

$$\left(\frac{p}{|X||Y||Z|} \right)^{2^{-(k+1)}} (|X||Y|)^{2^{-2^k}} \le p^{-\delta/(2l) + 2^{-l+1}} \le p^{-\delta/(4l)} \,,$$

provided

$$\frac{2^l}{l} \ge \frac{8}{\delta} \,.$$

It is easy to see that $l = \lceil 2\log(8/\delta)\rceil \ge 6$ is enough. Applying Theorem 46, we see that the second term in (104) is at most $|X||Y||Z|p^{-\frac{\delta}{8\log(8/\delta)+4}}$. The first term in this formula equals

$$|X||Y||Z| \cdot |Z|^{-1/2l} \le p^{-\delta/(4l)} \,,$$

provided $|Z| \ge p^{\delta/2}$ and hence this bound has the same quality. Suppose that $|Z| < p^{\delta/2}$. Then by (107), we obtain $|X||Y| \ge p^{1+\delta/2}$ and by a trivial bound for double exponential sums, we get

$$\sum_{x\in X,\, y\in Y,\, z\in Z} e(xyz) \ll |Z| \cdot \sqrt{p|X||Y|} = |X||Y||Z| \cdot \sqrt{p/(|X||Y|)} \le |X||Y||Z| \cdot p^{-\delta/4}$$

which is even better.

Now to get (109) we can replace all $A_i(x)$ to $A_i(x) - |A_i|/p$ if we want. Let S be the sum from (109). Also, let $\eta(x) = r_{A_1 A_2}(x)$ and $L = \log(|A_1||A_2||A_3|)$. Applying the Hölder inequality, we obtain

$$|S|^{2n} \le (|A_3| \dots |A_r|)^{2n-1} \sum_{a_3 \in A_3,\, \dots,\, a_r \in A_r} \left| \sum_x \eta(x) e(x a_3 \dots a_r) \right|^{2n}$$

$$= (|A_3| \dots |A_r|)^{2n-1} \sum_x (\eta *_{2n} \eta)(x) \sum_{a_3 \in A_3,\, \dots,\, a_r \in A_r} e(x a_3 \dots a_r)\,.$$

Applying the Hölder inequality as in Theorem 46 (see estimate (106)), combining with an analogue of (91) for D' and using $r = 4$, we obtain for any l

$$|A_3|^{-1} \sum_x (\eta *_{2n} \eta)(x) \sum_{a_3 \in A_3,\, \dots,\, a_r \in A_r} e(x a_3 \dots a_r) \frac{|A_4|}{|A_3|} \left(\frac{p \mathsf{D}'_{2l}(\eta *_{2n} \eta, A_3)}{|A_4|} \right)^{1/4l}$$

$$\ll \frac{|A_4|}{|A_3|} \Big(p|A_4|^{-1} L^8 (|A_1|^{2n} |A_2|^{2n} |A_3|)^{4l-2}$$

$$\times (\|\eta *_{2n} \eta\|_2^2 |A_3|)^{1-2^{-2l+1}} (\mathsf{E}^\times(\eta *_{2n} \eta, A_3))^{1/2^{2l-1}} \Big)^{1/4l}$$

$$\ll \frac{|A_4|}{|A_3|} \left(p|A_4|^{-1} L^{16} (|A_1|^{2n} |A_2|^{2n} |A_3|)^{4l-2} ((|A_1||A_2|)^{4n-1+2^{-2n+1}} |A_3|) |A_3|^{1/2^{2l-1}} \right)^{1/4l}$$

$$\ll |A_4| (|A_1||A_2|)^{8ln} \left(\frac{p}{|A_1||A_2||A_3||A_4|} \cdot L^{16} (|A_1||A_2|)^{2^{-2n+1}} |A_3|^{2^{-2l+1}} \right)^{1/4l}.$$

Here we have used the fact that $\mathsf{E}^\times(\eta *_{2n} \eta, A_3) \le \|\eta *_{2n} \eta\|_2^2 |A_3|^2$. So, taking $l = n$ such that $n = \lceil 0.5 \log(200/\delta) \rceil$, we obtain the required result. This completes the proof. □

7. An asymptotic variant of the Balog–Wooley decomposition theorem

Now we prove a result in the spirit of [2], [29], [42], [44]. The difference between our Theorem 48 and these results is that we have an asymptotic formula for the energy. Of course in formulae (110), (111) below the additive and multiplicative energy can be swapped (for some other sets B and C) and moreover can be replaced with other energies (see [44]).

Theorem 48. *Let $A \subseteq \mathbb{F}_p$ be a set and let $1 \le M \le p/(2|A|)$ be a parameter. There exist two disjoint subsets B and C of A such that $A = B \sqcup C$ and*

$$\mathsf{E}^+(B) - \frac{|B|^4}{p} \le \frac{|A|^{2/3} |B|^{7/3}}{M}\,, \tag{110}$$

and for any set $X \subseteq \mathbb{F}_p$ one has

$$\mathsf{E}^\times(C, X) \lesssim \frac{M^2 |X|^2 |A|^2}{p} + M^{3/2} |A| |X|^{3/2}\,. \tag{111}$$

Proof. Our proof is a sort of algorithm similar to the arguments of the proof of Theorem 41. At the first step put $B = A$ and $C = \emptyset$. Suppose that we have constructed B at some step of our algorithm. Write $f_B(x) = B(x) - |B|/p$. Then $\mathsf{E}^+(B) = \frac{|B|^4}{p} + \mathsf{E}^+(f_B, B)$. If

$$\mathsf{E}^+(f_B, B) = \sum_x B(x) r_{f_B + B - B}(x) \le \frac{|A|^{2/3} |B|^{7/3}}{M}\,,$$

then we are done. If not, then $\mathsf{E}^+(f_B,B) \ge \frac{|A|^{2/3}|B|^{7/3}}{M}$ and by the pigeonhole principle we find a set P such that $\Delta < |r_{f_B-B}(x)| \le 2\Delta$ for all $x\in P$ and

$$\frac{|A|^{2/3}|B|^{7/3}}{M} \le \mathsf{E}^+(f_B,B) \lesssim \Delta \sum_x B(x)|r_{f_B+P}(x)| \le \Delta \sum_x B(x) r_{B+P}(x) + \frac{\Delta |B|^2|P|}{p}$$
$$\le \Delta \sum_x B(x) r_{B+P}(x) + \frac{|B|^4}{p} \le 2\Delta \sum_x B(x) r_{B+P}(x)\,.$$

Here we have used the assumption $M \le p/(2|A|)$. Using Lemma 17 with $P=P$ and $A=B$, we find a set $B_* \subseteq B$ and a number q, $q\lesssim |B_*|$ such that for any $x\in B_*$ one has $r_{B+P}(x)\ge q$, and $\sum_x B(x) r_{B+P}(x) \sim |B_*|q$. We have

$$\mathsf{E}^\times(B_*,X) \le q^{-2}\left|\{(b+p)x=(b'+p')x' \;:\; x,x'\in X,\, b,b'\in B,\, p,p'\in P\}\right|\,.$$

Using Theorem 10 and the definition of q, we obtain

(112)
$$\mathsf{E}^\times(B_*,X) \ll q^{-2}\left(\frac{|X|^2|B|^2|P|^2}{p} + (|X||B||P|)^{3/2} + |X||B||P|\max\{|X|,|B|,|P|\}\right)$$
$$\lesssim (\mathsf{E}^+(f_B,B))^{-2}|B_*|^2\Delta^2\left(\frac{|X|^2|B|^2|P|^2}{p} + (|X||B||P|)^{3/2} + |X||B||P|\max\{|X|,|B|,|P|\}\right).$$

Now clearly,

$$\Delta|P| \le \sum_x r_{B-B}(x) + |B|^2 \le 2|B|^2 \tag{113}$$

and

$$\Delta^2|P| \le \sum_x r^2_{f_B-B}(x) = \mathsf{E}^+(f_B,B)\,. \tag{114}$$

Then using the last formulae, the fact that $B\subseteq A$ and returning to (112), we obtain

$$\mathsf{E}^\times(B_*,X) \lesssim (\mathsf{E}^+(f_B,B))^{-2}|B_*|^2$$
$$\times\left(\frac{|X|^2|B|^6}{p} + |X|^{3/2}|B|^{7/2}(\mathsf{E}^+(f_B,B))^{1/2} + \Delta^2|X||B||P|\max\{|X|,|B|,|P|\}\right)$$
$$\le \frac{M^2|X|^2|B_*|^2}{p} + M^{3/2}|A|^{-1}|B_*|^2|X|^{3/2}$$
$$+ M^2|A|^{-4/3}|B|^{-11/3}\Delta^2|B_*|^2|X||P|\max\{|X|,|B|,|P|\}\,. \tag{115}$$

Suppose that the third term in the last estimate is negligible. After that we consider $B\setminus B_*$ and continue our algorithm with this set. We obtain disjoint sets $A_1=B_*, A_2,\dots$ and let C be its union. Finally, in view of the norm property of $\mathsf{E}^\times(\cdot,X)$, we get an upper bound for $\mathsf{E}^\times(C,X)$, namely,

$$\mathsf{E}^\times(C,X) \le \left(\sum_j (\mathsf{E}^\times(A_j,X))^{1/2}\right)^2 \lesssim \left(\frac{M^2|X|^2}{p} + M^{3/2}|A|^{-1}|X|^{3/2}\right)\cdot\left(\sum_j |A_j|\right)^2$$
$$\le \frac{M^2|X|^2|A|^2}{p} + M^{3/2}|A||X|^{3/2}\,. \tag{116}$$

It remains to check that the third term in (115) is negligible. From (116), it follows that

$$M^3 \le |X| \le |A|^2/M^3 \tag{117}$$

because otherwise there is nothing to prove. Since, $\mathsf{E}^+(f_B, B) \ge \frac{|A|^{2/3}|B|^{7/3}}{M}$ we easily derive

$$|B| \ge \mathsf{E}^+(f_B, B)^{1/3} \gg |A|/M^{3/2}\,. \tag{118}$$

Using these bounds, as well as a trivial upper estimate $\mathsf{E}^+(f_B, B) \le |B|^3$ one can quickly check that

$$\mathsf{E}^+(f_B, B) \le M^{-1/2}|X|^{-1/2}|B|^{11/3}|A|^{1/3}\,, \quad \mathsf{E}^+(f_B, B) \le M^{-1/2}|X|^{1/2}|B|^{8/3}|A|^{1/3}$$

and

$$|B|^{1/3}M^{1/2} \le |X|^{1/2}|A|^{1/3}$$

and thus indeed the third term in (115) is negligible. This completes the proof. □

Notice that one cannot obtain an asymptotic formula as in (110) for both sets B and C. Indeed, it would imply that $|B+B|, |CC| \gg p$ but there are sets A having small sumsets and product sets, just put $A = P \cap \Gamma$, where P is a suitable arithmetic progression and Γ is a subgroup.

Now let us obtain a result on the sum–product phenomenon (of course one can replace below $+$ to $*$ and vice versa).

Corollary 49. *Let $A \subset \mathbb{F}_p$ be a set. Then either*

$$|A+A| \ge 5^{-1}\min\{|A|^{6/5}, p/2\}$$

or

$$|AA| \gtrsim \min\{p|A|^{-2/5}, |A|^{6/5}\}\,.$$

Proof. Apply Theorem 48 with $M = |A|^{1/5}$. We find two disjoint subsets B and C of A such that $A = B \sqcup C$ and estimates (110), (111) take place. If $|B| \ge |A|/2$ and $M|A| = |A|^{6/5} \le p/2$, then by (110) and the Cauchy–Schwarz inequality one has

$$|B|^4 \le |B+B|\left(\frac{|B|^4}{p} + \frac{|A|^{2/3}|B|^{7/3}}{M}\right) \le |A+A| \cdot \frac{3|A|^{2/3}|B|^{7/3}}{2M}$$

and hence $|A+A| \ge 5^{-1}|A|^{6/5}$. If $|B| \ge |A|/2$, then just consider a maximal set $A' \subseteq A$ of size $|A'|^{6/5} \le p/2$ and use the previous arguments. Finally, if $|C| \ge |A|/2$, then putting $X = A$ in (111), we obtain

$$|AA| \ge |AC| \ge \frac{|A|^2|C|^2}{\mathsf{E}^\times(A, C)} \gtrsim \min\{p|A|^{-2/5}, |A|^{6/5}\},$$

as required. □ □

8. Asymptotic formulae in $\mathrm{SL}_2(\mathbb{F}_p)$

Now we consider the action of $\mathrm{SL}_2(\mathbb{F}_p)$ on $\mathbb{F}_p$ and we begin with our version (see Theorem 50 below) of the so–called L_2–flattering lemma from [7] (also, see [9], [45]) which is a consequence of the celebrated Helfgott's Theorem 24. The proof of Theorem 50 can be found in the appendix.

Theorem 50. *Let μ be a symmetric probability measure on $\mathrm{SL}_2(\mathbb{F}_p)$ such that for a parameter $K \ge 1$ one has*
○ *$\mu(g\Gamma) \le K^{-1}$ for any proper subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{F}_p)$, $g \in \mathrm{SL}_2(\mathbb{F}_p)$ and*
○ *$\|\mu\|_\infty \le K^{-1}$.*
Then for any integer $k \le K^{c_*}$ the following holds:

$$0 \le \|\mu *_{2^k} \mu\|_2^2 - |\mathrm{SL}_2(\mathbb{F}_p)|^{-1} \le C_*^k K^{-c_* k}\,, \tag{119}$$

where $c_* \in (0,1)$, $C_* > 1$ are absolute constants.

Of course the first condition of Theorem 50 implies the second one (just consider Γ to be the trivial subgroup) but the author thinks that such formulation is more transparent.

Now we derive some consequences of Theorem 50 to sum–product phenomenon and we begin with some generalizations of arguments from [32]. Transformations

$$y = \frac{-1}{x+a}\,, \qquad y = \frac{-1}{x+a} + b,$$

correspond to $\mathrm{SL}_2(\mathbb{F}_p)$ matrices

$$s' = \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix} \in S'\,, \qquad s_{a,b} = \begin{pmatrix} b & -1+ab \\ 1 & a \end{pmatrix} \in S\,.$$

The collections S', S of such matrices are clearly connected with continued fractions

$$[a_1, a_2, \dots] = \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

and correspond to classical continuants (see, e.g., [26]), as well as continuants (entries) of the product of two matrices $\left(\begin{smallmatrix} 0 & 1 \\ 1 & a_1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & a_2 \end{smallmatrix}\right)$.

We need several properties of the set S and the first one can be found in [32] (or see the proof of Lemma 58 and Remark 60 below). It is easy to check that Lemma 51 does not hold for the set S'.

Lemma 51. *Suppose that in the definition of the set S one has $a \in C_1$, $b \in C_2$. For any $g_1, g_2 \in \mathrm{SL}_2(\mathbb{F}_p)$ and the standard Borel subgroup B the following holds:*

$$|g_1 \,\mathrm{B}\, g_2 \cap S| \le \max\{|C_1|, |C_2|\}\,. \tag{120}$$

Moreover, for any dihedral subgroup Γ one has

$$|g_1 \Gamma g_2 \cap S| \le 8 \max\{|C_1|, |C_2|\}\,. \tag{121}$$

Theorem 50, combining with Lemma 51, gives a consequence for continued fractions; see Theorem 52 below. (Indeed, consider the following two–step transformation $\frac{1}{a+\frac{1}{x+b}}$ with the correspondent map from $\mathrm{SL}_2(\mathbb{F}_p)$; then by the well–known connection of continued fractions with continuants, see, e.g., [26], we know that the components of the product of such matrices are denominators of the convergents. By the uniform distribution which follows from Theorem 50 we can represent any such denominator as well as the numerator and hence its ratio.) Another way to derive Theorem 52 iteratively applies to Corollary 61 below but this way gives worse dependence on k in $o_k(1)$.

Theorem 52. *Let $A \subseteq \mathbb{F}_p$ be a set $|A| > p^\varepsilon$, $\varepsilon > 0$. Then for any $k > C^{1/\varepsilon}$, where $C > 0$ is an absolute constant and for any $x \in \mathbb{F}_p$ one has*

$$|\{x = [a_1, a_2, \dots, a_k] \;:\; a_j \in A\}| = \frac{|A|^k}{p}(1 + o_k(1))\,.$$

Now we can formulate our "counting lemma". Here S can be any set of matrices satisfying (120), (121). Having a function $f : \mathbb{F}_p \to \mathbb{C}$ by $\langle f \rangle$ denote $\sum_{x \in \mathbb{F}_p} f(x)$.

Lemma 53. *Let $f_1, f_2 : \mathbb{F}_p \to \mathbb{C}$ be functions and $|S| > p^\varepsilon$. The number of the solutions to the equation*

$$s a_1 = a_2\,, \tag{122}$$

counting with weights $f_1(a_1)$, $f_2(a_2)$, and with the restriction $s \in S$ is

$$\frac{|S| \langle f_1 \rangle \langle f_2 \rangle}{p} + 2\theta \|f_1\|_2 \|f_2\|_2 |S| p^{-1/2^{k+2}}\,, \tag{123}$$

where $|\theta| \le 1$ and $k = k(\varepsilon)$.

Proof. Denote by σ the number of the solutions to equation (122). In terms of the generalized convolution, we have

$$\sigma = \sum_x f_2(x)(S * f_1)(x)\,.$$

Let $f(x) = f_1(x) - \langle f_1 \rangle/p$. Then

$$\sigma = \frac{|S|\langle f_1\rangle\langle f_2\rangle}{p} + \sum_x f_2(x)(S*f)(x) = \frac{|S|\langle f_1\rangle\langle f_2\rangle}{p} + \sigma_*\,. \tag{124}$$

Using the Cauchy–Schwarz inequality, we get

$$\sigma_*^2 \le \|f_2\|_2^2 \sum_x (S*f)^2(x) = \|f_2\|_2^2 \sum_x f(x)(S^{-1}*S*f)(x)\,.$$

Here $\mu(x) := (S^{-1}*S)(x) : \mathrm{SL}_2(\mathbb{F}_p) \to \mathbb{R}$ is the usual convolution on the group $\mathrm{SL}_2(\mathbb{F}_p)$. Notice that $\mu(x) = \mu(x^{-1})$ and that $\mu(x)$ is not a probability measure (but of course can easily be normalized). Also, $\|f\|_2^2 = \|f_1\|_2^2 - \langle f_1\rangle^2/p \le \|f_1\|_2^2$. Thus

$$\sigma_1 := \sigma_*^2 \le \|f_2\|_2^2 \sum_x f(x)(\mu * f)(x)$$

further by the Cauchy–Schwarz

$$\sigma_1^2 \le \|f_2\|_2^4 \|f\|_2^2 \sum_x (\mu*f)^2(x) \le \|f_2\|_2^4 \|f_1\|_2^2 \sum_x (\mu*f)^2(x)$$
$$= \|f_2\|_2^4 \|f_1\|_2^2 \sum_x f(x)(\mu*\mu*f)(x)$$

and we obtain by the iteration of the previous arguments (also, one can consult the proof of Corollary 31) that for any k one has

$$\sigma_1^{2^k} \le \|f_2\|_2^{2^{k+1}} \|f_1\|_2^{2^{k+1}-2} \sum_x f(x)(\mu *_{2^k} \mu * f)(x)\,, \tag{125}$$

where in $\mu *_{2^k} \mu$ the convolution on $\mathrm{SL}_2(\mathbb{F}_p)$ is taken 2^k-1 times (so, we have written the function μ exactly 2^k times). Now applying Lemma 22, we get

$$\sigma_* \le \|f_1\|_2\|f_2\|_2 \cdot (2p\|\mu *_{2^k} \mu\|_2)^{1/2^{k+1}} := \|f_1\|_2\|f_2\|_2 (2p\mathsf{T}^{1/2}_{2^{k+1}}(S))^{1/2^{k+1}}\,. \tag{126}$$

Here

$$\mathsf{T}_{2l}(S) = |\{ s_1^{-1}s'_1 \dots s_l^{-1}s'_l = w_1^{-1}w'_1 \dots w_l^{-1}w'_l \ : \ s_j, s'_j, w_j, w'_j \in S\}|\,.$$

Trivially, we have $\|\mu\|_\infty = |S|^{-1}$. Suppose that p is sufficiently large such that $|S| > p^\varepsilon > 60$, say, and hence in view of Lemma 51 we avoid all subgroups (1)–(3) from Theorem 23 in the sense that the conditions of Theorem 50 take place with $K = |S|^{1/2}/8$. Thus by Theorem 50, we find some $k = k(\varepsilon)$ such that

$$\mathsf{T}_{2^k}(S) \le 2|S|^{2^{k+1}} p^{-3}\,.$$

Hence in view of (126), we get

$$\sigma_* \le 2\|f_1\|_2\|f_2\|_2|S|p^{-1/2^{k+2}},$$

as required. □

Remark 54. From the proof of Theorem 50, it follows that the optimal choice of k is $k \sim \log p/\log|S|$. On the other hand, bound (123) is non-trivial if $k \ll \log\log p$. So, one can check that the assumption $|S| > p^\varepsilon$ can be relaxed to $\log|S| \gg \log p/\log\log p$ and under this condition we obtain a non-trivial bound in (123).

Now we obtain an interesting consequence of Lemma 53 to sets with small doubling (another result of the same sort about the products of sets with small doubling is contained in [32]). Combining Corollary 55 and Lemma 14 from Section 3 we derive Theorem 7 from the introduction.

Corollary 55. *Let $A_1, A_2, B \subseteq \mathbb{F}_p$, $|B| \ge p^\varepsilon$, $\varepsilon > 0$, and $|A_1+B| \le K_1|A_1|$, $|A_2+B| \le K_2|A_2|$. Then the number of the solutions to the equation*

$$r_{A_1^{-1}-A_2^{-1}}(1) = \left| \left\{ \frac{1}{a_1} - \frac{1}{a_2} = 1 \ : \ a_1 \in A_1,\, a_2 \in A_2 \right\} \right| \tag{127}$$

is at most

$$\frac{K_1K_2|A_1||A_2|}{p} + 2(K_1K_2|A_1||A_2|)^{1/2} p^{-1/2^{k+2}}\,, \tag{128}$$

where $k = k(\varepsilon)$.

Proof. Clearly, the number of the solutions to the equation (127) does not exceed

$$|B|^{-2} \left| \left\{ \frac{1}{x-b} - \frac{1}{y-c} = 1 \ : \ x \in A_1 + B,\, y \in A_2 + B,\, b, c \in B \right\} \right| .$$

In other words, we have

$$xy - (b+1)y - (c-1)x + (b+1)(c-1) + 1 = 0$$

or, equivalently, in terms of $\mathrm{SL}_2(\mathbb{F}_p)$ actions $s_{-(b+1),c-1} x = y$, where

$$s_{-(b+1),c-1} = \begin{pmatrix} c-1 & -1-(b+1)(c-1) \\ 1 & -(b+1) \end{pmatrix} \in S\,.$$

Applying Lemma 53 to sets $-(B+1)$, $C-1$, we obtain the required bound. This completes the proof. □

Thus when K_1, K_2 are small and sizes of A_1, A_2 are close to p our upper bound (128) is close to the right asymptotic formula for $r_{A_1^{-1}-A_2^{-1}}(1)$. The same can be proved in the case of Γ–invariant sets Q_1, Q_2 for its intersection $|Q_1 \cap (Q_2 + x)|$, where $x \neq 0$ is an arbitrary, see Section 4. So, these two phenomena are parallel to each other.

Now let us obtain an application to estimates for some exponential sums.

Corollary 56. *For any functions $f, g : \mathbb{F}_p \to \mathbb{C}$, $\langle f \rangle = 0$, and for any set B with $|B| \ge p^\varepsilon$, $\varepsilon > 0$ one has*

$$\sum_{x,y} f(x) g(y) \sum_{b_1, b_2 \in B} e\left(y \left(\frac{1}{x+b_1} + b_2 \right) \right) \ll \|f\|_2 \|g\|_2 \sqrt{p} |B|^2 p^{-\delta}\,. \tag{129}$$

Further, for any non-trivial multiplicative character χ, we get

$$\sum_{x,y} f(x) g(y) \sum_{b_1, b_2 \in B} \chi\left(y + b_2 + \frac{1}{x+b_1} \right) \ll \|f\|_2 \|g\|_2 \sqrt{p} |B|^2 p^{-\delta}\,, \tag{130}$$

and for $|Y| \ge p^\varepsilon$, one has

$$\sum_{x,y} f(x) Y(y) \sum_{b_1, b_2 \in B} \chi\left(y + b_2 + \frac{1}{x+b_1} \right) \ll_\varepsilon \|f\|_1 |B|^2 |Y| \cdot \left(\frac{p^{1/2-\delta} \|f\|_2^2}{\|f\|_1^2} \right)^{\varepsilon}\,. \tag{131}$$

Here $\delta = \delta(\varepsilon) > 0$.

Proof. Using the Cauchy–Schwarz inequality, we obtain

$$\left|\sum_{x,y} f(x)g(y) \sum_{b_1,b_2\in B} e\left(y\left(\frac{1}{x+b_1}+b_2\right)\right)\right|^2$$

$$\le \|g\|_2^2 p\cdot \sum_{x,x'} f(-x)\overline{f(-x')}\cdot |\{s_{b_1,b_2}x = s_{b'_1,b'_2}x' ~:~ b_1,b'_1\in -B,\, b_2,b'_2\in B\}| := \|g\|_2^2 p\cdot \sigma' \,.$$

Applying the arguments of the proof of Lemma 53 and the assumption $\sum_x f(x)=0$, we have

$$\sigma' \le 2\|f\|_2^2 |B|^4 p^{-1/2^{k+2}} := 2\|f\|_2^2 |B|^4 p^{-2\delta},$$

as required.

To obtain (130), we use the usual properties of multiplicative characters (see, e.g., [3]), namely, for any $a\neq 0$

$$\sum_x \overline{\chi(x)}\chi(x+a) = -1$$

to derive

$$\sigma^2 := \left|\sum_{x,y} f(x)g(y) \sum_{b_1,b_2\in B} \chi\left(y+b_2+\frac{1}{x+b_1}\right)\right|^2$$

$$\le \|g\|_2^2 (p-1)\cdot \sum_{x,x'} f(-x)\overline{f(-x')}\cdot |\{s_{b_1,b_2}x = s_{b'_1,b'_2}x' ~:~ b_1,b'_1\in -B,\, b_2,b'_2\in B\}|$$

$$-\|g\|_2^2 \sum_{x,x'} f(-x)\overline{f(-x')}\cdot (|B|^4 - |\{s_{b_1,b_2}x = s_{b'_1,b'_2}x' ~:~ b_1,b'_1\in -B,\, b_2,b'_2\in B\}|)$$

$$= \|g\|_2^2 p\cdot \sum_{x,x'} f(-x)\overline{f(-x')}\cdot |\{s_{b_1,b_2}x = s_{b'_1,b'_2}x' ~:~ b_1,b'_1\in -B,\, b_2,b'_2\in B\}|$$

and repeat the arguments.

Now let us use the usual Burgess' method; see, e.g., [24]. Namely, by the Hölder inequality and Weil's result (see [24, Theorem 11.23]), we get for any positive integer k

$$\sigma^{2k} \le (\|f\|_1 |B|^2)^{2k-2}\cdot \sum_{x,x'} f(x)\overline{f(x')} \left|\left\{ b_2+\frac{1}{x+b_1} = b'_2 + \frac{1}{x'+b'_1} ~:~ b_1,b'_1,b_2,b'_2\in B\right\}\right|$$

$$\times \left((2k)^k p|Y|^k + 2k\sqrt{p}|Y|^{2k}\right) \,.$$

Here as usual the term $(2k)^k p|Y|^k$ corresponds to the case when $y_1,\dots,y_k$ is a permutation of $y'_1,\dots,y'_k$ in

$$\sum_z |\sum_{y\in Y} \chi(y+z)|^{2k} = \sum_{y_1,\dots,y_k,\, y'_1,\dots,y'_k\in Y} \sum_z \chi(y_1+z)\dots\chi(y_k+z)\overline{\chi(y_1+z)}\dots\overline{\chi(y_k+z)}$$

and the term $2k\sqrt{p}|Y|^{2k}$ arises from the Weil's bound (see, e.g., [24] again). By Lemma 53 we find $l=l(\varepsilon)$ such that

(132)

$$\sum_{x,x'} f(x)\overline{f(x')} \left|\left\{ b_2+\frac{1}{x+b_1} = b'_2 + \frac{1}{x'+b'_1} ~:~ b_1,b'_1,b_2,b'_2\in B\right\}\right| \le 2\|f\|_2^2 |B|^4 p^{-1/2^{l+2}} \,.$$

Taking constant $k=\lceil 1/2\varepsilon\rceil$ such that $|Y|^k \gg_\varepsilon (2k)^k\sqrt{p}$, we obtain

$$\sigma \ll_\varepsilon \|f\|_1 |B|^2 p^{-1/k2^{l+3}} \cdot \left(\frac{\sqrt{p}\|f\|_2^2}{\|f\|_1^2}\right)^{1/2k} \le \|f\|_1 |B|^2 |Y|\cdot \left(\frac{p^{1/2-\delta}\|f\|_2^2}{\|f\|_1^2}\right)^{\varepsilon} \,.$$

Here we have denoted $1/2^{l+2}$ as δ. This completes the proof. □

Remark 57. The results above are non-trivial (suppose for simplicity that $f(x) = X(x)$ for some set X) if $|X| \gg p^{1/2-\delta}$ and the restriction to the lower bound for size of B can be extended to $\log |B| \gg \log p / \log \log p$.

Now we consider some *one–parametric* families of matrices in $\mathrm{SL}_2(\mathbb{F}_p)$ for which the above methods can be applied.

Lemma 58. *Let $B \subseteq \mathbb{F}_p$ and $S_{r_1,r_2} \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ be a set of the form*

$$s_b = \left(\begin{array}{cc} 1 & r_1(b) \\ r_2(b) & 1 + r_1(b)r_2(b) \end{array} \right) \in S_{r_1,r_2} \subseteq \mathrm{SL}_2(\mathbb{F}_p) \,,$$

where $r_1 = p_1/q_1, r_2 = p_2/q_2$ are non–constant rational functions such that

$$\{p_1p_2, p_1q_2, p_2q_1, q_1q_2\} \,, \{p_1q_1q_2, p_1p_2q_1, p_1^2p_2, q_1^2q_2, q_1^2p_2\}$$

are linearly independent over $\mathbb{F}_p$. Put

$$M := \max\{\deg(p_1), \deg(p_2), \deg(q_1), \deg(q_2)\} \,.$$

Then for any $g_1, g_2 \in \mathrm{SL}_2(\mathbb{F}_p)$ and the standard Borel subgroup B one has

$$|g_1 B g_2 \cap S_{r_1,r_2}| \le 2M \,. \tag{133}$$

Moreover, for any dihedral subgroup Γ one has

$$|g_1 \Gamma g_2 \cap S_{r_1,r_2}| \le 12M \,. \tag{134}$$

The same holds when $\{1, r_1, r_2\}$ are linearly dependent.

Proof. Take $a, b \in B$ and consider the equation

$$\left(\begin{array}{cc} xr & qx + y/r \\ zr & qz + w/r \end{array} \right) = \left(\begin{array}{cc} x & y \\ z & w \end{array} \right) \left(\begin{array}{cc} r & q \\ 0 & r^{-1} \end{array} \right) = \left(\begin{array}{cc} 1 & r_1 \\ r_2 & 1 + r_1r_2 \end{array} \right) \left(\begin{array}{cc} X & Y \\ Z & W \end{array} \right)$$

$$= \left(\begin{array}{cc} X + r_1 Z & Y + r_1 W \\ r_2 X + (1 + r_1r_2)Z & r_2 Y + (1 + r_1 r_2)W \end{array} \right) .$$

Here

$$\left(\begin{array}{cc} x & y \\ z & w \end{array} \right) \quad \text{and} \quad \left(\begin{array}{cc} X & Y \\ Z & W \end{array} \right)$$

are g_1 and g_2^{-1}, respectively. From $xr = X + r_1 Z$, $zr = r_2 X + (1 + r_1r_2)Z$, we have

$$zX + r_1 zZ = r_2 xX + xZ + r_1 r_2 xZ \,. \tag{135}$$

If $Z = 0$, then from $XW - YZ = 1$ one derives $X \neq 0$ and we arrive at $xr_2 = z$. Since $xw - yz = 1$, it follows that x, z cannot be zero simultaneously and hence r_2 is a constant. Similarly, we see that $x \neq 0$. By assumption $p_1p_2, p_1q_2, p_2q_1, q_1q_2$ are linearly independent. Hence multiplying (135) by q_1q_2, we obtain a non–zero polynomial (with the non–vanishing term xZp_1p_2) of degree at most $2M$. Thus equation (135) has at most $2M$ solutions.

Now consider any dihedral subgroup which is just a product of a cyclic group of order 4 (of order 2 in $\mathrm{PSL}_2(\mathbb{F}_p)$) and a cyclic group of order $(p \pm 1)/2$. It is easy to see that the conjugate class of any element of $\mathrm{SL}_2(\mathbb{F}_p)$ is the set of elements having the same trace and that an element with trace ± 2 is conjugated to $\pm \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$; see [55, (6.3)]. We have considered the case of elements with trace ± 2 already. As for the remaining case take any matrix of trace 2α and of the form $r_\varepsilon(\alpha, \beta) = \left(\begin{smallmatrix} \alpha & \varepsilon\beta \\ \beta & \alpha \end{smallmatrix}\right)$, where $\alpha^2 - \varepsilon\beta^2 = 1$ and $\alpha \neq \pm 1$ (hence $\varepsilon \neq 0$). One can check that for any n the element $r^n_\varepsilon(\alpha, \beta)$ has the same form, i.e., $r^n_\varepsilon(\alpha, \beta) = r_\varepsilon(\alpha_n, \beta_n)$ for some $\alpha_n, \beta_n \in \mathbb{F}_p$ and $\alpha_n^2 - \varepsilon\beta_n^2 = 1$. Then as above

$$\begin{pmatrix} \alpha x+\beta y & \varepsilon\beta x+\alpha y \\ \alpha z+\beta w & \varepsilon\beta z+\alpha w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} \alpha & \varepsilon\beta \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} 1 & r_1 \\ r_2 & 1+r_1r_2 \end{pmatrix} \begin{pmatrix} X & Y \\ Z & W \end{pmatrix}$$
$$= \begin{pmatrix} X+r_1Z & Y+r_1W \\ r_2X+(1+r_1r_2)Z & r_2Y+(1+r_1r_2)W \end{pmatrix}.$$

From this we have $X+r_1Z = \alpha x+\beta y$, $Y+r_1W = \varepsilon\beta x+\alpha y$. Hence we can find α,β via r_1, provided $\varepsilon x^2 \neq y^2$. After that, we get

$$Z = \alpha z + \beta w - r_2(X+r_1Z)\,. \tag{136}$$

Since α,β can be linearly expressed via r_1, we obtain a contradiction with the linear independence of $p_1p_2, p_1q_2, p_2q_1, q_1q_2$ provided $Z \neq 0$ (the term Zp_1p_2 does not vanish). If $Z=0$, then $W\neq 0$ and

$$\varepsilon\beta z+\alpha w = r_2Y+(1+r_1r_2)W\,. \tag{137}$$

We know that α,β can be found via r_1. It gives us a contradiction with linear independence of $p_1p_2, p_1q_2, p_2q_1, q_1q_2$ (the term Wp_1p_2 does not vanish).

It remains to consider the case $\varepsilon x^2 = y^2$. Then we obtain an analogue of (136)

$$W = \varepsilon\beta z+\alpha w - r_2(Y+r_1Z)\,. \tag{138}$$

If $\varepsilon z^2 \neq w^2$, then from $\alpha z+\beta w = r_2X+(1+r_1r_2)Z$, $\varepsilon\beta z+\alpha w = r_2Y+(1+r_1r_2)W$ we can find α,β which depends linearly on $Z+r_2(X+r_1Z)$, $W+r_2(Y+r_1W)$ and substituting them into $X+r_1Z = \alpha x+\beta y$, we obtain a contradiction with linear independence of $p_1p_2, p_1q_2, p_2q_1, q_1q_2$, provided $Z\neq 0$. More precisely, we get a dependence of the form

$$Ar_1r_2+Br_2+Zr_1+C=0\,,$$

where $A,B,C\in\mathbb{F}_p$ are some constants. If $A\neq 0$, then in the linear dependence between $p_1p_2, p_1q_2, p_2q_1, q_1q_2$ we have the non–vanishing term Ap_1p_2. Now if $A=0$, then $\{1,r_1,r_2\}$ are linearly dependent. Let $\omega = X+r_1Z$. Then from $\alpha x+\beta y=\omega$, $\alpha z+\beta w = Z+r_2\omega$, we obtain $\alpha = \omega(w-yr_2)-yZ$, $\beta = \omega(xr_2-z)+xZ$. It gives us in view of $\varepsilon x^2=y^2$ that

$$1=\alpha^2-\varepsilon\beta^2 = (\omega(w-yr_2)-yZ)^2-\varepsilon(\omega(xr_2-z)+xZ)^2$$
$$=\omega^2((w-yr_2)^2-2\varepsilon(xr_2-z)^2)-2\omega Z(y(w-yr_2)+\varepsilon x(xr_2-z))$$
$$=\omega^2(w^2-\varepsilon z^2-r_2(yw-xz\varepsilon))-2\omega Z(yw-xz\varepsilon)\,. \tag{139}$$

Since $\varepsilon z^2\neq w^2$, further $yw-xz\varepsilon\neq 0$, r_2 depends linearly on r_1 and $\omega = X+r_1Z$, $Z\neq 0$ it follows that (139) gives a non-trivial equation on r_1 of degree three. Now if $Z=0$, then $\omega = X\neq 0$ and from (139) we have a linear equation on r_2.

Finally, consider the case $\varepsilon x^2=y^2$ and $\varepsilon z^2 = w^2$. Put $Q_1 = X+r_1Z$ and $Q_2 = Z+r_2(X+r_1Z) = Z+r_2Q_1$. Then from $Q_1 = \alpha x+\beta y$, $Q_2 = \alpha z+\beta w$, we obtain $\alpha = wQ_1-yQ_2\,, \beta = -zQ_1+xQ_2$. Hence using $\varepsilon x^2 = y^2$ and $\varepsilon z^2=w^2$, we have

$$1=\alpha^2-\varepsilon\beta^2 = (wQ_1-yQ_2)^2-\varepsilon(-zQ_1+xQ_2)^2 = 2Q_1Q_2(\varepsilon xz-wy)$$
$$=2(Q_1Z+r_2(X+r_1Z)^2)(\varepsilon xz-wy)\,.$$

If $Z\neq 0$, then the last identity gives us a contradiction with linear independence of $\{p_1q_1q_2, p_1p_2q_1, p_1^2p_2, q_1^2q_2, q_1^2p_2\}$ because the term $2Z^2(\varepsilon xz-wy)p_1^2p_2$ does not vanish. If $Z=0$, then from the same equation we obtain $1=2X^2(\varepsilon xz-wy)r_2$ and hence r_2 is a constant.

Finally, a careful analysis of the proof shows that the same arguments work in the case when $\{1,r_1,r_2\}$ are linearly dependent. This completes the proof. □

Example 59. Let rational functions r_1,r_2 be just non–constant polynomials. Then $q_1=q_2=1$ and our independency conditions are satisfied.

Remark 60. By a similar argument Lemma 58 takes place for rational functions r_1, r_2 of several variables. Thus ideologically Lemma 51 follows from Lemma 58 (up to constants).

Corollary 61. *Let $p_1, p_2 \in \mathbb{F}_p[x]$ be any non–constant polynomials. Then for any $A, B \subseteq \mathbb{F}_p$, $|B| \ge p^\varepsilon$, $\varepsilon > 0$ one has*

$$\left| \left\{ p_1(b) + \frac{1}{a+p_2(b)} = p_1(b') + \frac{1}{a'+p_2(b')} \;:\; a, a' \in A,\, b, b' \in B \right\} \right| - \frac{|A|^2|B|^2}{p}$$

$$\le 2|A||B|^2 p^{-1/2^{k+2}}\,, \tag{140}$$

where $k = k(\varepsilon, \deg p_1, \deg p_2)$. In particular,

$$\left| \left\{ p_1(b) + \frac{1}{a+p_2(b)} \;:\; a \in A,\, b \in B \right\} \right| \gg \min\{p, |A|p^{1/2^{k+2}}\}\,. \tag{141}$$

Proof. Indeed, in terms of the set S_{p_1,p_2} the number of the solutions to (140) is

$$sa = s'a'\,, \qquad a, a' \in A\,, s, s' \in S_{p_2,p_1}\,,$$

or, equivalently, $(s')^{-1}sa = a'$ (we can assume that $a+p_2$ and $ap_1+1+p_1p_2$ are non-zero). Using Lemma 53, combining with Lemma 58, we obtain the required result. □

Of course Corollary 61 does not hold if either p_1 or p_2 has zero degree. Using the same arguments as in the proof of Corollary 56, we derive the following.

Corollary 62. *Let $B \subseteq \mathbb{F}_p$ and $p_1, p_2, q_1, q_2 \in \mathbb{F}_p[x]$ such that*

$$\{p_1, q_1\}\,, \{p_2, q_2\}\,, \{p_1p_2, p_1q_2, p_2q_1, q_1q_2\}\,, \{p_1q_1q_2, p_1p_2q_1, p_1^2p_2, q_1^2q_2, q_1^2p_2\}$$

are linearly independent over $\mathbb{F}_p$. Put

$$M := \max\{\deg(p_1), \deg(p_2), \deg(q_1), \deg(q_2)\}\,.$$

For any functions $f, g : \mathbb{F}_p \to \mathbb{C}$, $\sum_x f(x) = 0$, and for any set B with $|B| \ge p^\varepsilon$, $\varepsilon > 0$ one has

$$\sum_{x,y} f(x)g(y) \sum_{b\in B} e\left(y \left(\frac{q_1(b)q_2(b)x + p_1(b)q_2(b)}{p_2(b)q_1(b)x + q_1(b)q_2(b) + p_1(b)p_2(b)} \right) \right) \ll_M \|f\|_2 \|g\|_2 \sqrt{p} |B| p^{-\delta}\,. \tag{142}$$

Further, for any non-trivial multiplicative character χ and $\lambda \neq 0$, we get

$$\sum_{x,y} f(x)g(y) \sum_{b\in B} \chi\left(y + \frac{q_1(b)q_2(b)x + p_1(b)q_2(b)}{p_2(b)q_1(b)x + q_1(b)q_2(b) + p_1(b)p_2(b)} \right) \ll_M \|f\|_2 \|g\|_2 \sqrt{p} |B| p^{-\delta}\,. \tag{143}$$

Here $\delta = \delta(\varepsilon, M) > 0$.

Again, using the usual Burgess method one can obtain a non–trivial bound for sum (143) in the regime when (let $f(x) = X(x)$, $g(y) = Y(y)$ for simplicity) $|Y| \ge p^\varepsilon$, $|B| \ge p^\varepsilon$, and $|X| \gg_\varepsilon p^{1/2-\delta}$; see Remark 57 and the proof of Corollary 56.

The same method, combining with the results from [33] concerning *rich lines* (not rich hyperbolas) in $\mathbb{F}_p \times \mathbb{F}_p$ allows us to prove the following.

Theorem 63. *For any functions $f, g : \mathbb{F}_p \to \mathbb{C}$ and any sets A, B with $|B| \ge p^\varepsilon$, $|A| < p^{1-\varepsilon}$, $\varepsilon > 0$ one has*

$$\sum_{x,y} f(x)g(y) \sum_{b_1,b_2\in B} e(y(a+b_1)b_2) \ll \|f\|_2 \|g\|_2 \sqrt{p} |B|^2 p^{-\delta}\,,$$

where $\delta = \delta(\varepsilon) > 0$.

Again the result is non-trivial (suppose for simplicity that $f(x) = X(x)$ for some set X) if $|X| \gg p^{1/2-\delta}$ and the restriction to the lower bound for size of B can be extended to $\log|B| \gg \log p/\log\log p$.

9. On $\mathrm{GL}_2(\mathbb{F}_p)$–actions

In this section we consider the set of all non–degenerate matrices $\mathrm{GL}_2(\mathbb{F}_p)$ with coefficients from $\mathbb{F}_p$ and acting on the projective line. Also, let G be its subset. By $\det G$ denote the set $\det G := \{\det g \,:\, g \in G\} \subseteq \mathbb{F}_p^*$ and because $\mathrm{GL}_2(\mathbb{F}_p)$ is acting on $\mathbb{F}_p$ we can consider $G(A) := \{ga \,:\, g \in G,\, a \in A\}$ for any $A \subseteq \mathbb{F}_p$. Of course there is no expanding result similar to Theorem 24 in $\mathrm{GL}_2(\mathbb{F}_p)$ but nevertheless one can easily obtain the following.

Proposition 64. *Let $G \subseteq \mathrm{GL}_2(\mathbb{F}_p)$ be a set of matrices, $A \subseteq \mathbb{F}_p$, and let $\varepsilon > 0$ be a real number. Suppose that*
○ $|G| > p^\varepsilon$,
○ $|\det G| \le |G|p^{-\varepsilon}$,
○ $\sum_{x\in s\Gamma}(G^{-1} * G)(x) \le p^{-\varepsilon}\sum_{x\in \mathrm{SL}_2(\mathbb{F}_p)}(G^{-1} * G)(x)$ *for any proper subgroup* $\Gamma \subset \mathrm{SL}_2(\mathbb{F}_p)$, $s \in \mathrm{SL}_2(\mathbb{F}_p)$.
Then there is $\delta = \delta(\varepsilon) > 0$ such that

$$|G(A)| \gg \min\{p, |A|p^\delta\}\,.$$

Proof. Put $L = \log p$, $X = G(A)$. For any $\lambda \in \mathbb{F}_p^*$ consider $G_\lambda = \{g \in G \,:\, \det g = \lambda\}$. Using the Dirichlet principle, we find $\Lambda \subseteq \mathbb{F}_p^*$ and a number Δ such that $\Delta < |G_\lambda| \le 2\Delta$ on the set Λ and

$$\rho := \sum_{x\in \mathrm{SL}_2(\mathbb{F}_p)} (G^{-1} * G)(x) = \sum_\lambda |G_\lambda|^2 \ll L \sum_{\lambda\in\Lambda} |G_\lambda|^2 := L\rho_1\,. \tag{144}$$

Using the assumption $|\Lambda| \le |\det G| \le |G|p^{-\varepsilon}$ and the Cauchy–Schwarz inequality, we see that

$$\rho \ge |\det(G)|^{-1}\left(\sum_\lambda |G_\lambda|\right)^2 = \frac{|G|^2}{|\det G|} \ge |G|p^\varepsilon$$

and hence $\Delta \gg p^\varepsilon/L$. By the definition of the set Λ and the Cauchy–Schwarz inequality, we obtain

$$|A|^2\Delta^2|\Lambda|^2 \le \left(\sum_{\lambda\in\Lambda}|G_\lambda||A|\right)^2 = \left(\sum_{\lambda\in\Lambda}\sum_{x\in X}(G_\lambda * A)(x)\right)^2$$

$$\le |\Lambda||X|\sum_{\lambda\in\Lambda}\sum_x (G_\lambda * A)^2(x) = |\Lambda||X|\sum_{\lambda\in\Lambda}\sum_x (G_\lambda^{-1} * G_\lambda * A)(x)A(x) := |\Lambda||X|\sigma\,. \tag{145}$$

Further, consider $f(x) = \sum_{\lambda\in\Lambda}(G_\lambda^{-1} * G_\lambda)(x)$ with $\|f\|_1 = \rho_1$ and the measure $\mu(x) = f(x)/\rho_1$ and notice that

$$\sigma = \sum_{x\in A}(f * A)(x)\,.$$

Moreover,

$$\|\mu\|_\infty \ll |\Lambda|\Delta/(|\Lambda|\Delta^2) = \Delta^{-1} \ll Lp^{-\varepsilon}\,,$$

and by the assumption we see that for any proper subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{F}_p)$, $s \in \mathrm{SL}_2(\mathbb{F}_p)$ the following holds:

$$\mu(s\Gamma) = \rho_1^{-1}\sum_{x\in s\Gamma}\sum_{\lambda\in\Lambda}(G_\lambda^{-1} * G_\lambda)(x) \le \rho_1^{-1}\sum_{x\in s\Gamma}(G^{-1} * G)(x) \ll L\rho^{-1}\sum_{x\in s\Gamma}(G^{-1} * G)(x) \le Lp^{-\varepsilon}.$$

Using the arguments as in the proof of Lemma 53, we see that for some $\delta = \delta(\varepsilon) > 0$ one has

$$\sum_{\lambda \in \Lambda} \sum_{x} (G_\lambda^{-1} * G_\lambda * A)(x) A(x) - \frac{|A|^2 \rho_1}{p} \ll |A| \rho_1 p^{-\delta} \,.$$

Hence, returning to (145), we obtain

$$|A|^2 \Delta^2 |\Lambda|^2 \ll |\Lambda||X| \left(\frac{|A|^2}{p} + |A| p^{-\delta} \right) \sum_{\lambda \in \Lambda} |G_\lambda|^2 \ll |\Lambda|^2 \Delta^2 |X| \left(\frac{|A|^2}{p} + |A| p^{-\delta} \right) \,.$$

It follows that

$$|X| \gg \min\{p, |A| p^{\delta}\} \,.$$

This completes the proof. □

Remark 65. One can see from the proof that the condition $|\det G| \le |G| p^{-\varepsilon}$ can be refined to $\sum_\lambda |G_\lambda|^2 \ge |G| p^{\varepsilon}$.

Now we give the proof of a simple consequence of the theorem above (the constants 100 in (146), (147) are not really important and can certainly be decreased).

Lemma 66. *Let $B_1, B_2, B_3 \subseteq \mathbb{F}_p$ and $S \subseteq \mathrm{GL}_2(\mathbb{F}_p)$ be a set of the form*

$$s_{b_1,b_2,b_3} = \left(\begin{array}{cc} 1 & b_1 \\ b_2 & b_3 \end{array} \right) \in G \,.$$

Let $M = \max\{|B_1|, |B_2|, |B_3|\}$. Then for any $g_1, g_2 \in \mathrm{GL}_2(\mathbb{F}_p)$ one has

$$\sigma_{g_1 \mathrm{B}\, g_2}(S) \le 100 M^4 \,. \tag{146}$$

Moreover, for any dihedral subgroup Γ one has

$$\sigma_{g_1 \Gamma g_2}(S) \le 100 M^4 \,. \tag{147}$$

Proof. Take any $r_0, r_1, r_2, r_3 \in \mathbb{F}_p$ and consider the equation

$$\left(\begin{array}{cc} xr & qx + y/r \\ zr & qz + w/r \end{array} \right) \left(\begin{array}{cc} x & y \\ z & w \end{array} \right) \left(\begin{array}{cc} r & q \\ 0 & r^{-1} \end{array} \right) = \left(\begin{array}{cc} r_0 & r_1 \\ r_2 & r_3 \end{array} \right) \left(\begin{array}{cc} X & Y \\ Z & W \end{array} \right)$$

$$= \left(\begin{array}{cc} r_0 X + r_1 Z & r_0 Y + r_1 W \\ r_2 X + r_3 Z & r_2 Y + r_3 W \end{array} \right) \,.$$

From $xr = r_0 X + r_1 Z$, $zr = r_2 X + r_3 Z$, we have

$$r_0 z X + r_1 z Z = r_2 x X + r_3 x Z \,. \tag{148}$$

If $Z = 0$, then from $XW - YZ \neq 0$ one obtains $X \neq 0$ and we arrive to $xr_2 = zr_0$. Since $xw - yz \neq 0$, it follows that either x or z does not vanish and hence either r_0 or r_2 can be found uniquely. Similarly, one can consider the case $x = 0$ (Z is zero or not) and arrive at $r_0 X = -r_1 Z$. Hence either r_0 or r_1 can be found uniquely. Finally, if $Z \neq 0$ and $x \neq 0$, then we can find r_3 from (148). Now our matrix from $\mathrm{SL}_2(\mathbb{F}_p) \cap G^{-1}G$ has the form

$$(b'_3 - b'_1 b'_2)^{-2} \left(\begin{array}{cc} b'_3 & -b'_1 \\ -b'_2 & 1 \end{array} \right) \left(\begin{array}{cc} 1 & b_1 \\ b_2 & b_3 \end{array} \right) = (b'_3 - b'_1 b'_2)^{-2} \left(\begin{array}{cc} b'_3 - b'_1 b_2 & b_1 b'_3 - b'_1 b_3 \\ b_2 - b'_2 & b_3 - b_1 b'_2 \end{array} \right)$$

and such that

$$b_3 - b_1 b_2 = b'_3 - b'_1 b'_2 \neq 0 \,. \tag{149}$$

We need to estimate the number of the solutions to (149) with some restrictions as $xr_2 = zr_0$, $r_0 X = -r_1 Z$, and so on. The appeared systems of two polynomial equations are rather concrete, so it is not a difficult task (another way is to use the Bézout Theorem).

First of all notice that fixing a variable of equation (149), we obtain the contribution at most M^4 into the sum $\sigma_{g_1 \mathrm{B}\, g_2}(S)$. Second, if one expression among r_0, r_2, r_3 is fixed, then we substitute one appropriate variable into (149) and obtain the contribution at most M^4 into the sum $\sigma_{g_1 \mathrm{B}\, g_2}(S)$. If r_1 is a constant, then we consider two cases: $b_1 = 0$ and $b_1 \neq 0$. The last case allows us to substitute b'_3 into (149) and obtain a linear equation relatively to b_3 with the main coefficient $(b_1 - b'_1)$. Totally it gives the contribution at most $4M^4$. Now if $r_0 = Cr_2$ for some $C \neq 0$, then we substitute b'_2 into (149), obtain a linear equation relatively to b_2, and get the contribution at most $2M^4$. If $r_0 = Cr_1$, then either $b_1 = C^{-1}$ (contribution M^4) or $b_1 \neq C^{-1}$ and hence the substitution b'_3 into (149) gives us an equation of degree at most three and with five variables from B_j. Similarly, in the case when we find r_3 from (148) one obtains an equation degree at most three and with five variables from B_j. It gives at most $3M^4$ solutions and the total contribution into the sum $\sigma_{g_1 \mathrm{B}\, g_2}(S)$ can be estimated roughly as $100M^4$.

Now let us deal with the case of a dihedral subgroup which is just a product of a cyclic group of order 4 (of order 2 in $\mathrm{PSL}_2(\mathbb{F}_p)$) and a cyclic group of order $(p \pm 1)/2$. Then we use arguments from the proof of Lemma 58 and consider $r_\varepsilon(\alpha, \beta) = \left(\begin{smallmatrix} \alpha & \varepsilon\beta \\ \beta & \alpha \end{smallmatrix}\right)$, where $\alpha^2 - \varepsilon\beta^2 = 1$ and $\alpha \neq \pm 1$ (hence $\varepsilon \neq 0$). Again, one can check that for any n the element $r^n_\varepsilon(\alpha, \beta)$ has the same form, i.e., $r^n_\varepsilon(\alpha, \beta) = r_\varepsilon(\alpha_n, \beta_n)$ for some $\alpha_n, \beta_n \in \mathbb{F}_p$ and $\alpha_n^2 - \varepsilon\beta_n^2 = 1$. Then as above

$$\begin{pmatrix} \alpha x + \beta y & \varepsilon\beta x + \alpha y \\ \alpha z + \beta w & \varepsilon\beta z + \alpha w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} \alpha & \varepsilon\beta \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} r_0 & r_1 \\ r_2 & r_3 \end{pmatrix} \begin{pmatrix} X & Y \\ Z & W \end{pmatrix}$$

$$= \begin{pmatrix} r_0 X + r_1 Z & r_0 Y + r_1 W \\ r_2 X + r_3 Z & r_2 Y + r_3 W \end{pmatrix}.$$

From this we have $r_0 X + r_1 Z = \alpha x + \beta y$, $r_0 Y + r_1 W = \varepsilon\beta x + \alpha y$. Hence we can find α, β via r_0, r_1, provided $\varepsilon x^2 \neq y^2$. After that, we get

$$Z = Z(r_0 r_3 - r_1 r_2) = r_0(\alpha z + \beta w) - r_2(r_0 X + r_1 Z)\,. \tag{150}$$

Since α, β can be linearly expressed via r_0, r_1, we find $r_2 = (b_2 - b'_2)/(b_3 - b_1 b_2)^2$ from the last expression, provided $r_0 X + r_1 Z \neq 0$. It is easy to check that it gives us a nontrivial linear equation relatively to b'_2 because r_0, r_1 do not depend on b'_2. The possibility $r_0 X + r_1 Z = 0$ was considered above. In any case it gives the contribution at most $3M^4 + 6M^4 = 9M^4$ into the sum $\sigma_{g_1 \Gamma g_2}(S)$.

It remains to consider the case $\varepsilon x^2 = y^2$. Then we obtain an analogue of (150)

$$W = W(r_0 r_3 - r_1 r_2) = r_0(\varepsilon\beta z + \alpha w) - r_2(r_0 Y + r_1 W)\,. \tag{151}$$

If $\varepsilon z^2 \neq w^2$, then from $\alpha z + \beta w = r_2 X + r_3 Z$, $\varepsilon\beta z + \alpha w = r_2 Y + r_3 W$ we can find α, β as some linear combinations of r_2, r_3 and substituting them into $r_0 X + r_1 Z = \alpha x + \beta y$, we find r_0 or r_1 uniquely, provided $X \neq 0$ or $Z \neq 0$ (or use the arguments as above applying (150), (151)). In any case it gives the contribution at most $18M^4$ into the sum $\sigma_{g_1 \Gamma g_2}(S)$. Finally, consider the case $\varepsilon x^2 = y^2$ and $\varepsilon z^2 = w^2$. Put $Q_1 = r_0 X + r_1 Z$ and $Q_2 = r_2 X + r_3 Z$. Also, let $d = \det \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \neq 0$. Then from $Q_1 = \alpha x + \beta y$, $Q_2 = \alpha z + \beta w$, we obtain $\alpha = d^{-1}(wQ_1 - yQ_2)\,, \beta = d^{-1}(-zQ_1 + xQ_2)$. Hence

$$d^2 = d^2(\alpha^2 - \varepsilon\beta^2) = (wQ_1 - yQ_2)^2 - \varepsilon(-zQ_1 + xQ_2)^2 = 2Q_1 Q_2(\varepsilon xz - wy)$$

$$= 2(\varepsilon xz - wy)(r_0 X + r_1 Z)(r_2 X + r_3 Z)\,.$$

Using the definitions of r_j and formula (149) to exclude b'_3, we have

$$d^2(b_3 - b_1 b_2)^2 = 2(\varepsilon xz - wy)((b_3 - b_1 b_2 + b'_1 b'_2 - b'_1 b_2)X + (b_1 b_3 - b_1^2 b_2 + b_1 b'_1 b'_2 - b'_1 b_3)Z)((b_2 - b'_2)X + (b_3 - b_1 b'_2)Z)\,.$$

It gives us a quadratic equation on b_2 and the leading coefficient of this equation is

$$d^2 b_1^2 + 2(\varepsilon xz - wy) X (Z b_1^2 + X(b_1' + b_1)) .$$

If this coefficient does not vanish, then it gives us the contribution at most $2M^4$ into the sum $\sigma_{g_1 \Gamma g_2}(S)$. Suppose that $b_1 \neq 0$. In this case because $d \neq 0$ our coefficient vanishes iff $X \neq 0$ and $(2(\varepsilon xz - wy)Z + d^2 X^{-1}) b_1^2 + 2(\varepsilon xz - wy) X (b_1' + b_1) = 0$. Since $(\varepsilon xz - wy) \neq 0$, $X \neq 0$, we find b_1' uniquely. So, it gives us the contribution at most $2M^4$ into the sum $\sigma_{g_1 \Gamma g_2}(S)$. This completes the proof. □

Now we are ready to obtain a consequence of Proposition 64. Of course one can replace an upper bound for $|B_3 - B_1 B_2|$ to a lower bound for $\sum_x r^2_{B_1 - B_2 B_3}(x)$; see Remark 65 and formula (153) below. Other refinements are possible if one can estimate the number of the solutions to equation (149) with a fixed variable and under other restrictions, say,

$$C_0 r_0 + C_1 r_1 + C_2 r_2 + C_3 r_3 = 0 , \qquad \vec{0} \neq (C_0, C_1, C_2, C_3) \in \mathbb{F}_p^4 ,$$

more accurately (we need $p^{-\varepsilon} \sum_x r^2_{B_1 - B_2 B_3}(x)$ bound).

Corollary 67. *Let $A \subseteq \mathbb{F}_p$, $B_1, B_2, B_3 \subseteq \mathbb{F}_p$, $B := |B_1| = |B_2| = |B_3| > p^{\varepsilon}$. Suppose that $|B_3 - B_1 B_2| \le B^2 p^{-\varepsilon}$. Then there is $\delta = \delta(\varepsilon) > 0$ such that*

$$\left| \left\{ \frac{a + b_1}{a b_2 + b_3} \ : \ a \in A \,, b_j \in B_j \right\} \right| \gg \min\{p, |A| p^{\delta}\} . \tag{152}$$

Proof. Let $G = S_{b_1, b_2, b_3}$, $b_j \in B_j$ and define G_λ as in Proposition 64. Since $|B_3 - B_1 B_2| \le B^2 p^{-\varepsilon}$, it follows that $|\det G| \le |G| B^{-1} p^{-\varepsilon}$. Further, by Lemma 66 for any proper subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{F}_p)$, we have

$$\sum_{x \in s\Gamma} (G^{-1} * G)(x) \ll B^4$$

and

$$\sum_{x \in \mathrm{SL}_2(\mathbb{F}_p)} (G^{-1} * G)(x) = \sum_z r^2_{B_1 - B_2 B_3}(z) \ge \frac{(|B_1||B_2||B_3|)^2}{|B_3 - B_1 B_2|} \ge B^4 p^{\varepsilon} . \tag{153}$$

Thus all conditions of Proposition 64 take place for sufficiently large p. This completes the proof. □

10. Appendix

This section contains the proof of Lemma 22 and Theorem 50. Also, we obtain an upper bound for the energy E_k; see Theorem 68 and Corollary 69 below.

The proof of Lemma 22. Having a function f with $\sum_x f(x) = 0$, we consider the matrix $M(g, x) := f(g^{-1} x)$ of size $|\mathrm{SL}_2(\mathbb{F}_p)| \times p$ and its singular value decomposition [23]

$$M(g, x) = \sum_{j=1}^{p} \lambda_j u_j(g) \overline{v_j(x)} . \tag{154}$$

One can assume that $\lambda_1 \ge \lambda_2 \ge \dots \ge \lambda_p \ge 0$. Let $\vec{u} = (1, \dots, 1)$ be the vector having p ones. Since for any $y \in \mathbb{F}_p$ one has

$$(M^* M \vec{u})(y) = \sum_x \sum_g M(g, x) \overline{M(g, y)} = \sum_x \sum_g f(g^{-1} x) \overline{f(g^{-1} y)}$$

$$= \sum_g \overline{f(g^{-1} y)} \sum_x f(g^{-1} x) = p^{-1} |\mathrm{SL}_2(\mathbb{F}_p)| \cdot \left| \sum_x f(x) \right|^2 = 0 .$$

It follows that $\lambda_p = 0$. Here we have used the fact that for any $x \in \mathbb{F}_p$ the following holds: $|\mathrm{Stab}(x)| = p^{-1}|\operatorname{SL}_2(\mathbb{F}_p)|$. Further,

$$\sum_{j=1}^{p-1} |\lambda_j|^2 = \sum_{j=1}^{p} |\lambda_j|^2 = \sum_g \sum_x |M(g,x)|^2 = \sum_g \sum_x |f(g^{-1}x)|^2$$

$$= |\operatorname{SL}_2(\mathbb{F}_p)| \cdot \sum_x |f(x)|^2 = (p^3-p)\|f\|_2^2 \,. \tag{155}$$

It is easy to check that if $\vec{v}(x) \in \mathbb{F}_p^p$ is an eigenvector of $T := M^*M$, then for any $g \in \operatorname{SL}_2(\mathbb{F}_p)$ the vector $\vec{v}(gx)$ is another eigenvector of T and moreover $Tg\vec{v} = gT\vec{v}$. Thus the following linear operator Y_g defined by the formula $(Y_g h)(x) := h(gx)$, where h belongs to any eigenspace defines a representation because, obviously, $Y_{g_1}Y_{g_2} = Y_{g_1 g_2}$. By the famous Frobenius result [20] the dimension of all non-trivial irreducible representations of $\operatorname{SL}_2(\mathbb{F}_p)$ is at least $(p-1)/2$. It follows that for any eigenfunction $\vec{v}$, $\vec{v} \neq \vec{u}$ the multiplicity of the correspondent eigenvalue is at least $(p-1)/2$ (see details in [45], [10], [21]). Hence in view of (155), we obtain $\lambda_1 \le 2p\|f\|_2$. Finally, by formula (154), the orthogonality of the systems of functions u_j and v_j, the Hölder inequality, as well as our upper bound for λ_1, we have

$$\sum_x (F * f)(x)\varphi(x) = \sum_{g,x} M(g,x)F(g)\varphi(x) = \sum_{j=1}^{p-1} \lambda_j \langle F, \overline{u}_j\rangle\langle \varphi, v_j\rangle \le 2p\|F\|_2\|\varphi\|_2\|f\|_2 \,.$$

This completes the proof. □

The proof of Theorem 50. Clearly, one can assume that K is sufficiently large because otherwise (119) is trivial. Put $s = |\operatorname{SL}_2(\mathbb{F}_p)|$ and write $f(x) = \mu(x) - s^{-1}$. Then $\sum_x f(x) = 0$, $f(x^{-1}) = f(x)$, $\|f\|_1 \le 1+1 = 2$ and by induction one can check that $(f *_l f)(x) = (\mu *_l \mu)(x) - s^{-1}$, $l \in \mathbb{N}$. It gives that

$$\mathsf{T}_{2^k}(\mu) = \|\mu *_{2^k} \mu\|_2^2 = s^{-1} + \|f *_{2^k} f\|_2^2 = s^{-1} + \mathsf{T}_{2^k}(f) \,.$$

So, our task is to estimate $\|f *_{2^k} f\|_2^2$. Clearly, it is enough to prove the following bound:

$$\|f *_{2l} f\|_2^2 \ll \|f *_l f\|_2^2 \cdot K^{-c_*} := \|f *_l f\|_2^2/M \,, \tag{156}$$

where $c_* > 0$ is an absolute constant and $l \in \mathbb{N}$. Since

$$\|f *_{2l} f\|_2^2 = \sum_{x,y} (f *_{2l} f)(xy)(f *_{2l} f)(x)(f *_{2l} f)(y) \,, \tag{157}$$

it follows that by an analogue of Lemma 22 (applied to the natural action of $\operatorname{SL}_2(\mathbb{F}_p)$ onto $\operatorname{SL}_2(\mathbb{F}_p)$; see details in [18], say) that

$$\|f *_{2l} f\|_2^2 \le 2p\|f *_{2l} f\|_2 \|f *_l f\|_2^2$$

and this implies

$$\|f *_{2l} f\|_2^2 \le 4p^2\|f *_l f\|_2^4 \,.$$

Thus we can assume that

$$\|f *_l f\|_2^2 \ge \frac{1}{4Mp^2} \tag{158}$$

because otherwise there is nothing to prove. Now put $r(x) = (f *_l f)(x)$. Then, clearly,

$$\|r\|_\infty \le \|r\|_1 = \sum_x \left|(\mu *_l \mu)(x) - \frac{1}{s}\right| \le 1 + 1 = 2 \,.$$

From (157), we have

$$\mathsf{T}_{2l}(f) := \|f *_{2l} f\|_2^2 = \sum_{xy=zw} r(x)r(y)r(z)r(w)\,.$$

Put $\rho = \mathsf{T}_{2l}(f)/(8\|r\|_1^3)$. Since

$$\sum_{xy=zw \,:\, |r(x)|<\rho} r(x)r(y)r(z)r(w) \le \rho\|r\|_1^3 \le \mathsf{T}_{2l}(f)/8\,,$$

it follows that

$$\mathsf{T}_{2l}(f) \le 2 \sum_{xy=zw \,:\, |r(x)|,|r(y)|,|r(z)|,|r(w)|\ge\rho} r(x)r(y)r(z)r(w)\,.$$

Put $P_j = \{x \in \mathrm{SL}_2(\mathbb{F}_p) \;:\; \rho 2^{j-1} < |r(x)| \le \rho 2^j\}$ and $L = 8 + \log(2l)\cdot\log K$. By the assumption $k \le K^{c_*}$ and hence $L \ll k\log K \le K^{c_*}\log K$. Since $\sum_x \mu(x) = 1$, it follows that $\|\mu\|_\infty \ge s^{-1}$ and we obtain a rough upper bound for K, namely, $K \le s$. So, choosing c_* to be sufficiently small, we can suppose that for sufficiently large p one has $L < p^\epsilon$ with a given $\epsilon > 0$. Clearly, we can assume that $\mathsf{T}_{2^k}(f) \ge K^{-k}$ and hence for any x such that $|r(x)| \ge \rho$ one has

$$2^j \cdot 2^{-4} K^{-\log 2l}\|r\|_1^{-3} \le 2^j \cdot 2^{-4}\mathsf{T}_{2l}(f)\|r\|_1^{-3} = \rho 2^{j-1} < |r(x)| \le \|r\|_\infty \le 2\,.$$

It follows that the possible number of the sets P_j does not exceed L. Thus as in the proof of Theorem 25, we see that there is $P = P_{j_0}$, $\Delta = 2^{j_0-1}\rho$ such that

$$\mathsf{T}_{2l}(f) \le 2L^4(2\Delta)^4\mathsf{E}(P)\,.$$

Clearly, $\Delta^2|P| \le \mathsf{T}_l(f)$ and if (156) does not hold, then it gives us

$$M^{-1}\mathsf{T}_l(f) \le \mathsf{T}_{2l}(f) \le 2^5L^4\Delta^4|P|^3 \le 2^5L^4\mathsf{T}_l^2(f)|P|\,.$$

On the other hand, by the second assumption of the theorem and $K \le s$, we get

(159) $$\mathsf{T}_l(f) = \mathsf{T}_l(\mu) + s^{-1} \le \|\mu *_l \mu\|_\infty + s^{-1} \le \|\mu\|_\infty + s^{-1} \le 2K^{-1}\,.$$

Hence, combining the last two bounds, we obtain

(160) $$|P| \ge \frac{K}{2^6L^4M}\,.$$

Similarly, we have

$$M^{-1}\mathsf{T}_l(f) \le \mathsf{T}_{2l}(f) \le 2^5L^4\Delta^4|P|^3 \le 2^5L^4\mathsf{T}_l(f)(|P|\Delta)^2\,,$$

and hence

(161) $$|P|\Delta \ge \frac{1}{2^3L^2M^{1/2}}\,.$$

Also, we have

$$|P|\Delta \le \sum_{x\in P}|r(x)| \le \sum_x |r(x)| = \|r\|_1\,.$$

So, we see that if (156) has no place, then

$$\begin{aligned}\mathsf{T}_l(f)/M &\le \mathsf{T}_{2l}(f) \le 2L^4(2\Delta)^4\mathsf{E}(P)\\ &= 2^5L^4\Delta^4|P|^3(\mathsf{E}(P)/|P|^3) \le 2^5L^4(\Delta|P|)^2\mathsf{T}_l(f)(\mathsf{E}(P)/|P|^3)\,.\end{aligned}$$

In other words

$$\mathsf{E}(P) \ge |P|^3\cdot 2^{-5}L^{-4}M^{-1}(\Delta|P|)^{-2} \ge 2^{-7}L^{-4}M^{-1} = \zeta|P|^3\,.$$

By the Balog–Szemerédi–Gowers Theorem in the non–commutative case (see, e.g., [57, Corollary 2.46]), we see that there is $P_* \subseteq P$, $|P_*| \gg \zeta^C|P|$, $|P_*P_*^{-1}| \ll \zeta^{-C}|P_*|$, where $C > 0$ is an absolute constant. The fact $|P_*P_*^{-1}| \ll \zeta^{-C}|P_*|$ implies that there is a symmetric set H, $|H| \ll \zeta^{-C'}|P_*|$, containing the identity, and a set $|X| \ll \zeta^{-C'}$ such that $P_* \subseteq XH$ and

$$HH \subseteq XH \subseteq HXX \qquad \text{and} \qquad HH \subseteq HX \subseteq XXH; \tag{162}$$

see [57, Proposition 2.43]. Here $C' > 0$ is another absolute constant. Clearly, inclusions (162) combining with $|X| \ll \zeta^{-C'}$, imply

$$|H^3| = |H \cdot H^2| \le |H^2 \cdot X| \le |H \cdot X^2| \le |X|^2|H| \ll \zeta^{-2C'}|H| \,. \tag{163}$$

Further, since $P_* \subseteq XH$, we see that there is $x \in X$ such that

$$|H| \ge |P_* \cap xH| \ge |P_*|/|X| \gg \zeta^{C'}|P_*| \,. \tag{164}$$

By the inclusion $P_* \subseteq P$ and the definition of the set P, we have

$$\Delta\zeta^{C'}|P_*| \ll \Delta|P_* \cap xH| \le \sum_{z \in P_* \cap xH} |r(x)| \le \mu(xH) + |P_*|/s \le 2\mu(xH) \tag{165}$$

because otherwise in view of our choice of $\Delta \ge \rho$, we obtain

$$\mathsf{T}_{2l}(f)/(8\|r\|_1^3) = \rho \le \Delta \ll \zeta^{-C'}/s$$

and hence by (158), we derive (M is sufficiently small comparable to p and $L < p^\epsilon$ for sufficiently small ϵ, depending on C' only)

$$\mathsf{T}_{2l}(f) \ll L^{4C'} M^{C'} p^{-3} \ll L^{4C'} M^{C'+1} \mathsf{T}_l(f)/p \le \mathsf{T}_l(f)/M,$$

as required in (156). Thus we see that (165) takes place and whence by (161)

$$\mu(xH) \gg \Delta\zeta^{C'}|P_*| \gg \Delta|P|\zeta^{C'_1} \gg \zeta^{C'_1} L^{-2} M^{-1/2} \gg L^{-4C''} M^{-C''} \,. \tag{166}$$

Finally,

$$|H| \ll \zeta^{-C'}|P_*| \le \zeta^{-C'}\mathsf{T}_l(f)/\Delta^2 \le \zeta^{-C'}\mathsf{T}_l(f)/\rho^2 \ll \zeta^{-C'}\mathsf{T}_l(f)/\mathsf{T}^2_{2l}(f) \le p^{5/2} \,, \tag{167}$$

say, because otherwise (just the last inequality should be explained) in view of (158) and sufficiently small M, say, $M \le p^{1/12}$, we get

$$\mathsf{T}_{2l}(f) \ll \zeta^{-C'/2} p^{-5/4} \mathsf{T}_l^{1/2}(f) \ll \mathsf{T}_l(f)/M \,.$$

Using (167), lower bound (160), estimate (164), and recalling (163), we see in view of Theorem 24 that either our set H belongs to some proper subgroup Γ or

$$M^{2C'} L^{8C'} \gg \zeta^{-2C'} \gg |H|^c \gg (\zeta^{C'}|P_*|)^c \gg (\zeta^{C'+C}|P|)^c \gg K^c \zeta^{C'''} \,. \tag{168}$$

In the last inequality we have used lower bound (160). Now suppose that H belongs to a subgroup. By our assumption $\mu(g\Gamma) \le K^{-1}$ for any proper subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{F}_p)$, $g \in \mathrm{SL}_2(\mathbb{F}_p)$. Hence (166) gives us

$$K^{-1} \ge \mu(x\Gamma) \ge \mu(xH) \gg L^{-4C''} M^{-C''} \,. \tag{169}$$

Finding M satisfying both (168), (169) and using the assumption $k \le K^{c_*}$, we obtain the required dependence M on K. This completes the proof. □

Using the same method of the proof (one can check that a non–commutative analogue of Lemma 15 takes place and also, see [51, Theorem 27] and Theorem 27 above), we obtain the following.

Theorem 68. *Let μ be a symmetric probability measure on $\mathrm{SL}_2(\mathbb{F}_p)$ such that for a parameter $K \ge 1$ one has*
○ *$\mu(g\Gamma) \le K^{-1}$ for any proper subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{F}_p)$, $g \in \mathrm{SL}_2(\mathbb{F}_p)$ and*
○ *$\|\mu\|_\infty \le K^{-1}$.*
Put $f(x) = \mu(x) - |\mathrm{SL}_2(\mathbb{F}_p)|^{-1}$. Then there is $k \ll \log(\|\mu\|_2^{-1})/\log K$ such that $\mathsf{E}_{2^k}(f) \le 2\|f\|_2^{2^{k+1}}$.

Theorem 68 immediately implies (see the proof of bound (86) from Corollary 31) the following.

Corollary 69. *Let μ be a symmetric probability measure on $\mathrm{SL}_2(\mathbb{F}_p)$ such that for a parameter $K \ge 1$ one has*
○ $\mu(g\Gamma) \le K^{-1}$ *for any proper subgroup* $\Gamma \subset \mathrm{SL}_2(\mathbb{F}_p)$, $g \in \mathrm{SL}_2(\mathbb{F}_p)$ *and*
○ $\|\mu\|_\infty \le K^{-1}$.
Put $f(x) = \mu(x) - |\,\mathrm{SL}_2(\mathbb{F}_p)|^{-1}$. Then there is $k \ll \log(\|\mu\|_2^{-1})/\log K$ such that for an arbitrary function $h : \mathrm{SL}_2(\mathbb{F}_p) \to \mathbb{C}$ and any set $A \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ and a positive integer $s \le 2^k$ one has

$$\left|\sum_{x\in A} (h * f)^s(x)\right| \le |A| \|h\|_2^s \|f\|_2^s \left(\frac{2\mathsf{E}(A)}{|A|^4}\right)^{s/2^{k+2}} . \tag{170}$$

Acknowledgments

The author is grateful to Igor Shparlinski, Nikolay Moshchevitin, Brendan Murphy and Maxim Korolev for useful discussions.

References

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev, I. D. Shkredov, *Growth Estimates in Positive Characteristic via Collisions,* IMRN., Volume 2017, Issue 23 (2017), 7148–7189, https://doi.org/10.1093/imrn/rnw206 MR3802122

[2] A. Balog, T. Wooley, *A low–energy decomposition theorem,* The Quarterly Journal of Mathematics, 68.1 (2017): 207–226. MR3658289

[3] Berndt B. C., Evans R. J., Williams K. S., Gauss and Jacobi sums. John Wiley & Sons, Inc., New York, 1998. MR1625181

[4] J. Bourgain, *More on the sum–product phenomenon in prime fields and its applications,* Int. J. Number Theory, **1**:1 (2005), 1–32. MR2172328

[5] J. Bourgain, *Estimates on exponential sums related to the Diffie–Hellman distributions,* Geom. Funct. Anal., **15**:1 (2005), 1–34. MR2140627

[6] J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources,* Geom. Funct. Anal., **18**:5 (2009), 1477–1502. MR2481734

[7] J. Bourgain, *A modular Szemerédi–Trotter theorem for hyperbolas,* C. R. Math. Acad. Sci. Paris **350**:17–18 (2012), 793–796; arXiv:1208.4008v1 [math.CO] 20 Aug 2012. MR2989378

[8] J. Bourgain, M.-C. Chang, *Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors,* Geom. Funct. Anal., **16**:2 (2006), 327–366. MR2231466

[9] J. Bourgain, A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. (2), 167:2 (2008), 625–642. MR2415383

[10] J. Bourgain, M.Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields,* Math. Proc. Cambridge Philos. Soc., 146 (2009), no.1, 1–21. MR2461864

[11] J. Bourgain, M.Z. Garaev, *Sumsets of reciprocals in prime fields and multilinear Kloosterman sums,* Izvestiya: Mathematics 78.4 (2014): 656. MR3288401

[12] J. Bourgain, A. A. Glibichuk, 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. MR2225493

[13] J. Bourgain, N. Katz, T. Tao, *A sum–product estimate in finite fields and applications,* Geom. Funct. Anal., **14**:1 (2004), 27–57. MR2053599

[14] P. Erdős, E. Szemerédi, *On sums and products of integers,* Studies in pure mathematics, 213–218, Birkhäuser, Basel, 1983. MR820223

[15] M.Z. Garaev, *The sum–product estimate for large subsets of prime fields.* Proc. Amer. Math. Soc. **136**:8 (2008), 2735–2739. MR2399035

[16] M.Z. Garaev, *Sums and products of sets and estimates of rational trigonometric sums in fields of prime order,* Uspekhi Mat. Nauk, **65**:4 (2010), 599–658. MR2759693

[17] A.A. Glibichuk, S.V. Konyagin, *Additive Properties of Product Sets in Fields of Prime Order,* Additive combinatorics, CRM Proc. Lecture Notes, Amer. Math. Soc., Providence, RI, vol. 43 (2007): 279–286. MR2359478

[18] W.T. Gowers, *Quasirandom groups,* Combin. Probab. Comput., 17(3):363–387, 2008. MR2410393

[19] L. Guth, N. H. Katz. *On the Erdős distinct distances problem in the plane,* Ann. of Math. (2), **181**:1 (2015), 155–190. MR3272924

[20] G. Frobenius, *Über Gruppencharaktere, Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin,* 1896, 985–1021.

[21] N. Gill, *Quasirandom group actions,* Forum Math. Sigma. Vol. 4. 2016, e24; doi:10.1017/fms.2016.8. MR3542514

[22] H.A. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$*, Ann. of Math. (2), **167**:2 (2008), 601–623. MR2415382

[23] R.A. Horn, C.R. Johnson, *Matrix Analysis,* Cambridge University Press, Cambridge, 1985, xiii+561 pp. MR832183

[24] H. Iwaniec, E. Kowalski, *Analytic number theory,* AMS Colloqium Publications, Vol.53, AMS, Providence, RI (2004). MR2061214

[25] A. Iosevich, V. S. Konyagin, M. Rudnev, V. Ten, *Combinatorial complexity of convex sequences,* Discrete Comput. Geom. 35:1 (2006), 143–158. MR2183494

[26] A.Ya. Khinchin, *Continued fractions,* 4th ed., Nauka, Moscow 1978; English transl., Univ. Chicago Press, Chicago & London 1964. MR0161833

[27] S.V. Konyagin, *h–fold Sums from a Set with Few Products,* Moscow J. Combin. Number Theory, **4**:3 (2014), 14–20. MR3341776

[28] S.V. Konyagin, I.D. Shkredov, *On sum sets of sets, having small product sets,* Transactions of Steklov Mathematical Institute, **3**:290 (2015), 304–316. MR3488800

[29] S.V. Konyagin, I.D. Shkredov, *New results on sum-products in $\mathbb{R}$,* Proc. Steklov Inst. Math. **294** (2016), 87–98. MR3628494

[30] S. V. Konyagin, I. Shparlinski, *Character sums with exponential functions and their applications,* Cambridge Tracts in Math., vol. 136, Cambridge University Press, Cambridge, 1999. MR1725241

[31] S. Macourt, *Incidence Results and Bounds of Trilinear and Quadrilinear Exponential Sums,* SIAM J. Discrete Math., 32:2 (2018), 815–825. MR3782395

[32] N.G. Moshchevitin, B. Murphy, I.D. Shkredov, *Popular products and continued fractions,* preprint. arXiv:1808.05845.

[33] B. Murphy, *Upper and lower bounds for rich lines in grids,* arXiv:1709.10438v1 [math.CO] 29 Sep 2017.

[34] B. Murphy, G. Petridis, *A Second Wave of Expanders in Finite Fields,* Combinatorial and additive number theory, II, Springer Proc. Math. Stat., vol. 220, Springer, Cham, 2017. 215–238; arXiv:1701.01635v1 [math.CO] 6 Jan 2017. MR3754906

[35] B. Murphy, G. Petridis, *Products of Differences over Arbitrary Finite Fields,* arXiv:1705.06581v1 [math.CO] 18 May 2017.

[36] B. Murphy, G. Petridis, *A point–line incidence identity in finite fields, and applications,* Moscow J. Combin. Number Theory, 6(1):64–95, 2016. MR3529321

[37] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev, I. D. Shkredov, *New results on sum-product type growth over fields,* arXiv:1702.01003v2 [math.CO] 8 Feb 2017. MR3474329

[38] B. Murphy, M. Rudnev, I. D. Shkredov, Y.N. Shteinikov, *On the few products, many sums problem,* arXiv:1712.00410v1 [math.CO] 1 Dec 2017.

[39] G. Petridis, *Collinear triples and quadruples for Cartesian products in $\mathbb{F}_p^2$,* arXiv:1610.05620v1 [math.CO] 18 Oct 2016.

[40] G. Petridis, I.E. Shparlinski, *Bounds of trilinear and quadrilinear exponential sums,* arXiv:1604.08469v3 [math.NT] 6 Sep 2016.

[41] L. Rédei, *Lüchenhafte Polynome über endlichen Körpern,* Birkhäuser Verlag, Basel (1970). MR0294297

[42] O. Roche–Newton, M. Rudnev, I. D. Shkredov, *New sum–product type estimates over finite fields,* Adv. Math. **293** (2016), 589–605. MR3474329

[43] M. Rudnev, *On the number of incidences between points and planes in three dimensions,* Combinatorica, **38**:1 (2018), 219–254; doi:10.1007/s00493-016-3329-6. MR3776354

[44] M. Rudnev, I. D. Shkredov, S. Stevens, *On the energy variant of the sum–product conjecture,* arXiv:1607.05053.

[45] P. Sarnak, X.X.Xue, *Bounds for multiplicities of automorphic representations,* Duke Math. J. 64:1 (1991), 207–227. MR1131400

[46] T. Schoen, I. D. Shkredov, *Higher moments of convolutions,* J. Number Theory **133**:5 (2013), 1693–1737. MR3007128

[47] I.D. Shkredov, *Some new inequalities in additive combinatorics,* Moscow J. Combin. Number Theory, **3**:3–4 (2013), 189–239. MR3284125

[48] I.D. Shkredov, *Some new results on higher energies,* Transactions of MMS, **74**:1 (2013), 35–73. MR3235789

[49] I.D. Shkredov, *Some remarks on the Balog–Wooley decomposition theorem and quantities D^+, $D^\times$,* Proceedings of the Steklov Institute of Mathematics, **298**:1 (2017), 74–90.

[50] I.D. Shkredov, *Any small multiplicative subgroup is not a sumset,* arXiv:1702.01197v1 [math.NT] 3 Feb 2017.

[51] I.D. Shkredov, *Some remarks on the asymmetric sum–product phenomenon,* Moscow J. Combin. Number Theory, (2018), 101–126, dx.doi.org/10.2140/moscow.2018..101; arXiv:1705.09703v1 [math.NT] 26 May 2017.

[52] I.D. Shkredov, D. Zhelezov, *On additive bases of sets with small product set,* IMRN, Volume 2018, Issue 5 (2018), 1585–1599, https://doi.org/10.1093/imrn/rnw291; arXiv:1606.02320v2 [math.NT] 14 Jun 2016. MR3800633

[53] J. Solymosi, *Bounding multiplicative energy by the sumset,* Adv. Math., Volume **222**:2 (2009), 402–408. MR2538014

[54] S. Stevens, F. de Zeeuw, *An improved point-line incidence bound over arbitrary fields,* arXiv:1609.06284v2 [math.CO] 7 Oct 2016. MR3742451

[55] M. Suzuki, *Group Theory I,* Springer–Verlag, New York, 1982. MR648772

[56] T. Szőnyi, *Around Rédei's theorem,* Discrete Math. 208/209 (1999), 557–575. MR1725560

[57] T. Tao, V. Vu, *Additive combinatorics,* Cambridge Studies in Advanced Math., vol. 105, Cambridge University Press, Cambridge, 2006. MR2289012

[58] P. Thang, M. Tait, C. Timmons, *A Szemerédi–Trotter type theorem, sum–product estimates in finite quasifields, and related results,* J. Combin. Theory, Ser. A 147 (2017): 55–74. MR3589890

[59] L.A. Vinh, *The Szemerédi-Trotter type theorem and the sum-product estimate in finite fields,* Eur. J. Combin. **32**:8 (2011), 1177–1181. MR2838005

[60] F. de Zeeuw, *A short proof of Rudnev's point–plane incidence bound,* arXiv:1612.02719v1 [math.CO] 8 Dec 2016.

Steklov Mathematical Institute, ul. Gubkina, 8, Moscow, Russia, 119991 –and– IITP RAS, Bolshoy Karetny per. 19, Moscow, Russia, 127994 –and– MIPT, Institutskii per. 9, Dolgoprudnii, Russia, 141701

Email address: ilya.shkredov@gmail.com

Originally published in Russian