

ON A QUESTION OF DAVENPORT AND LEWIS AND NEW CHARACTER SUM BOUNDS IN FINITE FIELDS

MEI-CHU CHANG

ABSTRACT.

Let χ be a nontrivial multiplicative character of \mathbb{F}_{p^n} . We obtain the following results.

(1). Let $\varepsilon > 0$ be given. If $B = \{\sum_{j=1}^n x_j \omega_j : x_j \in [N_j + 1, N_j + H_j] \cap \mathbb{Z}, j = 1, \dots, n\}$ is a box satisfying $\prod_{j=1}^n H_j > p^{(\frac{2}{5} + \varepsilon)n}$, then for $p > p(\varepsilon)$ we have, denoting χ a nontrivial multiplicative character

$$\left| \sum_{x \in B} \chi(x) \right| \ll_n p^{-\frac{\varepsilon^2}{4}} |B|$$

unless n is even, χ is principal on a subfield F_2 of size $p^{n/2}$ and $\max_{\xi} |B \cap \xi F_2| > p^{-\varepsilon} |B|$.

(2). Assume $A, B \subset \mathbb{F}_p$ such that

$$|A| > p^{\frac{4}{9} + \varepsilon}, |B| > p^{\frac{4}{9} + \varepsilon}, |B + B| < K|B|.$$

Then

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

(3). Let $I \subset \mathbb{F}_p$ be an interval with $|I| = p^\beta$ and let $\mathcal{D} \subset \mathbb{F}_p$ be a p^β -spaced set with $|\mathcal{D}| = p^\sigma$. Assume $2\beta + \sigma - \frac{\beta\sigma}{1-\beta} > \frac{1}{2} + \delta$. Then for a non-principal multiplicative character χ

$$\left| \sum_{x \in I, y \in \mathcal{D}} \chi(x + y) \right| < p^{-\frac{\delta^2}{12}} |I| |\mathcal{D}|.$$

We also slightly improve a result of Karacuba.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$ -TEX

Introduction.

In this paper we obtain new character sum bounds in finite fields \mathbb{F}_q with $q = p^n$, using methods from additive combinatorics related to the sum-product phenomenon. More precisely, Burgess' classical amplification argument is combined with our estimate on the 'multiplicative energy' for subsets in \mathbb{F}_q . (See Proposition 1 in §1.) The latter appears as a quantitative version of the sum-product theorem in finite fields (see [BKT] and [TV]) following arguments from [G], [KS1] and [KS2].

Our first results relate to the work [DL] of Davenport and Lewis. We recall their result. Let $\{\omega_1, \dots, \omega_n\}$ be an arbitrary basis for \mathbb{F}_{p^n} over \mathbb{F}_p . Then elements of \mathbb{F}_{p^n} have a unique representation as

$$\xi = x_1\omega_1 + \dots + x_n\omega_n, \quad (0 \leq x_i < p). \quad (0.1)$$

We denote B a box in n -dimensional space, defined by

$$N_j + 1 \leq x_j \leq N_j + H_j, \quad (j = 1, \dots, n) \quad (0.2)$$

where N_j and H_j are integers satisfying $0 \leq N_j < N_j + H_j < p$, for all j .

Theorem DL. ([DL], Theorem 2) *Let $H_j = H$ for $j = 1, \dots, n$, with*

$$H > p^{\frac{n}{2(n+1)} + \delta} \text{ for some } \delta > 0 \quad (0.3)$$

and let $p > p_1(\delta)$. Then, with B defined as above

$$\left| \sum_{x \in B} \chi(x) \right| < (p^{-\delta_1} H)^n,$$

where $\delta_1 = \delta_1(\delta) > 0$.

For $n = 1$ (i.e. $\mathbb{F}_q = \mathbb{F}_p$) this is Burgess' result ($H > p^{\frac{1}{4} + \delta}$). But as n increases, the exponent in (0.3) tends to $\frac{1}{2}$. In fact, in [DL] the authors were quite aware of the shortcoming of their approach which they formulated as follows (see [DL], p130)

'The reason for this weakening in the result lies in the fact that the parameter q used in Burgess' method has to be a rational integer and cannot (as far as we can see) be given values in \mathbb{F}_q '.

In this paper we address to some extent their problem and are able to prove the following

2000 *Mathematics Subject Classification.* Primary 11L40, 11L26; Secondary 11A07, 11B75.

Key words. character sums, primitive roots, Davenport-Lewis, Paley Graph conjecture .

Research partially financed by the National Science Foundation.

Theorem 2*. *Let χ be a nontrivial multiplicative character of \mathbb{F}_{p^n} , and let $\varepsilon > 0$ be given. If*

$$B = \left\{ \sum_{j=1}^n x_j \omega_j : x_j \in [N_j + 1, N_j + H_j] \cap \mathbb{Z}, j = 1, \dots, n \right\}$$

is a box satisfying

$$\prod_{j=1}^n H_j > p^{(\frac{2}{5} + \varepsilon)n},$$

then for $p > p(\varepsilon)$

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

unless n is even and $\chi|_{F_2}$ is principal, where F_2 is the subfield of size $p^{n/2}$, in which case

$$\left| \sum_{x \in B} \chi(x) \right| \leq \max_{\xi} |B \cap \xi F_2| + O_n(p^{-\frac{\varepsilon^2}{4}} |B|).$$

Hence our exponent is uniform in n and supersedes [DL] for $n > 4$. The novelty of the method in this paper is to exploit the finite field combinatorics without the need to reduce the problem to a divisor issue in \mathbb{Z} or in the integers of an algebraic number field K (as in the papers [Bu3] and [Kar2]).

Let us emphasize that there are no further assumptions on the basis $\omega_1, \dots, \omega_n$. If one assumes $\omega_i = g^{i-1}$, ($1 \leq i \leq n$), where g satisfies a given irreducible polynomial equation (mod p)

$$a_0 + a_1 g + \dots + a_{n-1} g^{n-1} + g^n = 0, \text{ with } a_i \in \mathbb{Z},$$

or more generally, if

$$\omega_i \omega_j = \sum_{k=1}^n c_{ijk} \omega_k, \tag{0.4}$$

with c_{ijk} bounded and p taken large enough, a result of the strength of Burgess' theorem was indeed obtained (see [Bu3] and [Kar2]) by reducing the combinatorial problem to counting divisors in the ring of integers of an appropriate number field. But such reduction seems not possible in the general context considered in [DL].

Character estimates as considered above have many applications, e.g. quadratic non-residues, primitive roots, coding theory, etc. Corollary 3 in §2 is a standard

*The author is grateful to Andrew Granville for removing an additional restriction on the set B from an earlier version of this theorem.

consequence of Theorem 2 to the problem of primitive roots (see for instance [DL], p131).

The aim of [DL] (and in an extensive list of other works starting from Burgess' seminal paper [Bu1]) was to improve on the Polya-Vinogradov estimate (i.e. breaking the \sqrt{q} -barrier), when considering incomplete character sums of the form

$$\left| \sum_{x \in A} \chi(x) \right|, \quad (0.5)$$

where $A \subset \mathbb{F}_q$ has certain additive structure.

Note that the set B considered above has a small doubling set, i.e.

$$|B + B| < c(n)|B| \quad (0.6)$$

and this is the property relevant to us in our combinatorial Proposition 1 in §1.

In the case of a prime field ($q = p$), our method provides the following generalization of Burgess' inequality.

Theorem 4. *Let \mathcal{P} be a proper d -dimensional generalized arithmetic progression in \mathbb{F}_p with*

$$|\mathcal{P}| > p^{2/5+\varepsilon}$$

for some $\varepsilon > 0$. If \mathcal{X} is a non-principal multiplicative character of \mathbb{F}_p , we have

$$\left| \sum_{x \in \mathcal{P}} \mathcal{X}(x) \right| < p^{-\tau} |\mathcal{P}|$$

where $\tau = \tau(\varepsilon, d) > 0$ and assuming $p > p(\varepsilon, d)$.

See §4, where we also recall the notion of a 'proper generalized arithmetic progression'. Let us point out here that the proof of Proposition 1 below and hence Theorem 2, uses the full linear independence of the elements $\omega_1, \dots, \omega_n$ over the base field \mathbb{F}_p . Assuming in Theorem 2 only that B is a proper generalized arithmetic progression requires us to make a stronger assumption on $|B|$.

Next, we consider the problem of estimating character sums over sumsets of the form

$$\sum_{x \in A, y \in B} \chi(x + y), \quad (0.7)$$

where χ is a non-principal multiplicative character modulo p (we consider again only the prime field case for simplicity). In this situation, a well-known conjecture (sometimes referred to as the Paley Graph conjecture) predicts a nontrivial bound on (0.7) as soon as $|A|, |B| > p^\delta$, for some $\delta > 0$. Presently, such a result is only known (with no further assumptions) provided $|A| > p^{\frac{1}{2}+\delta}$ and $|B| > p^\delta$ for some $\delta > 0$. The problem is open even for the case $|A| \sim p^{\frac{1}{2}} \sim |B|$. Using Proposition 1 (combined with Freiman's theorem), we prove the following result.

Theorem 6. *Assume $A, B \subset \mathbb{F}_p$ such that*

- (a) $|A| > p^{\frac{4}{9}+\varepsilon}, |B| > p^{\frac{4}{9}+\varepsilon}$
- (b) $|B + B| < K|B|$.

Then

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

where $\tau = \tau(\varepsilon, K) > 0$, $p > p(\varepsilon, K)$ and χ is a non-principal multiplicative character of \mathbb{F}_p .

Assuming $B = I$ an interval, we obtain the next estimate.

Theorem 8. *Let $I \subset \mathbb{F}_p$ be an interval with $|I| = p^\beta$ and let $\mathcal{D} \subset \mathbb{F}_p$ be a p^β -spaced set modulo p with $|\mathcal{D}| = p^\sigma$. Assume*

$$2\beta + \sigma - \frac{\beta\sigma}{1-\beta} > \frac{1}{2} + \delta \tag{0.8}$$

for some $\delta > 0$. Then

$$\left| \sum_{x \in I, y \in \mathcal{D}} \chi(x + y) \right| < p^{-\frac{\delta^2}{12}} |I| \cdot |\mathcal{D}| \tag{0.9}$$

for a non-principal multiplicative character χ .

Note that Theorem 8 breaks Burgess' $\frac{1}{4}$ -threshold as soon as $\sigma > 0$. This theorem has various applications, in particular it gives new estimates on character sums over divisor functions in the spirit of [Kar3] and [Kar4]. We will not pursue them here in details.

The next result is a slight improvement of Karacuba's [Kar1].

Theorem 9. Let $I \subset [1, p]$ be an interval with $|I| = p^\beta$ and $S \subset [1, p]$ be an arbitrary set with $|S| = p^\alpha$. Assume that α, β satisfy

$$\varepsilon < \beta \leq \frac{1}{k} \text{ and } \left(1 - \frac{2}{3k}\right)\alpha + \frac{2}{3}\left(1 + \frac{2}{k}\right)\beta > \frac{1}{2} + \frac{1}{3k} + \varepsilon$$

for some $\varepsilon > 0$ and $k \in \mathbb{Z}_+$. Then

$$\sum_{y \in I} \left| \sum_{x \in S} \chi(x+y) \right| < p^{-\varepsilon'} |I| |S|$$

for some $\varepsilon' = \varepsilon'(\varepsilon) > 0$.

We believe that this is the first paper exploring the application of recent developments in combinatorial number theory (for which we especially refer to [TV]) to the problem of estimating (multiplicative) character sums. (Those developments have been particularly significant in the context of exponential sums with additive characters. See [BGK] and subsequent papers.) One could clearly foresee more investigations along these lines.

The paper is organized as follows. We prove Proposition 1 in §1, Theorem 2 in §2, Theorems 6 in §3, and Theorems 8, 9, 10 in §4.

Notations. Let $*$ be a binary operation on some ambient set S and let A, B be subsets of S . Then

- (1) $A * B := \{a * b : a \in A \text{ and } b \in B\}$.
- (2) $a * B := \{a\} * B$.
- (3) $AB := A * B$, if $*$ =multiplication.
- (4) $A^n := AA^{n-1}$.

Note that we use A^n for both the n -fold product set and n -fold Cartesian product when there is no ambiguity.

- (5) $[a, b] := \{i \in \mathbb{Z} : a \leq i \leq b\}$.

§1. Multiplicative energy of a box.

Let A, B be subsets of a commutative ring. Recall that the multiplicative energy of A and B is

$$E(A, B) = \left| \{(a_1, a_2, b_1, b_2) \in A \times A \times B \times B : a_1 b_1 = a_2 b_2\} \right|. \quad (1.1)$$

(See [TV] p.61.)

We will use the following (see [TV] Corollary 2.10)

Fact 1. $E(A, B) \leq E(A, A)^{1/2} E(B, B)^{1/2}$.

Proposition 1. Let $\{\omega_1, \dots, \omega_n\}$ be a basis for \mathbb{F}_{p^n} over \mathbb{F}_p and let $B \subset \mathbb{F}_{p^n}$ be the box

$$B = \left\{ \sum_{j=1}^n x_j \omega_j : x_j \in [N_j + 1, N_j + H_j], j = 1, \dots, n \right\},$$

where $1 \leq N_j < N_j + H_j < p$ for all j . Assume that

$$\max_j H_j < \frac{1}{2}(\sqrt{p} - 1) \quad (1.2)$$

Then we have

$$E(B, B) < C^n (\log p) |B|^{11/4} \quad (1.3)$$

for an absolute constant $C < 2^{\frac{9}{4}}$.

The argument is an adaptation of [G] and [KS1] with the aid of a result in [KS2]. The structure of B allows us to carry out the argument directly from [KS1] leading to the same statement as for the case $n = 1$.

We will use the following estimates from [KS1] (Corollaries 1.4-1.6). (See also [G].)

Let X, B_1, \dots, B_k be subsets of a commutative ring and $a, b \in X$. Then

Fact 2. $|B_1 + \dots + B_k| \leq \frac{|X+B_1| \dots |X+B_k|}{|X|^{k-1}}$.

Fact 3. $\exists X' \subset X$ with $|X'| > \frac{1}{2}|X|$ and $|X' + B_1 + \dots + B_k| \leq 2^k \frac{|X+B_1| \dots |X+B_k|}{|X|^{k-1}}$.

Fact 4. $|aX \pm bX| \leq \frac{|X+X|^2}{|aX \cap bX|}$.

Proof of Proposition 1.

Claim 1. $\mathbb{F}_p \not\subset \frac{B-B}{B-B}$.

Proof of Claim 1. Take $t \in \mathbb{F}_p \cap \frac{B-B}{B-B}$. Then $t \sum x_j \omega_j = \sum y_j \omega_j$ for some $x_j, y_j \in [-H_j, H_j]$, where $1 \leq j \leq n$ and $\sum x_j \omega_j \neq 0$. Since $tx_j = y_j$ for all $j = 1, \dots, n$, choosing i such that $x_i \neq 0$, it follows that

$$t \in \frac{[-H_i, H_i]}{[-H_i, H_i] \setminus \{0\}} \subset \frac{[-\frac{1}{2}(\sqrt{p}-1), \frac{1}{2}(\sqrt{p}-1)]}{[-\frac{1}{2}(\sqrt{p}-1), \frac{1}{2}(\sqrt{p}-1)] \setminus \{0\}}. \quad (1.4)$$

Since the set (1.4) is of size at most $\sqrt{p}(\sqrt{p}-1) < p$, it cannot contain \mathbb{F}_p . This proves our claim.

We may now repeat verbatim the argument in [KS1], with the additional input of the multiplicative energy.

Claim 2. There exist $b_0 \in B$, $A_1 \subset B$ and $N \in \mathbb{Z}_+$ such that

$$|aB \cap b_0B| \sim N \text{ for all } a \in A_1, \quad (1.5)$$

$$N |A_1| > \frac{E(B, B)}{|B| \log |B|} \quad (1.6)$$

and

$$\frac{A_1 - A_1}{A_1 - A_1} + 1 \neq \frac{A_1 - A_1}{A_1 - A_1}. \quad (1.7)$$

Proof of Claim 2.

From (1.1)

$$E(B, B) = \sum_{a, b \in B} |aB \cap bB|.$$

Therefore, there exists $b_0 \in B$ such that

$$\sum_{a \in B} |aB \cap b_0B| \geq \frac{E(B, B)}{|B|}.$$

Let A_s be the level set

$$A_s = \{a \in B : 2^{s-1} \leq |aB \cap b_0B| < 2^s\}.$$

Then for some s_0 with $1 \leq s_0 \leq \log_2 |B|$ we have

$$2^{s_0} |A_{s_0}| \log_2 |B| \geq \sum_{s=0}^{\log_2 |B|} 2^s |A_s| > \sum_{a \in B} |aB \cap b_0B| \geq \frac{E(B, B)}{|B|}.$$

(1.5) and (1.6) are obtained by taking $A_1 = A_{s_0}$ and $N = 2^{s_0}$.

Next we prove (1.7) by assuming the contrary. By iterating t times, we would have

$$\frac{A_1 - A_1}{A_1 - A_1} + t = \frac{A_1 - A_1}{A_1 - A_1} \text{ for } t = 0, 1, \dots, p-1. \quad (1.8)$$

Since $0 \in \frac{A_1 - A_1}{A_1 - A_1}$, (1.8) would imply that $\mathbb{F}_p \subset \frac{A_1 - A_1}{A_1 - A_1} \subset \frac{B - B}{B - B}$, contradicting Claim 1. Hence (1.7) holds.

Take $c_1, c_2, d_1, d_2 \in A_1, d_1 \neq d_2$, such that

$$\xi = \frac{c_1 - c_2}{d_1 - d_2} + 1 \notin \frac{A_1 - A_1}{A_1 - A_1}.$$

It follows that for any subset $A' \subset A_1$, we have

$$\begin{aligned} |A'|^2 &= |A' + \xi A'| = |(d_1 - d_2)A' + (d_1 - d_2)A' + (c_1 - c_2)A'| \\ &\leq |(d_1 - d_2)A' + (d_1 - d_2)A_1 + (c_1 - c_2)A_1|. \end{aligned} \quad (1.9)$$

In Fact 3, we take $X = (d_1 - d_2)A_1$, $B_1 = (d_1 - d_2)A_1$ and $B_2 = (c_1 - c_2)A_1$. Then there exists $A' \subset A_1$ with $|A'| = \frac{1}{2}|A_1|$ and by (1.9)

$$\begin{aligned} |A'|^2 &\leq |(d_1 - d_2)A' + (d_1 - d_2)A_1 + (c_1 - c_2)A_1| \\ &\leq \frac{2^2}{|A_1|} |A_1 + A_1| |(d_1 - d_2)A_1 + (c_1 - c_2)A_1|. \end{aligned} \quad (1.10)$$

Since $|A_1 + A_1| \leq |B + B| \leq 2^n |B|$,

$$\begin{aligned} 2^{-2}|A_1|^3 &\leq 2^{n+2}|B| |(d_1 - d_2)A_1 + (c_1 - c_2)A_1| \\ &\leq 2^{n+2}|B| |c_1 B - c_2 B + d_1 B - d_2 B|. \end{aligned} \quad (1.11)$$

Facts 2, 4 and (1.5) imply

$$2^{-2}|A_1|^3 \leq 2^{n+2}|B| \frac{|B + B|^8}{N^4 |B|^3}. \quad (1.12)$$

Thus

$$N^4 |A_1|^3 \leq 2^{9n+4} |B|^6 \quad (1.13)$$

and recalling (1.6)

$$E(B, B)^4 \leq (\log |B|)^4 |B|^5 N^4 |A_1|^3 < 2^{9n+4} (\log p)^4 |B|^{11}$$

implying (1.3). \square

§2. Burgess' method and the proof of Theorem 2.

The goal of this section is to prove the theorem below.

Theorem 2. Let χ be a non-principal multiplicative character of \mathbb{F}_{p^n} . Given $\varepsilon > 0$, there is $\tau > \frac{\varepsilon^2}{4}$ such that if

$$B = \left\{ \sum_{j=1}^n x_j \omega_j : x_j \in [N_j + 1, N_j + H_j] \cap \mathbb{Z}, j = 1, \dots, n \right\}$$

is a box satisfying

$$\prod_{j=1}^n H_j > p^{(\frac{2}{5} + \varepsilon)n},$$

then for $p > p(\varepsilon)$

$$\left| \sum_{x \in B} \chi(x) \right| \ll_n p^{-\tau} |B|,$$

unless n is even and $\chi|_{F_2}$ is principal, where F_2 is the subfield of size $p^{n/2}$, in which case

$$\left| \sum_{x \in B} \chi(x) \right| \leq \max_{\xi} |B \cap \xi F_2| + O_n(p^{-\tau} |B|).$$

First we will prove a special case of Theorem 2, assuming some further restriction on the box B .

Theorem 2'. Let χ be a non-principal multiplicative character of \mathbb{F}_{p^n} . Given $\varepsilon > 0$, there is $\tau > \frac{\varepsilon^2}{4}$ such that if

$$B = \left\{ \sum_{j=1}^n x_j \omega_j : x_j \in [N_j + 1, N_j + H_j], j = 1, \dots, n \right\}$$

is a box satisfying

$$\prod_{j=1}^n H_j > p^{(\frac{2}{5} + \varepsilon)n}$$

and also

$$H_j < \frac{1}{2}(\sqrt{p} - 1) \text{ for all } j, \tag{2.1}$$

then for $p > p(\varepsilon)$

$$\left| \sum_{x \in B} \chi(x) \right| \ll_n p^{-\tau} |B|. \tag{2.2}$$

We will need the following version of Weil's bound on exponential sums. (See Theorem 11.23 in [IK])

Theorem W. Let χ be a non-principal multiplicative character of \mathbb{F}_{p^n} of order $d > 1$. Suppose $f \in \mathbb{F}_{p^n}[x]$ has m distinct roots and f is not a d -th power. Then for $n \geq 1$ we have

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

Proof of Theorem 2'.

By breaking up B in smaller boxes, we may assume

$$\prod_{j=1}^n H_j \sim p^{(\frac{2}{5}+\varepsilon)n}. \quad (2.3)$$

Let $\delta > 0$ be specified later. Let

$$I = [1, p^\delta] \quad (2.4)$$

and

$$B_0 = \left\{ \sum_{j=1}^n x_j \omega_j : x_j \in [0, p^{-2\delta} H_j], j = 1, \dots, n \right\}. \quad (2.5)$$

Since $B_0 I \subset \left\{ \sum_{j=1}^n x_j \omega_j : x_j \in [0, p^{-\delta} H_j], j = 1, \dots, n \right\}$, clearly

$$\left| \sum_{x \in B} \chi(x) - \sum_{x \in B} \chi(x + yz) \right| < |B \setminus (B + yz)| + |(B + yz) \setminus B| < 2np^{-\delta}|B|$$

for $y \in B_0, z \in I$. Hence*

$$\sum_{x \in B} \chi(x) = \frac{1}{|B_0| |I|} \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) + O(np^{-\delta}|B|). \quad (2.6)$$

Estimate (up to an error term)

$$\begin{aligned} \left| \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) \right| &\leq \sum_{x \in B, y \in B_0} \left| \sum_{z \in I} \chi(x + yz) \right| \\ &= \sum_{x \in B, y \in B_0} \left| \sum_{z \in I} \chi(xy^{-1} + z) \right| \\ &= \sum_{u \in \mathbb{F}_{p^n}} w(u) \left| \sum_{z \in I} \chi(u + z) \right|, \end{aligned} \quad (2.7)$$

*This initial step of translation by a product is by now standard and was first used in [Kar2] in the context of character sums.

where

$$\omega(u) = \left| \left\{ (x, y) \in B \times B_0 : \frac{x}{y} = u \right\} \right|. \quad (2.8)$$

Observe that

$$\begin{aligned} \sum_{e \in \mathbb{F}_p^n} \omega(u)^2 &= |\{(x_1, x_2, y_1, y_2) \in B \times B \times B_0 \times B_0 : x_1 y_2 = x_2 y_1\}| \\ &= \sum_{\nu} |\{(x_1, x_2) : \frac{x_1}{x_2} = \nu\}| |\{(y_1, y_2) : \frac{y_1}{y_2} = \nu\}| \\ &\leq E(B, B)^{\frac{1}{2}} E(B_0, B_0)^{\frac{1}{2}} \\ &< 2^{\frac{9}{4}n+1} (\log p) |B|^{\frac{11}{8}} |B_0|^{\frac{11}{8}} \\ &< 2^{\frac{9}{4}n+1} (\log p) \left(|B| \right)^{\frac{11}{4}} p^{-\frac{11}{4}n\delta}, \end{aligned} \quad (2.9)$$

by the Cauchy-Schwarz inequality, Proposition 1 and (2.5).

Let r be the nearest integer to $\frac{n}{\varepsilon}$. Hence

$$\left| r - \frac{n}{\varepsilon} \right| \leq \frac{1}{2}. \quad (2.10)$$

By Hölder's inequality, (2.7) is bounded by

$$\left(\sum_{u \in \mathbb{F}_p^n} \omega(u)^{\frac{2r}{2r-1}} \right)^{1-\frac{1}{2r}} \left(\sum_{u \in \mathbb{F}_p^n} \left| \sum_{z \in I} \chi(u+z) \right|^{2r} \right)^{\frac{1}{2r}}. \quad (2.11)$$

Up to this point the proof is essentially that of Burgess. In his case the $\omega(u)$ are all small, that is $< p^{o(1)}$, and this bound can be injected at this point. However this is not necessarily the case in our application, so that we deal with the sum over the $\omega(u)$ somewhat differently. Since $\sum_u \omega(u) = |B_0| \cdot |B|$ and (2.9) holds, we have

$$\begin{aligned} \left(\sum_u \omega(u)^{\frac{2r}{2r-1}} \right)^{1-\frac{1}{2r}} &\leq \left[\sum \omega(u) \right]^{1-\frac{1}{r}} \left[\sum \omega(u)^2 \right]^{\frac{1}{2r}} \\ &< 2^{(\frac{9}{4}n+1)\frac{1}{2r}} \left(|B_0| \cdot |B| \right)^{1-\frac{1}{r}} \left(|B| \right)^{\frac{11}{8r}} (\log p) p^{-\frac{11}{8}\frac{n}{r}\delta}. \end{aligned} \quad (2.12)$$

The first inequality follows from the following fact, which is proved by using Hölder's inequality with $\frac{2r-2}{2r-1} + \frac{1}{2r-1} = 1$.

Fact 5. $(\sum_u f(u)^{\frac{2r}{2r-1}})^{1-\frac{1}{2r}} \leq [\sum f(u)]^{1-\frac{1}{r}} [\sum f(u)^2]^{\frac{1}{2r}}$.

Proof. Write $f(u)^{\frac{2r}{2r-1}} = f(u)^{\frac{2r-2}{2r-1}} f(u)^{\frac{2}{2r-1}}$. \square

Next, we bound the second factor of (2.11).

Let

$$q = p^n.$$

Write

$$\sum_{u \in \mathbb{F}_{p^n}} \left| \sum_{z \in I} \chi(u+z) \right|^{2r} \leq \sum_{z_1, \dots, z_{2r} \in I} \left| \sum_{u \in \mathbb{F}_q} \chi((u+z_1) \dots (u+z_r)(u+z_{r+1})^{q-2} \dots (u+z_{2r})^{q-2}) \right|. \quad (2.13)$$

For $z_1, \dots, z_{2r} \in I$ such that at least one of the elements is not repeated twice, the polynomial $f_{z_1, \dots, z_{2r}}(x) = (x+z_1) \dots (x+z_r)(x+z_{r+1})^{q-2} \dots (x+z_{2r})^{q-2}$ clearly cannot be a d -th power. Since $f_{z_1, \dots, z_{2r}}(x)$ has no more than $2r$ many distinct roots, Theorem W gives

$$\left| \sum_{u \in \mathbb{F}_q} \chi((u+z_1) \dots (u+z_r)(u+z_{r+1})^{q-2} \dots (u+z_{2r})^{q-2}) \right| < 2rp^{\frac{n}{2}}. \quad (2.14)$$

For those $z_1, \dots, z_{2r} \in I$ such that every root of $f_{z_1, \dots, z_{2r}}(x)$ appears at least twice, we bound $\sum_{u \in \mathbb{F}_q} \left| \sum_{z \in I} \chi(f_{z_1, \dots, z_{2r}}(u)) \right|$ by $|\mathbb{F}_q|$ times the number of such z_1, \dots, z_{2r} . Since there are at most r roots in I and for each z_1, \dots, z_{2r} there are at most r choices, we obtain a bound $|I|^r r^{2r} p^n$.

Therefore

$$\sum_{u \in \mathbb{F}_{p^n}} \left| \sum_{z \in I} \chi(u+z) \right|^{2r} < |I|^r r^{2r} p^n + 2r |I|^{2r} p^{\frac{n}{2}} \quad (2.15)$$

and

$$\left(\sum_{u \in \mathbb{F}_{p^n}} \left| \sum_{z \in I} \chi(u+z) \right|^{2r} \right)^{\frac{1}{2r}} \leq r |I|^{\frac{1}{2}} p^{\frac{n}{2r}} + 2 |I| p^{\frac{n}{4r}}. \quad (2.16)$$

Putting (2.7), (2.11), (2.12) and (2.16) together, we have

$$\begin{aligned}
& \frac{1}{|B_0| |I|} \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) \\
& < 4^{\frac{n}{r}} (\log p) \left(|B_0| |B| \right)^{-\frac{1}{r}} \left(|B| \right)^{1 + \frac{11}{8r}} p^{-\frac{11}{8} \frac{n}{r} \delta} \left(r |I|^{-\frac{1}{2}} p^{\frac{n}{2r}} + 2p^{\frac{n}{4r}} \right) \\
& < 4^{\frac{n}{r}} (\log p) p^{\frac{1}{r} 2n\delta - \frac{11}{8} \frac{n}{r} \delta} \left(|B| \right)^{1 - \frac{5}{8r}} \left(r p^{\frac{-\delta}{2}} p^{\frac{n}{2r}} + 2p^{\frac{n}{4r}} \right) \\
& < 4^{\frac{n}{r}} (\log p) 2r p^{\frac{n}{4r} + 2\delta \frac{n}{r} - \frac{11}{8} \frac{n}{r} \delta - \frac{5}{8r} (\frac{2}{5} + \varepsilon)n} |B| \\
& < 2 \cdot 4^{\frac{n}{r}} (\log p) r |B| p^{-\frac{5}{8} \frac{n}{r} (\varepsilon - \delta)}. \tag{2.17}
\end{aligned}$$

The second to the last inequality holds because of (2.3) and assuming $\delta \geq n/2r$.

Let

$$\delta = \frac{n}{2r}. \tag{2.18}$$

To bound the exponent $\frac{5}{8} \frac{n}{r} (\varepsilon - \delta) = \frac{5}{16} \varepsilon^2 \frac{n}{r\varepsilon} (2 - \frac{n}{r\varepsilon})$, we let

$$\theta = \frac{n}{\varepsilon r} - 1. \tag{2.19}$$

Then by (2.10),

$$|\theta| < \frac{1}{2r} < \frac{\varepsilon}{2n - \varepsilon} < \frac{3}{(10n - 3)} \leq \frac{3}{7} \tag{2.20}$$

and

$$\frac{5}{8} \frac{n}{r} (\varepsilon - \delta) = \frac{5}{16} \varepsilon^2 (1 + \theta)(1 - \theta) > \frac{25}{98} \varepsilon^2. \tag{2.21}$$

Returning to (2.6), we have

$$\left| \sum_{x \in B} \chi(x) \right| < cn\varepsilon^{-1} (\log p) p^{-\frac{25}{98} \varepsilon^2} |B| < np^{-\frac{\varepsilon^2}{4}} |B| \tag{2.22}$$

and thus proves Theorem 2'. \square

Our next aim is to remove the additional hypothesis (2.1) on the shape of B . We proceed in several steps and rely essentially on a further key ingredient provided by the following estimate. (See [PS].)

Proposition ♣*. Let χ be a non-principal multiplicative character of \mathbb{F}_q and let $g \in \mathbb{F}_q$ be a generating element, i.e. $\mathbb{F}_q = \mathbb{F}_p(g)$. For any integral interval $I \subset [1, p]$,

$$\left| \sum_{t \in I} \chi(g+t) \right| \leq c(n) \sqrt{p} \log p \quad (2.23)$$

Note that (2.23) is nontrivial as soon as $|I| \gg \sqrt{p} \log p$.

First we make the following observation (extending slightly the range of the applicability of Theorem 2').

Let $H_1 \geq H_2 \geq \dots \geq H_n$. If $H_1 \leq p^{\frac{1}{2} + \frac{\varepsilon}{2}}$, we may clearly write B as a disjoint union of boxes $B_\alpha \subset B$ satisfying the first condition in (2.1) and $|B_\alpha| > (\frac{1}{2} p^{-\frac{\varepsilon}{2}})^n |B| > 2^{-n} p^{(\frac{2}{5} + \frac{\varepsilon}{2})n}$. Since (2.1) holds for each B_α , we have

$$\left| \sum_{x \in B_\alpha} \chi(x) \right| < c n p^{-\tau} |B_\alpha|.$$

Hence

$$\left| \sum_{x \in B} \chi(x) \right| < c n p^{-\tau} |B|.$$

Therefore we may assume that $H_1 > p^{\frac{1}{2} + \frac{\varepsilon}{2}}$.

Proof of Theorem 2.

Case 1. n is odd.

We denote $I_i = [N_i + 1, N_i + H_i]$ and estimate using (2.23)

$$\left| \sum_{x \in B} \chi(x) \right| = \left| \sum_{\substack{x_i \in I_i \\ 2 \leq i \leq n}} \sum_{x_1 \in I_1} \chi\left(x_1 + x_2 \frac{\omega_2}{\omega_1} + \dots + x_n \frac{\omega_n}{\omega_1}\right) \right| \leq c(n) p^{\frac{1}{2}} \log p \frac{|B|}{H_1} + \varpi, \quad (2.24)$$

where

$$\varpi = \left| \sum_{x_1 \in I_1} \sum_{(x_2, \dots, x_n) \in D} \chi\left(x_1 + x_2 \frac{\omega_2}{\omega_1} + \dots + x_n \frac{\omega_n}{\omega_1}\right) \right| \quad (2.25)$$

and

$$D = \left\{ (x_2, \dots, x_n) \in I_2 \times \dots \times I_n : \mathbb{F}_p\left(x_2 \frac{\omega_2}{\omega_1} + \dots + x_n \frac{\omega_n}{\omega_1}\right) \neq \mathbb{F}_q \right\}.$$

*This was originally communicated to the author by Nick Katz as an extension of his work [K].

In particular,

$$\varpi \leq p|D| \leq p \sum_G \left| G \cap \text{Span}_{\mathbb{F}_p} \left(\frac{\omega_2}{\omega_1}, \dots, \frac{\omega_n}{\omega_1} \right) \right|,$$

where G runs over nontrivial subfields of \mathbb{F}_q . Since $q = p^n$ and n is odd, obviously $[\mathbb{F}_q : G] \geq 3$. Hence $[G : \mathbb{F}_p] \leq \frac{n}{3}$. Furthermore, since $\{\omega_1, \dots, \omega_n\}$ is a basis of \mathbb{F}_q over \mathbb{F}_p , $1 \notin \text{Span}_{\mathbb{F}_p} \left(\frac{\omega_2}{\omega_1}, \dots, \frac{\omega_n}{\omega_1} \right)$ and the proceeding implies that

$$\dim_{\mathbb{F}_p} \left(G \cap \text{Span}_{\mathbb{F}_p} \left(\frac{\omega_2}{\omega_1}, \dots, \frac{\omega_n}{\omega_1} \right) \right) \leq \frac{n}{3} - 1. \quad (2.26)$$

Therefore, under our assumption on $|H_1|$, back to (2.24)

$$\begin{aligned} \left| \sum_{x \in B} \chi(x) \right| &< c(n) \left((\log p) p^{-\frac{\varepsilon}{2}} |B| + p^{\frac{n}{3}} \right) \\ &< \left(c(n) (\log p) p^{-\frac{\varepsilon}{2}} + p^{-\frac{n}{15}} \right) |B|, \end{aligned}$$

since $|B| > p^{\frac{2}{5}n}$. This proves our claim.

We now treat the case when n is even. The analysis leading to the second part of Theorem 2 was kindly communicated by Andrew Granville to the author.

Case 2. n is even.

In view of the earlier discussion, our only concern is to bound

$$\varrho = \left| \sum_{x_1 \in I_1} \sum_{(x_2, \dots, x_n) \in D_2} \chi \left(x_1 + x_2 \frac{\omega_2}{\omega_1} + \dots + x_n \frac{\omega_n}{\omega_1} \right) \right| \quad (2.27)$$

with

$$D_2 = \left\{ (x_2, \dots, x_n) \in I_2 \times \dots \times I_n : \left(x_2 \frac{\omega_2}{\omega_1} + \dots + x_n \frac{\omega_n}{\omega_1} \right) \in F_2 \right\} \quad (2.28)$$

and F_2 the subfield of size $p^{n/2}$.

First, we note that since $1, \frac{\omega_2}{\omega_1}, \dots, \frac{\omega_n}{\omega_1}$ are independent, $\frac{\omega_j}{\omega_1} \in F_2$ for at most $\frac{n}{2} - 1$ many j 's. After reordering, we may assume that $\frac{\omega_j}{\omega_1} \in F_2$ for $2 \leq j \leq k$ and $\frac{\omega_j}{\omega_1} \notin F_2$ for $k+1 \leq j \leq n$, where $k \leq \frac{n}{2}$. We also assume that $H_{k+1} \leq \dots \leq H_n$. Fix x_2, \dots, x_{n-1} . Obviously there is no more than one value of x_n such that $x_2 \frac{\omega_2}{\omega_1} + \dots + x_n \frac{\omega_n}{\omega_1} \in F_2$, since otherwise $(x_n - x'_n) \frac{\omega_n}{\omega_1} \in F_2$ with $x_n \neq x'_n$ contradicting the fact that $\frac{\omega_n}{\omega_1} \notin F_2$.

Therefore,

$$|D_2| \leq |I_2| \cdots |I_{n-1}| \quad (2.29)$$

and

$$\varrho \leq \frac{|B|}{H_n}. \quad (2.30)$$

If $H_n > p^\tau$, we are done. Otherwise

$$H_{k+1} \cdots H_n \leq p^{(n-k)\tau} < p^{n\tau}. \quad (2.31)$$

Define

$$B_2 = \left\{ x_1 + x_2 \frac{\omega_2}{\omega_1} + \cdots + x_k \frac{\omega_k}{\omega_1} : x_i \in I_i, 1 \leq i \leq k \right\}.$$

Hence $B_2 \subset F_2$ and by (2.31)

$$|B_2| = \frac{|B|}{H_{k+1} \cdots H_n} > p^{(\frac{2}{5}-\tau)n} > p^{\frac{n}{3}}. \quad (2.32)$$

(We can assume $\tau < \frac{1}{15}$.)

Clearly, if $(x_2, \dots, x_n) \in D_2$, then $z = x_{k+1} \frac{\omega_{k+1}}{\omega_1} + \cdots + x_n \frac{\omega_n}{\omega_1} \in F_2$. Assume $\chi|_{F_2}$ is non-principal, it follows from the generalized Polya-Vinogradov inequality and (2.32) that

$$\left| \sum_{y \in B_2} \chi(y+z) \right| \leq (\log p)^{\frac{n}{2}} \max_{\psi} \left| \sum_{x \in F_2} \psi(x) \chi(x) \right| \leq (\log p)^{\frac{n}{2}} \cdot |F_2|^{\frac{1}{2}} \leq p^{-\frac{n}{15}} |B_2|, \quad (2.33)$$

where ψ runs over all additive characters. Therefore, clearly

$$\varrho \leq H_{k+1} \cdots H_n p^{-\frac{n}{15}} |B_2| = p^{-\frac{n}{15}} |B| \quad (2.34)$$

providing the required estimate.

If $\chi|_{F_2}$ is principal, then obviously

$$\varrho = H_1 \cdot |D_2| = \left| F_2 \cap \frac{1}{\omega} B \right| \quad (2.35)$$

and

$$\left| \sum_{x \in B} \chi(x) \right| = |\omega F_2 \cap B| + O_n(p^{-\tau} |B|). \quad (2.36)$$

This complete the proof of Theorem 2. \square

Remark 2.1. The conclusion of Theorem 2 certainly holds, if we replace the assumption of $\prod_{j=1}^n H_j > p^{(\frac{2}{5}+\varepsilon)n}$ by the stronger assumption

$$p^{\frac{2}{5}+\varepsilon} < H_j \text{ for all } j. \quad (2.37)$$

This improves on Theorem 2 of [DL] for $n > 4$. In [DL], the condition $H_j > p^{\frac{n}{2(n+1)}+\varepsilon}$ is required. Our assumption (2.37) is independent of n , while, in the [DL] result, when n goes to ∞ , the exponent $\frac{n}{2(n+1)}$ goes to $\frac{1}{2}$.

Remark 2.2. In the case of a prime field ($n = 1$), Burgess theorem (see [Bu1]) requires the assumption $H > p^{\frac{1}{4}+\varepsilon}$, for some $\varepsilon > 0$, which seems to be the limit of this method. For $n > 1$, the exact counterpart of Burgess' estimate seems unknown in the generality of an arbitrary basis $\omega_1, \dots, \omega_n$ of \mathbb{F}_{p^n} over \mathbb{F}_p , as considered in [DL] and here. Higher dimensional results of the strength of Burgess seem only known for certain special basis, in particular, basis of the form $\omega_j = g^j$ with given g generating \mathbb{F}_{p^n} . (See [Bu3], [Bu4] and [Kar2].)

Theorem 2 allows us to estimate the number of primitive roots of \mathbb{F}_{p^n} that fall into B .

We denote the Euler function by φ .

Corollary 3. *Let $B \subset \mathbb{F}_{p^n}$ be as in Theorem 2 and satisfying $\max_{\xi} |B \cap \xi F_2| < p^{-\varepsilon} |B|$ if n even. The number of primitive roots of \mathbb{F}_{p^n} belonging to B is*

$$\frac{\varphi(p^n - 1)}{p^n - 1} |B| (1 + o(p^{-\tau'}))$$

where $\tau' = \tau'(\varepsilon) > 0$ and assuming $n \ll \log \log p$.

§3. Some further implications of the method.

In what follows, we only consider for simplicity the case of a prime field (several statements below have variants over a general finite field, possibly with worse exponents).

3.1. Recall that a generalized d -dimensional arithmetic progression in \mathbb{F}_p is a set of the form

$$\mathcal{P} = a_0 + \left\{ \sum_{j=1}^d x_j a_j : x_j \in [0, N_j - 1] \right\} \quad (3.1)$$

for some elements $a_0, a_1, \dots, a_d \in \mathbb{F}_p$. If the representation of elements of \mathcal{P} in (3.1) is unique, we call \mathcal{P} *proper*. Hence \mathcal{P} is proper if and only if $|\mathcal{P}| = N_1 \cdots N_d$ (which we assume in the sequel).

Assume $|\mathcal{P}| < 10^{-d} \sqrt{p}$, hence $\mathbb{F}_p \neq \frac{\mathcal{P}-\mathcal{P}}{\mathcal{P}-\mathcal{P}}$ (in the considerations below, $|\mathcal{P}| \ll p^{1/2}$ so that there is no need to consider the alternative $|\mathcal{P}| \gg p^{1/2}$). Following the argument in [KS1] (or the proof of Proposition 1), we have

$$E(\mathcal{P}, \mathcal{P}) < c^d (\log p) |\mathcal{P}|^{11/4}. \quad (3.2)$$

Also, repeating the proof of Theorem 2, we obtain

Theorem 4. *Let \mathcal{P} be a proper d -dimensional generalized arithmetic progression in \mathbb{F}_p with*

$$|\mathcal{P}| > p^{2/5+\varepsilon} \quad (3.3)$$

for some $\varepsilon > 0$. If \mathcal{X} is a non-principal multiplicative character of \mathbb{F}_p , we have

$$\left| \sum_{x \in \mathcal{P}} \mathcal{X}(x) \right| < p^{-\tau} |\mathcal{P}| \quad (3.4)$$

where $\tau = \tau(\varepsilon, d) > 0$ and assuming $p > p(\varepsilon, d)$.

Theorem 4 is another extension of Burgess' inequality. A natural problem is to try to improve the exponent $\frac{2}{5}$ in (3.3) to $\frac{1}{4}$.

Let us point out one consequence of Theorem 4 which gives an improvement of a result in [HIS]. (See [HIS], Corollary 1.3.)

Corollary 5. *Given $C > 0$ and $\varepsilon > 0$, there is a constant $c = c(C, \varepsilon) > 0$ and a positive integer $k < k(C, \varepsilon)$, such that if $A \subset \mathbb{F}_p$ satisfies*

- (i) $|A + A| < C|A|$
- (ii) $|A| > p^{\frac{2}{5}+\varepsilon}$.

Then we have

$$|A^k| > cp.$$

Proof.

According to Freiman's structural theorem for sets with small doubling constants (see [TV]), under assumption (i), there is a proper generalized d -dimensional progression \mathcal{P} such that $A \subset \mathcal{P}$ and

$$d \leq C \tag{3.5}$$

$$\log \frac{|\mathcal{P}|}{|A|} < C^2(\log C)^3 \tag{3.6}$$

By assumption (ii), Theorem 4 applies to \mathcal{P} . Let τ be as given in Theorem 4. We fix

$$k \in \mathbb{Z}_+, \quad k > \frac{1}{\tau}. \tag{3.7}$$

(Hence $k > k(C, \varepsilon)$.) Denote by ν the probability measure on \mathbb{F}_p obtained as the image measure of the normalized counting measure on the k -fold product \mathcal{P}^k under the product map

$$\begin{aligned} \mathcal{P} \times \cdots \times \mathcal{P} &\longrightarrow \mathbb{F}_p \\ (x_1, \dots, x_k) &\longmapsto x_1 \cdots x_k. \end{aligned}$$

Hence by the Fourier inversion formula, we have

$$\begin{aligned} \nu(x) &= \frac{1}{p-1} \sum_{\chi} \chi(x) \hat{\nu}(\chi) = \frac{1}{p-1} \sum_{\chi} \chi(x) \left(\sum_t \nu(t) \overline{\chi(t)} \right) \\ &= \frac{|\mathcal{P}|^{-k}}{p-1} \sum_{\chi} \chi(x) \left(\sum_{y \in \mathcal{P}} \bar{\chi}(y) \right)^k \leq \frac{|\mathcal{P}|^{-k}}{p-1} \sum_{\chi} \left| \sum_{y \in \mathcal{P}} \chi(y) \right|^k, \end{aligned}$$

χ denoting a multiplicative character.

Applying the circle method and (3.4), we get

$$\max_{x \in \mathbb{F}_p^*} \nu(x) \leq \frac{1}{p-1} + \max_{\chi \text{ non-principal}} |\mathcal{P}|^{-k} \left| \sum_{x \in \mathcal{P}} \chi(x) \right|^k < \frac{1}{p-1} + p^{-\tau k} < \frac{2}{p}. \tag{3.8}$$

The last inequality is by (3.7). Assuming $A \subset \mathbb{F}_p^*$, we write

$$\begin{aligned} |A|^k &\leq |A^k| \max_{x \in \mathbb{F}_p^*} |\{(x_1, \dots, x_k) \in A \times \cdots \times A : x_1 \cdots x_k = x\}| \\ &\leq |A^k| |\mathcal{P}|^k \max_{x \in \mathbb{F}_p^*} \nu(x) \end{aligned}$$

implying by (3.6) and (3.8)

$$|A^k| > \left(\frac{|A|}{|\mathcal{P}|} \right)^k \frac{p}{2} > \frac{p}{2} \exp(-kC^2(\log C)^3) > c(C, \varepsilon)p.$$

This proves Corollary 5. \square

3.2. Recall the well-known Paley Graph conjecture stating that if $A, B \subset \mathbb{F}_p$, $|A| > p^\varepsilon$, $|B| > p^\varepsilon$, then

$$\left| \sum_{x \in A, y \in B} \chi(x + y) \right| < p^{-\delta} |A| |B| \quad (3.9)$$

where $\delta = \delta(\varepsilon) > 0$ and χ a non-principal multiplicative character.

An affirmative answer is only known in the case $|A| > p^{\frac{1}{2} + \varepsilon}$, $|B| > p^\varepsilon$ for some $\varepsilon > 0$ (as a consequence of Weil's inequality (2.14)). Even for $|A| > p^{1/2}$, $|B| > p^{1/2}$, an inequality of the form (3.9) seems unknown. On the other hand, for more structured sets A and B , better results can be obtained (See in particular [Kar1] and [FI].) In the rest of this section and the next section, we will establish further estimates in this vein.

Our first result provides a statement of this type, assuming A or B has a small doubling constant.

Theorem 6. *Assume $A, B \subset \mathbb{F}_p$ such that*

- (a) $|A| > p^{\frac{4}{9} + \varepsilon}$, $|B| > p^{\frac{4}{9} + \varepsilon}$
- (b) $|B + B| < K|B|$.

Then

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

where $\tau = \tau(\varepsilon, K) > 0$, $p > p(\varepsilon, K)$ and χ is a non-principal multiplicative character of \mathbb{F}_p .

Proof.

The argument is a variant of the proof of Theorem 2, so we will be brief. The case $|B| > p^{\frac{1}{2} + \varepsilon}$ is taken care of by Weil's estimate (2.14). Since we can dissect B into $\leq p^\varepsilon$ subsets satisfying assumptions (a) and (b), we may assume that $|B| < \frac{1}{2}(\sqrt{p} - 1)$. We denote the various constants (possibly depending on the constant K in assumption (b)) by C .

Let \mathcal{B}_1 be a generalized d -dimensional proper arithmetic progression in \mathbb{F}_p satisfying $B \subset \mathcal{B}_1$ and

$$d \leq K \quad (3.10)$$

$$\log \frac{|\mathcal{B}_1|}{|B|} < C. \quad (3.11)$$

Let

$$\mathcal{B}_2 = (-\mathcal{B}_1) \cup \mathcal{B}_1.$$

We take

$$\delta = \frac{\varepsilon}{4d}, \quad r = \left\lceil \frac{10}{\delta} \right\rceil. \quad (3.12)$$

Similar to the proof of Theorem 2, we take a proper progression $\mathcal{B}_0 \subset \mathcal{B}_2 \subset \mathbb{F}_p$ and an integral interval $I = [1, p^\delta]$ with the following properties

$$\begin{aligned} |B_0| &> p^{-2d\delta} |\mathcal{B}_2| \\ B - \mathcal{B}_0 I &\subset \mathcal{B}_2. \end{aligned} \quad (3.13)$$

Therefore,

$$|\mathcal{B}| \leq |\mathcal{B}_1| \leq e^{C(K)} |\mathcal{B}| \quad \text{and} \quad |\mathcal{B}_2| = 2|\mathcal{B}_1| - 1. \quad (3.14)$$

Estimate

$$\begin{aligned} \left| \sum_{x \in A, y \in B} \chi(x+y) \right| &\leq \sum_{y \in B} \left| \sum_{x \in A} \chi(x+y) \right| \\ &\leq |\mathcal{B}_0|^{-1} |I|^{-1} \sum_{\substack{y \in \mathcal{B}_2 \\ z \in \mathcal{B}_0, t \in I}} \left| \sum_{x \in A} \chi(x+y+zt) \right|. \end{aligned} \quad (3.15)$$

The second inequality is by (3.13). Write

$$\sum_{\substack{y \in \mathcal{B}_2 \\ z \in \mathcal{B}_0, t \in I}} \left| \sum_{x \in A} \chi(x+y+zt) \right| \leq (|\mathcal{B}_2| |\mathcal{B}_0| |I|)^{\frac{1}{2}} \left| \sum_{\substack{y \in \mathcal{B}_2, z \in \mathcal{B}_0, t \in I \\ x_1, x_2 \in A}} \chi\left(\frac{(x_1+y)z^{-1}+t}{(x_2+y)z^{-1}+t}\right) \right|^{\frac{1}{2}}. \quad (3.16)$$

The sum on the right-hand side of (3.16) equals

$$\begin{aligned} &\left| \sum_{u_1, u_2 \in \mathbb{F}_p} \nu(u_1, u_2) \sum_{t \in I} \chi\left(\frac{u_1+t}{u_2+t}\right) \right| \\ &\leq \left[\sum_{u_1, u_2} \nu(u_1, u_2)^{\frac{2r}{2r-1}} \right]^{1-\frac{1}{2r}} \left[\sum_{u_1, u_2} \left| \sum_{t \in I} \chi\left(\frac{u_1+t}{u_2+t}\right) \right|^{2r} \right]^{\frac{1}{2r}} \end{aligned} \quad (3.17)$$

where for $(u_1, u_2) \in \mathbb{F}_p^2$ we define

$$\nu(u_1, u_2) = |\{(x_1, x_2, y, z) \in A \times A \times \mathcal{B}_2 \times \mathcal{B}_0 : \frac{x_1+y}{z} = u_1 \text{ and } \frac{x_2+y}{z} = u_2\}|. \quad (3.18)$$

Hence

$$\sum_{u_1, u_2} v(u_1, u_2) = |A|^2 |\mathcal{B}_2| |\mathcal{B}_0| \quad (3.19)$$

and

$$\begin{aligned} & \sum_{u_1, u_2} \nu(u_1, u_2)^2 \\ &= \left| \left\{ (x_1, x_2, x'_1, x'_2, y, y', z, z') \in A^4 \times \mathcal{B}_2^2 \times \mathcal{B}_0^2 : \frac{x_i + y}{z} = \frac{x'_i + y'}{z'} \text{ for } i = 1, 2 \right\} \right| \\ &\leq |A|^3 \max_{x_1, x'_1} \left| \left\{ (y, y', z, z') \in \mathcal{B}_2^2 \times \mathcal{B}_0^2 : \frac{x_1 + y}{z} = \frac{x'_1 + y'}{z'} \right\} \right| \\ &\leq |A|^3 E(\mathcal{B}_0, \mathcal{B}_0)^{\frac{1}{2}} \max_x E(x + \mathcal{B}_2, x + \mathcal{B}_2)^{\frac{1}{2}} \\ &< |A|^3 \log p |\mathcal{B}_0|^{\frac{11}{8}} |\mathcal{B}_2|^{\frac{11}{8}} \\ &< C |A|^3 |\mathcal{B}_2|^{\frac{11}{4}} \end{aligned} \quad (3.20)$$

by Proposition 1 and Fact. Therefore, by Fact 5 (after (2.12)), (3.19) and (3.20), the first factor of (3.17) is bounded by

$$\begin{aligned} & \left[\sum \nu(u_1, u_2) \right]^{1 - \frac{1}{r}} \left[\sum \nu(u_1, u_2)^2 \right]^{\frac{1}{2r}} \\ &\leq C |A|^2 |\mathcal{B}_2| |\mathcal{B}_0| (|A|^{-\frac{1}{2}} |\mathcal{B}_2|^{-\frac{5}{8}} p^{2d\delta})^{\frac{1}{r}}. \end{aligned} \quad (3.21)$$

Next, write using Weil's inequality (2.14)

$$\begin{aligned} \sum_{u_1, u_2 \in \mathbb{F}_p} \left| \sum_{t \in I} \chi \left(\frac{u_1 + t}{u_2 + t} \right) \right|^{2r} &\leq \sum_{t_1, \dots, t_{2r} \in I} \left| \sum_{u \in \mathbb{F}_p} \chi \left(\frac{(u + t_1) \cdots (u + t_r)}{(u + t_{r+1}) \cdots (u + t_{2r})} \right) \right|^2 \\ &\leq p^2 |I|^r r^{2r} + Cr^2 p |I|^{2r}, \end{aligned} \quad (3.22)$$

so that the second factor in (3.17) is bounded by

$$Crp^{\frac{1}{r}} |I|^{\frac{1}{2}} + Cp^{\frac{1}{2r}} |I|. \quad (3.23)$$

Applying (3.14) and collecting estimates (3.16), (3.17), (3.21), (3.23) and assumption (a), we bound (3.15) by

$$\begin{aligned} \left| \sum_{x \in A, y \in B} \chi(x + y) \right| &< C |A| |B| |I|^{-\frac{1}{2}} (|A|^{-\frac{1}{2}} |B|^{-\frac{5}{8}} p^{2d\delta})^{\frac{1}{2r}} (\sqrt{r} p^{\frac{1}{2r}} |I|^{\frac{1}{4}} + p^{\frac{1}{4r}} |I|^{\frac{1}{2}}) \\ &< C \sqrt{r} |A| |B| (p^{-(\frac{4}{9} + \varepsilon) \frac{9}{8} + 2d\delta})^{\frac{1}{2r}} (p^{\frac{1}{2r} - \frac{\delta}{4}} + p^{\frac{1}{4r}}) \\ &< C \sqrt{r} |A| |B| (p^{\frac{1}{2} - \frac{9}{8}\varepsilon + 2d\delta - \frac{\delta}{2}r} + p^{-\frac{9}{8}\varepsilon + 2d\delta})^{\frac{1}{2r}}. \end{aligned} \quad (3.24)$$

Recall (3.12). The theorem follows by taking $\tau(\varepsilon) = \frac{\varepsilon^2}{128K}$ \square .

§4. The case of an interval.

We begin with the following technical lemma.

Lemma 7. *Let $A = \mathcal{D} + I \subset \mathbb{F}_p^*$, where $I = [0, p^\beta]$ is an interval and \mathcal{D} is a p^β -spaced set (mod p) with $|\mathcal{D}| = p^\sigma$. Let I_1, \dots, I_s be intervals, $I_i = [1, p^{\beta_i}]$, and $k_1, \dots, k_s \in \mathbb{Z}_+$ such that*

$$\beta + k_i \beta_i \leq 1, \text{ for } i = 1, \dots, s. \quad (4.1)$$

Denote

$$w(u) = \left| \left\{ (y, z_1, \dots, z_s) \in A \times I_1 \times \dots \times I_s : y \equiv uz_1 \dots z_s \pmod{p} \right\} \right|. \quad (4.2)$$

Then

$$\sum_u w(u)^2 < p^{\sigma\gamma + \frac{\varepsilon}{\log \log p}} |A| |I_1| \dots |I_s|, \quad (4.3)$$

where

$$\gamma = \frac{1}{k_1} + \dots + \frac{1}{k_s}.$$

Proof. Using multiplicative characters and Plancherel, we have

$$\sum_u w(u)^2 = \frac{1}{p-1} \sum_\chi \langle w, \chi \rangle^2,$$

where

$$\langle w, \chi \rangle = \sum_u w(u) \overline{\chi(u)} = \sum_{\substack{y \in A \\ z_i \in I_i}} \overline{\chi(y)} \chi(z_1) \dots \chi(z_s).$$

Hence

$$|\langle w, \chi \rangle| = \left| \sum_{y \in A} \chi(y) \right| \prod_i \left| \sum_{z_i \in I_i} \chi(z_i) \right|.$$

Using generalized Hölder inequality with $1 = (1 - \gamma) + \frac{1}{k_1} + \dots + \frac{1}{k_s}$, we have

$$\begin{aligned} & \sum_u w(u)^2 \\ &= \frac{1}{p-1} \sum_\chi \left| \sum_{y \in A} \chi(y) \right|^2 \prod_i \left| \sum_{z_i \in I_i} \chi(z_i) \right|^2 \\ &\leq \left(\frac{1}{p-1} \sum_\chi \left| \sum_{y \in A} \chi(y) \right|^2 \right)^{1-\gamma} \prod_i \left(\frac{1}{p-1} \sum_\chi \left| \sum_{y \in A} \chi(y) \right|^2 \left| \sum_{z \in I_i} \chi(z) \right|^{2k_i} \right)^{\frac{1}{k_i}} \end{aligned} \quad (4.4)$$

Note that in (4.4),

$$\frac{1}{p-1} \sum_{\chi} \left| \sum_{y \in A} \chi(y) \right|^2 = |A|. \quad (4.5)$$

To estimate $\frac{1}{p-1} \sum_{\chi} \left| \sum_{y \in A} \chi(y) \right|^2 \left| \sum_{z \in I_i} \chi(z) \right|^{2k_i}$, we write $A = \cup_{t \in \mathcal{D}} (I + t)$. Then

$$\left| \sum_{y \in A} \chi(y) \right|^2 \leq |\mathcal{D}| \sum_{t \in \mathcal{D}} \left| \sum_{y \in I+t} \chi(y) \right|^2 \leq |\mathcal{D}|^2 \left| \sum_{y \in J} \chi(y) \right|^2, \quad (4.6)$$

where $J = I + t$ is some translate of I .

Fixing $i = 1, \dots, s$ and $k = k_i$, we have

$$\begin{aligned} & \frac{1}{p-1} \sum_{\chi} \left| \sum_{y \in A} \chi(y) \right|^2 \left| \sum_{z \in I_i} \chi(z) \right|^{2k} \\ & \leq p^{2\sigma} \left| \left\{ (y, y', z_1, \dots, z_k, z'_1, \dots, z'_k) \in J^2 \times I_i^{2k} : yz_1 \cdots z_k \equiv y'z'_1 \cdots z'_k \pmod{p} \right\} \right| \\ & \leq p^{2\sigma + \frac{c}{\log \log p}} \left| \left\{ (y, y', z, z') \in J^2 \times [1, p^{k\beta_i}]^2 : yz \equiv y'z' \pmod{p} \right\} \right| \\ & < p^{2\sigma + \beta + k\beta_i + \frac{c}{\log \log p}}. \end{aligned} \quad (4.7)$$

Here we use (4.6), (4.1) and the estimate $E(J, J')$ for intervals $J, J' \subset \mathbb{F}_p$ with $|J| |J'| \leq p$. (See [FI].) Substituting (4.5) and (4.7) in (4.4) gives (4.3). \square

Next we consider the sum

$$\sum_{x \in I, y \in \mathcal{D}} \chi(x + y), \quad (4.8)$$

where $I \subset \mathbb{F}_p$ is an interval with $|I| = p^\beta$ and \mathcal{D} is p^β -spaced modulo p . Such sums were estimated in [FI]. In particular, Theorem 2' of [FI] gives a non-trivial estimate for (4.8) under the following assumptions

(*) \mathcal{D} lies in an interval of length D . Moreover, for some $r \in \mathbb{Z}_+$ and $\varepsilon > 0$

$$|I|D < p^{1 + \frac{1}{2r}} \quad \text{and} \quad |I||\mathcal{D}|^{\frac{1}{2}} > p^{\frac{1}{4} + \frac{1}{4r} + \varepsilon}. \quad (4.9)$$

Note that if we do not specify \mathcal{D} to be contained in an interval of size D , (hence $D = p$), the restriction (4.9) forces I and \mathcal{D} to satisfy

$$|\mathcal{D} + I| \sim |I||\mathcal{D}| > p^{\frac{1}{2} + 2\varepsilon}, \quad (4.10)$$

which can be dealt with in an elementary way.

Theorem 8. Let $I \subset \mathbb{F}_p$ be an interval with $|I| = p^\beta$ and let $\mathcal{D} \subset \mathbb{F}_p$ be a p^β -spaced set with $|\mathcal{D}| = p^\sigma$. Assume

$$2\beta + \sigma - \frac{\beta\sigma}{1-\beta} > \frac{1}{2} + \delta \quad (4.11)$$

for some $\delta > 0$. Then

$$\left| \sum_{x \in I, y \in \mathcal{D}} \chi(x+y) \right| < p^{-\frac{\delta^2}{12}} |I| \cdot |\mathcal{D}| \quad (4.12)$$

for a non-principal multiplicative character χ .

Proof. Let

$$\tau = \frac{\delta}{6}, \quad I_0 = [1, p^\tau], \quad (4.13)$$

and

$$R = \left\lfloor \frac{1}{2\tau} \right\rfloor. \quad (4.14)$$

Choose $k_1, \dots, k_s \in \mathbb{Z}_+$ such that

$$2\tau < \beta - (1-\beta)\gamma < 3\tau, \quad \text{where } \gamma = \sum_i \frac{1}{k_i}. \quad (4.15)$$

Set

$$\beta_i = \frac{1-\beta}{k_i}, \quad \text{and } I_i = [1, p^{\beta_i}] \quad (1 \leq i \leq s), \quad (4.16)$$

so that (4.1) is satisfied. Let $A = \mathcal{D} + I$. For any $z_0 \in I_0, \dots, z_s \in I_s$, we have

$$\sum_{x \in A} \chi(x) = \sum_{x \in A} \chi(x + z_0 z_1 \dots z_s) + O(|\mathcal{D}| p^{\tau + \beta_1 + \dots + \beta_s}). \quad (4.17)$$

Hence, by (4.15) and (4.16),

$$\begin{aligned} \left| \sum_{x \in A} \chi(x) \right| &= p^{-\tau - \beta_1 - \dots - \beta_s} \left| \sum_{\substack{x \in A \\ z_0 \in I_0, \dots, z_s \in I_s}} \chi(x + z_0 z_1 \dots z_s) \right| + O(|A| p^{-\tau}) \\ &= p^{-\tau - \beta_1 - \dots - \beta_s} \sum_u w(u) \left| \sum_{z \in I_0} \chi(u + z) \right| + O(|A| p^{-\tau}), \end{aligned} \quad (4.18)$$

where $w(u)$ is defined in (4.2).

By Hölder inequality, Fact 5 and Weil's estimate (cf (2.16)), the first term of (4.18) is bounded by

$$\begin{aligned} & p^{-\tau-\beta_1-\dots-\beta_s} \left(\sum_u w(u)^{\frac{2R}{2R-1}} \right)^{1-\frac{1}{2R}} \left(\sum_u \left| \sum_{z \in I_0} \chi(u+z) \right|^{2R} \right)^{\frac{1}{2R}} \\ & \leq p^{-\tau-\beta_1-\dots-\beta_s} \left[\sum_u w(u) \right]^{1-\frac{1}{R}} \left[\sum_u w(u)^2 \right]^{\frac{1}{2R}} \left(R|I_0|^{\frac{1}{2}} p^{\frac{1}{2R}} + 2|I_0| p^{\frac{1}{4R}} \right). \end{aligned} \quad (4.19)$$

Since $\sum w(u) = |A|p^{\beta_1+\dots+\beta_s}$ and $\sum w(u)^2$ is bounded by (4.3), we obtain the estimate (4.12) from our assumption (4.11) and the parameters chosen. \square

Remark 8.1 For $k \geq 2$, we denote by $\tau_k(n)$ the number of solutions of the equation $n = n_1 \cdots n_k$ with $n_i \in \mathbb{Z}_+$. From Theorem 8 and following the argument of [Kar3] and [Kar4], one may obtain new estimates on character sums of the form $\sum_{n \leq x} \tau_2(n) \chi(a+n)$ and more generally $\sum_{n \leq x} \tau_k(n) \chi(a+n)$. In [Kar3], nontrivial estimates are obtained assuming $x > p^{\frac{1}{2}+\delta}$ for arbitrary a with $(a, p) = 1$. Under the restriction $0 < |a| \leq \sqrt{p}$, the paper [Kar4] establishes nontrivial bounds under the weaker condition $x > p^{\frac{1}{2}-\frac{1}{2(k+1)}+\delta}$. From Theorem 8, we get for arbitrary a with $(a, p) = 1$, a nontrivial bound provided $x > p^{\rho_k+\delta}$, where $4\rho_k = k + \frac{3}{2} - \sqrt{k^2 - k + \frac{9}{4}}$. (In particular, $\rho_2 = \frac{1}{8}(7 - \sqrt{17}) = 0.359 \dots$) Details and related results will appear elsewhere.

Finally we establish some improvement over Karacuba's theorem [Ka1]. Recall the statement of [Ka1]. Let $I \subset [1, p]$ be an interval with $|I| = p^\beta$ and $S \subset [1, p]$ be an arbitrary set with $|S| = p^\alpha$. If for some $\varepsilon > 0$

$$\alpha > \varepsilon, \beta > \varepsilon \text{ and } \alpha + 2\beta > 1 + \varepsilon, \quad (4.20)$$

then for some $\varepsilon' > 0$

$$\sum_{y \in I} \left| \sum_{x \in S} \chi(x+y) \right| < p^{-\varepsilon'} |I| |S|. \quad (4.21)$$

We will prove the following

Theorem 9. *In the above setting, assume that α, β satisfy*

$$\varepsilon < \beta \leq \frac{1}{k} \text{ and } \left(3 - \frac{4}{k} \right) \alpha + 2\beta > \frac{3}{2} - \frac{1}{k}. \quad (4.22)$$

for some $\varepsilon > 0$ and $k \in \mathbb{Z}_+$. Then (4.21) holds for some $\varepsilon' = \varepsilon'(\varepsilon) > 0$.

To see the strength of Theorem 9, for example, we take $\alpha = \beta$, and let $k = 3$, then estimate (4.21) is valid, provided

$$\alpha, \beta > \frac{7}{22} + \varepsilon$$

which is a slight improvement over the condition $\alpha, \beta > \frac{1}{3}$ gotten from [Ka1].

The proof of Theorem 9 is a combination of variants of arguments used in [FI] (Theorem 3) and [Ka2], together with the following

Lemma 7'. *Let $I = [0, p^{\frac{1}{k}}]$ be an interval with $k \in \mathbb{Z}_+$ and $k \geq 2$, and let $A = \mathcal{D} + I$, where $\mathcal{D} \subset \mathbb{F}_p$ is a $p^{\frac{1}{k}}$ -spaced set. Then*

$$E(A, I) < p^{\frac{4}{\log \log p}} |\mathcal{D}|^{\frac{1}{k-1}} |I| |A|. \quad (4.23)$$

The proof of Lemma 7' follows from Lemma 7, applied with $\beta = \frac{1}{k}, s = 1, k_1 = k - 1, \beta_1 = \frac{1}{k}$. (Hence $I = I_1$.)

Proof of Theorem 9.

Take $\beta_1 = \beta - \tau$ with $\tau > 0$ and $\tau = o(1)$.

We partition $[1, p]$ in intervals I_j of size p^{β_1} and consider the intersections $S \cap I_j$. Up to a factor of $\log p$, one may clearly replace S by sets of the form

$$S = \bigcup_{\xi_r \in \mathcal{D}} (\xi_r + S_r), \quad (4.24)$$

where \mathcal{D} is a p^{β_1} -spaced set with $|\mathcal{D}| = p^\gamma$ and $S_r \subset [0, p^{\beta_1}]$ satisfying $|S_r| \sim p^{\beta_1 - \sigma}$ (for some σ independent of r) and $|\mathcal{D}| \cdot p^{\beta_1 - \sigma} > p^{-o(1)} |S|$. Hence

$$\alpha \geq \gamma + \beta_1 - \sigma > \alpha - o(1). \quad (4.25)$$

We will carry out two estimates.

Case 1. $\alpha + \beta - \sigma - \frac{\gamma}{k-1} > \frac{1}{2} + \delta$ for some $\delta > 0$.

We assume $\sigma < \beta_1 - \tau$ (more restrictive conditions will appear later).

By (4.24) and Cauchy-Schwarz, we have

$$\begin{aligned} \sum_{y \in I} \left| \sum_{x \in S} \chi(x + y) \right| &\leq \sum_{\xi_r \in \mathcal{D}} \sum_{y \in I} \left| \sum_{x \in S_r} \chi(\xi_r + x + y) \right| \\ &\leq |\mathcal{D}|^{\frac{1}{2}} |I|^{\frac{1}{2}} \left| \sum_{\xi_r \in \mathcal{D}, y \in I, x_1, x_2 \in S_r} \chi \left(\frac{\xi_r + x_1 + y}{\xi_r + x_2 + y} \right) \right|^{\frac{1}{2}}. \end{aligned}$$

It will suffice to establish a non-trivial bound on the inner sum

$$\sum_{\substack{\xi_r \in \mathcal{D}, y \in I \\ x_1 \neq x_2 \in S_r}} \chi\left(1 + \frac{x_1 - x_2}{\xi_r + x_2 + y}\right). \quad (4.26)$$

Denote V the interval $[0, p^{\frac{\tau}{2}}]$. We recall that $x_1 - x_2 \in [-p^{\beta-\tau}, p^{\beta-\tau}]$. After fixing r and $x_1, x_2 \in S_r$ in the summation (4.26), we may translate $y \in I$ by a product $t \cdot (x_1 - x_2)$ with $t \in V$. The error is $O(p^{-\frac{\tau}{2}} |I| (\sum_{\mathcal{D}} |S_r|^2))$.

Hence we obtain

$$\frac{1}{|V|} \sum_{\substack{\xi_r \in \mathcal{D}, y \in I, t \in V \\ x_1 \neq x_2 \in S_r}} \chi\left(1 + \frac{1}{\frac{\xi_r + y + x_2}{x_1 - x_2} + t}\right),$$

which we bound by

$$\frac{1}{|V|} \sum_{u \in \mathbb{F}_p} \eta(u) \left| \sum_{t \in V} \chi\left(1 + \frac{1}{u + t}\right) \right|. \quad (4.27)$$

Here

$$\eta(u) = \left| \left\{ (\xi_r, y, x_1, x_2) \in \mathcal{D} \times I \times S_r^2 : x_1 \neq x_2 \text{ and } u = \frac{\xi_r + y + x_2}{x_1 - x_2} \right\} \right|.$$

Under the assumption of the case, we claim

$$\left(\sum_u \eta(u) \right)^2 > p^{\frac{1}{2} + \delta} \left(\sum_u \eta(u)^2 \right). \quad (4.28)$$

It is obvious from the construction that

$$\sum_u \eta(u) \sim |\mathcal{D}| \cdot |I| \cdot p^{2(\beta_1 - \sigma)} \sim p^{\beta + \gamma + 2(\beta_1 - \sigma)}. \quad (4.29)$$

Also

$$\begin{aligned} & \sum_u \eta(u)^2 \\ &= \left| \left\{ (\xi_r, \xi_{r'}, y, y', x_1, x_2, x'_1, x'_2) : x_1 \neq x_2, x'_1 \neq x'_2 \text{ and } \frac{\xi_r + y + x_2}{x_1 - x_2} = \frac{\xi_{r'} + y' + x'_2}{x'_1 - x'_2} \right\} \right| \\ &\leq p^{2(\beta_1 - \sigma)} \left| \left\{ (\xi_r, \xi_{r'}, \bar{y}, \bar{y}', z, z') \in \mathcal{D}^2 \times [0, 2p^\beta]^2 \times [-p^{\beta_1}, p^{\beta_1}]^2 : \frac{\xi_r + \bar{y}}{z} = \frac{\xi_{r'} + \bar{y}'}{z'} \right\} \right| \\ &= p^{2(\beta_1 - \sigma)} E(\mathcal{D} + [0, 2p^\beta], [-p^{\beta_1}, p^{\beta_1}]). \end{aligned}$$

Applying Lemma 7' with $A = \mathcal{D} + [0, 2p^\beta]$ and $I = [0, 2p^{\beta_1}]$ where $\beta_1 < \beta \leq \frac{1}{k}$, we get

$$E(A, I) < p^{\beta + \beta_1 + (1 + \frac{1}{k-1})\gamma + o(1)}. \quad (4.30)$$

Hence

$$\sum_u \eta(u)^2 < p^{\beta + 3\beta_1 - 2\sigma + (1 + \frac{1}{k-1})\gamma + o(1)}. \quad (4.31)$$

and (4.28) holds by (4.29), (4.31) and recalling (4.25).

We follow the usual procedure (e.g. see the bounding of (4.11)), we have the bound $|I| |S| p^{-\frac{\delta^2}{4}}$.

Note that since we may assume $\alpha < \frac{1}{2} + o(1)$, the condition $\sigma < \beta_1 - \tau$ for τ small enough, is automatically satisfied under the assumption of this case.

Case 2. $2\alpha + \beta + \sigma - \frac{\gamma}{k-1} > 1 + \delta$ for some $\delta > 0$.

Since

$$\sum_{y \in I} \left| \sum_{x \in S} \chi(x + y) \right| \leq |I|^{\frac{1}{2}} \left| \sum_{\substack{x_1, x_2 \in S \\ y \in I}} \chi\left(\frac{x_1 + y}{x_2 + y}\right) \right|^{\frac{1}{2}},$$

we need a nontrivial estimate on

$$\sum_{\substack{x_1, x_2 \in S \\ y \in I}} \chi\left(\frac{x_1 + y}{x_2 + y}\right).$$

Making a translation $y \rightarrow y + zt$ with $z \in [1, p^{\beta_1}] = I_1, t \in V = [0, p^{\frac{\tau}{2}}]$ leads to

$$\frac{1}{|V|} \sum_{u_1, u_2 \in \mathbb{F}_p} \eta(u_1, u_2) \left| \sum_{t \in V} \chi\left(\frac{u_1 + t}{u_2 + t}\right) \right|, \quad (4.32)$$

where

$$\eta(u_1, u_2) = \left| \left\{ (x_1, x_2, y, z) \in S^2 \times I \times I_1 : u_i = \frac{x_i + y}{z}, \text{ for } i = 1, 2 \right\} \right|.$$

Let $\eta(u) = \eta(u_1, u_2)$. We will show that the assumption of this case implies

$$\left(\sum_u \eta(u) \right)^2 > p^{1+\delta} \left(\sum_u \eta(u)^2 \right). \quad (4.33)$$

Here

$$\sum_u \eta(u) = p^{2\alpha + \beta + \beta_1}.$$

Clearly, using the bound (4.30), we have

$$\begin{aligned}
& \sum_u \eta(u)^2 \\
&= \left| \left\{ (x_1, x_2, x'_1, x'_2, y, y', z, z') \in S^4 \times I^2 \times I_1^2 : \frac{x_i + y}{z} = \frac{x'_i + y'}{z'}, i = 1, 2 \right\} \right| \\
&\leq |S| \left| \left\{ (x, x', y, y', z, z') \in S^2 \times I^2 \times I_1^2 : \frac{x + y}{z} = \frac{x' + y'}{z'} \right\} \right| \\
&< p^\alpha \left| \left\{ (\xi_r, \xi_{r'}, x, x', y, y', z, z') \in \mathcal{D}^2 \times S^2 \times I^2 \times I_1^2 : \frac{\xi_r + x + y}{z} = \frac{\xi_{r'} + x' + y'}{z'} \right\} \right| \\
&< p^\alpha p^{2(\beta_1 - \sigma)} E(\mathcal{D} + [0, 2p^\beta], [0, p^{\beta_1}]) \\
&< p^{\alpha + \beta + 3\beta_1 - 2\sigma + (1 + \frac{1}{k-1})\gamma + o(1)}.
\end{aligned}$$

Proceeding in the same way as before, we obtain the bound $|I| |S| p^{-\frac{1}{2}(\frac{\delta^2}{2} - \beta_1)}$.

To reach condition (4.22), we assume Case 1 fails. Hence

$$\alpha + \beta - \sigma - \frac{\gamma}{k-1} < \frac{1}{2} + o(1)$$

and recalling (4.25), i.e.

$$\alpha + o(1) > \gamma + \beta - \sigma > \alpha - o(1)$$

(letting τ be small enough), it follows that

$$\left(1 + \frac{1}{k-1}\right)\sigma > \left(1 - \frac{1}{k-1}\right)\alpha + \left(1 + \frac{1}{k-1}\right)\beta - \frac{1}{2} - o(1).$$

Therefore the assumption of Case 2 will be satisfied if

$$\left(3 - \frac{4}{k}\right)\alpha + 2\beta > \frac{3}{2} - \frac{1}{k}.$$

This proves Theorem 9.

Acknowledgement. The author is grateful to Andrew Granville for removing some additional restriction on the set B in Theorem 2 in an earlier version of the paper, and to the referees for many helpful comments. The author would also like to thank J. Bourgain and Nick Katz for communication on Proposition \clubsuit , and Gwoho Liu for assistance.

REFERENCES

- [BGK]. J. Bourgain, A. Glibichuk, S. Konyagin, *Estimate for the number of sums and products and for exponential sums in fields of prime order*, submitted to J. London Math. Soc 73 (2006), 380-398.
- [BKT]. J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields and their applications*, GAFA 14 (2004), n1, 27–57.
- [Bu1]. D.A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc (3) 12 (1962), 179-192.
- [Bu2]. ———, *On primitive roots in finite fields*, Quarterly J. of Math., 8 (1937), 308-312.
- [Bu3]. ———, *Character sums and primitive roots in finite fields*, Proc. London Math. Soc (3) 37 (1967), 11-35.
- [Bu4]. ———, *A note on character sums over finite fields*, J. Reine Angew. Math. 255 (1972), 80-82.
- [DL]. Davenport, D. Lewis, *Character sums and primitive roots in finite fields*, Rend. Circ. Matem. Palermo-Serie II-Tomo XII-Anno (1963), 129-136.
- [FI]. J. Friedlander, H. Iwaniec, *Estimates for character sums*, Proc. Amer. Math. Soc. 119, No 2, (1993), 265-372.
- [G]. M. Garaev, *An explicit sum-product estimate in \mathbb{F}_p* , (preprint).
- [HIS]. D. Hart, A. Iosevich, J. Solymosi, *Sum product estimates in finite fields via Kloosterman sums*, IMRN (to appear).
- [IK]. H. Iwaniec, E. Kowalski, *Analytic number theory*, AMS Colloquium Publications, Vol 53 (2004).
- [Kar1]. A.A. Karacuba, *Distribution of values of Dirichlet characters on additive sequences*, Soviet Math. Dokl. 44 (1992), no. 1, 145–148.
- [Kar2]. ———, *Estimates of character sums*, Math. USSR-Izvestija Vol. 4 (1970), No. 1, 19-29.
- [Kar3]. ———, *A certain arithmetic sum*, Soviet Math Dokl, 12 (1971), No. 4, 1172-1174.
- [Kar4]. ———, *Character sums with weights*, Izv. Math. 64 (2) (2000), 249-263.
- [KS1]. Nets Katz, C-Y. Shen, *A slight improvement of Garaev’s sum product estimate*, (preprint).
- [KS2]. ———, *Garaev’s inequality in finite fields not of prime order*, (preprint).
- [K]. Nick Katz, *An estimate for character sums*, JAMS Vol 2, No 2 (1989), 197-200.
- [PS]. G.I. Perel’muter, I. Shparlinski, *Distribution of primitive roots in finite fields*, Russian Math. Surveys 45 (1990), no. 1, 223–224.
- [TV]. T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.