A short note on the multiplicative energy of the spectrum of a set

Shkredov I.D.

Abstract

We obtain an upper bound for the multiplicative energy of the spectrum of an arbitrary set from $\mathbb{F}_p$, which is the best possible up to the results on exponential sums over subgroups.

1 Introduction

Let p be a prime number and let A be a subset of the prime field $\mathbb{F}_p$. Denote by $\widehat{A}(r)$, $r \in \mathbb{F}_p$ the Fourier transform of the characteristic function of the set A, namely,

$$\widehat{A}(r) = \sum_{a \in A} e^{-\frac{2\pi i a r}{p}} \, .$$

Given a real number $\varepsilon \in (0, 1]$, define

$$\mathrm{Spec}_{\varepsilon}(A) = \{ r \in \mathbb{F}_p \ : \ |\widehat{A}(r)| \geqslant \varepsilon |A| \} \, . \tag{1}$$

The set $\mathrm{Spec}_{\varepsilon}(A)$ is called the *spectrum* or the *set of large exponential sums* of our set A. Such sets are studied in [18, Section 4.6], further, in [2]—[5], [11]—[14] and in many other papers. The spectrum appears naturally in any additive problem and, hence, it is important to know the structure of these sets. It is well–known that $\mathrm{Spec}_{\varepsilon}(A)$ has strong *additive* properties, see, e.g., [2], [3], [13]. This fact was used in [15] to obtain a new property of the spectrum, namely, that $\mathrm{Spec}_{\varepsilon}(A)$ has poor *multiplicative* structure. It coincides with the philosophy of the *sum–product* phenomenon, see, e.g., [18] that says that both additive and multiplicative structures do not exist simultaneously. Previously, we used the modern sum–product tools, see [9], [10] to demonstrate this poor multiplicative structure. Here we apply the main sum–product result of [9] directly and obtain

Theorem 1 *Let $A \subseteq \mathbb{F}_p$ be a set, $|A| = \delta p$ and $R \subseteq \mathrm{Spec}_{\varepsilon}(A) \setminus \{0\}$ be any set. Suppose that $p \leqslant \varepsilon^2 |A|^3$. Then*

$$|\{(x, y, z, w) \in R^4 \ : \ xy = zw\}| \ll \varepsilon^{-4} \delta^{-1} |R|^{3/2} \, . \tag{2}$$

Estimate (2) is stronger than the results of [15, Section 4] and moreover one can show (see Remarks 6, 9) that the bound in Theorem 1 is sharp up to our current knowledge of some number–theoretical questions. Also, in this paper we study other multiplicative characteristics of the spectrum, see Theorem 5 and Theorem 7, formula (15). As a byproduct we obtain by the

same method a purely sum–product result, namely, a new lower bound on $AA + AA$ for sets with small sumset.

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 $a = O(b \cdot \log^c |A|)$, $c > 0$.

2 Notation and preliminary results

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 $\widehat{f}$,

$$\widehat{f}(\xi) = \sum_{x \in \mathbb{F}_p} f(x) e(-\xi \cdot x), \tag{3}$$

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

$$\sum_{x \in \mathbb{F}_p} f(x)\overline{g(x)} = \frac{1}{p} \sum_{\xi \in \mathbb{F}_p} \widehat{f}(\xi)\overline{\widehat{g}(\xi)}. \tag{4}$$

Another particular case of (4) is

$$\sum_{y \in \mathbb{F}_p} \left| \sum_{x \in \mathbb{F}_p} f(x)g(y - x) \right|^2 = \frac{1}{p} \sum_{\xi \in \mathbb{F}_p} |\widehat{f}(\xi)|^2 |\widehat{g}(\xi)|^2. \tag{5}$$

In this paper we use the same letter to denote a set $A \subseteq \mathbb{F}_p$ and its characteristic function $A : \mathbb{F}_p \to \{0, 1\}$. Also, we write $f_A(x)$ for the *balanced function* of a set $A \subseteq \mathbb{F}_p$, namely, $f_A(x) = A(x) - |A|/p$.

Let $A \subseteq \mathbb{F}_p$ be a set, and $\varepsilon \in (0, 1]$ be a real number. We have defined the set $\mathrm{Spec}_\varepsilon(A)$ in (1) already. Clearly, $0 \in \mathrm{Spec}_\varepsilon(A)$, and $\mathrm{Spec}_\varepsilon(A) = -\mathrm{Spec}_\varepsilon(A)$. For further properties of $\mathrm{Spec}_\varepsilon(A)$ see, e.g., [2], [3], [13], [15]. Usually, we denote by δ the density of our set A, that is, $\delta = |A|/p$. From Parseval identity (4), we have a simple upper bound for size of the spectrum, namely,

$$|\mathrm{Spec}_\varepsilon(A)| \leqslant \frac{p}{|A|\varepsilon^2} = \frac{1}{\delta\varepsilon^2}. \tag{6}$$

Put $\mathsf{E}^+(A, B)$ for the *common additive energy* of two sets $A, B \subseteq \mathbb{F}_p$ (see, e.g., [18]), 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. One can consider $\mathsf{E}^+(f)$ for any complex function f as well. Sometimes we use representation function notations like $r_{AB}(x)$ or $r_{A+B}(x)$, which counts the number of ways $x \in \mathbb{F}_p$ can be expressed as a product ab or a sum $a + b$ with $a \in A$, $b \in B$, respectively. Put $\sigma^+(A) = \sum_{x \in A} r_{A-A}(x)$. Further clearly

$$\mathsf{E}^+(A, B) = \sum_x r_{A+B}^2(x) = \sum_x r_{A-B}^2(x) = \sum_x r_{A-A}(x) r_{B-B}(x)$$

and by (5),

$$\mathsf{E}^+(A, B) = \frac{1}{p} \sum_\xi |\widehat{A}(\xi)|^2 |\widehat{B}(\xi)|^2 \,. \tag{7}$$

Similarly, one can define $\mathsf{E}^\times(A, B)$, $\mathsf{E}^\times(A)$, $\mathsf{E}^\times(f)$ and so on.

Now we recall some results from the incidence geometry, see, e.g., [18, Section 8]. First of all, we need a general design bound for the number of incidences, see [16, 19, 20]. 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 $p \in \mathcal{P}$ and $\pi \in \Pi$, we write

$$\mathcal{I}(p, \pi) = \left\{ \begin{array}{ll} 1 & \text{if } q \in \pi \\ 0 & \text{otherwise.} \end{array} \right.$$

Put $\mathcal{I}(\mathcal{P}, \Pi) = \sum_{p \in \mathcal{P}, \pi \in \Pi} \mathcal{I}(p, \pi)$. We have (see [16])

Lemma 2 *For any functions $\alpha : \mathcal{P} \to \mathbb{C}$, $\beta : \Pi \to \mathbb{C}$ one has*

$$|\sum_{p, \pi} \mathcal{I}(p, \pi) \alpha(p) \beta(\pi)| \leqslant q \|\alpha\|_2 \|\beta\|_2 \,, \tag{8}$$

provided either $\sum_{p \in \mathcal{P}} \alpha(p) = 0$ or $\sum_{\pi \in \Pi} \beta(\pi) = 0$.

Of course, similar arguments work not just for points/planes incidences but, e.g., points/lines incidences and so on. A much more deep result on incidences is contained in [9] (or see [7, Theorem 8]). We formulate a combination of these results and Lemma 2, see [16].

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

$$\mathcal{I}(\mathcal{P}, \Pi) - \frac{|\mathcal{P}||\Pi|}{p} \ll |\mathcal{P}|^{1/2}|\Pi| + k|\mathcal{P}| \,. \tag{9}$$

Finally, we recall a simple asymptotic formula for the number of points/lines incidences in the case when the set of points forms a Cartesian product, see [17] and also [16].

Theorem 4 *Let $A, B \subseteq \mathbb{F}_p$ be sets, $|A| \leqslant |B|$, $\mathcal{P} = A \times B$, and $\mathcal{L}$ be a collection of lines in $\mathbb{F}_p^2$. Then*

$$\mathcal{I}(\mathcal{P}, \mathcal{L}) - \frac{|A||B||\mathcal{L}|}{p} \ll |A|^{3/4}|B|^{1/2}|\mathcal{L}|^{3/4} + |\mathcal{L}| + |A||B| \,. \tag{10}$$

3 The proof of the main results

Let $A \subseteq \mathbb{F}_p$ be a set. We write

$$\mathsf{E}_k^{\times}(A) = \sum_x r_{A/A}^k(x)$$

for any $k \geqslant 1$. Our aim is to obtain an upper bound for $\mathsf{E}_2^{\times}$–energy of the spectrum but before that we prove an optimal result for $\mathsf{E}_4^{\times}$ which is interesting in its own right. We use arguments similar to [8].

Theorem 5 *Let $A \subseteq \mathbb{F}_p$ be a set, $|A| = \delta p$ and $R = \operatorname{Spec}_{\varepsilon}(A) \setminus \{0\}$. Then*

$$\mathsf{E}_4^{\times}(R) \lesssim \varepsilon^{-16} \delta^{-4} \left(\frac{\mathsf{E}^+(f_A)}{|A|^3} \right)^2 . \tag{11}$$

P r o o f. Applying formula (7) and the definition of the spectrum (1), we notice that

$$\frac{(\varepsilon|A|)^4}{p} \cdot r_{R/R}(\lambda) \leqslant p^{-1} \sum_{x \in R,\, \lambda x \in R} |\widehat{A}(x)|^2 |\widehat{A}(\lambda x)|^2 \leqslant p^{-1} \sum_x |\widehat{f_A}(x)|^2 |\widehat{f_A}(\lambda x)|^2 = \mathsf{E}^+(f_A, \lambda f_A) .$$

Hence

$$\mathsf{E}_4^{\times}(R) \leqslant (\varepsilon|A|)^{-16} p^4 \sum_{\lambda} \mathsf{E}^+(f_A, \lambda f_A)^4 = (\varepsilon|A|)^{-16} p^4 \sum_{\lambda} r_{(f_A - f_A)/(f_A - f_A)}^4(\lambda) = (\varepsilon|A|)^{-16} p^4 \cdot \sigma .$$

By the Dirichlet principle there is $\Delta > 0$ and a set P such that $\Delta < |r_{f_A - f_A}(\lambda)| \leqslant 2\Delta$ on P and

$$\sigma \lesssim \Delta^4 \sum_{\lambda} r_{(f_A - f_A)/P}^4(\lambda) = \Delta^4 \sum_{\lambda} |\{\lambda p = a_1 - a_2 \;:\; p \in P\}|^4 ,$$

where a_1, a_2 have weights $f_A(a_1), f_A(a_2)$, correspondingly. Let $\tau > 0$ and S_{τ} be the set of all λ such that $|r_{(f_A - f_A)/P}(\lambda)| \geqslant \tau$. Since $r_{(f_A - f_A)/P}(\lambda) = r_{(A-A)/P}(\lambda) + \delta^2 p|P|$, it follows that

$$\tau|S_{\tau}| \leqslant \sum_{\lambda \in S_{\tau}} |r_{(f_A - f_A)/P}(\lambda)| \leqslant |A|^2 |P| + \delta^2 |P| p^2 = 2|A|^2 |P| .$$

In particular, $|S_{\tau}| \leqslant 2|A|^2 |P|/\tau$. The number of the solutions to the equation $sp = a_1 - a_2$ can be interpreted as the number of incidences between the set of lines $\mathcal{L} = S_{\tau} \times A$, counting with the weight $f_A(a_1)$ and the sets of points $\mathcal{P} = A \times P$, again counting with the weight $f_A(a_2)$. Applying Theorem 4, we obtain

$$\tau|S_{\tau}| = \mathcal{I}(\mathcal{P}, \mathcal{L}) \ll |A|^{3/2} |P|^{1/2} |S_{\tau}|^{3/4} + |S_{\tau}||A| + |A||P| . \tag{12}$$

If the first term dominates, then we have

$$|S_{\tau}| \ll |A|^6 |P|^2 / \tau^4 . \tag{13}$$

In view of the inequality $|S_\tau| \leqslant 2|A|^2|P|/\tau$ one can suppose that $\tau^3 \gg |A|^4|P| \geqslant |A|^3$ because otherwise it is nothing to prove. It gives us that $\tau \gg |A|$ and hence the second term in (12) is negligible. We will consider the case when the third term in (12) dominates later but now let us remark that in this case $\tau^3 \gg |A|^5|P|$ because otherwise it is nothing to prove. Thus, by summation of formula (13), we obtain

$$\sigma \lesssim |A|^6|P|^2$$

and hence

$$\mathsf{E}_4^\times(R) \lesssim (\varepsilon|A|)^{-16}p^4|A|^6\Delta^4|P|^2 \leqslant \varepsilon^{-16}\delta^{-4}\mathsf{E}^+(f_A)^2/|A|^6$$

as required. It remains to consider the case when the third term in (12) dominates and we know that $\tau^3 \gg |A|^5|P|$. In other words, if we consider the ordering

$$|r_{(f_A-f_A)/P}(s_1)| \geqslant |r_{(f_A-f_A)/P}(s_2)| \geqslant \ldots \geqslant |r_{(f_A-f_A)/P}(s_j)| \geqslant \ldots,$$

then there is an effective bound $|r_{(f_A-f_A)/P}(s_j)| \leqslant |A||P|j^{-1}$ for $j \geqslant J := (|P|/|A|)^{2/3}$. Again, by summation we obtain

$$\sigma \ll \sum_{j\geqslant J}(|A||P|/j)^4 \ll |A|^4|P|^4J^{-3} \ll |P|^2|A|^6$$

and it gives the same bound for $\mathsf{E}_4^\times(R)$. This completes the proof. $\qquad\qquad\square$

Remark 6 *Let A be a multiplicative subgroup of order $p^{2/3}$. Then the best known bound for the Fourier coefficients of A is $|\widehat{A}(r)| < \sqrt{p}$, $\forall r \neq 0$, see, e.g., [6]. On the other hand, taking R equals a coset of A belonging to $\mathrm{Spec}_\varepsilon(A) \setminus \{0\}$, we see that $\mathsf{E}_4^\times(R) \geqslant |R|^5 = |A|^5$. Applying formulae (4), (7), we get*

$$\mathsf{E}^+(f_A) < \left(\max_{r\neq 0}|\widehat{A}(r)|\right)^2|A|$$

and hence estimate (11) of Theorem 5 is tight (up to our current knowledge of the Fourier coefficients of multiplicative subgroups).

Unfortunately, the method of the proof of Theorem 5 works for $\mathsf{E}_4^\times(R)$ but not for $\mathsf{E}_k^\times(R)$ with $k < 4$. In this case we obtain

Theorem 7 *Let $A \subseteq \mathbb{F}_p$ be a set, $|A| = \delta p$ and $R \subseteq \mathrm{Spec}_\varepsilon(A) \setminus \{0\}$ be any set. Suppose that $p \leqslant \varepsilon^2|A|^3$. Then*

$$\mathsf{E}^\times(R) \ll \varepsilon^{-4}\delta^{-1}|R|^{3/2} . \tag{14}$$

Similarly,

$$\sigma^\times(R) \lesssim \varepsilon^{-4}\delta^{-1}|R|^{3/4}\left(\frac{\mathsf{E}^+(f_A)}{|A|^3}\right)^{1/2} + \varepsilon^{-4}\delta^{-1}\left(1 + \frac{|R|}{|A|}\right) . \tag{15}$$

P r o o f. Using the Fourier transform similar to the proof of Theorem 5, we have

$$\frac{(\varepsilon|A|)^4}{p} \cdot \mathsf{E}^\times(R) \leqslant p^{-1} \sum_{\lambda,\mu\in R} \sum_x |\widehat{f_A}(\lambda x)|^2 |\widehat{f_A}(\mu x)|^2 = \sum_x r^2_{(f_A-f_A)R}(x)\,.$$

Clearly, the last quantity can be interpreted as points/planes incidences (with weights), see [1]. Here the number of the points and planes is at most $O(|A|^2|R|)$. Finally, using our assumption, we get from (6)

$$|R| \leqslant \frac{p}{\varepsilon^2|A|} \leqslant |A|^2\,.$$

Applying Theorem 3, we obtain

$$\sum_x r^2_{(f_A-f_A)R}(x) \ll |A|^3|R|^{3/2}\,.$$

It follows that

$$\mathsf{E}^\times(R) \ll \varepsilon^{-4}\delta^{-1}|R|^{3/2}\,.$$

as required.

Similarly,

$$\sigma^\times(R) \leqslant (\varepsilon|A|)^{-4} \sum_{\lambda\in R}\sum_x |\widehat{f_A}(x)|^2|\widehat{f_A}(\lambda x)|^2 = \varepsilon^{-4}\delta^{-1}|A|^{-3}\sum_{\lambda\in R} r_{(f_A-f_A)/(f_A-f_A)}(\lambda)\,.$$

After that we can use the arguments and the notation from the proof of Theorem 5 (with $S_\tau = R$) and derive that

$$\sum_{\lambda\in R} r_{(f_A-f_A)/(f_A-f_A)}(\lambda) \lesssim \Delta|P|^{1/2}|R|^{3/4}|A|^{3/2} + \Delta|A|(|P|+|R|) \ll$$

$$\ll (\mathsf{E}^+(f_A))^{1/2}|R|^{3/4}|A|^{3/2} + |A|^3 + |A|^2|R|\,.$$

Here we have used a trivial bound $\Delta \leqslant 2|A|$. It gives us

$$\sigma^\times(R) \lesssim \varepsilon^{-4}\delta^{-1}|R|^{3/4}(\mathsf{E}^+(f_A)/|A|^3)^{1/2} + \varepsilon^{-4}\delta^{-1} + \varepsilon^{-4}\delta^{-1}|R|/|A|$$

and this coincides with (15). □

Example 8 *Let $\varepsilon \gg 1$, $R = \operatorname{Spec}_\varepsilon(A) \setminus \{0\}$, and let size of R is comparable with the upper bound which is given by (6), namely, $|R| \gg \delta^{-1}\varepsilon^{-2} \gg \delta^{-1}$. Then $\mathsf{E}^\times(R) \lesssim |R|^{5/2}$. It means that we have a non–trivial estimate for the multiplicative energy of the spectrum in this case. Similarly, we always have $\mathsf{E}^+(f_A) < |A|^3$, so $\sigma^\times(R) \lesssim |R|^{7/4} + |R|^2/|A|$.*

Remark 9 *The same construction as in Remark 6 shows the tightness of bounds (14), (15), again up to our current knowledge of the Fourier coefficients of multiplicative subgroups.*

In the same vein we obtain a result on the growth of $AA+AA$, which improves [16, Theorem 32] for small $\mathsf{E}_4^\times(A)$.

Theorem 10 *Let $A \subseteq \mathbb{F}_p$ be sets. Then*

$$\sum_x r^2_{AA+AA}(x) - \frac{|A|^8}{p} \lesssim |A|^4 (\mathsf{E}_4^\times(A))^{1/2} + \mathsf{E}_4^\times(A)|A|^2. \tag{16}$$

P r o o f. Without loosing of the generality, one can assume that $0 \notin A$. We need to estimate the number of the solutions to the equation

$$a_1/a \cdot a_1'/a' + a_2/a \cdot a_2'/a' - a_3/a \cdot a_3'/a' = 1,$$

where $a, a', a_j, a_j' \in A$, $j = 1, 2, 3$. Put

$$\mathsf{C}_4^\times(A)(\alpha, \beta, \gamma) := |A \cap \alpha A \cap \beta A \cap \gamma A|.$$

One can check that

$$\sum_{\alpha, \beta, \gamma} \mathsf{C}_4^\times(A)(\alpha, \beta, \gamma) = |A|^4,$$

and

$$\sum_{\alpha, \beta, \gamma} \mathsf{C}_4^\times(A)(\alpha, \beta, \gamma)^2 = \mathsf{E}_4^\times(A). \tag{17}$$

In these terms, we want to bound the sum

$$\sigma := \sum_{\alpha, \beta, \gamma} \sum_{\alpha', \beta', \gamma'} \mathsf{C}_4^\times(A)(\alpha, \beta, \gamma) \mathsf{C}_4^\times(A)(\alpha', \beta', \gamma') \delta(\alpha\alpha' + \beta\beta' - \gamma\gamma' = 1),$$

where $\delta(x = 1)$ equals one iff $x = 1$. Using the Dirichlet principle as in the proof of Theorems 5, 7, we find two numbers $\Delta_1, \Delta_2 > 0$ and two corresponding sets of points and planes $\mathcal{P}, \Pi$ such that

$$\sigma \lesssim \Delta_1 \Delta_2 \sum_{\alpha, \beta, \gamma} \sum_{\alpha', \beta', \gamma'} \mathcal{P}(\alpha, \beta, \gamma) \Pi(\alpha', \beta', \gamma') \delta(\alpha\alpha' + \beta\beta' - \gamma\gamma' = 1).$$

Without loosing of the generality, suppose that $|\mathcal{P}| \leqslant |\Pi|$. Also, notice that $|\mathcal{P}|, |\Pi| \leqslant |A|^4$. Applying Theorem 3 (previously inserting the balanced function $f_A(x) = A(x) - |A|/p$ as in the proofs of Theorems 5, 7) with the maximal number of collinear points $k \leqslant |A|^2$ and using formula (17), combining with Lemma 8, we get

$$\sigma \lesssim \Delta_1 \Delta_2 |\mathcal{P}||\Pi|^{1/2} + \Delta_1 \Delta_2 k|\mathcal{P}| + |\mathcal{P}|^{1/2} \mathsf{E}_4^\times(f_A) \leqslant$$

$$\leqslant (\Delta_2^2 |\Pi|)^{1/2} \Delta_1 |\mathcal{P}| + k(\Delta_1^2 |\mathcal{P}|)^{1/2} (\Delta_2^2 |\Pi|)^{1/2} + |A|^2 \mathsf{E}_4^\times(f_A) \leqslant$$

$$\leqslant (\mathsf{E}_4^\times(A))^{1/2} |A|^4 + \mathsf{E}_4^\times(A)|A|^2.$$

This completes the proof. $\qquad\square$

Corollary 11 *Let $A \subseteq \mathbb{F}_p$, $|A + A| = K|A|$ and $|A + A|^3 |A| \leqslant p^3$. Then*

$$|AA + AA| \gtrsim \min\{p, \Omega_K(|A|^2)\}.$$

P r o o f. Using [7, Lemma 18] (where, actually, a better dependence on K is suggested) or just applying the arguments of the proof of Theorem 5, we get

$$\mathsf{E}_4^\times(r_{B+C}) - \frac{|B|^8|C|^8}{p^3} \lesssim \mathsf{E}^+(B,C)^2|B|^3|C|^3\,.$$

Putting $B = A + A$, $C = -A$ and noting that $|A|A(x) \leqslant r_{B+C}(x)$, we obtain

$$\mathsf{E}_4^\times(A) - \frac{|A+A|^8}{p^3} \lesssim |A+A|^5|A|^{-1}\,. \tag{18}$$

Obviously, by the Cauchy–Schwartz inequality, we have

$$|A|^8 \leqslant |AA+AA| \cdot \sum_x r_{AA+AA}^2(x)\,. \tag{19}$$

By Theorem 10, we get

$$\sum_x r_{AA+AA}^2(x) - \frac{|A|^8}{p} \lesssim |A|^4(\mathsf{E}_4^\times(A))^{1/2} + \mathsf{E}_4^\times(A)|A|^2\,.$$

If the term $\frac{|A|^8}{p}$ dominates in the last formula, we have from (19) that $|AA+AA| \gg p$. Otherwise in view of (18) and our condition $|A+A|^3|A| \leqslant p^3$, we see that

$$|A|^8 \lesssim |AA+AA| \cdot \left(|A|^4(\mathsf{E}_4^\times(A))^{1/2} + \mathsf{E}_4^\times(A)|A|^2\right) \ll |AA+AA| \cdot K^5|A|^6\,.$$

This completes the proof. $\quad\square$

Considering $A = \{1, 2, \ldots, n\}$, where n is sufficiently small comparable to p, we see that Corollary 11 is the best possible up to logarithms.

References

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev, I. D. Shkredov, *Growth Estimates in Positive Characteristic via Collisions,* International Mathematics Research Notices, Volume 2017, Issue 23 (2017), 7148–7189, https://doi.org/10.1093/imrn/rnw206

[2] T. F. Bloom, *A quantitative improvement for Roth's theorem on arithmetic progressions,* doi: 10.1112/jlms/jdw010.

[3] M.–C. Chang, *A polynomial bound in Freiman's theorem,* Duke Math. J. **113** (2002) no. 3, 399–419.

[4] B. Green, *Some constructions in the inverse spectral theory of cyclic groups,* Comb. Prob. Comp. **12** (2003) no. 2, 127–138.

[5] B. Green, *Spectral structure of sets of integers,* Fourier analysis and convexity (survey article, Milan 2001), Appl. Numer. Harmon. Anal., Birkhauser Boston, Boston, MA (2004), 83–96.

[6] S. V. KONYAGIN, I. SHPARLINSKI, *Character sums with exponential functions,* Cambridge University Press, Cambridge, 1999.

[7] B. MURPHY, G. PETRIDIS, OL. ROCHE–NEWTON, M. RUDNEV, I. D. SHKREDOV, *New results on sum-product type growth over fields,* arXiv:1702.01003v2 [math.CO] 8 Feb 2017, accepted.

[8] G. PETRIDIS, *Products of Differences in Prime Order Finite Fields,* arXiv:1602.02142 [math.CO] 5 Feb 2016.

[9] M. RUDNEV, *On the number of incidences between planes and points in three dimensions,* Combinatorica, 2017. First published online, doi:10.1007/s00493-016-3329-6.

[10] M. RUDNEV, I. D. SHKREDOV, AND S. STEVENS, *On the energy variant of the sum–product conjecture,* arXiv:1607.05053.

[11] T. SANDERS, *On certain other sets of integers,* Journal d'Analyse Mathmatique 116.1 (2012): 53–82.

[12] T. SANDERS, *On Roth's theorem on progressions,* Annals of Mathematics (2011): 619–636.

[13] I. D. SHKREDOV, *On Sets of Large Exponential Sums,* Izvestiya of Russian Academy of Sciences, **72**:1 (2008), 161–182.

[14] I. D. SHKREDOV, *On sumsets of dissociated sets,* Online Journal of Analytic Combinatorics, **4** (2009), 1–26.

[15] I. D. SHKREDOV, *An application of the sum–product phenomenon to sets having no solutions to several linear equations,* Sbornik Math., **209**:4 (2018), 117–142.

[16] I. D. SHKREDOV, *On asymptotic formulae in some sum–product questions,* arXiv:1802.09066v2 [math.NT] 2 Mar 2018.

[17] S. STEVENS, F. DE ZEEUW, *An improved point-line incidence bound,* arXiv: 1609.06284v2 [math.CO] 7 Oct 2016.

[18] T. TAO, V. VU, *Additive combinatorics,* Cambridge University Press 2006.

[19] P. THANG, M. TAIT, C. TIMMONS, *A Szemerédi–Trotter type theorem, sum–product estimates in finite quasifields, and related results,* Journal of Combinatorial Theory, Series A 147 (2017): 55–74.

[20] L.A. VINH, *A Szemerédi-Trotter type theorem and sum-product estimate over finite fields,* Eur. J. Comb. **32**:8 (2011), 1177–1181.

I.D. Shkredov
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
`ilya.shkredov@gmail.com`