Exponential sum estimate over subgroup in an arbitrary finite field

J. Bourgain*, A. Glibichuk†

1 Introduction.

The purpose of this paper is to establish some exponential sums estimates over multiplicative subgroup extending the result of J. Bourgain [1].

Let $p > 2$ be a prime, $\mathbb{F}_q$ be the a finite field of $q = p^r$ elements, and $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$, so that $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. For sets $X \subset \mathbb{F}_q$, $Y \subset \mathbb{F}_q$, and for a (possibly, partial) binary operation $* : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q$ we let

$$X * Y = \{x * y : x \in X, y \in Y\}.$$

We will write XY instead of $X * Y$ if $*$ is multiplication in $\mathbb{F}_q$; and, for an element $\lambda \in \mathbb{F}_q$, we write

$$\lambda * A = \{\lambda\}A.$$

We shall omit the $*$ sign if it doesn't confuse reading of the formula. Hereafter $|A|$ stands for the cardinality of a set A. For an arbitrary $x \in \mathbb{F}_q$ we define a trace function $Tr(x) = 1 + x^p + x^{p^2} + \ldots + x^{p^{r-1}}$ and for given a we introduce a character $\psi(x) = e^{\frac{2\pi i Tr(ax)}{p}}$.

Let us recall one of the results of [1].

*Institute for Advanced Study, Olden Lane , Princeton, NJ 08540, USA.
E-mail: bourgain@ias.edu.

†Instituto de Matemáticas, Universidad Nacional Autónoma de México, Campus Morelia, Apartado Postal 61-3 (Xangari), C.P. 58089, Morelia, Michoacán, México.
E-mail: aanatol@matmor.unam.mx.

Theorem 1. *Let $H \subset \mathbb{F}_p$ be a multiplicative subgroup with $|H| > p^{\frac{C}{\log\log p}}$ for some sufficiently large constant $C > 1$. Then*

$$\max_{(a,p)=1} \left| \sum_{x \in H} e^{2\pi i a x} \right| < e^{-\log^{C'} p} |H|$$

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

M. Garaev [2, chapter 4] proved the following theorem.

Theorem 2. *Let $3 \leqslant n \leqslant 1.44 \ln\ln p$ be a natural number and $c > 0$ be an arbitrary fixed constant. For any subsets $X_1, X_2, \ldots, X_n \subset \mathbb{F}_p \setminus \{0\}$ with*

$$|X_1| \cdot |X_2| \cdot (|X_3| \cdots |X_n|)^{\frac{1}{81}} > p^{1+c}$$

there is an estimate

$$\left| \sum_{x_1 \in X_1} \cdots \sum_{x_n \in X_n} e^{2\pi i x_1 \ldots x_n} \right| < C|X_1| \cdots |X_n| p^{-\frac{0.45c}{2^n}}$$

for some absolute constant $C > 0$.

An easy corollary of Theorem 2 is an exponential sum estimate for multiplicative subgroup, which can be considered as an explicit version of Theorem 1.

Corollary 1. *If H is a multiplicative subgroup of $\mathbb{F}_p^*$ with cardinality*

$$|H| > e^{\frac{57 \ln p}{\ln\ln p}}$$

then

$$\max_{(a,p)=1} \left| \sum_{x \in H} e^{2\pi i a x} \right| = o(|H|)$$

when $p \to \infty$.

The presence of a nontrivial subfields is an obvious obstacle when one is trying to extend above mentioned statements to arbitrary finite fields. Usual restriction on the cardinality of the subgroup is not sufficient in finite fields and we need to require more.

J. Bourgain [3, theorem B] have obtained a multilinear exponential sum estimate in an arbitrary finite field.

Theorem 3. *Let $0 < \delta, \delta_2 < 1$ and $r \in \mathbb{Z}_+, r \geqslant 2$. Let q be sufficiently large and $A_1, \ldots, A_r \subset \mathbb{F}_q$ satisfy*

$$|A_i| > q^{\delta} \quad for \quad 1 \leqslant i \leqslant r$$

$$|A_i \cap (aG + b)| < q^{-\delta_2}|A_i| \quad for \quad 2 \leqslant i \leqslant r, \tag{1}$$

whenever $a, b \in \mathbb{F}_q$ and G a proper subfield and

$$|A_1| \prod_{i=2}^{r} |A_i|^{\frac{1}{2}} > q^{1+\delta}.$$

Then we have

$$\left| \sum_{x_1 \in A_1, x_2 \in A_2, \ldots, x_r \in A_r} \psi(x_1 x_2 \cdots x_r) \right| < q^{-\delta'} |A_1| \ldots |A_r|$$

where we may take $\delta' = C^{-\frac{r}{\delta_2}} \left(\frac{\delta}{r}\right)^{Cr}$ for some absolute constant $C > 0$.

In present paper we'll establish the following theorem.

Theorem 4. *Take an arbitrary n with $3 \leqslant n \leqslant 0.9 \log_2 \log_2 q$ and let $A_1, A_2, \ldots, A_n \subset \mathbb{F}_q^*$. Take an arbitrary number $0 < \eta \leqslant 1$ and define $\gamma = \min\left(1, \frac{5215}{4}\eta\right)$. Suppose that $|A_i| \geqslant 3, i = 1, 2, \ldots, n$ and suppose that for every $j = 3, 4, \ldots, n$, an element d and a proper subfield S the condition*

$$|A_j \cap dS| \leqslant |A_j|^{1-\eta}$$

holds. Assume further that

$$|A_1| \cdot |A_2| \cdot (|A_3| \cdot |A_4| \cdots |A_n|)^{\frac{\gamma}{156450}} > q^{1+\varepsilon}.$$

Then for sufficiently large q there is an exponential sum estimate

$$\left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \cdots \sum_{a_n \in A_n} \psi(a_1 a_2 \ldots a_n) \right| < 100 |A_1||A_2| \cdots |A_n| q^{-\frac{0.45\varepsilon}{2^n}}.$$

As a simple consequence of Theorem 4 we'll establish an extension of Theorem 1. It is easy to see that Theorem 5 doesn't follows from Theorem 3.

Theorem 5. *Let $0 < \eta \leqslant 1$ be an arbitrary number and H be a multiplicative subgroup of $\mathbb{F}_q^*$ with*

$$|H| \geqslant q^{\frac{\max\left(\frac{135}{\eta}, 176006.25\right)}{\log_2 \log_2 q}}. \tag{2}$$

Suppose that for any proper subfield S the condition

$$|H \cap S| \leqslant |H|^{1-\eta}$$

holds. Then for sufficiently large q there is an exponential sum estimate

$$\left|\sum_{h \in H} \psi(h)\right| < 100|H| \cdot 2^{-4{,}5 \cdot 10^{-3} (\log_2 q)^{0.1}}.$$

We must note that the exponent $\max\left(\frac{135}{\eta}, 176006.25\right)$ in the condition (2) can be significantly improved if one combines Lemma 1 from [3] with ideas of proof of sum-product result from one of the paper of M. Garaev [4] or [2, chapter 3]. We won't do it because this doesn't change radically Theorem 5. We can also point that in Theorem 4 the condition (1) of Theorem 3 has been relaxed.

In section 2 we prove sum-product estimates which are used in section 3 to obtain theorems 4 and 5. Section 3 heavily relies on ideas of M. Garaev [4, chapter 4].

Acknowledgement. The authors would like to thank M. Garaev and S. Konyagin for their helpful comments on the draft of the paper.

2 Sum-product estimate.

Below in statements of lemmas all the subsets are assumed to be non-empty. The first two lemmas are due to Ruzsa [5, 6]. They hold for subsets of any abelian group, but here we state them only for subsets of $\mathbb{F}_q$.

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

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

Lemma 2. *For any subsets $X, B_1, \dots, B_k$ of $\mathbb{F}_q$ we have*

$$|B_1 + B_2 + \dots + B_k| \leqslant \frac{|X + B_1||X + B_2| \dots |X + B_k|}{|X|^{k-1}}.$$

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

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

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

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.

Lemma 3. *For any given subsets $X, Y \subseteq \mathbb{F}_q$ there is an element $\xi \in \mathbb{F}_q^*$ with*

$$|X + \xi Y| \geqslant \frac{|X||Y|(q-1)}{|X||Y| + (q-1)}.$$

Moreover, the following inequality holds

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

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

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

It is obvious that

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

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

and

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

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 exactly one η satisfying the equality $x_1 + y_1\eta = x_2 + y_2\eta$. Therefore,

$$\sum_{\xi \in \mathbb{F}_q^*} \sum_{s \in \mathbb{F}_q} (f_\xi^+(s))^2 \leqslant |X||Y|(q-1) + |X|^2|Y|^2.$$

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

$$\sum_{s\in\mathbb{F}_q}(f_\xi^+(s))^2 \leqslant |X||Y| + \frac{|X|^2|Y|^2}{q-1}.$$

By Cauchy-Schwartz,

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

Observing that

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

one can yield the second assertion of Lemma 3.

Combining two last inequalities we see that

$$|X+\xi Y| \geqslant \frac{|X|^2|Y|^2}{|X||Y| + \frac{|X|^2|Y|^2}{q-1}} = \frac{|X||Y|(q-1)}{|X||Y| + (q-1)}.$$

Lemma 3 now follows. ■

Definition 2. For any given subsets $X, Y \subset \mathbb{F}_q, |Y| > 1$ we denote

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

Lemma 4 is a simple extension of the lemma 2.50 from the book of T. Tao and V. Vu [7].

Lemma 4. *Consider two arbitrary subsets $X, Y \subset \mathbb{F}_q, |Y| > 1$. The given element $\xi \in \mathbb{F}_q$ 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 not injective only when $|X+\xi*Y| < |X||Y|$. On the other side, non-injectivity of F mean 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 4 now follows. ■

Lemma 5 uses ideas of S. Konyagin told the author in private communication. It also employs partially a method from the paper of N. Katz and C. Shen [8].

Lemma 5. *Given any subsets $A, B \subset \mathbb{F}_q$ such that $|A| > 1$ and B is not contained in any proper subfield of $\mathbb{F}_q$. Then*

$$\max\{|A+AB|, |A-AB|\} \geqslant \frac{1}{2^{\frac{1}{4}}}|A|^{\frac{6}{7}} \min\{|A||B|, q\}^{\frac{1}{7}}. \qquad (3)$$

Proof. Take an arbitrary element $a \in A, a \neq 0$ and notice that $1 \in \frac{1}{a} * A$. Now we substitute the set A with $\frac{1}{a} * A$ and this doesn't change the inequality (3). Let us consider four cases.

Case 1. If $Q[A, B] = \mathbb{F}_q, |A||B| < q$ then applying lemma 3 we see that one can find an element $\xi \in \mathbb{F}_q^*$ such that

$$|A + \xi B| \geqslant \frac{|A||B|(q-1)}{|A||B| + (q-1)} \geqslant \frac{1}{2}|A||B|.$$

Since $Q[A, B] = \mathbb{F}_q$ then there exist elements $a_1, a_2 \in A, b_1, b_2 \in B, b_1 \neq b_2$ with $\xi = \frac{a_1 - a_2}{b_1 - b_2}$. Therefore,

$$|b_1 A - b_2 A + a_1 B - a_2 B| \geqslant \frac{1}{2}|A||B|.$$

Applying lemma 2 one can deduce that

$$\frac{|A + b_1 A||A - b_2 A||A + a_1 B||A - a_2 B|}{|A|^3} \geqslant |b_1 A - b_2 A + a_1 B - a_2 B| \geqslant \frac{1}{2}|A||B|$$

and now it is easy to see that

$$|A + AB|^2 |A - AB|^2 \geqslant \frac{1}{2}|A|^4 |B|$$

and this completes proof of the lemma 5 in this case.

Case 2. If $Q[A, B] = \mathbb{F}_q, |A||B| \geqslant q$ then applying lemma 3 we see that there is $\xi^{'}$ with

$$|A + \xi^{'} B| \geqslant \frac{|A||B|(q-1)}{|A||B| + (q-1)} \geqslant \frac{1}{2}q.$$

Again, there is elements $a_1^{'}, a_2^{'} \in A, b_1^{'}, b_2^{'} \in B, b_1^{'} \neq b_2^{'}$ such that $\xi^{'} = \frac{a_1^{'} - a_2^{'}}{b_1^{'} - b_2^{'}}$. Therefore,

$$|b_1^{'} A - b_2^{'} A + a_1^{'} B - a_2^{'} B| \geqslant \frac{1}{2}q.$$

Applying lemma 2 we obtain

$$\frac{|A+b_1'A||A-b_2'A||A+a_1'B||A-a_2'B|}{|A|^3} \geqslant |b_1'A - b_2'A + a_1'B - a_2'B| \geqslant \frac{1}{2}q$$

and now it is obviously follows that

$$|A+AB|^2|A-AB|^2 \geqslant \frac{1}{2}|A|^3 q.$$

This completes proof of the lemma 5 in this case.

Case 3. If $1+Q[A,B] \not\subset Q[A,B]$ then one can find elements $a_1'', a_2'' \in A, b_1'', b_2'' \in B, b_1'' \neq b_2''$ such that $\xi'' := 1 + \frac{a_1''-a_2''}{b_1''-b_2''} \notin Q[A,B]$. Hence, applying Lemma 4 we get the equality $|A||B| = |A+\xi'' B|$. Now from obvious identity

$$|A+\xi'' B| = |(b_1''-b_2'')A + (a_1''-a_2'')B + (b_1''-b_2'')B|$$

and Lemma 2 one can easily deduce the inequality

$$|A||B| = |(b_1''-b_2'')A + (a_1''-a_2'')B + (b_1''-b_2'')B| \leqslant$$

$$\leqslant \frac{|A+A||A+B||(a_1-a_2)B + (b_1-b_2)A|}{|A|^2} \leqslant$$

$$\leqslant \frac{|A+A||A+B||A+a_1B||A-a_2B||A+b_1A||A-b_2A|}{|A|^5}.$$

Again, by Lemma 2 we see that

$$|A+A| \leqslant \frac{|A+AB|^2}{|AB|} \leqslant \frac{|A+AB|^2}{|A|}.$$

Combining all the previous inequalities it is easy to see that

$$|A||B| = |A+\xi'' B| \leqslant \frac{|A+AB|^5|A-AB|^2}{|A|^6} \Rightarrow$$

$$\Rightarrow |A+AB|^5|A-AB|^2 \geqslant |A|^7|B|.$$

This completes proof of the Lemma 5 in this case.

Case 4. If $1+Q[A,B] = Q[A,B]$ and $Q[A,B] \neq \mathbb{F}_q$ then consider three sets:

$$G = \{g \in \mathbb{F}_q : g + Q[A,B] = Q[A,B]\}$$

$$F = \{r \in \mathbb{F}_q : rQ[A,B] \subseteq Q[A,B]\}$$
$$F_0 = \{f \in \mathbb{F}_q : fG \subseteq G\}.$$

It is obvious that G is an additive subgroup of $\mathbb{F}_q$ and therefore F_0 is a subfield. Let us take an arbitrary elements $r \in F, g \in G$ and observe that if $r \neq 0$ then $Q[A,B] = rQ[A,B]$ since $|Q[A,B]| = |rQ[A,B]|$ and $rQ[A,B] \subseteq Q[A,B]$. If $r = 0$ then $0 = rg \in F_0$. Now suppose that $r \neq 0$. In view of $rg + Q[A,B] = rg + rQ[A,B] = r(g + Q[A,B]) = rQ[A,B] = Q[A,B]$ it is obvious that $rg \in G$ and therefore $F \subset F_0$. Notice that $F \neq \{0\}$ since $1 \in F$. If $F = \mathbb{F}_q$ then obviously $Q[A,B] = \mathbb{F}_q$ so we returning to the cases 1 and 2, and we can suppose that F is a proper subfield. It is easy to see that $B \not\subset F$, hence there is an element $b \in B$ such that $bQ[A,B] \not\subset Q[A,B]$ and one can find elements $a_1^{III}, a_2^{III} \in A, b_1^{III}, b_2^{III} \in B$ with $\xi^{III} = b\frac{a_1^{III} - a_2^{III}}{b_1^{III} - b_2^{III}} \notin Q[A,B]$. Using Lemma 4, we deduce the equality

$$|A||B| = |A + \xi^{III}B| = |(b_1^{III} - b_2^{III})A + b(a_1^{III} - a_2^{III})B|.$$

Applying Lemma 2, we see that

$$|A||B| = |(b_1^{III} - b_2^{III})A + b(a_1^{III} - a_2^{III})B| \leqslant$$
$$\leqslant \frac{|A + bA||(b_1^{III} - b_2^{III})A + (a_1^{III} - a_2^{III})B|}{|A|} \leqslant$$
$$\leqslant \frac{|A + bA||A + b_1^{III}A||A - b_2^{III}A||A + a_1^{III}B||A - a_2^{III}B|}{|A|^4} \leqslant$$
$$\leqslant \frac{|A + AB|^3|A - AB|^2}{|A|^4}.$$

Now it directly follows that

$$|A + AB|^3|A - AB|^2 \geqslant |A|^5|B|.$$

Lemma 5 is proved. ■

For any nonempty subsets $A \subset \mathbb{F}_q, B \subset \mathbb{F}_q, G \subset A \times B$ we define

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

Let us recall the Balog-Szemeredi-Gowers result (see the paper of B. Sudakov, E. Szemeredi and V. Vu [9], Theorem 4.1, p. 138 and Corollary 4.6, p. 143).

Proposition 1. *(i) Let A, B be finite subsets of an additive group and $|A| = n \geqslant |B|$. Assume $G \subset A \times B$ and*

$$|G| > \frac{1}{K_1} n^2, \qquad |A^+_G B| < K_2 n$$

for some $K_1, K_2 \geqslant 1$. Then there are $A' \subset A, B' \subset B$ such that

$$|A'| > \frac{1}{16K_1^2} n, |B'| > \frac{n}{4K_1} \text{ and } |A' + B'| < 2^{12} K_1^5 K_2^3 n.$$

(ii) If in part (i) $A = B$, then there is a subset $A' \subset A$ satisfying

$$|A'| > \frac{n}{4K_1} \text{ and } |A' + A'| < 2^{28} K_1^{13} K_2^6 |A'|.$$

We shall use the following result from the book of T. Tao and V. Vu [7] (Lemma 2.30, p. 80).

Lemma 6. *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*

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

The Proposition 2 uses ideas and generalizes Theorem C from the paper of J. Bourgain [1].

Proposition 2. *Assume that $A \subseteq \mathbb{F}_q, B \subseteq \mathbb{F}_q$, $|A| = q^\alpha, |B| = q^\beta$, $\alpha \geqslant \beta$ and take an arbitrary $0 < \eta \leqslant 1$. Suppose further that for every nontrivial subfield $S \subset \mathbb{F}_q$ and every element $d \in \mathbb{F}_q$ 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 $\gamma = \min\left(\beta, \frac{5215}{4}\beta\eta, 1 - \alpha\right)$.

Proof. Let $A, B \subseteq \mathbb{F}_q$ be as in Proposition 2 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

$$E_+(A, bA) > \frac{C}{2}|B|^{-\delta}|A|^3 \text{ for } b \in B_1. \tag{4}$$

Fix $b \in B_1$. By the Lemma 6 applied to (4) one can deduce that there is $G^{(b)} \subset A \times bA, |G^{(b)}| > \frac{C}{4}|B|^{-\delta}|A|^2$ such that

$$|A +_G bA| < \frac{4}{C}|B|^{\delta}|A|.$$

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

$$|A_1^{(b)}| > \frac{C^2}{2^8}|B|^{-2\delta}|A|,$$

$$|A_2^{(b)}| > \frac{C}{2^4}|B|^{-\delta}|A|,$$

$$|A_1^{(b)} + bA_2^{(b)}| < \frac{2^{28}}{C^8}|B|^{8\delta}|A|. \tag{5}$$

Write

$$\frac{C^3}{2^{12}}|B_1||B|^{-3\delta}|A|^2 < \sum_{b \in B_1} |A_1^{(b)} \times A_2^{(b)}|$$

$$\leqslant |A| \left[\sum_{b,b' \in B_1} \left| \left(A_1^{(b)} \cap A_1^{(b')} \right) \times \left(A_2^{(b)} \cap A_2^{(b')} \right) \right| \right]^{\frac{1}{2}}$$

by Cauchy-Schwartz. Hence

$$\frac{C^8}{2^{26}}|B|^{2-8\delta}|A|^2 < \sum_{b,b' \in B_1} \left| \left(A_1^{(b)} \cap A_1^{(b')} \right) \times \left(A_2^{(b)} \cap A_2^{(b')} \right) \right|$$

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

$$|B_2| > \frac{C^8}{2^{27}}|B|^{1-8\delta} \tag{6}$$

$$|A_1^{(b)} \cap A_1^{(b_0)}|, |A_2^{(b)} \cap A_2^{(b_0)}| > \frac{C^8}{2^{27}}|B|^{-8\delta}|A| \text{ for } b \in B_2. \quad (7)$$

Let us estimate by Lemma 1

$$|b_0A_2^{(b_0)} - bA_2^{(b_0)}| \leqslant |b_0A_2^{(b_0)} + A_1^{(b_0)}||A_1^{(b_0)} + bA_2^{(b_0)}||A_1^{(b_0)}|^{-1}$$

$$|b_0A_2^{(b_0)} + bA_2^{(b_0)}| \leqslant |b_0A_2^{(b_0)} + A_1^{(b_0)}||A_1^{(b_0)} + bA_2^{(b_0)}||A_1^{(b_0)}|^{-1}$$

$$|A_1^{(b_0)} + bA_2^{(b_0)}| \leqslant |A_1^{(b_0)} + A_1^{(b)}||A_1^{(b)} + bA_2^{(b_0)}||A_1^{(b)}|^{-1}$$

$$|A_1^{(b)} + bA_2^{(b_0)}| \leqslant |A_1^{(b)} + bA_2^{(b)}||A_2^{(b_0)} + A_2^{(b)}||A_2^{(b)}|^{-1}.$$

Hence, by (5)

$$|b_0A_2^{(b_0)} \pm bA_2^{(b_0)}| < \frac{2^{76}}{C^{21}}|B|^{21\delta}|A_1^{(b_0)} + A_1^{(b)}||A_2^{(b_0)} + A_2^{(b)}||A|^{-1}. \quad (8)$$

Also, by (7), (5) and Lemma 2,

$$|A_1^{(b_0)} + A_1^{(b)}| \leqslant \frac{|A_1^{(b_0)} + A_1^{(b_0)}||A_1^{(b)} + A_1^{(b)}|}{|A_1^{(b_0)} \cap A_1^{(b)}|}$$

$$< 2^{27}\frac{|B|^{8\delta}}{|A|}\frac{|A_1^{(b_0)} + b_0A_2^{(b_0)}|^2}{|A_2^{(b_0)}|}\frac{|A_1^{(b)} + bA_2^{(b)}|^2}{|A_2^{(b)}|} < \frac{2^{147}}{C^{42}}|B|^{42\delta}|A|$$

and similarly one can see that

$$|A_2^{(b_0)} + A_2^{(b)}| < \frac{2^{155}}{C^{44}}|B|^{44\delta}|A|.$$

Combining last inequalities with (8), we obtain

$$|b_0A_2^{(b_0)} \pm bA_2^{(b_0)}| < \frac{2^{378}}{C^{107}}|B|^{107\delta}|A| \quad \text{for all } b \in B_2. \quad (9)$$

Applying Lemma 1 we see that

$$|A_2^{(b_0)} + A_2^{(b_0)}| = |b_0A_2^{(b_0)} + b_0A_2^{(b_0)}| \leqslant \frac{|A_1^{(b_0)} + b_0A_2^{(b_0)}|^2}{|A_1^{(b_0)}|} < \frac{2^{64}}{C^{18}}|B|^{18\delta}|A| \quad (10)$$

$$|A_2^{(b_0)} - A_2^{(b_0)}| = |b_0A_2^{(b_0)} - b_0A_2^{(b_0)}| \leqslant \frac{|A_1^{(b_0)} + b_0A_2^{(b_0)}|^2}{|A_1^{(b_0)}|} < \frac{2^{64}}{C^{18}}|B|^{18\delta}|A| \quad (11)$$

Now we redefine $A_2^{(b_0)}$ by A and $\frac{B_2}{b_0}$ by B and from (9), (10) and (11) one can deduce the following properties (for $\delta < \frac{1}{440}$):

$$|A+A| < \frac{2^{70}}{C^{19}}|B|^{20\delta}|A| \tag{12}$$

$$|A+bA| < \frac{2^{389}}{C^{108}}|B|^{110\delta}|A| \text{ for all } b \in B \tag{13}$$

$$|A-A| < \frac{2^{70}}{C^{19}}|B|^{20\delta}|A| \tag{14}$$

$$|A-bA| < \frac{2^{389}}{C^{108}}|B|^{110\delta}|A| \text{ for all } b \in B. \tag{15}$$

Our aim is to derive contradiction from (12)-(15), if δ is a sufficiently small constant.

Let $\xi \in \mathbb{F}_q$ and assume that

$$\min_{B' \subset B, |B'| > \frac{C^{216}}{2^{782}}|B|^{1-220\delta}} |A+\xi B'| < \frac{2^{529}}{C^{146}}|B|^{150\delta}|A|. \tag{16}$$

By Lemma 3,

$$|A+\xi B'| \geqslant \frac{|A|^2|B'|^2}{E_+(A,\xi B')}.$$

It is follows from (16) that

$$|\{(a_1,a_2,b_1,b_2) \in A\times A\times B\times B : a_1-a_2 = \xi(b_1-b_2)\}| =$$
$$= E_+(A,\xi B) > \frac{C^{578}}{2^{2093}}|A||B|^{2-590\delta}. \tag{17}$$

We denote $\Omega = \Omega_\delta$ the set of $\xi \in \mathbb{F}_q$ satisfying (16).

Clearly from (17) follows that

$$\frac{C^{578}}{2^{2093}}|\Omega||A||B|^{2-590\delta} \leqslant |A|^2|B|^2$$

and therefore

$$|\Omega| < \frac{2^{2093}}{C^{578}}|B|^{590\delta}|A|. \tag{18}$$

Returning to (13), let $b \in B$. Then by Lemma 3,

$$E_+(A,bA) > \frac{C^{108}}{2^{389}}|A|^3|B|^{-110\delta}.$$

Hence,

$$|\{(a_1,a_2,a_3,a_4,b)\in A^4\times B: a_1-a_2=b(a_3-a_4)\}|>\frac{C^{108}}{2^{389}}|A|^3|B|^{1-110\delta}$$

and we may specify $\bar{a},\bar{\bar{a}}\in A$ such that

$$|\{(a_1,a_2,b)\in A^2\times B: a_2-\bar{\bar{a}}=b(a_1-\bar{a})\}|>\frac{C^{108}}{2^{389}}|A||B|^{1-110\delta}.$$

Then there is a set $A_0\subset A$ satisfying

$$\begin{aligned} |A_0|&>\frac{C^{108}}{2^{390}}|B|^{-110\delta}|A| \\ |(A-\bar{\bar{a}})\cap B\cdot(a-\bar{a})|&>\frac{C^{108}}{2^{390}}|B|^{1-110\delta}\ \text{ for }\ a\in A_0. \end{aligned} \tag{19}$$

For $a\in A_0$, let $B_a\subset B$ satisfy

$$\begin{aligned} (a-\bar{a})B_a&\subset A-\bar{\bar{a}} \\ |B_a|&>\frac{C^{108}}{2^{390}}|B|^{1-110\delta}. \end{aligned} \tag{20}$$

Let us define

$$\mathcal{G}=\left\{(a,a')\in A_0\times A_0: |B_a\cap B_{a'}|>\frac{C^{216}}{2^{782}}|B|^{1-220\delta}\right\}.$$

Hence, by Cauchy-Schwartz we have

$$\frac{C^{108}}{2^{390}}|B|^{1-110\delta}|A_0|\leqslant\sum_{a\in A_0}|B_a|=\sum_{b\in B}\sum_{a\in A_0}1_{B_a}(b)$$

$$\leqslant|B|^{\frac{1}{2}}\left(\sum_{a,a'\in A_0}|B_a\cap B_{a'}|\right)^{\frac{1}{2}}\leqslant\frac{C^{108}}{2^{391}}|B|^{\frac{1}{2}}|A_0||B|^{\frac{1}{2}-110\delta}+|B||\mathcal{G}|^{\frac{1}{2}}$$

implying by (19)

$$|\mathcal{G}|>\frac{C^{216}}{2^{782}}|B|^{-220\delta}|A_0|^2>\frac{C^{432}}{2^{1562}}|B|^{-440\delta}|A|^2. \tag{21}$$

Let $(a,a^{'}) \in \mathcal{G}$ and $b \in B$. We denote $B^{'} = B_a \cap B_{a'}$ for which by definition of $\mathcal{G}$

$$|B^{'}| > \frac{C^{216}}{2^{782}}|B|^{1-220\delta}.$$

Then, denoting

$$\xi_1 = (a^{'} - \bar{a}) + b(a - \bar{a})$$
$$\xi_2 = (a^{'} - \bar{a}) - b(a - \bar{a})$$

we have by (20), (12)-(15) and Lemma 2,

$$|A + \xi_1 B^{'}| \leqslant |A + b(a - \bar{a})B_a + (a^{'} - \bar{a})B_{a'}|$$
$$\leqslant |A + b(A - \bar{\bar{a}}) + A - \bar{\bar{a}}| < \frac{2^{529}}{C^{146}}|B|^{150\delta}|A|$$
$$|A + \xi_2 B^{'}| \leqslant |A + A - \bar{\bar{a}} - b(A - \bar{\bar{a}})| < \frac{2^{529}}{C^{146}}|B|^{150\delta}|A|.$$

Now we see that ξ_1 and ξ_2 satisfies (16). Hence $\xi_1, \xi_2 \in \Omega$. This shows that

$$(a - \bar{a})B \pm (a^{'} - \bar{a}) \subset \Omega \text{ whenever } (a,a^{'}) \in \mathcal{G}. \tag{22}$$

Let us define

$$A_1 = \left\{ a \in A_0 : |\mathcal{G}(a)| > \frac{C^{432}}{2^{1563}}|B|^{-440\delta}|A| \right\}$$

satisfying by (21)

$$|A_1| > \frac{C^{432}}{2^{1563}}|B|^{-440\delta}|A|.$$

Now we need to estimate $|A \pm (A_1 - \bar{a})B|$. Fix $x_1 = \tilde{a} + (a - \bar{a})b$ and $x_2 = \tilde{a} - (a - \bar{a})b$ where $\tilde{a} \in A, a \in A_1, b \in B$. If $a^{'} \in \mathcal{G}(a)$, then by (22) we have

$$x_1 = (\tilde{a} - a^{'} + \bar{a}) + ((a - \bar{a})b + a^{'} - \bar{a}) \in (A - A_1 + \bar{a}) + \Omega$$

$$x_2 = (\tilde{a} - a^{'} + \bar{a}) + (a^{'} - \bar{a} - (a - \bar{a})b) \in (A - A_1 + \bar{a}) + \Omega$$

and $|\mathcal{G}(a)| > \frac{C^{432}}{2^{1563}}|B|^{-440\delta}|A|$ since $a \in A_1$.

Denoting

$$\sigma : (A - A_1 + \bar{a}) \times \Omega \to \mathbb{F}_q$$

the restriction of the sum - map we showed that

$$|\sigma^{-1}(x)| > \frac{C^{432}}{2^{1563}}|B|^{-440\delta}|A|$$

if $x \in A \pm (A_1 - \bar{a})B$. Consequently, according to (12) and (18) it is easy to see that

$$|A \pm (A_1 - \bar{a})B| \leqslant \frac{|A - A_1||\Omega|}{2^{-1563}|B|^{-440\delta}|A|} < \frac{2^{3726}}{C^{1029}}|B|^{1050\delta}|A|. \qquad (23)$$

Redefining $\mathcal{A} = A_1 - \bar{a}$ and $\mathcal{B} = B$ and using the condition (6) we see that

$$|\mathcal{B}| > \frac{C^8}{2^{27}} q^{\beta(1-8\delta)}.$$

If for any proper subfield S the restriction

$$|B \cap dS| < \frac{C^8}{2^{27}} q^{\beta(1-8\delta)}$$

holds (in this formula we taking an original unmodified set B from the statement of Proposition 2) then $\mathcal{B}$ is not contained in S and we can apply Lemma 5. We get the inequality

$$\max\{|\mathcal{A} + \mathcal{A}\mathcal{B}|, |\mathcal{A} - \mathcal{A}\mathcal{B}|\} \geqslant \frac{1}{2^{\frac{1}{4}}}|\mathcal{A}|^{\frac{6}{7}} \min\{|\mathcal{A}||\mathcal{B}|, q\}^{\frac{1}{7}}. \qquad (24)$$

Recalling an estimate (23) we can rewrite it as

$$|\mathcal{A} \pm \mathcal{A}\mathcal{B}| < \frac{2^{5289}}{C^{1461}}|\mathcal{B}|^{1490\delta}|\mathcal{A}|. \qquad (25)$$

If

$$C = 2^{\frac{21157}{5844}} = 12,2975...$$

then the inequality (25) is equivalent to

$$|\mathcal{A} \pm \mathcal{A}\mathcal{B}| < \frac{1}{2^{\frac{1}{4}}}|\mathcal{B}|^{1490\delta}|\mathcal{A}|. \qquad (26)$$

Now we can take

$$\delta = \frac{1}{10430} \min\left(1, \frac{1-\alpha}{\beta}, \frac{5215}{4}\eta\right)$$

to get a contradiction between inequalities (26) and (24). Proposition 2 now follows. ■

The Corollary 2 generalizes and uses ideas of the Theorem 6 from the paper of J. Bourgain [1].

Corollary 2. *Assume that $A \subseteq \mathbb{F}_q, B \subseteq \mathbb{F}_q$, $|A| = q^{\alpha}, |B| = q^{\beta}, \alpha \geqslant \beta$ and take an arbitrary $0 < \eta \leqslant 1$. Suppose further that for every nontrivial subfield $S \subset \mathbb{F}_q$ and every element $d \in \mathbb{F}_q$ the set B satisfies the restriction*

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

Then

$$|A-A|\frac{|A|^2|B|^2}{E_{\times}(A,B)} \geqslant \frac{1}{3}q^{\frac{\gamma}{31290}}|A|^2$$

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

Proof. Assume that for some $\rho > 0$ we have

$$|A-A|\frac{|A|^2|B|^2}{E_{\times}(A,B)} < \frac{1}{52^{\frac{1}{3}}}|B|^{\rho}|A|^2. \tag{27}$$

In particular,

$$E_{\times}(A,B) = |\{(a,b,a_1,b_1) \in A \times B \times A \times B : ab = a_1b_1\}| > 52^{\frac{1}{3}}|A||B|^{2-\rho}$$

and we may specify $b_0 \in B, b_0 \neq 0$ such that

$$52^{\frac{1}{3}}|A||B|^{1-\rho} < |\{(a,b) \in A \times B : ab \in b_0A\}| \leqslant \sum_{b \in B}|A \cap \frac{b}{b_0}A|.$$

Recalling Proposition 2 we see that

$$\sum_{b \in B} E_+\left(A, \frac{b}{b_0}A\right) \leqslant 13|B|^{1-\delta}|A|^3$$

where $\delta = \frac{1}{10430}\min\left(1, \frac{1-\alpha}{\beta}, \frac{5215}{4}\eta\right)$. Obviously,

$$\frac{1}{13}|A|^{-2}|B|^{\delta-\rho}\sum_{b \in B} E_+\left(A, \frac{b}{b_0}A\right) \leqslant |A||B|^{1-\rho}$$

and therefore

$$\sum_{b \in B}\left(\frac{2}{52^{\frac{1}{3}}}|A \cap \frac{b}{b_0}A| - \frac{1}{13}|A|^{-2}|B|^{\delta-\rho}E_+\left(A, \frac{b}{b_0}A\right)\right) > |A||B|^{1-\rho}$$

Now we may fix $b_1 \in B$ with

$$|A \cap \frac{b_1}{b_0}A| > \frac{52^{\frac{1}{3}}}{2}|A||B|^{-\rho} + \frac{52^{\frac{1}{3}}}{26}|A|^{-2}|B|^{\delta-\rho}E_+\left(A, \frac{b_1}{b_0}A\right). \qquad (28)$$

We denote

$$A' = A \cap \frac{b_1}{b_0}A.$$

Then by lemma 3, (27) and (28)

$$\frac{1}{52^{\frac{1}{3}}}|B|^{\rho}|A| > |A - A'| \geqslant \frac{|A|^2|A'|^2}{E_+(A, A')} \geqslant$$

$$\geqslant \frac{|A|^2|A'|^2}{E_+(A, \frac{b_1}{b_0}A)} > \frac{52^{\frac{1}{3}}}{26}|A'||B|^{\delta-\rho} > \frac{1}{52^{\frac{1}{3}}}|A||B|^{\delta-2\rho}$$

and therefore $\rho > \frac{\delta}{3}$. Corollary 2 now follows. ■

3 Exponential sum estimate.

We shall use the following simple lemma.

Lemma 7. *Let ψ be an additive character of $\mathbb{F}_q$ and $a(n), b(m), n, m = 1, 2, \ldots, p$ be a complex numbers with*

$$\sum_{n=0}^{q-1}|a(n)|^2 = N, \qquad \sum_{m=0}^{q-1}|b(m)|^2 = M.$$

Then

$$\left|\sum_{n=0}^{q-1}\sum_{m=0}^{q-1}a(n)b(m)\psi(nm)\right| \leqslant \sqrt{qNM}.$$

Proof. Let us estimate

$$\left|\sum_{n=0}^{q-1}\sum_{m=0}^{q-1}a(n)b(m)\psi(nm)\right| \leqslant \sum_{n=0}^{q-1}|a(n)|\left|\sum_{m=0}^{q-1}b(m)\psi(mn)\right|$$

and define

$$W = \sum_{n=0}^{q-1}|a(n)|\left|\sum_{m=0}^{q-1}b(m)\psi(mn)\right|.$$

Now by Cauchy-Schwartz we obtain

$$W^2 \leqslant N \sum_{n=0}^{q-1} \left| \sum_{m=0}^{q-1} b(m)\psi(mn) \right|^2 =$$

$$= N \sum_{m_1=0}^{q-1} \sum_{m_2=0}^{q-1} \sum_{n=0}^{q-1} b(m_1)\overline{b(m_2)}\psi(n(m_1 - m_2)) = qNM.$$

Lemma 7 is proved. ■

We shall need a special form of Balog-Szemeredi-Gowers theorem, which can be found in the paper of J. Bourgain and M. Garaev [10, lemma 2.2]. Despite the fact that in this paper the result stated for $\mathbb{F}_p$ it's true for any abelian group.

Proposition 3. *Let $A \subset \mathbb{F}_q, B \subset \mathbb{F}_q, E \subset A \times B$ be such that $|G| \geqslant \frac{|A||B|}{K}$. There exists s subset $A' \subset A$ such that $|A'| \geqslant \frac{|A|}{10K}$ and*

$$|A_G^+ B|^4 \geqslant \frac{|A' - A'||A||B|^2}{10^4 K^5}.$$

The proofs of Lemmas 8, 9 and Theorem 4 repeat arguments from the paper of the paper of M. Garaev [2, chapter 4] (see also result of J. Bourgain and M. Garaev [10]).

Lemma 8. *Given an arbitrary subsets $A, B \subset \mathbb{F}_q^*, |A| = q^\alpha, |B| = q^\beta$ and natural numbers $s_1, s_2, \ldots, s_N \in \mathbb{F}_q^*, N > 0$, any $\delta > 0$ and $0 < \eta \leqslant 1$. Suppose further that for every nontrivial subfield $S \subset \mathbb{F}_q$ and every element $d \in \mathbb{F}_q$ the set B satisfies the restriction*

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

and for $a \in A$ the inequality holds

$$\left| \sum_{b \in B} \sum_{n=1}^{N} \psi(abs_n) \right| \geqslant \delta |B| N.$$

Then there is a subset $C \subset \mathbb{F}_q^*$ with cardinality

$$|C| > \frac{1}{94} \delta^{\frac{16}{5}} |A||B|^{\frac{\gamma}{156450}}$$

such that for every $c \in C$ there is an estimate

$$\left|\sum_{n=1}^{N} \psi(cs_n)\right| \geqslant \frac{1}{2}\delta^2 N,$$

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

Proof. Assume that $\delta^2 < 10|A|^{-1}$. Then fix any element $a_0 \in A$ and define

$$C = \left\{c \in a_0 B : \left|\sum_{n=1}^{N} \psi(cs_n)\right| \geqslant \frac{1}{2}\delta N\right\}.$$

Then $|C| \geqslant \frac{1}{2}\delta|B|$ and therefore, from our assumption we see that

$$\frac{1}{94}\delta^{\frac{16}{5}}|A||B|^{\frac{\min\left(1,\frac{5215}{4}\eta\right)}{156450}} \leqslant \frac{1}{94}|A||B|\delta^3 < \frac{10}{47}|C| < |C|.$$

The second property of the set C easily follows from its definition.

Now we can suppose that $\delta^2|A| \geqslant 10$. Let us note that for some complex numbers α_a with $|\alpha_a| = 1$ we have

$$\sum_{a\in A}\sum_{b\in B}\sum_{n=1}^{N} \alpha_a \psi(abs_n) \geqslant \delta|A||B|N$$

and therefore for some $n = n_0$ we obtain

$$\sum_{b\in B}\left|\sum_{a\in A} \alpha_a \psi(abs_{n_0})\right| \geqslant \delta|A||B|.$$

By lemma 7 it is follows that $\delta^2|A||B| \leqslant q$.

From the statement of the lemma 8 one can easily find an element $b_0 \in B$ with

$$\sum_{a\in A}\left|\sum_{n=1}^{N} \psi(ab_0 s_n)\right| \geqslant \delta|A|N.$$

Changing summation order we see that there are complex numbers $\alpha_a^{'}$, $|\alpha_a^{'}| = 1, a \in A$ for which

$$\sum_{n=1}^{N}\left|\sum_{a\in A} \alpha_a^{'} \psi(ab_0 s_n)\right| \geqslant \delta|A|N.$$

Applying Cauchy-Schwartz and then changing order of summation we deduce

$$\sum_{a_1\in A}\sum_{a_2\in A}\left|\sum_{n=1}^{N}\psi((a_1-a_2)b_0s_n)\right|\geqslant\delta^2|A|^2N.$$

Since also $\delta^2|A|\geqslant 10$ then

$$\sum_{\substack{a_1,a_2\in A\\ a_1\neq a_2}}\left|\sum_{n=1}^{N}\psi((a_1-a_2)b_0s_n)\right|\geqslant 0.9\delta^2|A|^2N.$$

Let us define

$$G=\left\{(a_1,a_2)\in A\times A: a_1\neq a_2, \left|\sum_{n=1}^{N}\psi((a_1-a_2)b_0s_n)\right|\geqslant 0.5\delta^2N\right\}.$$

Then

$$|G|\geqslant 0.4\delta^2|A|^2.$$

Applying Lemma 3 with $K=\frac{1}{0.4\delta^2}$ we derive existence of the set $A_1\subset A$ of cardinality $|A_1|\geqslant 0,04\delta^2|A|$ such that

$$|A_{\overline{G}}A|^4\geqslant\frac{|A_1-A_1||A|^3\delta^{10}}{976562.5}.$$

Defining $C_1=(A_{\overline{G}}A)b_0$ we get

$$|C_1|^4\geqslant\frac{|A_1-A_1||A|^3\delta^{10}}{976562.5}. \tag{29}$$

We can also assume that $|A_1|\leqslant\delta^2|A|$ (if A_1 is too large then we can remove the required number of elements not affecting the inequality (29)). Moreover, by definition for every $c\in C_1$ we have

$$\left|\sum_{n=1}^{N}\psi(cs_n)\right|\geqslant 0.5\delta^2N.$$

For a given $a\in A_1$ let us define

$$B_{(a)}=\left\{b\in B:\left|\sum_{n=1}^{N}\psi(abs_n)\right|\geqslant 0.5\delta N\right\}.$$

Then $|B_{(a)}| \geqslant 0.5\delta|B|$. Denoting

$$C_2 = \{ab : a \in A_1, b \in B_a\}.$$

Clearly, the number of pairs (a, b) with $a \in A_1, b \in B_{(a)}$ is at least $0.5|A_1||B|$ and the number of solutions of the equation

$$a_1 b_1 = a_2 b_2, \qquad a_1 \in A_1, b_1 \in B_{(a_1)}, \qquad a_2 \in A_1, b_2 \in B_{(a_2)}$$

is at most $E_\times(A_1, B)$ and thus using arguments from proof of the Lemma 3 we obtain

$$|C_2| \geqslant \frac{\delta^2 |A_1|^2 |B|}{4E_\times(A_1, B)}. \tag{30}$$

Moreover, by definition for every $c \in C_2$ we have

$$\left| \sum_{n=1}^{N} \psi(abs_n) \right| \geqslant 0.5\delta N.$$

Now it's suffices to show that one of the sets C_1 or C_2 has a cardinality required by the statement of the Lemma 8. From (29) and (30) we deduce

$$|C_1|^4 |C_2| \geqslant \frac{\delta^{12} |A_1|^2 |A|^3 |B|^2 |A_1 - A_1|}{3906250 E_\times(A_1, B)}.$$

By the Corollary 2 and an inequality $|A_1| \geqslant 0,04\delta^2|A|$ follows that

$$|C_1|^4 |C_2| \geqslant \frac{1}{11718750} \delta^{12} |A|^3 |A_1|^2 \min\left\{ |B|, \frac{q}{|A_1|}, |B|^{\frac{5215}{4}\eta} \right\}^{\frac{1}{31290}} \geqslant$$

$$\geqslant \frac{1}{7324972249} \delta^{16} |A|^5 \min\left\{ |B|, \frac{q}{|A_1|}, |B|^{\frac{5215}{4}\eta} \right\}^{\frac{1}{31290}}.$$

Finally, since $\delta^2 \leqslant \frac{q}{|A||B|}$ then

$$|C_1|^4 |C_2| \geqslant \frac{1}{7324972249} \delta^{16} |A|^5 |B|^{\frac{\gamma}{31290}},$$

where $\gamma = \min\left(1, \frac{5215}{4}\eta\right)$. Lemma 8 now follows. ■

Lemma 9. *Given an arbitrary subsets* $A, B \subset \mathbb{F}_q^*, |A| = q^\alpha, |B| = q^\beta, |B| \geqslant 3$, *natural numbers* $s_1, s_2, \ldots, s_N \in \mathbb{F}_q^*, N > 0$, *any* $\Delta > 0$ *and* $0 < \eta \leqslant 1$. *Suppose further that for every nontrivial subfield* $S \subset \mathbb{F}_q$ *and every element* $d \in \mathbb{F}_q$ *the set* B *satisfies the restriction*

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

and

$$\sum_{a\in A}\left|\sum_{b\in B}\sum_{n=1}^{N}\psi(abs_n)\right| \geqslant \Delta|A||B|N.$$

Then there is a subset C *with cardinality*

$$|C| \geqslant \frac{1}{163}|A||B|^{\frac{\gamma}{156450}}\Delta^{\frac{16}{5}}(\log_2|B|)^{-\frac{16}{5}}$$

such that

$$\sum_{c\in C}\left|\sum_{n=1}^{N}\psi(cs_n)\right| \geqslant \frac{\Delta^2}{50(\log_2|B|)^2}N|C|,$$

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

Proof. Obviously there is an element $b_0 \in B$ with

$$\sum_{a\in A}\left|\sum_{n=1}^{N}\psi(ab_0s_n)\right| \geqslant \Delta|A|N.$$

If $\Delta \leqslant 10|B|^{-1}$ then we can define $C = b_0A$ and this completes proof of the Lemma 9. Now we can suppose that $\Delta > 10|B|^{-1}$. Therefore,

$$\sum_{a\in A}{}'\left|\sum_{b\in B}\sum_{n=1}^{N}\psi(abs_n)\right| \geqslant 0.9\Delta|A||B|N,$$

where the dash sign means that the we sum up only the values of $a \in A$ such that

$$N \leqslant \left|\sum_{b\in B}\sum_{n=1}^{N}\psi(abs_n)\right| \leqslant |B|N.$$

The interval $[N, |B|N]$ contain at most $2\log_2|B|$ subintervals of the type $[2^{j-1}N, 2^jN)$ with $2 \leqslant 2^j \leqslant 2|B|$. Thus there is a subset $A_1 \subset A$ and a number $0 \leqslant \delta \leqslant 1$ such that

$$\delta N|B| \leqslant \left|\sum_{b\in B}\sum_{n=1}^{N}\psi(abs_n)\right| < 2\delta N|B| \quad \text{for every } x \in A_1$$

and moreover,

$$\delta|A_1|\log_2|B| \geqslant 0.2\Delta|A|.$$

In particular,

$$\delta \geqslant 0.2\Delta(\log_2|B|)^{-1}, \qquad |A_1| \geqslant 0.2\Delta|A|(\log_2|B|)^{-1}.$$

Applying Lemma 8 to A_1 instead of the set A we deduce existence of $C_1 \subset \mathbb{F}_q^*$ with cardinality

$$|C_1| \geqslant \frac{1}{94}|A_1||B|^{\frac{\min\left(1,\frac{5215}{4}\eta\right)}{156450}}\delta^{\frac{16}{5}} \geqslant \frac{1}{163}|A||B|^{\frac{\min\left(1,\frac{5215}{4}\eta\right)}{156450}}\Delta^{\frac{16}{5}}(\log_2|B|)^{-\frac{16}{5}}$$

such that for every $c \in C_1$ we have

$$\left|\sum_{n=1}^{N}\psi(cs_n)\right| \geqslant 0.5\delta^2 N \geqslant \frac{\Delta^2}{50(\log_2|B|)^2}N|C_1|.$$

Summing up the last inequality by all the elements $c \in C_1$ we completing proof of the Lemma 9. ■

We repeat statements of the theorems 4 and 5 for reader's convenience.

Theorem 4. *Take an arbitrary n with $3 \leqslant n \leqslant 0.9\log_2\log_2 q$ and let $A_1, A_2, \ldots, A_n \subset \mathbb{F}_q^*$. Take an arbitrary number $0 < \eta \leqslant 1$ and define $\gamma = \min\left(1, \frac{5215}{4}\eta\right)$. Suppose that $|A_i| \geqslant 3, i = 1, 2, \ldots, n$ and suppose that for every $j = 3, 4, \ldots, n$, an element d and a proper subfield S the condition*

$$|A_j \cap dS| \leqslant |A_j|^{1-\eta}$$

holds. Assume further that

$$|A_1|\cdot|A_2|\cdot(|A_3|\cdot|A_4|\cdots|A_n|)^{\frac{\gamma}{156450}} > q^{1+\varepsilon}. \tag{31}$$

Then for sufficiently large q there is an exponential sum estimate

$$\left|\sum_{a_1\in A_1}\sum_{a_2\in A_2}\cdots\sum_{a_n\in A_n}\psi(a_1a_2\ldots a_n)\right| < 100|A_1||A_2|\cdots|A_n|q^{-\frac{0.45\varepsilon}{2^n}}.$$

Proof. Let us denote

$$C = 163^{\frac{5(n-2)}{13\cdot 2^{n-1}-16}} \cdot 50^{\frac{13\cdot 2^{n-2}+3-8n}{13\cdot 2^{n-2}-8}}.$$

It is easy to see that $1 < C < 100$. Suppose that

$$\frac{1}{|A_1||A_2|\dots|A_n|}\sum_{a_1\in A_1}\left|\sum_{a_2\in A_2}\cdots\sum_{a_n\in A_n}\psi(a_1a_2\dots a_n)\right| \geqslant C\Delta(\log_2 q)^2$$

for some $\Delta > 0$. By Lemma 9 there is a subset $A_1^{'} \subset \mathbb{F}_q^*$ with cardinality

$$|A_1^{'}| \geqslant \frac{C^{\frac{16}{5}}}{163}|A_1||A_n|^{\frac{\gamma}{156450}}\Delta^{\frac{16}{5}}$$

such that

$$\frac{1}{|A_1^{'}||A_2|\dots|A_{n-1}|(\log_2 q)^2}\sum_{a_1^{'}\in A_1^{'}}\left|\sum_{a_2\in A_2}\cdots\sum_{a_{n-1}\in A_{n-1}}\psi(a_1^{'}a_2\dots a_{n-1})\right| \geqslant \frac{C^2\Delta^2}{50}.$$

Applying Lemma 9 again for the last inequality we establish existence of the subset $A_2^{'} \subset \mathbb{F}_q^*$ with cardinality

$$|A_2^{'}| \geqslant \frac{C^{2\cdot\frac{16}{5}}}{163\cdot 50^{\frac{16}{5}}}|A_1^{'}||A_{n-1}|^{\frac{\gamma}{156450}}\Delta^{2\frac{16}{5}} \geqslant$$

$$\geqslant \frac{C^{\frac{16}{5}(1+2)}}{163^2\cdot 50^{\frac{16}{5}}}|A_1|(|A_{n-1}||A_n|)^{\frac{\gamma}{156450}}\Delta^{\frac{16}{5}(1+2)}$$

with

$$\frac{1}{|A_2^{'}||A_2|\dots|A_{n-2}|(\log_2 q)^2}\sum_{a_2^{'}\in A_2^{'}}\left|\sum_{a_2\in A_2}\cdots\sum_{a_{n-2}\in A_{n-2}}\psi(a_1^{'}a_2\dots a_{n-2})\right| \geqslant \frac{C^4\Delta^4}{50^3}.$$

Continuing described iteration process one obtains on $n-2$-th step a subset $A_{n-2}^{'} \subset \mathbb{F}_q^*$ with cardinality

$$|A_{n-2}^{'}| \geqslant \frac{C^{\frac{16}{5}(2^{n-2}-1)}}{163^{n-2}\cdot 50^{\frac{16}{5}(2^{n-2}-n+1)}}|A_1|(|A_3|\dots|A_n|)^{\frac{\gamma}{156450}}\Delta^{\frac{16}{5}(2^{n-2}-1)} \qquad (32)$$

such that

$$\frac{1}{|A'_{n-2}||A_2|(\log_2 q)^2}\sum_{a'_{n-2}\in A'_{n-2}}\left|\sum_{a_2\in A_2}\psi(a'_{n-2}a_2)\right| \geqslant \frac{C^{2^{n-2}}\Delta^{2^{n-2}}}{50^{2^{n-2}-1}}.$$

By Lemma 7 we can estimate

$$\frac{C^{2^{n-2}}\Delta^{2^{n-2}}}{50^{2^{n-2}-1}} \leqslant \sqrt{\frac{q}{|A'_{n-2}||A_2|}}$$

and recalling inequalities (31) and (32) we deduce

$$\frac{C^{2^{n-1}}\Delta^{2^{n-1}+\frac{16}{5}(2^{n-2}-1)}}{50^{2^{n-1}-2}} < q^{-\varepsilon}\cdot\frac{163^{n-2}\cdot 50^{\frac{16}{5}(2^{n-2}-n+1)}}{C^{\frac{16}{5}(2^{n-2}-1)}}$$

From our choice of the constant C the last formula is satisfied if

$$\Delta^{2^{n+1}} < q^{-\varepsilon}.$$

Since $n \leqslant 0.9\log_2\log_2 q$ then for sufficiently large q we have

$$(\Delta(\log_2 q)^2)^{2^{n+1}} < q^{-\varepsilon}(\log_2 q)^{2^{n+2}} \leqslant q^{-0.9\varepsilon}.$$

Thus,

$$\Delta(\log_2 q)^2 < q^{-\frac{0.9\varepsilon}{2^{n+1}}}.$$

Theorem 4 is proved. ■

The theorem 5 is a simple corollary of the theorem 4.

Theorem 5. *Let $0 < \eta \leqslant 1$ be an arbitrary number and H be a multiplicative subgroup of $\mathbb{F}_q^*$ with $|H| \geqslant q^{\frac{\max\left(\frac{135}{\eta},176006.25\right)}{\log_2\log_2 q}}$. Suppose that for any proper subfield S the condition*

$$|H\cap S| \leqslant |H|^{1-\eta}$$

holds. Then for sufficiently large q there is an exponential sum estimate

$$\left|\sum_{h\in H}\psi(h)\right| < 100|H|\cdot 2^{-4{,}5\cdot 10^{-3}(\log_2 q)^{0.1}}.$$

Proof. Suppose that there is a proper subfield $S \subset \mathbb{F}_q$ and an element $d \notin S$ such that $|H \cap dS| > |H|^{1-\eta}$. Without loss of generality we can suppose that $d \in H$. Now $\frac{1}{d}H = H$ and therefore $H \cap dS = \frac{1}{d}H \cap S = H \cap S$. We got an inequality $|H \cap S| > |H|^{1-\eta}$, which contradicts statement of Theorem 5. It was established that for every element d and a proper subfield S the condition

$$|H \cap dS| \leqslant |H|^{1-\eta}$$

holds. Let us notice that for every natural k we have

$$\frac{1}{|H|^{k-1}} \left| \sum_{h_1 \in H} \sum_{h_2 \in H} \cdots \sum_{h_k \in H} \psi(h_1 h_2 \ldots h_k) \right| = \left| \sum_{h \in H} \psi(h) \right| .$$

Now application of the Theorem 4 with $\varepsilon = 0.01$, $n = [0.9 \log_2 \log_2 q]$, $A_1 = A_2 = \ldots = A_n = H$ completes proof of the Theorem 5. ■

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] M. Z. Garaev, *Sums and products of sets and rational exponential sums estimates in prime fields,* preprint.

[3] J. Bourgain, *On exponential sums in finite fields*, preprint.

[4] M. Z. Garaev, *A quantified version of Bourgain's sum-product estimate in $\mathbb{F}_p$ for subsets of incomparable sizes,* Electronic Journal of Combinatorics, vol. 15, 2008, Research paper 58, 8pp.

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

[8] N. Katz, C. Shen, *Garaev's inequality in finite fields not of prime order*, Online Journal of Analytic Combinatorics, N 3, 2008, ♯ 3.

[9] B. Sudakov, E. Szemeredi, V. Vu, *On a question of Erdös and Moser*, Duke Math. J., 129 (2005), N 1, 129 — 155.

[10] J. Bourgain, 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.