Character sums estimates and an application to a problem of Balog

Tomasz Schoen and Ilya D. Shkredov*

Abstract

We prove new bounds for sums of multiplicative characters over sums of set with small doubling and applying this result we break the square–root barrier in a problem of Balog concerning products of differences in a field of prime order.

1. Introduction

For a prime number $p$ let $\mathbb{F}_p$ be the prime field and let $\chi$ be a nontrivial multiplicative character modulo $p$. We will deal with a problem of estimating the exponential sum of the form

$$\sum_{a \in A, b \in B} \chi(a + b),$$

where $A, B$ are arbitrary subsets of the field $\mathbb{F}_p$. Such exponential sums were studied by numerous authors, see e.g. [6], [8], [9], [12]–[14], [22], [25]. One of the most important conjecture concerning character sums is the Paley graph conjecture, see [6].

**Conjecture 1** For every $\delta > 0$ there is $\tau = \tau(\delta) > 0$ such that for every prime number $p > p(\tau)$ and for any set $A, B \subseteq \mathbb{F}_p$ with $|A| > p^\delta$ and $|B| > p^\delta$ we have

$$\left| \sum_{a \in A, b \in B} \chi(a + b) \right| < p^{-\tau} |A| |B|.$$

Currently there are very few results regarding the above conjecture. The only affirmative answer was obtained in the following case

$$|A| > p^{\frac{1}{2}+\delta}, \quad |B| > p^\delta,$$

see [12]—[14]. M.–C. Chang [6] proved a result towards the conjecture for sets $A$ and $B$, where one of them has a small sumset. Her work was continued in [9], [22], [25] and currently the best result is the following theorem of Volostnov [25].

*The author is supported by the grant of the Russian Government N 075-15-2019-1926.
Theorem 2 Let $A, B \subset \mathbb{F}_p$ and $K, L, \delta > 0$ be such that

$$|A|, |B| > p^{\frac{1}{3} + \delta}, \quad \text{and} \quad |A + A| < K|A|, |B + B| < L|B|.$$  

Then there is a positive function $C(K)$ such that for any nontrivial multiplicative character $\chi$ modulo $p$ one has

$$\left| \sum_{a \in A, b \in B} \chi(a + b) \right| \ll p^{-\delta^2/C(K)}|A||B|,$$

provided that $p > p(\delta, K, L)$.

The following theorem is the main result of our paper.

Theorem 3 Let $A, B \subset \mathbb{F}_p$ and $K, L, \delta > 0$ be such that $|A| > p^\delta$, $|B| > p^{1/3 + \delta}$,

$$|A||B|^2 > p^{1 + \delta} \quad \text{and} \quad |A + A| < K|A|, |B + B| < L|B| \leq p^{\delta/2}|B|.$$  

Then there is an absolute constant $c > 0$ such that for any nontrivial multiplicative character $\chi$ modulo $p$ one has

$$\left| \sum_{a \in A, b \in B} \chi(a + b) \right| \ll \exp(-c(\delta^4 \log p/((\log K)^2)^{1/3})|A||B|),$$

provided that $(\log K)^5 \ll \delta^4 \log p$.

In the previous works [6], [22], [25] the doubling $K$ can tend to infinity very slowly as the function $C(K)$ has an exponential nature. However, our result is applicable for a much wider range of $K \ll \exp((\delta^4 \log p)^{1/5})$, where $\delta > 0$ satisfies the assumptions of Theorem 3. A new structural result given in section 4, is what makes our approach much more effective and it does not require us to use Freiman’s theorem. Using similar argument one can also avoid any constraints for doubling and size of $B$.

Theorem 4 Let $A, B \subset \mathbb{F}_p$ and $K, \delta > 0$ be such that $|A| > p^\delta$,

$$|A^2|B|^3 > p^{2 + \delta}, \quad \text{and} \quad |A + A| < K|A|.$$  

Then for any nontrivial multiplicative character $\chi$ modulo $p$ one has

$$\left| \sum_{a \in A, b \in B} \chi(a + b) \right| \ll \delta \exp(-c(\delta^4 \log p/((\log K)^2)^{1/3})|A||B|),$$

provided that $(\log K)^5 \ll \delta^4 \log p$.

We apply Theorem 3 to prove a new sum-product type result. Let us recall a well-known Theorem of Balog [1, Theorem 1] (see also [15]).
Theorem 5 Let $A \subseteq \mathbb{F}_q$, $q = p^s$ with $|A| \geq q^{1/2+1/2^k}$ for some positive integer $k$. If $A$ is an additive subgroup of $\mathbb{F}_q$ assume additionally that $|A| \geq q^{1/2} + 1$. Then

$$(A - A)^{2k+1} = \mathbb{F}_q.$$ 

It is easy to see that Balog’s theorem does not hold for set of size smaller than $q^{1/2}$. Let $A$ to be a nontrivial subfield of $\mathbb{F}_p^2$ then $|A| = p = |\mathbb{F}_p^2|^{1/2}$ and any combinations of sums and products of elements from $A$ belong to $A$. However, one may hope for an improvement of the Balog’s result for fields $\mathbb{F}_p$, when $p$ is a prime number. We break the square–root barrier in Theorem 5 for subsets of $\mathbb{F}_p$ and we only need a few operations to generate the whole field.

Theorem 6 There is a positive constant $c$ such that for every $A \subseteq \mathbb{F}_p$ with

$$|A| \gg \exp(-c(\log p)^{1/5})p^{1/2}$$

we have

$$\frac{2A - 2A}{A - A} = \mathbb{F}_p \quad \text{or} \quad \left(\frac{A - A}{A - A}\right)^2 (A - A) = \mathbb{F}_p. \quad (7)$$

Since $A - A \subseteq 2A - 2A$ we obtain the following Balog-type result.

Corollary 7 There is a positive constant $c$ such that for every set $A \subseteq \mathbb{F}_p$ with

$$|A| \gg \exp(-c(\log p)^{1/5})p^{1/2}$$

we have

$$\frac{(2A - 2A)^3}{(2A - 2A)^2} = \mathbb{F}_p.$$ 

It was proven in [10] that any two sets $A, B$ with all sums belonging to the set of quadratic residues satisfy $|A||B| \leq \frac{p-1}{2} + |B \cap (-A)|$. It almost solves a well–known Sárközy’s conjecture [19] on additive decompositions of the quadratic residues except for the case when $A + B$ equals exactly the set of quadratic residues and when the sum is direct. It immediately follows from Theorem 3 (also see Theorem 4 below) that such sets $A$ and $B$ cannot have small doubling.

2. Notation

In this section we collect notation used in the paper. Throughout the paper by $p$ we always mean an odd prime number and we put $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$. We denote the Fourier transform of a function $f : \mathbb{F}_p \to \mathbb{C}$ by

$$\hat{f}(\xi) = \sum_{x \in \mathbb{F}_p} f(x)e(-\xi \cdot x), \quad (8)$$
where \( e(x) = e^{2\pi ix/p} \). The Plancherel formula states that

\[
\sum_{x \in \mathbb{F}_p} f(x)\overline{g(x)} = \frac{1}{p} \sum_{\xi \in \mathbb{F}_p} \hat{f}(\xi)\overline{\hat{g}(\xi)}. \tag{9}
\]

The convolution of functions \( f, g : \mathbb{F}_p \to \mathbb{C} \) is defined by

\[
(f * g)(x) := \sum_{y \in \mathbb{F}_p} f(y)g(x - y). \tag{10}
\]

Clearly, we have

\[
\hat{f} \hat{g} = \hat{f * g}. \tag{11}
\]

We use the same capital letter to denote set \( A \subseteq \mathbb{R}^\mathbb{F}_p \) and its characteristic function \( \chi_A : \mathbb{R}^\mathbb{F}_p \to \{0,1\} \). For any two sets \( A, B \subseteq \mathbb{F}_p \), the additive energy of \( A \) and \( B \) is defined by

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

If \( A = B \), then we simply write \( E^+(A) \) for \( E^+(A, A) \). Combining (9) and (11), we derive

\[
E^+(A, B) = \frac{1}{p} \sum_{\xi \in \mathbb{F}_p} |\hat{A}(\xi)|^2 |\hat{B}(\xi)|^2. \tag{12}
\]

The multiplicative energy \( E^\times(A, B) \) is defined in an analogous way and it can be expressed similarly by applying the Fourier transform on group \( \mathbb{R}^\mathbb{F}_p \) and the multiplicative convolution. Given any two sets \( A, B \subseteq \mathbb{F}_p \), define the sumset, the product set and the quotient set of \( A \) and \( B \) as

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

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

and

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

respectively. We define \( k \)-fold sumsets and product sets analogously, for example \( 2A - 2A = A + A - A - A \) and \( (A - A)^2 = (A - A)(A - A) \).

All logarithms are to base 2. The signs \( \ll \) and \( \gg \) are the usual Vinogradov symbols. For a positive integer \( n \), we put \( [n] = \{1, \ldots, n\} \).

### 4. Multiplicative structures in sumsets

This section is devoted to prove the heart of our argument Proposition 10. The next lemma directly follows from Proposition 4.1 in [18].

**Lemma 8** Suppose that \( G = (G, +) \) is a group and \( k \in \mathbb{N} \). Let \( A \subseteq G \) be a finite non-empty set such that \( |A + A| \leq K|A| \). Then there is a set \( X \subseteq A - A \) of size

\[
|X| \geq \exp\left(-O((k \log K)^2)\right) |A| \tag{13}
\]

such that \( kX \subseteq 2A - 2A \).
We also use a classical result of Bukh [3] that provides an upper bound for a sum of dilates of a set in terms of the additive doubling of that set. Bukh’s theorem was slightly refined in [4] and [5] but application of these results do not lead to significant improvement of our main theorems.

**Lemma 9** Let $A$ be a finite subset of an abelian group such that $|A + A| \leq K|A|$. Then for any $\lambda_i \in \mathbb{Z}\setminus\{0\}$ we have
\[
|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq K^O(\Sigma_i \log(1 + |\lambda_i|))|A|.
\]

The next result is an important ingredient of our approach, which shows that additively rich sets contain product of surprisingly large sets. Our argument is based on [7].

**Proposition 10** Let $A \subseteq \mathbb{F}_p$ be a set such that $|A + A| \leq K|A|$. There exists an absolute constant $C > 0$ such that for any positive integers $d \geq 2$ and $l$ there is a set $Z$ of size $|Z| \geq \exp(-C l^3 d^2 (\log K)^2) |A|$ with
\[
[d^l] \cdot Z \subseteq 2A - 2A.
\]

**Proof.** Let $l$ and $d \geq 2$ be positive integers and $X$ be a set retrieved by applying Lemma 8 to set $A$ and $k = 2(d(l - 1) + 1)$, so $|X| \geq \exp(-C(ld \log K)^2)|A|$. We define a map
\[
f : X^{l+1} \to (X + X) \times (X + d \cdot X) \times \cdots \times (X + d^{l-1} \cdot X)
\]
by
\[
f(\vec{x}) = (x_1 + x_0, x_2 + dx_0, \ldots, x_l + d^{l-1}x_0),
\]
where $\vec{x} = (x_0, x_1, \ldots, x_l)$. Let $\mathcal{X}$ be the image of $f$ then by Lemma 9 and the Plünnecke inequality [24] we have
\[
|\mathcal{X}| \leq |X + X||X + d \cdot X| \cdots |X + d^{l-1} \cdot X|
\]
\[
\leq |(A - A) + (A - A)||(A - A) + d \cdot (A - A)| \cdots |(A - A) + d^{l-1} \cdot (A - A)|
\]
\[
\leq \exp(O(l^2 \log d \log K))|A - A|^l
\]
\[
= \exp(O(l^2 \log d \log K))|A|^l.
\]
For a vector $\vec{z} \in \mathcal{X}$ put
\[
r(\vec{z}) = |\{\vec{x} \in X^{l+1} : f(\vec{x}) = \vec{z}\}|.
\]
Clearly,
\[
\sum_{\vec{z} \in \mathcal{X}} r(\vec{z}) = |X|^{l+1},
\]
so there is a $\vec{z}$ such that
\[
r(\vec{z}) \geq |X|^{l+1} / |\mathcal{X}| \geq \exp(-O(l^2 \log d \log K))|X|^{l+1} |A|^{-l}
\]
\[
\geq \exp(-O(l^3 (d \log K)^2))|A|.
\]
Put $Y = \{ \underline{y} \in X^{l+1} : f(\underline{y}) = \underline{v} \}$ and let $\underline{v} \in Y$ be a fixed element. Then for any $\underline{y} \in Y$ and any $j \in [0, l-1]$ we have
\[
d^j(x_0 - y_0) = x_j - y_j \in X - X.
\]
Observe that for distinct vectors $\underline{y}, \underline{y}' \in Y$ the corresponding coefficients $y_0$ and $y'_0$ must also be distinct and hence elements $x_0 - y_0$ with $\underline{y} \in Y$ form a set of size at least $\exp\left(-O\left(l^3 (d \log K)^2\right)\right)|A|$. Denote this set by $Z$, then $d \cdot Z \subseteq X - X$ for $j \in [0, l-1]$, so
\[
[d^l \cdot Z] \subseteq (l(d-1) + 1)(X - X) = 2(l(d-1) + 1)X \subseteq 2A - 2A,
\]
which concludes the proof. \hfill \Box

4. PROOF OF THE MAIN RESULTS

First let us list results that we will use over the course of Theorem 3 proof. The next lemma can be found in [11] and it is a corollary to Weil's bound.

**Lemma 11** Let $\chi$ be a nontrivial multiplicative character, $I$ be a discrete interval in $\mathbb{F}_p$, and $r$ be a positive integer. Then
\[
\sum_{u_1, u_2 \in \mathbb{F}_p} \left| \sum_{t \in I} \chi(u_1 + t) \overline{\chi}(u_2 + t) \right|^{2r} < p^2 |I|^r r^{2r} + 4r^2 p |I|^{2r}.
\]

We will also need a corollary to points/planes incidences theorem of Rudnev [17].

**Theorem 12** Let $p$ be an odd prime, $\mathcal{P} \subseteq \mathbb{F}_p^3$ be a set of points and $\Pi$ be a collection of planes in $\mathbb{F}_p^3$. Suppose that $|\mathcal{P}| \leq |\Pi|$ and that $k$ is the maximum number of collinear points in $\mathcal{P}$. Then the number of point–planes incidences satisfies
\[
|\{(q, \pi) \in \mathcal{P} \times \Pi : q \in \pi\}| - |\mathcal{P}| |\Pi| \leq |\mathcal{P}|^{1/2} |\Pi| + k |\Pi|.
\]

**Corollary 13** Let $A, B \subseteq \mathbb{F}_p$ be such that $|A|, |B| < \sqrt{p}$ and $|A + A| \leq K|A|$, $|B + B| \leq L|B|$. Then the system
\[
\begin{align*}
\frac{b_1}{a} &= \frac{b'_1}{a'} \\
\frac{b_2}{a} &= \frac{b'_2}{a'}
\end{align*}
\]
has
\[
O(K^{5/4} L^{5/2} |A||B|^2 \log p + |A|^2 |B|) \quad (17)
\]
solutions in $(a, a', b_1, b'_1, b_2, b'_2) \in A^2 \times B^4$. Furthermore, for an arbitrary set $B$ with $K \leq |B|$ there are at most
\[
O(K^{3/2} |A||B|^{5/2}) \quad (18)
\]
solutions.
Proof. The first part of the corollary is [25, Lemma 2], so it is enough to prove (18). Denote by σ the number of the solutions to (16). Clearly, we have σ ⩽ |B||E^x(A, B)| ⩽ |B|^2|A|^2. Thus, we can assume that |B| ⩽ |A|^2/K^3, as otherwise |B|^2|A|^2 ⩽ K^{3/2}|A||B|^{5/2} and the assertion follows. Since every x ∈ A can be written in |A| ways as x = s − a, s ∈ A + A and a ∈ A it follows that

\[ E^x(A, B) \leq |A|^{-2}|\{(s - a)b = (s' - a')b' : s, s' ∈ A + A, a, a' ∈ A, b, b' ∈ B}\|. \]

Next, we apply Theorem 12 with

\[ \mathcal{P} = \{(s, b', a'b') : a' ∈ A, b' ∈ B, s ∈ A + A\} \]

and

\[ \Pi = \{(x - a)b = s'y - z : a ∈ A, b ∈ B, s' ∈ A + A\}. \]

If all elements of A, B and A + A are nonzero then |Π| = |A||B||A + A|, otherwise one can remove zero from those sets. Observe that every incidence between a plane (x − a)b = s'y − z from Π and a point (s, b', a'b') from \( \mathcal{P} \) gives a solution to

\[ (s - a)b = (s' - a')b' \]

and each solution to (19) provides a point/plane incidence. One can easily check that the maximal number of collinear points (points belonging a line) in \( \mathcal{P} \) is just the maximal size of "skew Cartesian product" (s, b', a'b'), so k = max{∥A∥, ∥B∥, ∥A + A∥} = max{∥B∥, ∥A + A∥}. By Theorem 12, in view of \( K \leq |B| \leq |A|^2/K^3 \) and \( |A| < \sqrt{p} \), we have

\[
\sigma \ll \frac{|A + A|^2|A|^2|B|^2}{p} + (|A||A + A||B|)^{3/2} + |A||B||A + A||B| + |A + A| \]

\[
\ll \frac{|A + A|^2|B|^3}{p} + K^{3/2}|A||B|^{5/2} \ll K^{3/2}|A||B|^{5/2}.
\]

This completes the proof. \( \square \)

Now we are ready to prove Theorem 3 and Theorem 4.

Proof of Theorem 3. Let \( l \) and \( r \geq 2 \) be parameters that will be specified later. By applying Proposition 10 to the set \( A, l \) and \( d = 2 \) there is a set \( Y \) with \( |A| \geq |Y| \geq \exp (-Cl^3 (\log K)^2) |A| \) such that \( I \cdot Y \subseteq 2A - 2A \), where \( I := [2^l] \). For fixed \( x ∈ I, y ∈ Y \) we have

\[
\left| \sum_{a ∈ A, b ∈ B} χ(a + b) \right| \leq \sum_{a ∈ A} \left| \sum_{b ∈ B} χ(a + b) \right| = \sum_{a ∈ A} \left| \sum_{b ∈ B} χ(a + b + xy) \right|,
\]

so

\[
\left| \sum_{a ∈ A, b ∈ B} χ(a + b) \right|^{4r} \leq (|I||Y|)^{-4r} \left( \sum_{a ∈ 3A - 2A} \left| \sum_{x ∈ I, y ∈ Y} \sum_{b ∈ B} χ(a + b + xy) \right| \right)^{4r}.
\]

For \( a ∈ 3A - 2A \) we put \( B_a := B + a \) and

\[
\sigma := \sigma_a = \sum_{x ∈ I, y ∈ Y} \left| \sum_{b ∈ B} χ(a + b + xy) \right| = \sum_{x ∈ I, y ∈ Y} \left| \sum_{b ∈ B_a} χ(b + xy) \right|.
\]
After applying the Cauchy–Schwarz inequality we obtain
\[
\sigma^2 = \left( \sum_{x \in I, y \in Y} \left| \sum_{b \in B_a} \chi(b + xy) \right| \right)^2 \\
\leq |I||Y| \left( \sum_{b,b' \in B_a} \sum_{x \in I, y \in Y} \chi(b + xy)\chi(b' + xy) \right) \\
= |I||Y| \sum_{u_1,u_2} \nu(u_1,u_2) \sum_{x \in I} \chi(u_1 + x)\chi(u_2 + x),
\]
where
\[
\nu(u_1,u_2) = \left| \{(b,b',z) \in B_a^2 \times Y : b/y = u_1, b'/y = u_2 \} \right|.
\]
From the Hölder inequality we have
\[
\sigma^{4r} \leq (|I||Y|)^{2r} \left( \sum_{u_1,u_2} \nu(u_1,u_2) \right)^{2r-2} \left( \sum_{u_1,u_2} \nu^2(u_1,u_2) \left( \sum_{x \in I} \chi(u_1 + x)\chi(u_2 + x) \right)^{2r} \right).
\]
Since \( \sum_{u_1,u_2} \nu(u_1,u_2) = |B|^2|Y| \) and \( \sum_{u_1,u_2} \nu^2(u_1,u_2) \) is the number of solutions to (16) it follows from Lemma 11 and Lemma 13 that
\[
\sigma^{4r} \ll (|I||Y|)^{2r}(|B|^2|Y|)^{2r-2}(K_y^{5/4}L^{5/2}|Y|^2|B|^2 \log p + |Y|^2|B|)(p^2|I|^r r^{2r} + 4r^2 p|I|^{2r}), \tag{22}
\]
where \( K_Y = |Y + Y|/|Y| \leq K|A|/|Y| \). We assume that
\[
K_y^{5/4}L^{5/2}|Y|^2 \log p \geq |Y|^2|B|.
\]
Furthermore, suppose that \( l \) satisfies the inequality \( |l|^r = 2^{l^r} r^{2r} p \), then
\[
\sigma^{4r} \ll r^2 p|I|^r (|I||Y|)^{2r}(|B|^2|Y|)^{2r-2} L^{5/2} K^{5/4} A^{5/4}|B|^2 Y^{-1/4} \log p.
\]
Now we go back to bound (21). By the Plünnecke inequality [24] we have \( |3A - 2A| \leq K^5|A| \), hence
\[
\left| \sum_{a \in A, b \in B} \chi(a + b) \right|^{4r} \ll K^5 r^2 p|I|^r (|I||Y|)^{-2r}(|B|^2|Y|)^{2r-2} L^{5/2} K^{5/4} A^{5/4}|B|^2 Y^{-1/4} \log p
\]
\[
= r^2 (|A||B|)^{4r} \cdot \left( \frac{K^{5r+5/4}L^{5/4} A^{5/4} p \log p}{|Y|^{9/4}|B|^2} \right).
\]
Recall that \( |Y| \geq \exp(-Ct^3(d \log K)^2) |A| \), so
\[
\left| \sum_{a \in A, b \in B} \chi(a + b) \right|^{4r} \ll r^2 (|A||B|)^{4r} \cdot \left( \frac{K^{C_1 t^3 \log K + r} L^{5/4} p \log p}{|A||B|^2} \right)
\]
for an absolute constant \( C_1 > 0 \). Now we choose parameters for the above inequality. By the assumption \( L < p^{\delta/2} \) and \( |A||B|^2 \geq p^{1+\delta} \) hence \( L^{5/4} p \log p (|A||B|^2)^{-1} < p^{-\delta/4} \). We put
\[
l = \Theta((d \log p / (\log K)^2)^{1/3})
\]
and
\[ r = \Theta((\log p)/l) = \Theta(\delta^{-1/3}(\log K)^{2/3} \cdot (\log p)^{2/3}) \]
such that the inequalities \( K^{C_1 3^3 \log K} < p^{\delta/16} \) and \( 2^r \geq r^2 p \) are satisfied. Furthermore, by the assumption it follows that \( K^{5r} < p^{\delta/16} \). Thus, we have
\[ \left| \sum_{a \in A, b \in B} \chi(a + b) \right| \ll 2^{-c_3/64} |A||B| \ll \exp(-c_4'(\delta \log p/(\log K)^{1/3})|A||B|) \]  
for some absolute constants \( c, c' > 0 \).

To complete the proof assume now that \( |Y|^2|B| > K^{5/4} L^{5/2} |Y||B|^2 \log p \). Then the same argument leads to the estimate
\[ \left| \sum_{a \in A, b \in B} \chi(a + b) \right|^{4r} \ll r^2(|A||B|)^{4r} \cdot \left( \frac{K^{5r} p}{|B|^3} \right) , \]
hence the required inequality holds provided that \( |B| > p^{1/3+\delta} \), which completes the proof. \( \square \)

**Proof of Theorem 4.** If \( |B| > p^{1/2+\delta/5} \) then we use Karacuba’s result (3) hence we may assume that \( |B| \leq p^{1/2+\delta/5} \). Then \( |A| > p^{1/4+\delta/5} \) so \( K \leq |B| \) and we can apply (4). Closely following the proof of Theorem 3 and using (4) we obtain the estimate
\[ \left| \sum_{a \in A, b \in B} \chi(a + b) \right|^{4r} \ll K^{5r}|A|^{4r} p^2 I^{2r} (|I||Y|)^{-2r} (|B^2||Y|)^{2r-2} K^{3/2} |A|^{3/2} |B|^{5/2} |Y|^{-1/2} \log p \]
\[ = 5r^2(|A||B|)^{4r} \cdot \left( \frac{KC(r^3 \log K + r) p \log p}{|A||B|^{3/2}} \right) . \]
The choice of parameters \( l, r \) from Theorem 3 provides the required upper bound. \( \square \)

**Proof of Theorem 6**

The next two lemmas from [16] (see also [23]) and [20] will be used in the proof of Theorem 6. A modern form of Lemma 14 can be found in [2].

**Lemma 14** Let \( A \subseteq \mathbb{F}_p \) be a set with \( |A| > 1 \). Then
\[ \left| \frac{A - A}{A} \right| \geq \min \left\{ p, \frac{|A|^2 + 3}{2} \right\} . \]

**Lemma 15** Let \( A \) be a subset of an abelian group such that \( E^+(A) = |A|^3/K \). Then there exists \( A' \subseteq A \) such that \( |A'| \gg |A|/K \) and
\[ |A' - A'| \ll K^4 |A'| . \]
Proof of Theorem 6. Put $|A| = \sqrt{p}M$, where $1 \leq M \leq \exp(c \log p)^{1/5})$, and let $Q = \frac{A - A}{M}$. By Lemma 14 we have $|Q| \geq p/(2M^2)$. Suppose that $\frac{A - A}{M} \not\equiv \mathbb{F}_p$, and let $\xi \not\equiv \frac{A - A}{M}$. Equivalently, if $a_i \in A$ then $a_1 = a_2$ and $a_3 + a_4 - a_5 - a_6 = 0$, so there are $|A|E^+(A)$ solutions to this equation. In terms of Fourier transform the number of solutions to (24) can be written as

$$|A|E^+(A) = p^{-1} \sum_x |\hat{A}(\xi x)|^2 |\hat{A}(x)|^4 \geq \frac{|A|^6}{p} = \frac{|A|^4}{M^2}.$$ 

Hence

$$E^+(A) \geq |A|^3/M^2$$

and by Lemma 15 there is $A' \subseteq A$ such that $|A'| \gg |A|M$ and $|A' + A'| \ll M^4|A'|$. Using multiplicative Fourier coefficients, the number of representations of any $z \in \mathbb{F}_p^*$ in the form $q/q'(a - b)$ with $q, q' \in Q$ and $a, b \in A$ equals

$$\frac{1}{p - 1} \sum_{\chi} |\sum_{x \in Q} \chi(x)|^2 \left( \sum_{a,b \in A'} \chi(z(a - b)) \right).$$

By Theorem 3 there are positive constants $c, C$ such that the above quantity can be bounded from below by

$$(2p)^{-1}|Q|^2 |A'|^2 - C \exp(-c(\log p/(\log M)^2)_{1/3})|Q||A'|^2,$$

which is greater than

$$(4M^2)^{-1}|Q||A'|^2 - C \exp(-c(\log p/(\log M)^2)_{1/3})|Q||A'|^2,$$

for a positive constant $c$. If (25) is positive for every $z$, then $QQ(A - A) = \mathbb{F}_p$. However, our assumption on the size of $A$ implies that

$$C \exp(c(\log p/(\log M)^2)_{1/3}) > 4M^2,$$

which concludes the proof.

References


Faculty of Mathematics and Computer Science,
Adam Mickiewicz University,
Umultowska 87, 61-614 Poznań, Poland
schoen@amu.edu.pl

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