ESTIMATES FOR CHARACTER SUMS
IN FINITE FIELDS OF ORDER $p^2$ and $p^3$

Mikhail Gabdullin $^{1,2}$
Lomonosov Moscow State University
Krasovskii Institute of Mathematics and Mechanics, Yekaterinburg

Abstract
We obtain nontrivial bounds on character sums over “boxes” of volume $p^{n(1/4+\varepsilon)}$ in finite fields of order $p^n$ for the cases $n = 2$ and $n = 3$.

1 Introduction

Let $p$ be a prime number, $\mathbb{F}_{p^n}$ be the finite field of order $p^n$, and $\{\omega_1, \ldots, \omega_n\}$ be a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Let, further, $N_i, H_i$ be integers such that $1 \leq H_i \leq p$, $i = 1, \ldots, n$. Define $n$-dimensional parallelepiped $B \subseteq \mathbb{F}_{p^n}$ as follows:

$$B = \left\{ \sum_{i=1}^{n} x_i \omega_i : N_i + 1 \leq x_i \leq N_i + H_i, \; 1 \leq i \leq n \right\}.$$ 

We are interested in estimates for sums $\sum_{x \in B} \chi(x)$, where $\chi$ is a nontrivial multiplicative character of $\mathbb{F}_{p^n}$, with the possible weakest restrictions on $B$. First we give a survey of known results in this direction. In the case $n = 1$, more than half a century Burgess’s estimate [Burg1] remains to be the strongest one: for every $\varepsilon > 0$ there exists a $\delta > 0$ such that for all $H \geq p^{1/4+\varepsilon}$ the following inequality holds:

$$\left| \sum_{x=N+1}^{N+H} \chi(x) \right| \ll \varepsilon p^{-\delta} H.$$ 

Also Burgess [Burg2] proved an analog of this inequality for $n = 2$ and special bases and Karatsuba [Kar1], [Kar2] generalized it for arbitrary finite fields; so, for instance, in [Kar2] the case of basis $\omega_i = g^i$ is considered, where $g$ is a root of an irreducible polynom of degree $n$ over $\mathbb{F}_p$. With this connection it looks natural to find estimates which hold uniformly over all bases of $\mathbb{F}_{p^n}$. Davenport and Lewis were the first to obtain such a result [DL].

---

$^1$ The work is supported by the grant from Russian Science Foundation (Project 14-11-00702).

$^2$ E-mail: gabdullin.mikhail@yandex.ru
**Theorem A** ([DL]). For every $\varepsilon > 0$ there exists a $\delta > 0$ such that if

$$H_1 = \ldots = H_n = H > p^{\frac{n}{2n+2}+\varepsilon},$$

then

$$\left| \sum_{x \in B} \chi(x) \right| \leq (p^{-\delta}H)^n.$$

Let us note that in Theorem A the exponent $\frac{n}{2n+2}$ tend to $1/2$ as $n \to \infty$. Theorem A was strengthened by Chang [Ch].

**Theorem B** ([Ch]). Let $\varepsilon > 0$ and a parallelepiped $B$ obeys the condition $\prod_{i=1}^n H_i > p^{(\frac{2}{5}+\varepsilon)n}$. Then

$$\left| \sum_{x \in B} \chi(x) \right| \ll_{n,\varepsilon} p^{-\varepsilon^2/4}|B|$$

in the case where $n$ is odd and in the case where $n$ is even and $\chi|_{\mathbb{F}_{p^n/2}}$ is nontrivial character, and

$$\left| \sum_{x \in B} \chi(x) \right| \leq \max_{\xi} |B \cap \xi \mathbb{F}_{p^n/2}| + O_{n,\varepsilon}(p^{-\varepsilon^2/4}|B|)$$

otherwise.

Let us note that on the condition $|B| = \prod_{i=1}^n H_i > p^{(2/5+\varepsilon)n}$ it is generally impossible to obtain nontrivial estimates for sums $\sum_{x \in B} \chi(x)$ even if $\chi$ is nontrivial; indeed, one has to take into account the situation where $B$ is the subfield $\mathbb{F}_{p^n/2}$ and $\chi$ is the nontrivial character of $\mathbb{F}_{p^n}$ which is identical on $\mathbb{F}_{p^n/2}$. That is why one has to consider different cases which are described in Theorem B.

Further, Chang [Ch2] obtained nontrivial estimates for character sums for the case $n = 2$, $H_1, H_2 > p^{1/4+\varepsilon}$. Konyagin [Kon] generalised this result for arbitrary finite fields.

**Theorem C** ([Kon]). Let $\varepsilon > 0$ and $H_i > p^{1/4+\varepsilon}$ for all $1 \leq i \leq n$. Then

$$\left| \sum_{x \in B} \chi(x) \right| \ll_{n,\varepsilon} p^{-\varepsilon^2/2}|B|.$$

The aim of the present paper is to prove the following result for the cases $n = 2$ and $n = 3$. 
**Theorem.** Let $n \in \{2, 3\}$, $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_{p^n}$ and $|B| \geq p^{n(1/4+\varepsilon)}$, and let us assume that $H_1 \leq \ldots \leq H_n$. Then

$$\left| \sum_{x \in B} \chi(x) \right| \ll_{\varepsilon} |B| p^{-\varepsilon^2/12},$$

if $\chi|_{\mathbb{F}_p}$ is not identical, and

$$\left| \sum_{x \in B} \chi(x) \right| \ll_{\varepsilon} |B| p^{-\varepsilon^2/12} + |B \cap \omega_n \mathbb{F}_p|$$

otherwise.

Since $\{\omega_1, \ldots, \omega_n\}$ is a basis, we thus have

$$|B \cap \omega_n \mathbb{F}_p| = \begin{cases} H_n, & \text{if } 0 \in \cap_{i=1}^{n-1} [N_i + 1, N_i + H_i], \\ 0, & \text{otherwise}, \end{cases}$$

and in the second case of the Theorem in fact the estimate $\sum_{x \in B} \chi(x) \ll_{\varepsilon} |B| p^{-\varepsilon^2/12} + H_n$ holds. Besides, similarly to the remark for Theorem B, on the condition ($|B| \geq p^{n(1/4+\varepsilon)}$) it is generally impossible to obtain nontrivial results, since one has to keep in mind the case where $B = \mathbb{F}_p$ and $\chi$ is the nontrivial character which is identical on $\mathbb{F}_p$. Let us stress that on the condition of theorem C such a situation is impossible because of the restriction $H_i > p^{1/4+\varepsilon}$, $1 \leq i \leq n$.

The key ingredient in the proofs of Theorems B and C and the Theorem of the present paper is a bound for the quantity

$$E(B) = \# \{(x, y, w, t) \in B^4 : xy = wt\},$$

which is called the multiplicative energy of the set $B$. Using tools from additive combinatorics, Chang proved that $E(B) \ll_{n} |B|^{11/4} \log p$ for parallelepipeds such that $H_i < \frac{1}{2}(\sqrt{p} - 1)$ (see [Ch], Proposition 1 ), whereas Konyagin, using geometric number theory, established the bound $E(B) \ll_{n} |B|^2 \log p$ for parallelepipeds with $H_1 = \ldots = H_n \leq \sqrt{p}$ (see [Kon], Lemma 1). We generalize Lemma 1 from [Kon] for the cases $n = 2$, $n = 3$ and distinct edges and prove the following.

**The Key Lemma.** Let $n \in \{2, 3\}$ and suppose that $H_1 \leq \ldots \leq H_n < \sqrt{p}/2$. Then we have

$$E(B) \ll |B|^2 \log^3 p.$$
In the proof of the Theorem we closely follow [Ch]: firstly, we prove
the desired bound in the case where all the edges are less than \(\sqrt{p/2}\) (this
argument is now standard and was used in [Ch], [Kon], and had been
elaborated by Karatsuba in his work [Kar1]); it also immediately implies
the statement for the case where all edges are less than \(p^{1/2+\varepsilon/2}\). After that
we prove the Theorem in the case \(H_3 > p^{1/2+\varepsilon/2}\). In fact, one can see from
the proof that in the last case one can write a slightly better bound for the
character sum, namely, \(\sum_{x \in B} \chi(x) \ll \varepsilon |B| p^{-\varepsilon/3} + |B \cap \omega_3 \mathbb{F}_p|\).

We prove the Key Lemma and the Theorem in the technically more
difficult case \(n = 3\) (the case \(n = 2\) is absolutely similar). We prove the
Key Lemma in Section 2 and the Theorem in Section 3.

The author would like to thank Nicholas Katz for providing an exten-
sion of his result (see Theorem E below), which is crucial for the proof of
the Theorem in the case \(H_3 > p^{1/2+\varepsilon/2}\).

## 2 Proof of the Key Lemma

Set

\[ Z' = \frac{B \setminus \{0\}}{B \setminus \{0\}} = \{ z \in \mathbb{F}_p^3 : \exists x, y \in B \setminus \{0\}, \; xz = y \}. \]

If \(x^1, x^2, x^3, x^4 \in B\), \(x^1 x^2 = x^3 x^4\) and \((x^1, x^4) \neq (0, 0), (x^2, x^3) \neq (0, 0)\),
then for some \(z \in Z'\) we have \(x^1 z = x^3, x^4 z = x^2\). Thus

\[ E(B) \leq 2|B|^2 + \sum_{z \in Z'} f_2(z), \tag{2.1} \]

where \(f(z)\) is the number of solutions to the equation \(xz = y\) where \(x, y \in B\). Define

\[ B_0 = \left\{ \sum_{i=1}^3 x_i \omega_i : -H_i \leq x_i \leq H_i, \; 1 \leq i \leq 3 \right\}, \]

\[ Z = \frac{B_0 \setminus \{0\}}{B_0 \setminus \{0\}}, \quad f_0(z) = \# \{(x, y) \in B_0^2 : xz = y\}. \]

Note that if \((x_1, y_1), \ldots, (x_k, y_k) \in B^2\) are distinct solutions to the equation
\(xz = y\), then \((0, 0), (x_2 - x_1, y_2 - y_1), \ldots, (x_k - x_1, y_k - y_1)\) are distinct
solutions to the same equation in \(B_0^2\). Thus \(f(z) \leq f_0(z)\); besides, \(f_0(z) = 1\)
for \(z \in \mathbb{F}_p^* \setminus Z\). Therefore,

\[ \sum_{z \in Z'} f^2(z) \leq \sum_{z \in Z} f_0^2(z) + |Z' \setminus Z|. \]
Further, $|Z'| \leq |B|^2$. Recalling (2.1), we see that

$$E \leq 3|B|^2 + \sum_{z \in Z} f_0^2(z),$$

and it suffices to estimate the sum

$$S = \sum_{z \in Z} f_0^2(z).$$

We can rewrite $S$ as

$$S = S_1 + S_2,$$

where

$$S_1 = \sum_{z \in Z \setminus F_p} f_0^2(z).$$ (2.2)

and

$$S_2 = \sum_{z \in F_p} f_0^2(z)$$ (2.3)

The claim now follows from the following two lemmas.

**Lemma 1** We have

$$S_1 \ll |B|^2 \log p.$$  

**Lemma 2** We have

$$S_2 \ll |B|^2 \log^3 p.$$  

2.1 Proof of Lemma 1

For a fixed $z \in Z$ define the lattice $\Gamma_z \subset \mathbb{Z}^6$:

$$\Gamma_z = \{(x_1, x_2, x_3, y_1, y_2, y_3) \in \mathbb{Z}^6 : z \sum_{i=1}^{3} x_i \omega_i = \sum_{i=1}^{3} y_i \omega_i \}.$$  

For fixed $x_1, x_2, x_3 \in \mathbb{Z}$ the condition $(x_1, x_2, x_3, y_1, y_2, y_3) \in \Gamma_z$ defines each of numbers $y_1, y_2, y_3$ modulo $p$. Thus,

$$\{|(x_1, x_2, x_3, y_1, y_2, y_3) \in \Gamma_z : |x_i|, |y_i| \leq M, 1 \leq i \leq 3| = \frac{(2M)^6}{p^3} (1 + o(1)), \quad M \to \infty.$$
Hence
\[ \operatorname{mes} \left( \mathbb{R}^6 / \Gamma_z \right) = p^3. \]

Define the set
\[ D = \{(x_1, x_2, x_3, y_1, y_2, y_3) \in \mathbb{R}^6 : |x_i|, |y_i| \leq H_i, \ 1 \leq i \leq 3\}; \]
then we have \( f_0(z) = |\Gamma_z \cap D| \). Let us recall that \( i \)-th successive minima
\[ \lambda_i = \lambda_i(z) = \lambda_i(D, \Gamma_z) \]
of the set \( D \) with respect to \( \Gamma_z \) is defined as the least \( \lambda > 0 \) such that the
set \( \lambda D \) contains \( i \) linearly independent vectors of \( \Gamma_z \). Obviously, \( \lambda_1(z) \leq \ldots \leq \lambda_6(z) \) and \( \lambda_1(z) \leq 1 \) of and only if \( z \in Z \). Further, from Minkowski’s
second theorem (see, for instance, [TV], Theorem 3.30) we have
\[ \prod_{i=1}^{6} \lambda_i \gg \frac{\operatorname{mes}(\mathbb{R}^6 / \Gamma_z)}{\operatorname{mes}D} \gg p^3 |B|^{-2}. \quad (2.4) \]

It is well-known (see [BHW], Proposition 2.1, or Exercise 3.5.6, [TV]), that
the number \( f_0(z) \) of points of \( \Gamma_z \) in the set \( D \) obeys the inequality
\[ f_0(z) \ll \prod_{i=1}^{6} \max\{1, \lambda_i^{-1}\}. \quad (2.5) \]

Now we are going to obtain lower bounds for \( \lambda_1(z), \lambda_2(z), \lambda_3(z) \), where
\( z \in Z \setminus \mathbb{F}_p \).

Firstly, since \( z \in Z \), then \( \lambda_1(z) \leq 1 \). Besides, \( H_2^{-1} \leq \lambda_1(z) \) (otherwise
there exists a non-zero vector \((0, 0, u_3, 0, 0, u_6) \in \Gamma_z\) such that \(|u_3|, |u_6| < H_3 H_2^{-1} \) and \( zu_3 \omega_3 = u_6 \omega_3 \), which contradicts our assumption that \( z \notin \mathbb{F}_p \).

Further, we prove that \( \lambda_2(z) \geq H_1^{-1} \). To show this, assume for contradiction that \( \lambda_2(z) < H_1^{-1} \). Then we can find two linearly independent over \( \mathbb{Z} \) vectors \( \mathbf{u} = (0, u_2, u_3, 0, u_5, u_6), \mathbf{v} = (0, v_2, v_3, 0, v_5, v_6) \in \Gamma_z \) such that
\(|u_2|, |u_3|, |v_2|, |v_3| < H_2 H_1^{-1} < \sqrt{p/2}, |u_5|, |u_6|, |v_5|, |v_6| < H_3 H_1^{-1} < \sqrt{p/2} \), and
\[ \begin{cases} (u_2 \omega_2 + u_3 \omega_3) z = u_5 \omega_2 + u_6 \omega_3, \\ (v_2 \omega_2 + v_3 \omega_3) z = v_5 \omega_2 + v_6 \omega_3. \end{cases} \quad (2.6) \]

Suppose that the vectors \((u_2, u_3)\) and \((v_2, v_3)\) are linearly independent
over \( \mathbb{F}_p \). It means that the map \( x \mapsto xz \) is a bijection from the subspace
\( \operatorname{Lin}\{\omega_2, \omega_3\} \) to itself. Let
\[ z \omega_1 = a_1 \omega_1 + a_2 \omega_2 + a_3 \omega_3; \]
we claim that \( z = a_1 \). Indeed, otherwise the map \( x \mapsto x(z - a_1) \) is also a bijection from Lin\{\( \omega_2, \omega_3 \)\} to itself, and we have \( \omega_1 \in \text{Lin}\{\omega_2, \omega_3\} \), which is false. Thus \( z = a_1 \); but that contradicts to the assumption that \( z \notin \mathbb{F}_p \).

Therefore the vectors \((u_2, u_3)\) and \((v_2, v_3)\) have to be linearly dependent over \( \mathbb{F}_p \). Then the determinant of the matrix \( \begin{pmatrix} u_2 & u_3 \\ v_2 & v_3 \end{pmatrix} \) equals to zero modulo \( p \). But all its elements are integers bounded in magnitude by \( \sqrt{p}/2 \); thus the absolute value of this determinant is less than \( p \), and it has to be equal to zero in \( \mathbb{Z} \). Therefore the vectors \((u_2, u_3)\) and \((v_2, v_3)\) are linearly dependent over \( \mathbb{Z} \).

The vector \( v = (0, v_2, v_3, 0, v_4, v_5, 0) \) is non-zero; suppose that \((v_2, v_3) \neq (0, 0)\) and let \( v_2 \neq 0 \) (the case \( v_3 \neq 0\) can be easily treated in a similar way). Multiplying the second equation of (2.6) by \( u_2/v_2 \) and subtracting it from the first one, we get

\[
(u_5u_2/v_2 - v_5)\omega_2 + (u_6u_2/v_2 - v_6)\omega_3 = 0.
\]

Since \( \{\omega_1, \omega_2, \omega_3\} \) is a basis and \( |u_5u_2 - v_5v_2| < p \), \( |u_6u_2 - v_6v_2| < p \), then \( u_5u_2 - v_5v_2 = u_6u_2 - v_6v_2 = 0 \), hence \( u = \frac{u_2}{v_2} v \). But this contradicts to the fact that the vectors \( u \) and \( v \) are linearly independent over \( \mathbb{R} \).

Finally, if \( v_2 = v_3 = 0 \), then \((v_5, v_6) \neq (0, 0)\) and the same arguments are valid with \( 1/z \) instead of \( z \); one can prove in a similar manner that the vectors \((v_5, v_6)\) and \((u_5, u_6)\) are linearly dependent and get the contradiction with the choice of \( u \) and \( v \).

Thus, for \( z \in \mathbb{Z}\setminus\mathbb{F}_p \) we have \( 1 \geq \lambda_1(z) \geq H_2^{-1} \) and \( \lambda_3(z) \geq \lambda_2(z) \geq H_1^{-1} \). Define

\[
Z_j = \{ z \in \mathbb{Z}\setminus\mathbb{F}_p : 2^{j-1} \leq H_2\lambda_1 < 2^j \}, \quad 1 \leq j \leq J := \log_2 H_2 + 1.
\]

Note that the vector \( u \in \lambda_1(z)D \cap \Gamma_z \) corresponding to an element \( z \in Z_j \) defines \( z \). Indeed, let \( u = (u_1, u_2, u_3, u_4, u_5, u_6) \) and define the elements \( x, y \in \mathbb{F}_p^3 \) as follows: \( x = u_1\omega_1 + u_2\omega_2 + u_3\omega_3 \), \( y = u_4\omega_1 + u_5\omega_2 + u_6\omega_3 \). Then we have \( z = xy^{-1} \). Therefore, \( |Z_j| \) is at most the number of integers points in the box \( 2^j H_2^{-1} D \). Setting \( j_1 = \log_2 (H_2/H_1) \), we see that

\[
|Z_j| \leq |2^j H_2^{-1} D \cap \mathbb{Z}^6| \ll \prod_{i=1}^{3} \max\{1, H_i 2^j H_2^{-1}\}^2 \leq \begin{cases} 2^{4j} H_3^2 H_2^{-2}, & \text{if } 1 \leq j < j_1; \\ 2^{6j} |B|^2 H_2^{-6}, & \text{if } j_1 \leq j \leq J. \end{cases} \quad (2.7)
\]
Further, set $s = s(z) = \max\{j : \lambda_j \leq 1\}$ and

$$Z^s = \{ z \in Z \setminus \mathbb{F}_p : s(z) = s \}.$$ 

Recalling the definition (2.2) of the sum $S_1$, we have

$$S_1 \leq \sum_{s=1}^{6} \sum_{z \in Z^s} f_0^2(z).$$

Further we treat the cases of different $s$ in a bit routine way.

For $s \leq 3$ we set $Z_j^s = Z^s \cap Z_j$. Then

$$\sum_{z \in Z^s} f_0^2(z) \leq \sum_{j} \sum_{z \in Z_j^s} f_0^2(z).$$

We will often use the trivial bound $|Z_j^s| \leq |Z_j|$.

Let $s = 1$. By (2.5) we have $f_0(z) \ll \lambda_1^{-1}$. Using (2.7) and the fact that for $z \in Z_j$ the bound $\lambda_1^{-1}(z) \ll 2^{-j}H_2$ holds, we obtain

$$\sum_{j} \sum_{z \in Z_j^1} f_0^2(z) \ll \sum_{j} \sum_{z \in Z_j^1} \lambda_1^{-2} \ll \sum_{j} |Z_j^1|2^{-2j}H_2^2 \ll$$

$$\sum_{1 \leq j < j_1} 2^{4j}H_3^2H_2^{-2}2^{-2j}H_2^2 + \sum_{j_1 \leq j \leq J} |B|^{26j}H_2^{-6}2^{-2j}H_2^2 \ll$$

$$H_3^2 \sum_{j_1 \leq j \leq J} 2^{2j} + |B|^{2}H_2^{-4} \sum_{j \leq J} 2^{4j} \ll |B|^2. \quad (2.8)$$

Let $s = 2$; by (2.5) we have $f_0(z) \ll \lambda_1^{-1}\lambda_2^{-1}$. Let $z \in Z_j$; in the case $j < j_1$ we use the bounds $\lambda_1^{-1} \ll 2^{-j}H_2$ and $\lambda_2^{-1} \ll H_1$, and in the case $j \geq j_1$ — the bound $\lambda_2^{-1} \ll \lambda_1^{-1} \ll 2^{-j}H_2$. Also recalling (2.7), we see that

$$\sum_{j} \sum_{z \in Z_j^2} f_0^2(z) \ll \sum_{j} \sum_{z \in Z_j^2} \lambda_1^{-2}\lambda_2^{-2} \ll$$

$$\sum_{1 \leq j < j_1} |Z_j^2|2^{-2j}H_2^{-2}H_1^2 + \sum_{j_1 \leq j \leq J} |Z_j^2|2^{-4j}H_2^4 \ll$$

$$\sum_{j \leq j_1} 2^{4j}H_3^2H_2^{-2}2^{-2j}H_2^2H_1^2 + \sum_{j \leq J} |B|^{26j}H_2^{-6}2^{-4j}H_2^4 \ll |B|^2. \quad (2.9)$$

Let $s = 3$; by (2.5) we get $f_0(z) \ll \lambda_1^{-1}\lambda_2^{-1}\lambda_3^{-1}$. Let $z \in Z_j$; in the case $j < j_1$ we use the bounds $\lambda_1^{-1} \ll 2^{-j}H_2$ and $\lambda_3^{-1} \ll \lambda_2^{-1} \ll H_1$, and in the
Among the cases $s > 3$ we first consider $s = 6$. Taking into account (2.4) and (2.5), we obtain

$$
\sum_{z \in \mathbb{Z}^6} f_0^2(z) \ll \sum_{z \in \mathbb{Z}} |B|^4 p^{-6} \leq |B|^4 |B|^{-2} p^{-6} \leq |B|^2 p^{4.5 - 6} = |B|^2
$$

(2.11)

(here we use the fact that $|B| \leq p^{1.5}$, which holds due to $H_1 \leq H_2 \leq H_3 \leq \sqrt{p/2}$).

Finally, we treat the cases $s = 4$ and $s = 5$. Define the polar lattice $\Gamma^*_z$ as follows:

$$
\Gamma^*_z = \left\{ (u_1, \ldots, u_6) \in \mathbb{R}^6 : \sum_{i=1}^3 u_i x_i + \sum_{i=1}^3 u_{i+3} y_i \in \mathbb{Z} \quad \forall (x_1, \ldots, y_3) \in \Gamma_z \right\}.
$$

Note that $\Gamma_z \supseteq p \mathbb{Z}^6$ implies $\Gamma^*_z \subseteq p^{-1} \mathbb{Z}^6$. Define the polar set

$$
D^* = \{(u_1, \ldots, v_3) \in \mathbb{R}^6 : \sum_{i=1}^3 |u_i x_i| + \sum_{i=1}^3 |v_i y_i| \leq 1 \text{ for all } (x_1, \ldots, y_3) \in D\}
$$

Clearly

$$
D^* = \{(u_1, \ldots, v_3) \in \mathbb{R}^6 : \sum_{i=1}^3 (|u_i| + |v_i|) H_i \leq 1\}.
$$

Let $\lambda^*_1 = \lambda^*_1(z)$ be the first successive minima of the set $D^*$ with respect to $\Gamma^*_z$. By [Ban], Proposition 3.6, we have

$$
\lambda^*_1 \lambda_6 \ll 1. \quad (2.12)
$$

Thus, taking into account (2.4) and (2.5), in the case $s = 5$ we have

$$
f_0(z) \ll \prod_{i=1}^5 \lambda_i^{-1}(z) = \lambda_6(z) \prod_{i=1}^6 \lambda_i^{-1}(z) \ll \lambda_6 |B|^2 p^{-3} \ll (\lambda^*_1)^{-1} |B|^{2} p^{-3},
$$

(2.13)
and in the case \( s = 4 \)

\[
f_0(z) \ll \prod_{i=1}^{4} \lambda_i^{-1}(z) \leq \lambda_6^{-1} \prod_{i=1}^{6} \lambda_i^{-1}(z) \ll \lambda_6^2 |B|^2 p^{-3} \ll (\lambda_1^*)^{-2} |B|^2 p^{-3}. \quad (2.14)
\]

The contribution to the sum \( \sum_{z \in \mathbb{Z}^6} f_0^2(z) \) (or \( \sum_{z \in \mathbb{Z}^4} f_0^2(z) \)) from those \( z \in \mathbb{Z}^5 \) (respectively \( z \in \mathbb{Z}^4 \)) for which \( \lambda_1^*(z) \geq 1 \) can be estimated similarly to the case \( s = 6 \) (see (2.11)). Thus we can assume \( \lambda_1^*(z) \leq 1 \). Then we have \( \lambda_1^* \geq H_1 p^{-1} \) (since if \( \lambda < H_1 p^{-1} \), then due to \( \Gamma_z^* \subseteq p^{-1} \mathbb{Z}^6 \) we see that \( \lambda \mathbb{D}^* \cap \Gamma_z^* = \{0\} \)). Set

\[ Z_j' = \{ z \in \mathbb{Z} : 2^{j-1} \leq \frac{p \lambda_1^*(z)}{H_1} < 2^j \}, \quad j = 1, ..., \log_2(p/H_1) + 1 \].

We claim that the vector \( u \in \lambda_1^*(z) \mathbb{D}^* \cap \Gamma_z^* \) corresponding to an element \( z \in Z_j' \) defines this element \( z \). Suppose for contradiction that there is a non-zero vector \( u = (u_1/p, ..., u_3/p) \in \Gamma_z^* \cap \Gamma_z^* \), where \( z' \neq z'' \) and \( u_1, v_i \in \mathbb{Z} \); we also have \( \sum_{i=1}^{3} |u_i| + \sum_{i=1}^{3} |v_i| < 2^j \). Take an arbitrary element \( x = \sum_{i=1}^{3} x_i \omega_i \in \mathbb{F}_p \) and set \( y' = xz' = \sum_{i=1}^{3} y'_i \omega_i, y'' = xz'' = \sum_{i=1}^{3} y''_i \omega_i \). Then

\[
(x_1, x_2, x_3, y'_1, y'_2, y'_3) \in \Gamma_{z'}, \quad (x_1, x_2, x_3, y''_1, y''_2, y''_3) \in \Gamma_{z''},
\]

and by the definition of the polar set

\[
\sum_{i=1}^{3} x_i u_i/p + \sum_{i=1}^{3} y'_i v_i/p \in \mathbb{Z}, \quad \sum_{i=1}^{3} x_i u_i/p + \sum_{i=1}^{3} y''_i v_i/p \in \mathbb{Z}.
\]

But then

\[
\sum_{i=1}^{3} (y'_i - y''_i) v_i \equiv 0 \pmod{p}.
\]

Note the numbers \( y'_i - y''_i \) can be arbitrary (they are the coefficients of the element \( y' - y'' \) which is equal to \( x(z' - z'') \) and, since \( z' - z'' \neq 0 \), can be equal to a given element provided we take the appropriate \( x \)). Thus \( v_i \equiv 0 \pmod{p} \), and since \( |v_i| < 2^j \leq p \), then \( v_i = 0 \). So we see that

\[
\sum_{i=1}^{3} x_i u_i = 0
\]

for all \( (x_1, x_2, x_3) \in \mathbb{Z}^3 \), and hence \( u_i = 0 \). But this contradicts to the fact that the vector \( (u_1, ..., v_3) \) is non-zero. Therefore, the vector \( u \in \lambda_1^*(z) \mathbb{D}^* \cap \Gamma_z^* \) corresponding to an element \( z \in Z_j' \) indeed defines \( z \).
The vector \((u_1, \ldots, u_3) \in \frac{2^j H}{p} D^* \cap \Gamma^*_z\) obeys the inequality \(\sum_{i=1}^{3} (|u_i| + |v_i|)H_i \leq 2^j H_1\); hence, \(|u_i|, |v_i| \leq 2^j H_1 H_i^{-1}\). Thus we see that \(|Z'_j| \leq \prod_{i=1}^{3} \max(1, 2^j H_1 H_i^{-1})^2\). Setting \(j_2 = \log_2(H_3/H_1)\) and \(j_3 = \log_2(p/H_1)+1\), we have

\[
|Z'_j| \leq \begin{cases} 2^{2j}, & \text{if } 1 \leq j < j_1; \\ 2^{4j} H_1^2 H_2^{-2}, & \text{if } j_1 \leq j < j_2; \\ 2^{6j} H_1^6 |B|^{-2}, & \text{if } j_2 \leq j \leq j_3. \end{cases} \tag{2.15} \]

For \(s = 4\) and \(s = 5\) define

\[Z^s_j = Z^s \cap Z'_j;\]

below we will use the trivial bound \(|Z^s_j| \leq |Z'_j|\) and apply (2.15). Recalling the bound (2.13) and taking into account that \(\lambda_1^*(z) \asymp 2^j H_1/p\) for \(z \in Z'_j\), we obtain

\[
\sum_{z \in Z^5} f_0^2(z) \leq |B|^{4} p^{-6} \sum_{j} \sum_{z \in Z^5_j} (\lambda_1^*(z))^{-2} \leq \\
|B|^{4} p^{-6} \sum_{1 \leq j < j_1} 2^{2j-2j} H_1^{-2} p^2 + |B|^{4} p^{-6} \sum_{j_1 \leq j < j_2} H_1^2 H_2^{-2} 2^{4j-2j} H_1^{-2} p^2 + \\
|B|^{4} p^{-6} \sum_{j_2 \leq j < j_3} H_1^6 |B|^{-2} 2^{6j-2j} H_1^{-2} p^2 \leq \\
|B|^{4} p^{-4} H_1^{-2} \log p + |B|^{4} p^{-4} H_2^{-2} \sum_{j \leq j_2} 2^{2j} + |B|^{2} p^{-4} H_1^4 \sum_{j \leq j_3} 2^{4j} \ll \\
|B|^2 (1 + |B|^2 p^{-4} H_3^2 |B|^{-2} + |B|^2 p^{-4} H_1^{-2} \log p) \ll |B|^2. \tag{2.16} \]

In the case \(s = 4\), using (2.14), in a similar way we get

\[
\sum_{z \in Z^5} f_0^2(z) \leq |B|^{4} p^{-6} \sum_{j} \sum_{z \in Z^5_j} (\lambda_1^*(z))^{-4} \leq \\
|B|^{4} p^{-6} \sum_{1 \leq j < j_1} 2^{2j-4j} H_1^{-4} p^4 + |B|^{4} p^{-6} \sum_{j_1 \leq j < j_2} H_1^2 H_2^{-2} 2^{4j-4j} H_1^{-4} p^4 + \\
|B|^{4} p^{-6} \sum_{j_2 \leq j < j_3} H_1^6 |B|^{-2} 2^{6j-4j} H_1^{-4} p^4 \leq \\
|B|^{4} p^{-2} H_1^{-4} + |B|^{4} p^{-2} H_1^{-2} H_2^{-2} \sum_{j \leq j_2} 1 + |B|^{2} p^{-2} H_1^2 \sum_{j \leq j_3} 2^{2j} \ll \\
|B|^2 (1 + |B|^2 p^{-2} H_3^2 (\log p) |B|^{-2} + |B|^2 p^{-2} H_1^{-4}) \ll |B|^2. \tag{2.17} \]

Putting the bounds (2.8)-(2.11) and (2.16)-(2.17) together, we see that
$S_1 \ll |B|^2 \log p,$
as desired.

### 2.2 Proof of Lemma 2

Fix $z \in \mathbb{F}_p$. Let $x = \sum_{i=1}^{3} x_i \omega_i$ and $y = \sum_{i=1}^{3} y_i \omega_i$; then the equality $xz = y$ is equivalent to the equalities $zx_i \equiv y_i \pmod{p}$, $1 \leq i \leq 3$. Hence

$$f_0(z) = f_1(z) f_2(z) f_3(z),$$

where

$$f_i(z) = \# \{(x_i, y_i) \in [-H_i, H_i]^2 : x_i z \equiv y_i \pmod{p} \}.$$

Recalling the definition (2.3) of the sum $S_2$, we see that

$$S_2 = \sum_{z \in \mathbb{F}_p^*} f_0^2(z) = \sum_{z \in \mathbb{F}_p} f_1^2(z) f_2^2(z) f_3^2(z) \leq \prod_{i=1}^{3} \left( \sum_{z \in \mathbb{F}_p} f_i^2(z) \right). \quad (2.18)$$

The sums $\sum_{z \in \mathbb{F}_p} f_i^2(z)$ can be estimated as the sum $S_1$ in the previous subsection. We go over the details quickly. Fix $i \in \{1, 2, 3\}$ and denote for the brevity $H = H_i$,

$$D = [-H, H]^2, \quad Z = \mathbb{Z}^2 \setminus [0, H][0] \setminus [H, 0],$$

$$\Gamma_z = \{(x, y) \in \mathbb{Z}^2 : x z \equiv y \pmod{p} \};$$

let $\lambda_l = \lambda_l(z)$ be the $l$-th successive minima of $D$ with respect to $\Gamma_z$, $l = 1, 2$. Then for all $z \in \mathbb{F}_p^*$ we have

$$\text{mes}(\mathbb{R}^2/\Gamma_z) = p,$$

and Minkowski’s second theorem gives us

$$\lambda_1 \lambda_2 \gg pH^{-2}. \quad (2.19)$$

In our notation we have $f_i(z) = |D \cap \Gamma_z|$. By Proposition 2.1 from [BHW] we see that

$$f_i(z) \ll \prod_{i=1}^{2} \max\{1, \lambda_i^{-1}(z)\}.$$
Clearly, $H^{-1} \leq \lambda_1 \leq 1$ for $z \in Z$. Define the set

$$Z_j = \{z \in Z : 2^{j-1} \leq H\lambda_1(z) < 2^j\}, \ j = 1, \ldots, \lfloor \log_2 H \rfloor + 1,$$

and let $s(z) = \max\{l : \lambda_l(z) \leq 1\}$ and $Z^s = \{z \in Z : s(z) = s\}$. The vector $(u_1, u_2) \in \lambda_1(z)D \cap \Gamma_z$ corresponding to an element $z \in Z_j$ defines $z$. Thus

$$|Z_j| \ll \left| \frac{2^j}{H} D \cap \mathbb{Z}^2 \right| \ll 2^{2j}$$

and

$$\sum_{z \in Z^1} f_i^2(z) \ll \sum_{j} \sum_{z \in Z^1 \cap Z_j} \lambda_1^{-2}(z) \ll \sum_{j=1}^{\lfloor \log_2 H \rfloor + 1} 2^{2j} H^2 2^{-2j} \ll H^2 \log p. \quad (2.20)$$

Finally, using (2.19) and the fact that $H \leq \sqrt{p}$, we find

$$\sum_{z \in Z^2} f_i^2(z) \ll |Z^2| p^{-2} H^4 \leq H^6 p^{-2} \leq H^2. \quad (2.21)$$

Putting (2.20) and (2.21) together, we obtain

$$\sum_{z \in \mathbb{F}_p^*} f_i^2(z) \ll H^2 \log p.$$

Recalling (2.18), we get

$$S_2 \ll \prod_{i=1}^{3} (H_i^2 \log p) = |B|^2 \log^3 p.$$

This completes the proof of Lemma 2 and the Key Lemma.

### 3 Proof of the Theorem.

In this section we closely follow to the paper [Ch]. We would like to stress, however, that the arguments in the case $H_3 < \sqrt{p}/2$ (additive shift $x \mapsto x + yz$ and double application of Hölder’s inequality) are now standard and were used in works [Ch], [Kon] and had been elaborated by Karatsuba in his work [Kar1]. Additive shift itself was used earlier in works of Vinogradov (see [Vin1], [Vin2], [Vin3]) and probably rises from ideas of van der Corput and H.Weil (see, for instance, [vdC], [W1], [W2]).
3.1 The case $H_3 < \sqrt{p/2}$.

Dividing $B$ to smaller parallelepipeds, we may assume that $|B| \asymp p^{3(1/4+\varepsilon)}$. Let $\delta = \delta(\varepsilon) > 0$ be chosen later. Set

$$I = [1, p^\delta] \cap \mathbb{Z}$$

and

$$B_0 = \left\{ \sum_{i=1}^3 x_i \omega_i : x_i \in [0, p^{-2\delta} H_i] \cap \mathbb{Z}, 1 \leq i \leq 3 \right\}.$$

Note that $\#([0, p^{-2\delta} H_i] \cap \mathbb{Z}) \asymp 1 + p^{-2\delta} H_i \gg p^{-2\delta} H_i$, and, hence, we have

$$|B_0| \gg p^{-6\delta}|B|. \quad (3.1)$$

Since $B_0 I \subseteq \left\{ \sum_{i=1}^3 x_i \omega_i : x_i \in [0, p^{-\delta} H_i] \cap \mathbb{Z}, 1 \leq i \leq 3 \right\}$, for all $y \in B_0$, $z \in I$ we have

$$\left| \sum_{x \in B} \chi(x) - \sum_{x \in B} \chi(x + yz) \right| \leq |B \setminus (B + yz)| + |(B + yz) \setminus B| \leq 6p^{-\delta}|B|.$$

Thus

$$\sum_{x \in B} \chi(x) = \frac{1}{|B_0||I|} \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) + O(p^{-\delta}|B|). \quad (3.2)$$

Further,

$$\left| \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) \right| \leq \sum_{x \in B, y \in B_0} \left| \sum_{z \in I} \chi(x + yz) \right| \leq$$

$$\sum_{x \in B, y \in B_0 \setminus \{0\}} \left| \sum_{z \in I} \chi(xy^{-1} + z) \right| + |B||I| =$$

$$\sum_{u \in \mathbb{F}_p^3} \tau(u) \left| \sum_{z \in I} \chi(u + z) \right| + |B||I|,$$

where

$$\tau(u) = \#\{(x, y) \in B \times (B_0 \setminus \{0\}) : xy^{-1} = u\}.$$
Let $r$ be a positive integer to be chosen later. Using Hölder’s inequality twice, we obtain

$$\left| \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) \right| \leq \left( \sum_{u \in \mathbb{F}_{p^3}} \tau(u)^{1-1/r} \right)^{1/r} \left( \sum_{u \in \mathbb{F}_{p^3}} \chi(u + z) \right)^r + |B||I| \leq \left( \sum_{u \in \mathbb{F}_{p^3}} \tau(u) \right)^{1-1/r} \left( \sum_{u \in \mathbb{F}_{p^3}} \chi(u + z) \right)^{2r} + |B||I|. \quad (3.3)$$

Now we have to estimate three sums which have appeared in the last line of (3.3). Firstly,

$$\sum_{u \in \mathbb{F}_{p^3}} \tau(u) = |B|(|B_0| - 1) \leq |B||B_0|. \quad (3.4)$$

Further, $\tau(0) \leq |B_0|$ and hence

$$\tau(0)^2 \leq |B_0|^2 \leq |B||B_0|. $$

Using the Cauchy-Schwarz inequality and the Key Lemma, we see that

$$\sum_{u \in \mathbb{F}_{p^3}} \tau^2(u) = \#\{(x_1, x_2, y_1, y_2) \in B \times B \times B_0 \times B_0 : x_1y_2 = x_2y_1 \neq 0\} = \sum_{\nu \in \mathbb{F}_{p^3}^*} \#\{(x_1, x_2) \in B^2 : \frac{x_1}{x_2} = \nu\} \#\{(y_1, y_2) \in B_0^2 : \frac{y_1}{y_2} = \nu\} \leq E(B)^{1/2} E(B_0)^{1/2} \ll |B||B_0| \log^3 p.$$

Putting together the last two inequalities, for the second sum we get the bound

$$\sum_{u \in \mathbb{F}_{p^3}} \tau^2(u) \ll |B||B_0| \log^3 p. \quad (3.5)$$

In order to estimate the third sum we will use the following theorem.
Theorem D ([Sch], Theorem 2C’, p.43). Let $\chi$ be a multiplicative character of $\mathbb{F}_{p^n}$ of order $d > 1$. Assume that a polynomial $f \in \mathbb{F}_{p^n}[x]$ has $m$ distinct roots and is not $d$-th power. Then

$$\left| \sum_{x \in \mathbb{F}_{p^n}} \chi(f(x)) \right| \leq (m - 1)p^{n/2}.$$

We have

$$\sum_{u \in \mathbb{F}_{p^3}} \left| \sum_{z \in I} \chi(u + z) \right|^{2r} \leq$$

$$\sum_{z_1, \ldots, z_{2r} \in I} \left| \sum_{u \in \mathbb{F}_{p^3}} \chi((u + z_1) \ldots (u + z_r)(u + z_{r+1})^{q-2} \ldots (u + z_{2r})^{q-2}) \right|.$$

We call a tuple $(z_1, \ldots, z_{2r})$ good if at least one of its elements occurs exactly once, and call it bad otherwise. By Theorem D we have the bound

$$\left| \sum_{u \in \mathbb{F}_{p^3}} \chi((u + z_1) \ldots (u + z_r)(u + z_{r+1})^{q-2} \ldots (u + z_{2r})^{q-2}) \right| < 2rp^{3/2}$$

for any good tuple $(z_1, \ldots, z_{2r})$. We can estimate the number of good tuples trivially by $|I|^{2r}$ and thus see that the contribution from them is at most $2rp^{3/2}|I|^{2r}$. Further, in any bad tuple every element occurs at least twice, and hence it contains at most $r$ distinct elements. They can be chosen in at most $|I|^r$ ways, and hence the number of bad tuples does not exceed $|I|^r r^{2r}$. We can estimate the contribution from each bad tuple trivially by $p^3$, and thus see that the contribution from bad tuples is at most $p^3|I|^r r^{2r}$. Therefore,

$$\sum_{u \in \mathbb{F}_{p^3}} \left| \sum_{z \in I} \chi(u + z) \right|^{2r} \leq 2rp^{3/2}|I|^{2r} + p^3|I|^r r^{2r},$$

and hence

$$\left( \sum_{u \in \mathbb{F}_{p^3}} \left| \sum_{z \in I} \chi(u + z) \right|^{2r} \right)^{1/(2r)} \ll p^{3/(4r)}|I| + p^{3/(2r)}|I|^{1/2}. \quad (3.6)$$
Putting the bounds (3.4)-(3.6) into (3.3), we get

\[
\frac{1}{|B_0||I|} \left| \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) \right| \ll \frac{1}{|B_0||I|} \left| (|B||B_0|)^{1-\frac{1}{r}} (|B||B_0| \log^3 p)^{\frac{1}{2r}} \left( p^{3/(4r)}|I| + rp^{3/(2r)}|I|^{1/2} \right) + |B||B_0|^{-1} \right.
\]

\[
= |B| \left( |B||B_0| \right)^{-1/2r} (\log p)^{3/(2r)} \left( p^{3/(4r)} + rp^{3/(2r)} |I|^{-1/2} \right) + |B||B_0|^{-1}.
\]

Recalling the bound (3.1) and the assumption on the quantity $|B|$ and taking into account the $|I| \gg \varepsilon p^\delta/2$ (recall that $\delta$ will be depending only on $\varepsilon$), we have

\[
\frac{1}{|B_0||I|} \left| \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) \right| \ll \varepsilon |B| p^{-3/(4r) - 3(\varepsilon - \delta)/r} (\log p)^{3/(2r)} \left( p^{3/(4r)} + rp^{3/(2r)} |I|^{-\delta/2} \right) + O(p^{6\delta}).
\]

Set $\delta = \frac{3}{2r}$. Then

\[
\frac{1}{|B_0||I|} \left| \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) \right| \ll |B| p^{-3(\varepsilon - \delta)/r} (\log p)^{3/(2r)} + O(p^{6\delta}).
\]

Recalling (3.2) and the fact that $3/r = 2\delta$, we get

\[
\left| \sum_{x \in B} \chi(x) \right| \ll |B| p^{-2\delta(\varepsilon - \delta)} (\log p)^{\delta} + p^{6\delta} + |B| p^{-\delta}. \tag{3.7}
\]

We choose $r$ so that $\delta = 3/(2r)$ is close to $\varepsilon/2$. To be more precise, let $r$ be the nearest integer to the number $3\varepsilon^{-1}$; then

\[
\left| r - \frac{3}{\varepsilon} \right| \leq 1/2
\]

and

\[
r = 3\varepsilon^{-1} + 0.5\theta,
\]

where $|\theta| \leq 1$. Thus

\[
\delta = \frac{3}{2r} = \frac{3}{2(3\varepsilon^{-1} + 0.5\theta)} = \frac{\varepsilon}{2 + \theta \varepsilon / 3}
\]
and hence $\frac{1}{3}\varepsilon < \frac{6}{13}\varepsilon \leq \delta \leq \frac{6}{11}\varepsilon$ (we may assume $\varepsilon < 1/2$). Since $|B| \gg p^{3/4+3\varepsilon}$, then $p^{6\delta} \ll |B|p^{-\varepsilon} \leq |B|p^{-\varepsilon/3}$, and we can rewrite (3.7) as

$$\left| \sum_{x \in B} \chi(x) \right| \ll \varepsilon |B|p^{-2\delta(\varepsilon-\delta)}(\log p)^{\delta} + |B|p^{-\varepsilon/3}.$$ 

Finally,

$$2\delta(\varepsilon - \delta) \geq 2(6\varepsilon/13)(5\varepsilon/11) = 60\varepsilon^2/143 > \varepsilon^2/3.$$ 

Hence

$$\left| \sum_{x \in B} \chi(x) \right| \ll \varepsilon |B|p^{-\varepsilon^2/3}.$$ 

This concludes the proof of the Theorem in the case $H_3 \leq \sqrt{p}/2$.

3.2 The case $H_3 \leq p^{1/2+\varepsilon/2}$.

In this case we can divide each edge which has length greater than $\sqrt{p}/2$ into $O(p^{\varepsilon/2})$ “almost equal” pieces of length less than $\sqrt{p}/2$ but greater than $\sqrt{p}/2$. So $B$ can be divided into $O((p^{\varepsilon/2})^3)$ parallelepipeds $B_\alpha$ of volume $\gg p^{-3\varepsilon^2/2}p^{3(1/4+\varepsilon)} = p^{3(1/4+\varepsilon)/2}$. According to the previous case

$$\left| \sum_{x \in B_\alpha} \chi(x) \right| \ll \varepsilon |B_\alpha|p^{-\varepsilon^2/12}$$

for all $\alpha$, and thus

$$\left| \sum_{x \in B} \chi(x) \right| \ll \varepsilon |B|p^{-\varepsilon^2/12}.$$ 

3.3 The case $H_3 > p^{1/2+\varepsilon/2}$.

We need the following extension of a result of Katz [K].

**Theorem E.** Let $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_{p^n}$ and $g \in \mathbb{F}_{p^n}$ be a generating element, i.e., $\mathbb{F}_{p^n} = \mathbb{F}_p(g)$. Then for any interval $I \subseteq [1, p] \cap \mathbb{Z}$ we have

$$\left| \sum_{t \in I} \chi(g + t) \right| \leq c(n)\sqrt{p \log p}.$$ 

18
We can rewrite the initial sum as

\[ \left| \sum_{x \in B} \chi(x) \right| = \left| \sum_{(x_1, x_2) \in I_1 \times I_2} \sum_{x_3 \in I_3} \chi(x_1 \frac{\omega_1}{\omega_3} + x_2 \frac{\omega_2}{\omega_3} + x_3) \right|, \quad (3.8) \]

where \( I_i = [N_i + 1, N_i + H_i] \cap \mathbb{Z} \). Define the set \( A \) as follows:

\[ A = \left\{ (x_1, x_2) \in I_1 \times I_2 : \mathbb{F}_p(x_1 \frac{\omega_1}{\omega_3} + x_2 \frac{\omega_2}{\omega_3}) \neq \mathbb{F}_{p^3} \right\}. \]

Since 3 is a prime number, \( \mathbb{F}_p \) is the only nontrivial subfield of \( \mathbb{F}_{p^3} \), and we have

\[ A = \left\{ (x_1, x_2) \in I_1 \times I_2 : x_1 \frac{\omega_1}{\omega_3} + x_2 \frac{\omega_2}{\omega_3} \in \mathbb{F}_p \right\}. \]

Further, the elements \( 1, \frac{\omega_1}{\omega_3}, \frac{\omega_2}{\omega_3} \) are linearly independent over \( \mathbb{F}_p \), and hence \( x_1 \frac{\omega_1}{\omega_3} + x_2 \frac{\omega_2}{\omega_3} \in \mathbb{F}_p \) if and only if \( x_1 = x_2 = 0 \). We thus see that

\[ A = \begin{cases} \{(0, 0)\}, & \text{if } 0 \in I_1 \cap I_2. \\ \emptyset, & \text{otherwise.} \end{cases} \]

Now let us turn to equality (3.8). If a pair \( (x_1, x_2) \) does not belong to \( A \), then by Theorem E and the assumption on \( H_3 \) we have

\[ \left| \sum_{x_3 \in I_3} \chi(x_1 \frac{\omega_1}{\omega_3} + x_2 \frac{\omega_2}{\omega_3} + x_3) \right| \ll \sqrt{p} \log p \leq H_3 p^{-\varepsilon/2} \log p. \]

Thus we can bound the number of pairs \( (x_1, x_2) \) which do not belong to \( A \) trivially by \( |I_1||I_2| \), we obtain

\[ \left| \sum_{(x_1, x_2) \in (I_1 \times I_2) \setminus D} \sum_{x_3 \in I_3} \chi(x_1 \omega_1 + x_2 \omega_2 + x_3 \omega_3) \right| \ll \varepsilon |B| p^{-\varepsilon/3}. \]

This concludes the proof of the Theorem in the case \( 0 \notin I_1 \cap I_2 \). Now suppose that \( 0 \in I_1 \cap I_2 \). By arguing as before we see that it suffices to estimate the sum

\[ S' = \sum_{x_3 \in I_3} \chi(x). \]

If \( \chi|_{\mathbb{F}_p} \) is not identical, then by the Polya-Vinogradov inequality and the assumption on \( H_3 \) we have

\[ |S'| \leq \sqrt{p} \log p \ll \varepsilon H_3 p^{-\varepsilon/3} \ll \varepsilon |B| p^{-\varepsilon/3}. \]
This completes the proof in the case where \(0 \in I_1 \cap I_2\) and \(\chi|_{\mathbb{F}_p}\) is not identical.

Finally we consider the case where \(\chi|_{\mathbb{F}_p}\) is the trivial character. Then

\[|S'| \leq H_3,\]

and thus we see that in the case \(H_3 \geq p^{1/2+\varepsilon/2}\) we always have the bound

\[\left| \sum_{x \in B} \chi(x) \right| \leq \varepsilon |B| p^{-\varepsilon/3} + H_3.\]

The claim follows.

References

[Ban] W. Banaszczyk, “Inequalities for convex bodies and polar reciprocal lattices in \(\mathbb{R}^n\)”, Discrete Comput. Geom. 13 (2), 217-231 (1995).

[BHW] U. Betke, M. Henk, J. M. Wills, “Successive-minima-types inequalities”, Discrete Comput. Geom., 9:2 (1993), 165-175.

[Burg1] D. A. Burgess, “On character sums and primitive roots”, Proc. London Math. Society (3), 12 (1962), 179-192.

[Burg2] D. A. Burgess, “Character sums and primitive roots in finite fields”, Proc. London Math. Society (3), 17 (1967), 11-25.

[Ch] M.-Ch. Chang, “On a question of Davenport and Lewis and new character sums bounds in finite fields”, Duke Math. J. 145 (3), 409-442 (2008).

[Ch2] M.-Ch. Chang, “Burgess inequality in \(\mathbb{F}_{p^2}\)”, Geom. Funct. Anal. Vol. 19 (2009), 1001-1016.

[DL] H. Davenport and D. J. Lewis, “Character sums and primitive roots in finite fields”, Rend. Circ. Mat. Palermo(2), 12 (2), 129-136 (1963).

[K] N. Katz, “An estimate for character sums”, JAMS Vol. 2, No 2 1989, 197-200.

[Kar1] A. A. Karatsuba, “Character sums and primitive roots in finite fields”, Soviet Math. Dokl. 9, 755–757 (1968).
[Kar2] A. A. Karatsuba, “On estimates of character sums”, Math. USSR-Izv. 4, 19–29 (1970).

[Kon] S. V. Konyagin, “Estimates of character sums in finite fields”, Mathematical Notes, 2010, Vol. 88, No. 4, pp. 503–515.

[TV] T. Tao and V. Vu, “Additive Combinatorics”, Cambridge Stud. Adv. Math., Vol. 105.

[Vin1] I. M. Vinogradov, Appendix 1 to the book: Hua Lo-Keng, “The Method of Trigonometric Sums and its Application in the Theory of Numbers”, M. Izd-vo, Mir, 1964.

[Vin2] I. M. Vinogradov, “A new estimate of the function $\zeta(1 + it)$”, Izv. Akad. Nauk SSSR Ser. Mat., 22:2 (1958), 161–164.

[Vin3] I. M. Vinogradov, “The method of trigonometrical sums in the theory of numbers”, Trudy Mat. Inst. Steklov., 23, Acad. Sci. USSR, Moscow–Leningrad, 1947, 3–109

[vdC] J.G. van der Corput, “Vershärfung der Abschätzung beim Teilerproblem”, Math. Ann., 87:1-2 (1922), s. 39-65, Satz 2.

[W1] H. Weil, “Über die Gleichverteilung von Zahlen mod Eins”, Math. Ann., 77 (1916), s. 313-352.

[W2] H. Weil, “Zur Abschätzung von $\zeta(1 + it)$, Math. Z., 10 (1921), s.88-101.

[Sch] W. M. Schmidt, “Equations over Finite Fields: An Elementary Approach”, Lecture Notes in Math. (Springer-Verlag, Berlin, 1976), Vol. 536.