Average estimate for additive energy in prime field.

Glibichuk Alexey*

Abstract

Assume that $A \subseteq \mathbb{F}_p, B \subseteq \mathbb{F}_p^*, \frac{1}{4} \leqslant \frac{|B|}{|A|}, |A| = p^\alpha, |B| = p^\beta$. We will prove that for $p \geqslant p_0(\beta)$ one has

$$\sum_{b \in B} E_+(A, bA) \leqslant 15p^{-\frac{\min\{\beta, 1-\alpha\}}{308}}|A|^3|B|.$$

Here $E_+(A, bA)$ is an additive energy between subset A and it's multiplicative shift bA. This improves previously known estimates of this type.

1 Introduction.

Let X be a non-empty set endowed with a binary operation $* : X \times X \to X$. Then one can define the operation * on pairs of subsets $A, B \subset X$ by the formula $A*B = \{a*b : a \in A, b \in B\}$. In particular, if A and B are subsets of a ring, we have two such operations: addition $A+B := \{a+b : a \in A, b \in B\}$ and multiplication $AB = A \times B := \{ab : a \in A, b \in B\}$. For given element b we define operation $b*A = b \times A$. The sign $*$ may be omitted when there is no danger of confusion. We write $|A|$ for the cardinality of A. We take the ring to be the field $\mathbb{F}_p$ of p elements, where p is an arbitrary prime. All sets are assumed to be subsets of $\mathbb{F}_p$. Given any set $Y \subset \mathbb{F}_p$, we write $Y^* := Y \setminus \{0\}$ for the set of invertible elements of Y. We shall always assume that p is a prime. Given any real number y, we write $[y]$ for its integer part (the largest

*Technion, Israel Institute of Technology, Haifa, Israel.
E-mail:glibichu@tx.technion.ac.il.

integer not exceeding y), and denote the fractional part of y by $\{y\}$. We also define the operation $h + A = \{h\} + A$ which adds an arbitrary element $h \in \mathbb{F}_p$ to the set A.

Definition 1. For subsets $A, B \subset \mathbb{F}_p$ we denote

$$E_+(A,B) = |\{(a_1,a_2,b_1,b_2) \in A \times A \times B \times B : a_1 - a_2 = b_1 - b_2\}|,$$

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

Numbers $E_+(A,B)$ and $E_\times(A,B)$ are said to be an **additive energy** and a **multiplicative energy** of sets A and B respectively.

In the paper [1] J. Bourgain proved the following result.

Theorem 1. *Assume $A \subset \mathbb{F}_p, B \subset \mathbb{F}_p$ and $|A| = p^\alpha, |B| = p^\beta$ with $\alpha \geqslant \beta$. Then*

$$\sum_{b \in B} E_+(A, bA) < C_1 p^{c_2\gamma} |A|^3 |B|$$

where $\gamma = \min(\beta, 1-\alpha)$ and C_1, c_2 are absolute constants (independent on α, β).

In the same paper J. Bourgain deduces from Theorem 1 sum-product estimate for two different subsets. Further, J. Bourgain and author [2] of this paper extended Theorem 1 to the case of an arbitrary finite field. More precisely, we proved the following result.

Theorem 2. *Take arbitrary subsets A, B of a finite field $\mathbb{F}_q$ with $q = p^r$ elements, such that $|A| = q^\alpha, |B| = q^\beta, \alpha \geqslant \beta$ and an arbitrary $0 < \eta \leqslant 1$. Suppose further that for every nontrivial subfield $S \subset \mathbb{F}_q$ and every element $d \in Fq$ the set B satisfies the restriction*

$$|B \cap dS| \leqslant 4|B|^{1-\eta}.$$

Then

$$\sum_{b \in B} E_+(A, bA) \leqslant 13 q^{-\frac{\gamma}{10430}} |A|^3 |B|$$

where $\gamma = \min\left(\beta, \frac{5215}{4}\beta\eta, 1-\alpha\right)$.

In this paper we also deduced from the Theorem 2 a new character sum estimate over a small multiplicative subgroup. J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin and D. Kutzarova [3] applied Theorem 2 to one of the problems of sparse signal recovery and several others branches of coding theory. Also, M. Rudnev and H. Helfgott [4] used method, proposed in the proof of the Theorem 1 to obtain an new explicit point-line incidence result in $\mathbb{F}_p$. These examples demonstrate that estimates like Theorems 1 and 2 have wide range of applications.

In the current paper a slightly modified version of the method from paper [4] will be used to obtain an improvement of the Theorem 2 in the case of prime field $\mathbb{F}_p$. We will establish the following theorem.

Theorem 3. *Assume that* $A \subseteq \mathbb{F}_p, B \subseteq \mathbb{F}_p^*$, $\frac{1}{4} \leqslant \frac{|B|}{|A|}$, $|A| = p^\alpha, |B| = p^\beta$. *Then for* $p \geqslant p_0(\beta)$

$$\sum_{b \in B} E_+(A, bA) \leqslant 15p^{-\frac{\min\{\beta, 1-\alpha\}}{308}} |A|^3 |B|.$$

Ideas of M. Rudnev and H. Helfgott in context of this problem working only when $|B| \geqslant K|A|$ for some absolute constant K. Case when $|A|$ is small comparatively to $|B|$ was analyzed by another method. This method is elementary in some extent and gives the following estimate.

Theorem 4. *Assume that* $A \subseteq \mathbb{F}_p, B \subseteq \mathbb{F}_p^*$, $|A| = p^\alpha, |B| = p^\beta$. *Then for* $p \geqslant p_0(\alpha, \beta)$ *we have*

$$\sum_{b \in B} E_+(A, bA) \leqslant Cp^{-\frac{\min\{\beta, 1-\alpha\}}{2240}} |A|^3 |B|,$$

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

As we see, Theorem 4 gives worse estimate than Theorem 3, but it still better than one delivered by the Theorem 2.

In section 2 we stating preliminary results which will be used in proofs of Theorems 3 and 4. Theorem 3 is proved in the Section 3, Theorem 4 is proved in the Section 4.

Acknowledgements. The author thank professor S. Konyagin and M. Rudnev for useful discussions helped me to improve the final result.

2 Preliminary results.

All the subsets in the Lemmas below are assumed to be non-empty. The first two lemmas is due to Ruzsa [5, 6]. It holds for subsets of any abelian group, but here we state them only for the subsets of $\mathbb{F}_p$.

Lemma 1. *For any subsets X, Y, Z of $\mathbb{F}_p$ we have*

$$|X - Z| \leqslant \frac{|X - Y||Y - Z|}{|Y|}.$$

Lemma 2. *Let $Y, X_1, X_2, \dots, X_k$ be sets of $\mathbb{F}_p$. Then*

$$|X_1 + X_2 + \ldots + X_k| \leqslant \frac{\prod_{i=1}^{k} |Y + X_i|}{|Y|^{k-1}}.$$

Definition 2. For any nonempty subsets $A \subset \mathbb{F}_p, B \subset \mathbb{F}_p, G \subset A \times B$, we define their *partial sum*

$$|A \overset{+}{_G} B| = \{a + b : (a, b) \in G\}.$$

Let us recall the modification of Balog-Szemeredi-Gowers result (see the paper of J. Bourgain and M. Garaev [7], Lemma 2.3).

Proposition 1. *Let A and B be subsets of $\mathbb{F}_p$ and $G \subset A \times B$ be such that $|G| \geqslant \frac{|A||B|}{K}$ for some $K > 0$. Then there exist subsets $A' \subset A, B' \subset B$ and a number Q, with*

$$|A'| \geqslant \frac{|A|}{4\sqrt{2}K}, \qquad \frac{|A|}{8\sqrt{2}K^2 \ln(e|A|)} \leqslant Q \leqslant 2|A'|, \qquad |B'| \geqslant \frac{|A||B|}{8\sqrt{2}QK^2 \ln(e|A|)}$$

such that

$$|A \overset{+}{_G} B|^3 \geqslant |A' + B'| \frac{Q|B|}{256K^3 \ln(e|A|)}.$$

We shall use the following result from the book of T. Tao and V. Vu [8] (Lemma 2.30, p. 80).

Lemma 3. *If $E_+(A, B) > \frac{1}{K}|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}, K \geqslant 1$, then there is $G \subset A \times B$ satisfying*

$$|G| > \frac{1}{2K}|A||B| \text{ and } |A \overset{+}{_G} B| < 2K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}.$$

This lemma represents a known technical approach for estimating sum-product sets, see, for example [9], [10].

Lemma 4. *For any given subsets $X, Y \subseteq \mathbb{F}_p, G \subset \mathbb{F}_p^*$ there is an element $\xi \in G$ with*

$$|X + \xi Y| \geqslant \frac{|X||Y||G|}{|X||Y| + |G|}.$$

Moreover, the following inequality holds

$$|X + \xi Y| > \frac{|X|^2|Y|^2}{E_+(X, \xi Y)}.$$

Proof. Let us take an arbitrary element $\xi \in G$ and $s \in \mathbb{F}_p$ and denote

$$f_\xi^+(s) := |\{(x, y) \in X \times Y : x + y\xi = s\}|.$$

It is obvious that

$$\sum_{s \in \mathbb{F}_p} (f_\xi^+(s))^2 = |\{(x_1, y_1, x_2, y_2) \in X \times X \times Y \times Y : x_1 + y_1\xi = x_2 + y_2\xi\}|$$

$$= |X||Y| + |\{(x_1, y_1, x_2, y_2) \in X \times X \times Y \times Y : x_1 \neq x_2, x_1 + y_1\xi = x_2 + y_2\xi\}|$$

and

$$\sum_{s \in \mathbb{F}_p} f_\xi^+(s) = |X||Y|. \tag{1}$$

Let us observe that for every $x_1, x_2 \in X, y_1, y_2 \in Y$ such that $x_1 \neq x_2$, there is at most one $\eta \in G$ satisfying the equality $x_1 + y_1\eta = x_2 + y_2\eta$. Therefore,

$$\sum_{\xi \in G} \sum_{s \in \mathbb{F}_p} (f_\xi^+(s))^2 \leqslant |X||Y||G| + |X|^2|Y|^2.$$

From the last inequality it directly follows that there is an element $\xi \in G$ such that

$$\sum_{s \in \mathbb{F}_p} (f_\xi^+(s))^2 \leqslant |X||Y| + \frac{|X|^2|Y|^2}{|G|}. \tag{2}$$

According to Cauchy-Schwartz,

$$\left(\sum_{s \in \mathbb{F}_p} f_\xi^+(s) \right)^2 \leqslant |X + \xi Y| \sum_{s \in \mathbb{F}_p} (f_\xi^+(s))^2. \tag{3}$$

Observing that

$$\sum_{s\in\mathbb{F}_p^*}(f_\xi^+(s))^2 = E_+(X,\xi Y)$$

one can yield the second assertion of Lemma 4.

Combining inequalities (1), (2) and (3) we see that

$$|X+\xi Y| \geqslant \frac{|X|^2|Y|^2}{|X||Y|+\frac{|X|^2|Y|^2}{|G|}} = \frac{|X||Y||G|}{|X||Y|+|G|}.$$

Lemma 4 now follows. ■

Definition 3. For any given subsets $X, Y \subset \mathbb{F}_p, |Y| > 1$ we denote

$$Q[X,Y] = \frac{X-X}{(Y-Y)\setminus\{0\}} := \left\{\frac{x_1-x_2}{y_1-y_2} : x_1,x_2\in X, y_1,y_2\in Y, y_1\neq y_2\right\}.$$

If $X = Y$ then $Q[X,X] = Q[X]$.

Lemma 5 is a simple extension of Lemma 2.50 from the book by T. Tao and V. Vu [8].

Lemma 5. *Consider two arbitrary subsets $X, Y \subset \mathbb{F}_p, |Y| > 1$. The given element $\xi \in \mathbb{F}_p$ is contained in $Q[X,Y]$ if and only if $|X+\xi * Y| < |X||Y|$.*

Proof. Let us consider a mapping $F : X\times Y$ to $X+\xi * Y$ defined by the identity $F(x,y) = x+\xi y$. F can be non-injective only when $|X+\xi * Y| < |X||Y|$. On the other side, the non-injectivity of F means that there are elements $x_1, x_2 \in X$, $y_1, y_2 \in Y$ such that $(x_1,y_1)\neq(x_2,y_2)$ and $F(x_1,y_1) = F(x_2,y_2)$. It is obvious that $y_1\neq y_2$ since otherwise $x_1 = x_2$ and we have achieved a contradiction with condition $(x_1,y_1)\neq(x_2,y_2)$. Hence, $\xi = (x_1-x_2)/(y_2-y_1) \in Q[X,Y]$. Lemma 5 now follows. ■

We need the following Lemma due to C.-Y. Shen [11].

Lemma 6. *Let X_1 and X_2 be two sets. Then for any $\varepsilon\in(0,1)$ there exist at most $\frac{\ln\frac{1}{\varepsilon}}{|X_2|}\min\{|X_1+X_2|,|X_1-X_2|\}$ additive translates of X_2 whose union contains not less than $(1-\varepsilon)|X_1|$ elements of X_1.*

Proof. For simplicity, we assume that $|X_1+X_2| \leqslant |X_1-X_2|$. The case when $|X_1+X_2| > |X_1-X_2|$ can be considered similarly. Using Lemma 4 we deduce

$$|\{(x,y,x_1,y_1) \in X_1 \times X_2 \times X_1 \times X_2 : x+y = x_1+y_1\}| \geqslant \frac{|X_1|^2|X_2|^2}{|X_1+X_2|}.$$

Now we can fix two elements $x_*^1 \in X_1, y_*^1 \in X_2$ for which the equation $x_*^1 + y = x + y_*^1, x \in X_1, y \in X_2$ has at least $\frac{|X_1||X_2|}{|X_1+X_2|}$ solutions and, therefore, $|(x_*^1+X_2) \cap (y_*^1+X_1)| \geqslant \frac{|X_1||X_2|}{|X_1+X_2|}$. Denoting $K = \frac{|X_1+X_2|}{|X_2|}$ we can observe that

$$|X_1 \cap (x_*^1 - y_*^1 + X_2)| \geqslant \frac{|X_1|}{K}. \tag{4}$$

Obviously, from (4) it is follows that

$$|X_1^1| := |X_1 \setminus (x_*^1 - y_*^1 + X_2)| \leqslant \left(1 - \frac{1}{K}\right)|X_1|.$$

We can repeat previous arguments for sets X_1^1 and X_2 and find elements $x_*^2 \in X_1^1$ and $y_*^2 \in X_2$ such that

$$|X_1^1 \cap (x_*^2 - y_*^2 + X_2)| \geqslant \frac{|X_1^1|}{K}$$

$$|X_1^2| := |X_1^1 \setminus (x_*^2 - y_*^2 + X_2)| \leqslant \left(1 - \frac{1}{K}\right)|X_1^1| \leqslant \left(1 - \frac{1}{K}\right)^2|X_1|.$$

On i-th iteration we finding elements $x_*^i \in X_1^{i-1}$ and $y_*^i \in X_2$ with

$$|X_1^{i-1} \cap (x_*^i - y_*^i + X_2)| \geqslant \frac{|X_1^{i-1}|}{K}$$

$$|X_1^i| := |X_1^{i-1} \setminus (x_*^i - y_*^i + X_2)| \leqslant \left(1 - \frac{1}{K}\right)|X_1^{i-1}| \leqslant \left(1 - \frac{1}{K}\right)^i|X_1|.$$

We stop when $|X_1^n| < \varepsilon|X_1|$ for some n. It is easy to see that we will make not more than $\ln\left(\frac{1}{\varepsilon}\right)K$ steps. The last observation finishes the proof of the Lemma 6. ■

We also need the following sum-product estimate of M. Z. Garaev [12, Theorem 3.1].

Theorem 5. *Let $A, B \subset \mathbb{F}_p$ be an arbitrary subsets. Then*

$$|A-A|^2 \cdot \frac{|A|^2|B|^2}{E_\times(A,B)} \geqslant C|A|^3 L^{\frac{1}{9}} (\log_2 L)^{-1},$$

where $L = \min\left\{|B|, \frac{p}{|A|}\right\}$ and $C > 0$ is an absolute constant.

3 Proof of the Theorem 3.

Let $A, B \subseteq \mathbb{F}_p$ be as in Theorem 3 and $\delta > 0$, $C > 1$ (to be specified). Assume

$$\sum_{b \in B} E_+(A, bA) > C|B|^{1-\delta}|A|^3.$$

Hence there is a subset $B_1 \subseteq B$ such that

$$|B_1| > \frac{C}{2}|B|^{1-\delta}$$

and

$$E_+(A, bA) > \frac{C}{2}|B|^{-\delta}|A|^3 \text{ for } b \in B_1. \tag{5}$$

Fix $b \in B_1$. By the application of Lemma 3 to (5), one can deduce that there is $G^{(b)} \subset A \times bA, |G^{(b)}| > \frac{C}{4}|B|^{-\delta}|A|^2$ such that

$$|A \overset{+}{_{G^{(b)}}} bA| < \frac{4}{C}|B|^{\delta}|A|.$$

Now, by Proposition 1, there are $Q_{(b)}, A_1^{(b)}, A_2^{(b)} \subset A$ such that

$$|A_1^{(b)}| > \frac{C}{2^4\sqrt{2}}|B|^{-\delta}|A|, \tag{6}$$

$$\frac{C^2}{2^7\sqrt{2}\ln(e|A|)}|A||B|^{-2\delta} \leqslant Q_{(b)} \leqslant 2|A_1^{(b)}|, \tag{7}$$

$$|A_2^{(b)}| > \frac{C^2}{2^7\sqrt{2}Q_{(b)}\ln(e|A|)}|B|^{-2\delta}|A|^2, \tag{8}$$

$$|A_1^{(b)} + bA_2^{(b)}| < \frac{2^{20}}{C^6 Q_{(b)}}\ln(e|A|)|B|^{6\delta}|A|^2. \tag{9}$$

Write

$$\frac{C^3}{2^{12}\ln(e|A|)}|B_1||B|^{-3\delta}|A|^2 < \sum_{b\in B_1}|A_1^{(b)}\times A_2^{(b)}|$$
$$\leqslant |A|\left[\sum_{b,b'\in B_1}\left|\left(A_1^{(b)}\cap A_1^{(b')}\right)\times\left(A_2^{(b)}\cap A_2^{(b')}\right)\right|\right]^{\frac{1}{2}}$$

by Cauchy-Schwartz. Hence

$$\frac{C^6}{2^{24}\ln^2(e|A|)}|B_1|^2|B|^{-6\delta}|A|^2 < \sum_{b,b'\in B_1}\left|\left(A_1^{(b)}\cap A_1^{(b')}\right)\times\left(A_2^{(b)}\cap A_2^{(b')}\right)\right|$$

and there is some $b_0\in B_1, B_2\subset B_1$ such that

$$|B_2| > \frac{C^7}{2^{26}\ln^2(e|A|)}|B|^{1-7\delta} \tag{10}$$

$$|A_1^{(b)}\cap A_1^{(b_0)}|, |A_2^{(b)}\cap A_2^{(b_0)}| > \frac{C^6}{2^{25}\ln^2(e|A|)}|B|^{-6\delta}|A| \text{ for } b\in B_2. \tag{11}$$

Let us estimate from (6), (8), (9), (11) and Lemma 1

$$|b_0A_1^{(b_0)}+bA_1^{(b_0)}| \leqslant \frac{|A_1^{(b_0)}+bA_2^{(b_0)}||A_1^{(b_0)}+b_0A_2^{(b_0)}|}{|A_2^{(b_0)}|} \leqslant$$
$$\leqslant \frac{2^{27}\sqrt{2}\ln^2(e|A|)}{C^8}|B|^{8\delta}|A_1^{(b_0)}+bA_2^{(b_0)}| \tag{12}$$

$$|A_1^{(b_0)}+bA_2^{(b_0)}| \leqslant \frac{|A_1^{(b_0)}+bA_2^{(b)}||A_2^{(b_0)}+A_2^{(b_0)}|}{|A_2^{(b)}\cap A_2^{(b_0)}|} \leqslant$$
$$\leqslant \frac{|A_1^{(b_0)}+bA_2^{(b)}||A_1^{(b_0)}+b_0A_2^{(b_0)}|^2}{|A_2^{(b)}\cap A_2^{(b_0)}||A_1^{(b_0)}|} \leqslant$$
$$\leqslant \frac{2^{69}\sqrt{2}\ln^4(e|A|)}{C^{19}Q^2_{(b_0)}}|A|^2|B|^{19\delta}|A_1^{(b_0)}+bA_2^{(b)}| \tag{13}$$

$$|A_1^{(b_0)} + bA_2^{(b)}| \leqslant \frac{|A_1^{(b)} + bA_2^{(b)}||A_1^{(b_0)} + A_1^{(b_0)}|}{|A_1^{(b_0)} \cap A_1^{(b)}|} \leqslant$$
$$\leqslant \frac{|A_1^{(b)} + bA_2^{(b)}||A_1^{(b_0)} + b_0A_2^{(b_0)}|^2}{|A_1^{(b_0)} \cap A_1^{(b)}||A_2^{(b_0)}|} \leqslant$$
$$\leqslant \frac{2^{92}\sqrt{2}\ln^6(e|A|)}{C^{26}Q_{(b)}Q_{(b_0)}}|B|^{26\delta}|A|^3. \quad (14)$$

Hence, by (12), (13) and (14)

$$|b_0A_1^{(b_0)} + bA_1^{(b_0)}| \leqslant \frac{2^{189}\sqrt{2}\ln^{12}(e|A|)}{C^{53}Q_{(b_0)}^3Q_{(b)}}|B|^{53\delta}|A|^5.$$

Using (7) finally we obtain

$$|b_0A_1^{(b_0)} + bA_1^{(b_0)}| \leqslant \frac{2^{219}\sqrt{2}\ln^{16}(e|A|)}{C^{61}}|B|^{61\delta}|A|.$$

Now we redefine $A_1^{(b_0)}$ by A' and $\frac{B_2}{b_0}$ by B' one can deduce the following properties (for $\delta < \frac{1}{440}$):

$$|A' + bA'| < \frac{2^{219}\sqrt{2}\ln^{16}(e|A|)}{C^{61}}|B|^{61\delta}|A| \text{ for all } b \in B' \quad (15)$$

$$|B'| > \frac{C^7}{2^{26}\ln^2(e|A|)}|B|^{1-7\delta} \quad (16)$$

$$|A'| > \frac{C}{2^4\sqrt{2}}|B|^{-\delta}|A|. \quad (17)$$

Our aim is to get contradiction from (15), (16) and (17).

Let us use the symbol

$$K = \max_{b\in B'}|A' + bA'| \qquad \text{so} \qquad K < \frac{2^{219}\sqrt{2}\ln^{16}(e|A|)}{C^{61}}|B|^{61\delta}|A|. \quad (18)$$

Now we use Lemma 4 to establish that

$$E_+(A', bA') = |\{(a_1, a_2, a_3, a_4) \in A' \times A' \times A' \times A' : a_1 + a_2b = a_3 + a_4b\}| \geqslant$$
$$\geqslant \frac{|A'|^4}{|A' + bA'|} \geqslant \frac{|A'|^4}{K}.$$

Summing over all $b \in B'$ we obviously obtain

$$|\{(a_1, a_2, a_3, a_4, b) \in A' \times A' \times A' \times A' \times B' : a_1 + a_2 b = a_3 + a_4 b\}| \geqslant \frac{|A'|^4 |B'|}{K}.$$

There are some elements $\widetilde{a}_2, \widetilde{a}_3 \in A'$ such that

$$|\{(a_1, a_4, b) \in A' \times A' \times B' : a_1 - \widetilde{a}_3 = (a_4 - \widetilde{a}_2) b\}| \geqslant \frac{|A'|^2 |B'|}{K}.$$

Let $A_1' = A' - \widetilde{a}_3, A_2' = A' - \widetilde{a}_2$ be translates of A' by $\widetilde{a}_3$ and $\widetilde{a}_2$ respectively. Then

$$|\{(a_1, a_2, b) \in A_1' \times A_2' \times B' : a_1 = a_2 b\}| \geqslant \frac{|A'|^2 |B'|}{K}.$$

There is some $a_* \in A_2'$ such that

$$|\{(a_1, b) \in A_1' \times B' : a_1 = a_* b\}| \geqslant \frac{|A'||B'|}{K}.$$

Thus, we have a subset $B_1' \subset (A_1' \cap a_* B')$ of cardinality

$$|B_1'| \geqslant \frac{|A'||B'|}{K}.$$

In original notations B_1' lies in the intersection of $\frac{a_*}{b_0} B_2$ and some translate of $A_1^{(b_0)}$; besides by the bounds (16), (17) and (18)

$$|B_1'| > \frac{C^{69}}{2^{250} \ln^{18}(e|A|)} |B|^{1-69\delta}. \tag{19}$$

We consider three cases.

1) Case 1. Suppose that $Q[B_1'] \neq \mathbb{F}_p$. It is clear that $1 + Q[B_1'] \neq Q[B_1']$ since otherwise $Q[B_1'] = \mathbb{F}_p$. The latter mean that there are elements $a, b, c, d \in B_1'$ with $1 + \frac{a-b}{c-d} \notin Q[B_1']$. Now we recall that B_1' is a subset of $\frac{a_*}{b_0} B_2$ so we can regard a, b, c, d as elements of B_2. Observe, that for an arbitrary subset $B_1'' \subset B_1', |B_1''| \geqslant 0.98 |B_1'|$ we have $1 + \frac{a-b}{c-d} \notin Q[B_1'']$ since $Q[B_1''] \subset Q[B_1']$. Therefore, by Lemma 5, for these elements $a, b, c, d \in B_2$ we have

$$(0.98)^2 |B_1'|^2 \leqslant |B_1''|^2 = \left| B_1'' + \left(B_1'' + \frac{a-b}{c-d} B_1'' \right) \right| \leqslant \left| B_1'' + B_1'' + \frac{a-b}{c-d} B_1'' \right|. \tag{20}$$

We now use Lemma 6. Let us first show that for any $b_1 \in B_2$ we can cover 99% of the elements of the set $b_1 B_1^{'}$ (a subset of the translation of $b_1 A_1^{(b_0)}$) or $-b_1 B_1^{'}$ by at most $\frac{2^{109}\ln(100)\ln^8(e|A|)}{C^{28}}|B|^{28\delta}$ additive translates of the set $b_0 A_1^{(b_0)}$. Indeed $b_0 A_1^{(b_1)} \cap A_1^{(b_0)}$ is a subset of $b_0 A_1^{(b_0)}$, and by Lemma 6 and Lemma 1) we can cover 99% of the elements of either $b_1 B_1^{'}$ or $-b_1 B_1^{'}$ by at most

$$\frac{\ln(100)}{|b_0 A_1^{(b_1)} \cap A_1^{(b_0)}|} \min\left\{|b_0 A_1^{(b_1)} \cap A_1^{(b_0)} + b_1 B_1^{'}|, |b_0 A_1^{(b_1)} \cap A_1^{(b_0)} - b_1 B_1^{'}|\right\} \leqslant$$

$$\leqslant \frac{\ln(100)}{|A_1^{(b_1)} \cap A_1^{(b_0)}|} \min\left\{|b_0 A_1^{(b_1)} \cap A_1^{(b_0)} + b_1 A_1^{(b_0)}|, |b_0 A_1^{(b_1)} \cap A_1^{(b_0)} - b_1 A_1^{(b_0)}|\right\} \leqslant$$

$$\leqslant \frac{\ln(100)|A_1^{(b_1)} \cap A_1^{(b_0)} + b_1 A_2^{(b_0)} \cap A_2^{(b_1)}||A_1^{(b_0)} + b_0 A_2^{(b_0)} \cap A_2^{(b_1)}|}{|A_1^{(b_1)} \cap A_1^{(b_0)}||b_0 b_1 A_2^{(b_1)} \cap A_2^{(b_0)}|} \leqslant$$

$$\leqslant \frac{\ln(100)|A_1^{(b_1)} + b_1 A_2^{(b_1)}||A_1^{(b_0)} + b_0 A_2^{(b_0)}|}{|A_1^{(b_1)} \cap A_1^{(b_0)}||A_2^{(b_1)} \cap A_2^{(b_0)}|} \leqslant \frac{2^{105}\ln(100)\ln^8(e|A|)}{C^{28}}|B|^{28\delta}$$

additive translates of $b_0 A_1^{(b_1)} \cap A_1^{(b_0)}$ and whence of $b_0 A_1^{(b_0)}$. In the last estimate we have used (7), (9) and (11).

This altogether enables us to choose $B_1^{''}$ as a subset containing at least 98% of the elements from $B_1^{'}$ such that $(a-b)B_1^{''}$ gets covered by at most $\frac{2^{210}\ln^2(100)\ln^{16}(e|A|)}{C^{56}}|B|^{56\delta}$ translates of $b_0 A_1^{(b_0)} + b_0 A_1^{(b_0)}$. Similarly, we can find a subset $\widetilde{A}_1^{(b_0)}$ containing at least 98% of the elements of $A_1^{(b_0)}$ such that $(c-d)\widetilde{A}_1^{(b_0)}$ gets covered by at most $\frac{2^{210}\ln^2(100)\ln^{16}(e|A|)}{C^{56}}|B|^{56\delta}$ translates of $b_0 A_1^{(b_0)} + b_0 A_1^{(b_0)}$. Now we apply Lemma 2 to (20) as follows

$$\left|B_1^{''} + B_1^{''} + \frac{a-b}{c-d}B_1^{''}\right| \leqslant \frac{|\widetilde{A}_1^{(b_0)} + B_1^{''} + B_1^{''}||\widetilde{A}_1^{(b_0)} + \frac{a-b}{c-d}B_1^{''}|}{|\widetilde{A}_1^{(b_0)}|} \leqslant$$

$$\leqslant \frac{2^4\sqrt{2}|B|^{\delta}}{C|A|}|A_1^{(b_0)} + A_1^{(b_0)} + A_1^{(b_0)}||\widetilde{A}_1^{(b_0)} + \frac{a-b}{c-d}B_1^{''}| \leqslant$$

$$\leqslant \frac{2^{87}\ln^6(e|A|)}{C^{25}}|B|^{25\delta}|\widetilde{A}_1^{(b_0)} + \frac{a-b}{c-d}B_1^{''}| \quad (21)$$

The covering arguments above implies that

$$|\widetilde{A}_1^{(b_0)} + \frac{a-b}{c-d}B_1^{''}| \leqslant \frac{2^{420}\ln^4(100)\ln^{32}(e|A|)}{C^{112}}|B|^{112\delta}|A_1^{(b_0)} + A_1^{(b_0)} + A_1^{(b_0)} + A_1^{(b_0)}| \leqslant$$

$$\leqslant \frac{2^{530}\ln^4(100)\ln^{40}(e|A|)}{C^{144}}|B|^{144\delta}|A|.$$

Comparing to (19) and using the condition $\frac{|B|}{|A|} \geqslant \frac{1}{4}$, for large p we deduce

$$\frac{(0.98)^2 C^{138}}{2^{500}\ln^{36}(e|A|)}|B|^{2-138\delta} < \frac{2^{613}\ln^4(100)\ln^{46}(e|A|)}{C^{169}}|B|^{169\delta}|A| \Leftrightarrow$$

$$\Leftrightarrow \frac{|B|^{2-307\delta}}{|A|\ln^{82}(e|A|)} < \frac{2^{1113}\ln^4(100)}{(0,98)^2C^{307}} \Rightarrow |B|^{1-308\delta} < \frac{2^{1115}\ln^4(100)}{(0,98)^2C^{307}}. \qquad (22)$$

Now we define $C = \frac{2^{\frac{1115}{307}}\ln^{\frac{4}{307}}(100)}{(0.98)^{\frac{2}{307}}}$ and from (22) deduce the inequality

$$|B| < |B|^{308\delta}$$

which is false when $\delta \leqslant \frac{1}{308}$. This finishes proof of the Theorem 3 in case 1.

2) Case 2. Suppose that $|B_1^{'}| > \sqrt{p}$. It is clear that $Q[B_1^{'}] = \mathbb{F}_p$ since for an arbitrary $\xi \in \mathbb{F}_p$ the equality $|B_1^{'} + \xi B_1^{'}| = |B_1^{'}|^2$ is impossible (simply because $|B_1^{'}|^2 > p$). Let us take arbitrary elements $\xi \in \mathbb{F}_p^*$, $s \in \mathbb{F}_p$, an arbitrary subset $|B_1^{''}| \geqslant 0.96|B_1^{'}|$ and denote

$$f_\xi(s) := |\{(b_1,b_2) \in B_1^{'} \times B_1^{'} : b_1 + \xi b_2 = s\}|$$

$$f_\xi^{'}(s) := |\{(b_1,b_2) \in B_1^{''} \times B_1^{''} : b_1 + \xi b_2 = s\}|$$

It is obvious that

$$\sum_{s\in\mathbb{F}_p}(f_\xi(s))^2 = |\{(b_1,b_2,b_3,b_4) \in B_1^{'} \times B_1^{'} \times B_1^{'} \times B_1^{'} : b_1 + \xi b_2 = b_3 + \xi b_4\}|$$

$$= |B_1^{'}|^2 + |\{(b_1,b_2,b_3,b_4) \in B_1^{'} \times B_1^{'} \times B_1^{'} \times B_1^{'} : b_1 \neq b_3, b_1 + \xi b_2 = b_3 + \xi b_4\}|$$

and

$$\sum_{s\in\mathbb{F}_p} f_\xi(s) = |B_1^{'}|^2$$

$$\sum_{s\in\mathbb{F}_p} f_\xi^{'}(s) = |B_1^{''}|^2.$$

Let us observe that for every $b_1, b_2, b_3, b_4 \in B_1^{'}$ such that $b_1 \neq b_3$, there is at most one $\eta \in \mathbb{F}_p^*$ satisfying the equality $b_1 + \eta b_2 = b_3 + \eta b_4$. Therefore,

$$\sum_{\xi\in\mathbb{F}_p^*}\sum_{s\in\mathbb{F}_p}(f_\xi(s))^2 \leqslant |B_1^{'}|^2(p-1) + |B_1^{'}|^4.$$

From the last inequality it directly follows that there is an element $\xi \in \mathbb{F}_p^*$ such that

$$\sum_{s \in \mathbb{F}_p} (f_\xi^{'}(s))^2 \leqslant \sum_{s \in \mathbb{F}_p} (f_\xi(s))^2 \leqslant |B_1^{'}|^2 + \frac{|B_1^{'}|^4}{p-1}.$$

Note that this ξ is independent on $B_1^{''}$. According to Cauchy-Schwartz,

$$\left(\sum_{s \in \mathbb{F}_p} f_\xi^{'}(s) \right)^2 \leqslant |B_1^{''} + \xi B_1^{''}| \sum_{s \in \mathbb{F}_p} (f_\xi^{'}(s))^2.$$

Now we see that

$$|B_1^{''} + \xi B_1^{''}| \geqslant \frac{|B_1^{''}|^4 (p-1)}{|B_1^{'}|^2 (p-1) + |B_1^{'}|^4} \geqslant \frac{(0.96)^4 |B_1^{'}|^4 (p-1)}{|B_1^{'}|^2 (p-1) + |B_1^{'}|^4} \geqslant (0.96)^4 \frac{p-1}{2}. \tag{23}$$

Reminding that $Q[B_1^{'}] = \mathbb{F}_p$, we can find elements $a, b, c, d \in B_1^{'}$, such that $\xi = \frac{a-b}{c-d}$ (again, we can regard them as elements of B_2). Using similar covering arguments as in proof of the case 1 we can deduce that we can choose $B_1^{''}$ as a subset containing at least 96% of the elements from $B_1^{'}$ such that $(a-b)B_1^{''} + (c-d)B_1^{''}$ gets covered by at most $\frac{2^{420} \ln^4(100) \ln^{32}(e|A|)}{C^{112}} |B|^{112\delta}$ translates of $b_0 A_1^{(b_0)} + b_0 A_1^{(b_0)} + b_0 A_1^{(b_0)} + b_0 A_1^{(b_0)}$. Now we see that

$$\left| B_1^{''} + \frac{a-b}{c-d} B_1^{''} \right| \leqslant \frac{2^{420} \ln^4(100) \ln^{32}(e|A|)}{C^{112}} |B|^{112\delta} |A_1^{(b_0)} + A_1^{(b_0)} + A_1^{(b_0)} + A_1^{(b_0)}| \leqslant$$

$$\leqslant \frac{2^{530} \ln^4(100) \ln^{40}(e|A|)}{C^{144}} |B|^{144\delta} |A|.$$

Again, comparing to (23) and using the condition $\frac{|B|}{|A|} \geqslant \frac{1}{4}$, we deduce

$$(0.96)^4 \frac{p}{4} \leqslant (0.96)^4 \frac{p-1}{2} < \frac{2^{530} \ln^4(100) \ln^{40}(e|A|)}{C^{144}} |B|^{144\delta} |A| \Rightarrow$$

$$\Rightarrow \frac{p}{4} < \frac{2^{530} \ln^4(100)}{C^{144} (0.96)^4} p^{145\beta\delta + \alpha} \tag{24}$$

Now we define $C = \frac{2^{\frac{265}{72}} \ln^{\frac{1}{36}}(100)}{(0.96)^{\frac{1}{36}}}$ and from (24) deduce the inequality

$$p < p^{145\beta\delta + \alpha}$$

which is false when $\delta \leqslant \frac{1-\alpha}{145\beta}$. This concludes proof of the Theorem in case 2.

3) Case 3. Suppose that $Q[B_1^{'}] = \mathbb{F}_p$ and $|B_1^{''}| \leqslant \sqrt{p}$. Repeating arguments from the proof of case 2 for an arbitrary subset $B_1^{''} \subset B_1^{'}, |B_1^{''}| \geqslant 0.96|B_1^{'}|$ we finding elements $a, b, c, d \in B_2$ independent on the subset $B_1^{''}$ with

$$\left| B_1^{''} + \frac{a-b}{c-d} B_1^{''} \right| \geqslant (0.96)^4 \frac{|B_1^{'}|^2}{2}.$$

Using similar covering arguments as in proof of the case 1 we can deduce that we can choose $B_1^{''}$ as a subset containing at least 96% of the elements from $B_1^{'}$ such that $(a-b)B_1^{''} + (c-d)B_1^{''}$ gets covered by at most $\frac{2^{420}\ln^4(100)\ln^{32}(e|A|)}{C^{112}}|B|^{112\delta}$ translates of $b_0A_1^{(b_0)} + b_0A_1^{(b_0)} + b_0A_1^{(b_0)} + b_0A_1^{(b_0)}$. Now we see that

$$\left| B_1^{''} + \frac{a-b}{c-d} B_1^{''} \right| \leqslant \frac{2^{420}\ln^4(100)\ln^{32}(e|A|)}{C^{112}}|B|^{112\delta}|A_1^{(b_0)} + A_1^{(b_0)} + A_1^{(b_0)} + A_1^{(b_0)}| \leqslant$$

$$\leqslant \frac{2^{530}\ln^4(100)\ln^{40}(e|A|)}{C^{144}}|B|^{144\delta}|A|.$$

Comparing to (19) and using the condition $\frac{|B|}{|A|} \geqslant \frac{1}{4}$, we deduce

$$\frac{(0.96)^4 C^{138}}{2^{500}\ln^{36}(e|A|)}|B|^{2-138\delta} < \frac{2^{530}\ln^4(100)\ln^{40}(e|A|)}{C^{144}}|B|^{144\delta}|A| \Leftrightarrow$$

$$\Leftrightarrow \frac{|B|^{2-282\delta}}{|A|\ln^{76}(e|A|)} < \frac{2^{1030}\ln^4(100)}{(0,96)^4C^{282}} \Rightarrow |B|^{1-283\delta} < \frac{2^{1032}\ln^4(100)}{(0,96)^4C^{282}}. \qquad (25)$$

Now we define $C = \frac{2^{\frac{516}{141}}\ln^{\frac{2}{141}}(100)}{(0.96)^{\frac{2}{141}}}$ and from (25) deduce the inequality

$$|B| < |B|^{283\delta}$$

which is false when $\delta \leqslant \frac{1}{283}$. Note that in all the cases the meaning assigned for the constant C is strictly less than 15. The Theorem 3 is proved. ■

4 Proof of the Theorem 4.

As in the proof of the Proposition 3 we assume contrary, i.e.

$$\sum_{b\in B} E_+(A, bA) > C|B|^{1-\delta}|A|^3$$

for some $C > 0$, $\delta > 0$. Following arguments in the beginning of the proof of the Proposition 3, we finding $A^{'} \subset A$ and $B^{'} \subset \mathbb{F}_p^*, 1 \in B^{'}$ (which is in fact a subset of a multiplicative shift of B) such that

$$|A^{'} + bA^{'}| < \frac{2^{219}\sqrt{2}\ln^{16}(e|A|)}{C^{61}}|B|^{61\delta}|A| = K \text{ for all } b \in B^{'} \qquad (26)$$

$$|B^{'}| > \frac{C^7}{2^{26}\ln^2(e|A|)}|B|^{1-7\delta} \qquad (27)$$

$$|A^{'}| > \frac{C}{2^4\sqrt{2}}|B|^{-\delta}|A|. \qquad (28)$$

Using Lemma 4 we obtain

$$|\{(a_1, a_2, a_3, a_4) \in A^{'} \times A^{'} \times A^{'} \times A^{'} : a_1 + ba_2 = a_3 + ba_4\}| > \\ > \frac{|A^{'}|^4}{K} \text{ for all } b \in B^{'}.$$

Summing up by all $b \in B^{'}$ one gets

$$|\{(a_1, a_2, a_3, a_4, b) \in A^{'} \times A^{'} \times A^{'} \times A^{'} \times B^{'} : a_1 + ba_2 = a_3 + ba_4\}| > \\ > \frac{|A^{'}|^4|B^{'}|}{K} \text{ for all } b \in B^{'}.$$

Now we can fix elements $a_3^0, a_2^0 \in A^{'}$ such that

$$|\{(a_1, a_4, b) \in A^{'} \times A^{'} \times B^{'} : a_1 - a_3^0 = b(a_4 - a_2^0)\}| > \frac{|A^{'}|^2|B^{'}|}{K}. \qquad (29)$$

We denote

$$f(s) = |\{(a, b) \in A^{'} \times B^{'} : b(a - a_2^0) = s\}|,$$

$$g(s) = \begin{cases} 1, & \text{if } s \in A^{'} - a_3^0; \\ 0, & \text{otherwise.} \end{cases}$$

Clearly,

$$|\{(a_1, a_4, b) \in A' \times A' \times B' : a_1 - a_3^0 = b(a_4 - a_2^0)\}| = \sum_{s\in\mathbb{F}_p} f(s)g(s), \quad (30)$$

$$\sum_{s\in\mathbb{F}_p} f^2(s) = E_\times(A' - a_2^0, B'). \quad (31)$$

Now, by Cauchy-Schwartz,

$$\left(\sum_{s\in\mathbb{F}_p} f(s)g(s)\right)^2 \leqslant \sum_{s\in\mathbb{F}_p} f^2(s) \sum_{s\in\mathbb{F}_p} g^2(s)$$

and, by (30) and (31), one can deduce

$$E_\times(A' - a_2^0, B') > \frac{|A'|^3|B'|}{K^2}.$$

Consider two cases.

Case 1. Assume that $|A'||B'| \leqslant p$. Applying Theorem 5 one obtains

$$\frac{K^4}{|A'|} > |A' - A'|^2 \cdot \frac{|A'|^2|B'|^2}{E_\times(A' - a_2^0, B')} \geqslant C_1 \frac{|A'|^3|B'|^{\frac{1}{9}}}{\log_2(|B'|)}.$$

Using (26), (27) and (28) we deduce

$$\frac{C_1 C^{\frac{43}{9}} |B|^{\frac{1}{9} - \frac{43}{9}\delta} |A|^4}{2^{\frac{188}{9}} \ln^{\frac{2}{9}}(e|A|) \log_2(|B|)} < \frac{2^{878} \ln^{64}(e|A|)}{C^{244}} |B|^{244\delta} |A|^4 \Rightarrow$$

$$|B|^{\frac{1}{9}} < \frac{2^{\frac{8090}{9}} \ln^{\frac{578}{9}}(e|A|) \log_2(|B|)}{C_1 C^{\frac{2239}{9}}} |B|^{\frac{2239}{9}\delta}. \quad (32)$$

Defining $C = \frac{2^{\frac{8090}{2239}}}{C_1^{\frac{9}{2239}}}$, we observe that for sufficiently large p from (32) follows the inequality

$$|B|^{\frac{1}{9}} < |B|^{\frac{2240}{9}\delta}.$$

which gives a contradiction when $\delta = \frac{1}{2240}$. This completes proof of the Theorem 4 in this case.

Case 2. Assume that $|A^{'}||B^{'}| > p$. Again, applying Theorem 5 we obtain

$$\frac{K^4}{|A'|} > |A^{'} - A^{'}|^2 \cdot \frac{|A^{'}|^2|B^{'}|^2}{E_{\times}(A' - a_2^0, B')} \geqslant C_1 \frac{|A^{'}|^{\frac{26}{9}} p^{\frac{1}{9}}}{\log_2 p}.$$

Using (26) and (28) we deduce

$$\frac{C_1 C^{\frac{35}{9}} |A|^{\frac{35}{9}} p^{\frac{1}{9}}}{2^{\frac{35}{2}} |B|^{\frac{35}{9}} \log_2 p} < \frac{2^{878} \ln^{64}(e|A|)}{C^{244}} |B|^{244\delta} |A|^4 \Rightarrow$$

$$\Rightarrow \frac{2^{\frac{1791}{2}} \ln^{64}(e|A|) \log_2 p}{C^{\frac{2231}{9}} C_1} |A|^{\frac{1}{9}} |B|^{\frac{2231}{9}\delta} > p^{\frac{1}{9}}. \tag{33}$$

Defining $C = \frac{2^{\frac{19119}{4462}}}{C_1^{\frac{9}{2231}}}$, we observe that for sufficiently large p from (33) follows the inequality

$$p^{\frac{1}{9}} < |B|^{\frac{2232}{9}\delta} |A|^{\frac{1}{9}}.$$

which gives a contradiction when $\delta = \frac{1-\alpha}{2232}$. Theorem 4 is proved. ■

References

[1] J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, Geometric and Functional Analysis, vol. 18, N 5, 2009 , pp. 1477 – 1502.

[2] J. Bourgain, A. Glibichuk, *Exponential sum estimate over subgroup in an arbitrary finite field*, accepted for publication in Journal de Analyze Mathématiques.

[3] J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin, D. Kutzarova, *Explicit constructions of RIP matrices*, Proc. 43rd ACM Symposium of the Theory of Computing (STOC), pp. 637—644 (2011).

[4] H. Helfgott, M. Rudnev, *An explicit incidence theorem in $\mathbb{F}_p$*, preprint, arXiv:1001.1980v2.

[5] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Scientia, Ser. A, 3 (1989), 97 – 109.

[6] I. Z. Ruzsa, *Sums of finite sets*, Number theory (New York, 1991 – 1995), 281 – 293, Springer, New York, 1996.

[7] J. Bourgain and M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sums bounds in prime fields*, Mathematical proceedings of the Cambridge Philosophical Society, vol. 146 (2009), part 1, pp. 1 – 21.

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

[9] J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields and their applications*, Geom and Funct. Anal., **14** (2004), 27–57.

[10] J. Bourgain, S. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C.R. Acad. Sci. Paris, Ser. I, **337** (2003), 75–80.

[11] Chun-Yen Shen, *Quantitative sum product estimates on different sets*, Electron. J. Combin., 15 (2008), no. 1.

[12] M. Z. Garaev, *Sums and products of sets and estimates of rational trigonometric sums in fields of prime order*, Russian Mathematical Surveys, 2010, vol. 65, no. 4, pp. 599–658