# ON A QUESTION OF DAVENPORT AND LEWIS ON CHARACTER SUMS AND PRIMITIVE ROOTS IN FINITE FIELDS

Mei-Chu Chang

Abstract.

Let $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_{p^n}$. We obtain the following results related to Davenport-Lewis' paper [DL] and the Paley Graph conjecture.

(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

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

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

As a corollary, we bound the number of primitive roots in $B$ by

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

(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

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

**Introduction.**

In this paper we obtain new character 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

$$\xi = x_1\omega_1 + \ldots + x_n\omega_n, \qquad (0 \le x_i < p). \tag{0.1}$$

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

$$N_j + 1 \le x_j \le N_j + H_j, \qquad (j = 1, \dots, n) \tag{0.2}$$

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

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

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

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

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

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

For $n = 1$ (i.e. $\mathbb{F}_q = \mathbb{F}_p$) we are recovering 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**[1]**.** *Let $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_{p^n}$, and let $\varepsilon > 0$ be given. If*

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

*is a box satisfying*

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

*then for $p > p(\varepsilon)$*

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

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

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

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 [Kar]).

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

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

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' was indeed obtained (see [Bu3] and [Kar]) by reducing the combinatorial problem to counting divisors in the 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. We only mention the following consequence of Theorem 2 to the problem of primitive roots (see for instance [DL], p131).

---

[1] The author is grateful to Andrew Granville for removing some additional restriction on the set $B$ in an earlier version of this theorem.

**Corollary 3.** *Let $B \subset \mathbb{F}_{p^n}$ be as in Theorem 2 and satisfying* $\max_\xi \big|B \cap \xi F_2\big| < p^{-\varepsilon}|B|$ *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 $n \ll \log\log p$.*

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

$$\Big|\sum_{x\in A}\chi(x)\Big|, \tag{0.5}$$

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

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

$$|B+B| < c(n)|B| \tag{0.6}$$

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 nontrivial multiplicative character of $\mathbb{F}_p$, we have*

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

*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

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

where $\chi$ is a nontrivial 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 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

**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*

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

*where $\tau = \tau(\varepsilon, K) > 0$, $p > p(\varepsilon, K)$ and $\chi$ is a nontrivial multiplicative character of $\mathbb{F}_p$.*

This result may be compared with those obtained in [FI] on estimating (0.7) assuming the sets $A, B$ have certain extra structure (for instance, assuming $A = B$ is a large subset of an interval). We also consider the case when $B$ is an interval, in which case we can obtain a stronger result. (See Theorem 8.)

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, Corollary 3 in §3 and Theorem 6 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

$$E(A, B) = \Big|\big\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : a_1 b_1 = a_2 b_2\big\}\Big|. \tag{1.1}$$

(See [TV] p.61.)

We will use the following

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

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

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

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

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

*Then we have*

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

*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]. (See also [G].)

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

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

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

**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 $t\Sigma x_j\omega_j = \Sigma y_j\omega_j$ for some $x_j, y_j \in [-H_j, H_j]$, where $1 \leq j \leq n$ and $\Sigma x_j\omega_j \neq 0$. Since $tx_j = y_j$ for all $j = 1, \dots, n$, choosing $i$ such that $x_i \neq 0$, it follows that

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

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*

$$|aB \cap b_0 B| \sim N \text{ for all } a \in A_1, \tag{1.5}$$

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

*and*

$$\frac{A_1 - A_1}{A_1 - A_1} + 1 \neq \frac{A_1 - A_1}{A_1 - A_1}. \tag{1.7}$$

*Proof of Claim 2.*

F rom (1.1)

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

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

$$\sum_{a\in B} |aB \cap b_0 B| \geq \frac{E(B,B)}{|B|}.$$

Let $A_s$ be the level set

$$A_s = \{a \in B : 2^{s-1} \le |aB \cap b_0 B| < 2^s\}.$$

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

$$2^{s_0}\ |A_{s_0}|\ \log_2 |B| \ge \sum_{s=0}^{\log_2 |B|} 2^s |A_s| > \sum_{a\in B} |aB \cap b_0 B| \ge \frac{E(B,B)}{|B|}.$$

(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

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

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 $c_1, c_2, d_1, d_2 \in A_1, d_1 \ne d_2$, such that

$$\xi = \frac{c_1 - c_2}{d_1 - d_2} + 1 \not\subset \frac{A_1 - A_1}{A_1 - A_1}.$$

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

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

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)

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

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

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

Facts 2, 4 and (1.5) imply

$$2^{-2}|A_1|^3 \le 2^{n+2}|B|\frac{|B+B|^8}{N^4\ |B|^3}. \tag{1.12}$$

Thus

$$N^4|A_1|^3 \le 2^{9n+4}|B|^6 \tag{1.13}$$

and recalling (1.6)

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

implying (1.3). $\square$

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

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

**Theorem 2.** *Let $\chi$ be a nontrivial 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 $p > p(\varepsilon)$*

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

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

$$\Big|\sum_{x\in B}\chi(x)\Big| \le \max_\xi\big|B\cap\xi F_2\big| + O_n(p^{-\tau}|B|).$$

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

**Theorem 2'.** *Let* $\chi$ *be a nontrivial 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* $p > p(\varepsilon)$

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

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

**Theorem W.** *Let* $\chi$ *be a nontrivial 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*

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

*Proof of Theorem 2'.*

By breaking up $B$ in smaller boxes, we may assume

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

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

$$I = [1, p^{\delta}] \tag{2.4}$$

and

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

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

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

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

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

Estimate

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

where

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

Observe that

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

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

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

$$\Big| r - \frac{n}{\varepsilon} \Big| \leq \frac{1}{2}. \tag{2.10}$$

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

$$\Big(\sum_{u\in\mathbb{F}_{p^n}} \omega(u)^{\frac{2r}{2r-1}}\Big)^{1-\frac{1}{2r}}\Big(\sum_{u\in\mathbb{F}_{p^n}} \big|\sum_{z\in I}\chi(u+z)\big|^{2r}\Big)^{\frac{1}{2r}}. \tag{2.11}$$

Since $\sum\omega(u)=|B_0|\cdot|B|$ and (2.9) holds, we have

$$\begin{aligned}\Big(\sum_{u} \omega(u)^{\frac{2r}{2r-1}}\Big)^{1-\frac{1}{2r}} &\le\Big[\sum\omega(u)\Big]^{1-\frac{1}{r}}\Big[\sum\omega(u)^2\Big]^{\frac{1}{2r}}\\ &<2^{(\frac{9}{4}n+1)\frac{1}{2r}}\Big(|B_0|\cdot|B|\Big)^{1-\frac{1}{r}}\Big(|B|\Big)^{\frac{11}{8r}}(\log\ p)\,p^{-\frac{11}{8}\frac{n}{r}\delta}.\end{aligned} \tag{2.12}$$

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.** $(\sum_{u} f(u)^{\frac{2r}{2r-1}})^{1-\frac{1}{2r}}\le[\sum f(u)]^{1-\frac{1}{r}}[\sum f(u)^2]^{\frac{1}{2r}}$.

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

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

Let

$$q=p^n.$$

Write

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

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 that $2r$ many distinct roots, Theorem W gives

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

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 $\sum|\sum_{u\in\mathbb{F}_q}\chi(f_{z_1,\dots,z_{2r}}(u))|$ 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

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

and

$$\Big(\sum_{u\in\mathbb{F}_{p^n}} \Big|\sum_{z\in I}\chi(u+z)\Big|^{2r}\Big)^{\frac{1}{2r}} \le r|I|^{\frac{1}{2}} p^{\frac{n}{2r}} + 2|I|p^{\frac{n}{4r}}. \tag{2.16}$$

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

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

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

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

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

Then by (2.10),

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

and

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

Returning to (2.6), we have

$$\Big|\sum_{x\in B}\chi(x)\Big| < cn\varepsilon^{-1}(\log\ p)p^{-\frac{25}{98}\varepsilon^2}|B| < np^{-\frac{\varepsilon^2}{4}}|B| \tag{2.19}$$

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 a result of Nick Katz.

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

Let $H_1 \geq H_2 \geq \cdots \geq H_n$. 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 $B_\alpha$, we have

$$\Big|\sum_{x\in B_\alpha}\chi(x)\Big| < cnp^{-\tau}|B_\alpha|.$$

Hence

$$\Big|\sum_{x\in B}\chi(x)\Big| < cnp^{-\tau}|B|.$$

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

Next we recall some results of Nick Katz.

**Proposition K1.** ([K1]) *Let $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_q$ and let $g \in \mathbb{F}_q$ be a generating element, i.e. $\mathbb{F}_q = \mathbb{F}_p(g)$. Then*

$$\big|\sum_{t\in\mathbb{F}_p}\chi(g+t)\big| \leq (n-1)\sqrt{p} \tag{2.21}$$

It was pointed out by N. Katz that a similar result remains valid when an extra additive character appears.

**Proposition K2.** ([K2]) *Under the same assumption as Proposition K1. We have*

$$\max_a\big|\sum_{t\in\mathbb{F}_p}e_p(at)\ \chi(g+t)\big| \leq c(n)\sqrt{p}. \tag{2.22}$$

Following a standard argument, we may restate Proposition K2 for incomplete sums.

**Proposition K3.** *Under the same assumption as Proposition K1. For any integral interval* $I \subset [1,p]$,

$$\Big|\sum_{t\in I}\chi(g+t)\Big| \le c(n)\sqrt{p}\ \log p \tag{2.23}$$

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

*Proof of Proposition K3.* Let $\mathbb{I}_I$ be the indicator function of $I$. Write $\mathbb{I}_I(t) = \sum_a \widehat{\mathbb{I}_I}(a)e_p(at)$. Then $\sum_a |\widehat{\mathbb{I}_I}(a)| \le c\log p$. Hence

$$\Big|\sum_{t\in I}\chi(g+t)\Big| \le \Big|\sum_a |\widehat{\mathbb{I}_I}(a)| \sum_{t\in\mathbb{F}_p}\chi(g+t)e_p(at)\Big| \le c(n)\sqrt{p}\ \log p$$

by Proposition K2. □

*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)

$$\Big|\sum_{x\in B}\chi(x)\Big| = \Big|\sum_{\substack{x_i\in I_i\\ 2\le i\le n}}\sum_{x_1\in I_1}\chi\Big(x_1+x_2\frac{\omega_2}{\omega_1}+\cdots+x_n\frac{\omega_n}{\omega_1}\Big)\Big| \le c(n)p^{\frac{1}{2}}\log p\frac{|B|}{H_1}+(*), \tag{2.24}$$

where

$$(*) = \Big|\sum_{x_1\in I_1}\sum_{(x_2,\dots,x_n)\in D}\chi\Big(x_1+x_2\frac{\omega_2}{\omega_1}+\cdots+x_n\frac{\omega_n}{\omega_1}\Big)\Big| \tag{2.25}$$

and

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

In particular,

$$(*) \le p\,|D| \le p\sum_G \Big|G\bigcap \operatorname{Span}_{\mathbb{F}_p}\Big(\frac{\omega_2}{\omega_1},\dots,\frac{\omega_n}{\omega_1}\Big)\Big|,$$

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

$$\dim_{\mathbb{F}_p}\Big(G\bigcap \operatorname{Span}_{\mathbb{F}_p}\Big(\frac{\omega_2}{\omega_1},\dots,\frac{\omega_n}{\omega_1}\Big)\Big) \le \frac{n}{3}-1. \tag{2.26}$$

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

$$\Big|\sum_{x\in B}\chi(x)\Big| < c(n)\Big((\log p)p^{-\frac{\varepsilon}{2}}|B| + p^{\frac{n}{3}}\Big)$$
$$< \Big(c(n)(\log p)p^{-\frac{\varepsilon}{2}} + p^{-\frac{n}{13}}\Big)\ |B|,$$

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

$$(*_2) = \Big|\sum_{x_1\in I_1}\ \sum_{(x_2,\dots,x_n)\in D_2}\chi\Big(x_1 + x_2\frac{\omega_2}{\omega_1} + \cdots + x_n\frac{\omega_n}{\omega_1}\Big)\Big| \tag{2.27}$$

with

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

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 $2\le j\le k$ and $\frac{\omega_j}{\omega_1}\notin F_2$ for $k+1\le j\le n$, where $k\le\frac{n}{2}$. We also assume that $H_{k+1}\le\dots\le H_n$. Fix $x_2,\dots,x_{n-1}$. Obviously there is no more than one value of $x_n$ such that $x_2\frac{\omega_2}{\omega_1}+\cdots+x_n\frac{\omega_n}{\omega_1}\in F_2$, since otherwise $(x_n - x_n')\frac{\omega_n}{\omega_1}\in F_2$ with $x_n\ne x_n'$ contradicting the fact that $\frac{\omega_n}{\omega_1}\notin F_2$.

Therefore,

$$|D_2| \le |I_2|\cdots|I_{n-1}| \tag{2.29}$$

and

$$(*_2) \le \frac{|B|}{H_n}. \tag{2.30}$$

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

$$H_{k+1}\cdots H_n \le p^{(n-k)\tau}. \tag{2.31}$$

Define

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

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

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

(We can assume $\tau < \frac{2}{15}$.)

Clearly, if $(x_2, \ldots, x_n) \in D_2$, then $z = x_{k+1} \frac{\omega_{k+1}}{\omega_1} + \cdots + x_n \frac{\omega_n}{\omega_1} \in F_2$. Assume $\chi|_{F_2}$ non-principal, it follows from the generalized Polya-Vinogradov inequality (proved as that of Proposition K3) and (2.32 ) that

$$\Big| \sum_{y \in B_2} \chi(y+z) \Big| \le (\log p)^{\frac{n}{2}} \max_{\psi} \Big| \sum_{x \in F_2} \psi(x) \chi(x) \Big| \le (\log p)^{\frac{n}{2}} \cdot |F_2|^{\frac{1}{2}} \le p^{-\frac{n}{13}} |B_2|, \tag{2.33}$$

where $\psi$ runs over all additive characters. Therefore, clearly

$$(*_2) \le H_{k+1} \cdots H_n p^{-\frac{n}{13}} |B_2| = p^{-\frac{n}{13}} |B| \tag{2.34}$$

providing the required estimate.

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

$$(*_2) = H_1 \cdot |D_2| = \Big| F_2 \cap \frac{1}{\omega} B \Big| \tag{2.35}$$

and

$$\Big| \sum_{x \in B} \chi(x) \Big| = \big| F_2 \cap B \big| + O_n(p^{-\tau} |B|). \tag{2.36}$$

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

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

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 $\infty$, the exponent $\frac{n}{2(n+1)}$ goes to $\frac{1}{2}$.

## §3. Distribution of primitive roots.

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

We denote the Euler function by $\phi$.

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

$$\frac{\varphi(p^n-1)}{p^n-1}|B|(1+o(p^{-\tau'})) \tag{3.1}$$

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

The deduction from Theorem 2 follows the argument of Burgess [Bu2]. We include it here for the readers' convenience.

*Proof.* Let $p_1, \dots, p_s$ be all the distinct primes of $p^n - 1$ and let $H_{p_i} < \mathbb{F}^*_{p^n}$ be the subgroup of order $|H_{p_i}| = \frac{p^n-1}{p_i}$. Then $\alpha$ is a primitive root of $\mathbb{F}_{p^n}$ if and only if $\prod(1 - \mathbb{I}_{H_{p_i}}(\alpha)) = 1$, where $\mathbb{I}_H$ is the indicator function of $H$.

Let

$$m = p_1 \cdots p_s.$$

Then

$$\begin{aligned}\prod(1-\mathbb{I}_{H_{p_i}}) &= \sum_{r\geq 0}(-1)^r \sum_{i_1<\cdots<i_r} \mathbb{I}_{H_{p_{i_1}}\cap\cdots\cap H_{p_{i_r}}}\\ &= \sum_{d|p^n-1} \mu(d)\, \mathbb{I}_{H_d}\\ &= \sum_{d|m}\mu(d)\,\mathbb{I}_{H_d}.\end{aligned}$$

Here $\mu$ is the Möbius function. (Recall that $\mu(d) = (-1)^r$, if $d$ is the product of $r$ distinct primes, $\mu(d) = 0$ otherwise.)

Observe that

$$\mathbb{I}_{H_d} \;=\; \frac{1}{d}\sum_{\chi^d=1}\chi \;=\; \frac{1}{d}\sum_{d_1|d}\;\sum_{\chi\in\mathcal{E}_{d_1}}\chi,$$

where $\chi$ is a multiplicative character and $\mathcal{E}_{d_1} = \{\chi : \operatorname{ord}(\chi) = d_1\}$.

Then

$$\begin{aligned}\sum_{d|m}\mu(d)\Big(\frac{1}{d}\sum_{d_1|d}\sum_{\chi\in\mathcal{E}_{d_1}}\chi\Big) &= \sum_{d_1|m}\frac{\mu(d_1)}{d_1}\Big(\sum_{\chi\in\mathcal{E}_{d_1}}\chi\Big)\Big(\sum_{r|\frac{m}{d_1}}\frac{\mu(r)}{r}\Big)\\ &=\frac{\phi(p^n-1)}{p^n-1}\sum_{d_1|m}\frac{\mu(d_1)}{\phi(d_1)}\Big(\sum_{\chi\in\mathcal{E}_{d_1}}\chi\Big)\\ &=\frac{\phi(p^n-1)}{p^n-1}\sum_{d_1|p^n-1}\frac{\mu(d_1)}{\phi(d_1)}\Big(\sum_{\chi\in\mathcal{E}_{d_1}}\chi\Big).\end{aligned}$$

The second identity is because

$$\sum_{r|\frac{m}{d_1}} \frac{\mu(r)}{r} = \prod_{p_i|\frac{m}{d_1}} \Big(1 - \frac{1}{p_i}\Big) = \frac{\phi(\frac{m}{d_1})}{\frac{m}{d_1}} = \frac{d_1}{\phi(d_1)} \frac{\phi(p^n-1)}{p^n-1}.$$

Let $k$ be the number of primitive roots of $\mathbb{F}_{p^n}$ in the box $B$. Then

$$\begin{aligned} k =& \frac{\phi(p^n-1)}{p^n-1} \sum_{a\in B} \sum_{d|p^n-1} \frac{\mu(d)}{\phi(d)} \big( \sum_{\chi\in\mathcal{E}_d} \chi(a)\big) \\ =& \frac{\phi(p^n-1)}{p^n-1} \Big( |B| + \sum_{\substack{d|p^n-1 \\ d>1}} \frac{\mu(d)}{\phi(d)} \big( \sum_{\chi\in\mathcal{E}_d} \sum_{a\in B} \chi(a)\big)\Big). \end{aligned}$$

Hence, by Theorem 2,

$$\begin{aligned} \Big| k - \frac{\phi(p^n-1)}{p^n-1} \, |B| \Big| &< \frac{\phi(p^n-1)}{p^n-1} \sum_{\substack{d|p^n-1 \\ d>1}} \frac{1}{\phi(d)} \phi(d) p^{-\tau} \, |B| \\ &< \frac{\phi(p^n-1)}{p^n-1} \, \exp\Big(\frac{\log p^n}{\log\log p^n}\Big) \, p^{-\tau} |B|. \qquad \square \end{aligned}$$

**Remark 3.1.** 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 (see [Bu3] when $n = 2$ and basis of the form $\omega_j = g^j$ with given $g$ generating $\mathbb{F}_{p^n}$, see [Bu4] and [Kar]).

## §4. 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).

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

$$\mathcal{P} = a_0 + \Big\{ \sum_{j=1}^{d} x_j a_j : x_j \in [0, N_j - 1] \Big\} \tag{4.1}$$

for some elements $a_0, a_1, \dots, a_d \in \mathbb{F}_p$. If the representation of elements of $\mathcal{P}$ in (4.1) 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

$$E(\mathcal{P}, \mathcal{P}) < c^d (\log\ p) |\mathcal{P}|^{11/4}. \tag{4.2}$$

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*

$$|\mathcal{P}| > p^{2/5+\varepsilon} \tag{4.3}$$

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

$$\Big| \sum_{x \in \mathcal{P}} \mathcal{X}(x) \Big| < p^{-\tau} |\mathcal{P}| \tag{4.4}$$

*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 (4.3) 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 $k < k(\varepsilon)$, 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

$$d \leq C \tag{4.5}$$

$$\log \frac{|\mathcal{P}|}{|A|} < C^2 (\log C)^3 \tag{4.6}$$

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

$$k \in \mathbb{Z}_+, \quad k > \frac{1}{\tau}. \tag{4.7}$$

(Hence $k > k(\varepsilon)$.) Denote by $\nu$ 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

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

Hence by the Fourier inversion formula, we have

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

$\chi$ denoting a multiplicative character.

Applying the circle method and (4.4), we get

$$\begin{aligned} \max_{x \in \mathbb{F}_p^*} \nu(x) &\leq \frac{1}{p-1} + \max_{\chi \text{ nontrivial}} \ |\mathcal{P}|^{-k} \Big| \sum_{x \in \mathcal{P}} \chi(x) \Big|^k \\ &< \frac{1}{p-1} + p^{-\tau k} \\ &< \frac{2}{p}. \end{aligned} \tag{4.8}$$

The last inequality is by (4.7). Assuming $A \subset \mathbb{F}_p^*$, we write

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

implying by (4.6) and (4.8)

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

This proves Corollary 5. $\square$

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

$$
\Big|\sum_{x\in A, y\in B} \chi(x+y)\Big| < p^{-\delta}|A|\ |B| \tag{4.9}
$$

where $\delta = \delta(\varepsilon) > 0$ and $\chi$ a nontrivial multiplicative character.

An affirmative answer is only known in the case $|A| > p^{\frac{1}{2}+\varepsilon}, |B| > p^\varepsilon$ for some $\varepsilon > 0$ $\big($as a consequence of Weil's inequality (2.14)$\big)$. Even for $|A| > p^{1/2}, |B| > p^{1/2}$, an inequality of the form (4.9) seems unknown.

Next 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*

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

*where $\tau = \tau(\varepsilon, K) > 0$, $p > p(\varepsilon, K)$ and $\chi$ is a nontrivial 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 $\le p^\varepsilon$

subsets satisfying assumptions (a) and (b), we may assume that $|B| < \frac{1}{2}(\sqrt{p}-1)$. We denote the various constants $\big($possibly depending on the constant $K$ in assumption (b)$\big)$ 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

$$d \le K \tag{4.10}$$

$$\log \frac{|\mathcal{B}_1|}{|B|} < C. \tag{4.11}$$

Let

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

We take

$$\delta = \frac{\varepsilon}{4d}, \quad r = \left[\frac{10}{\delta}\right]. \tag{4.12}$$

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

$$|B_0| > p^{-2d\delta}|\mathcal{B}_2|$$

$$B - \mathcal{B}_0 I \subset \mathcal{B}_2. \tag{4.13}$$

Therefore,

$$|\mathcal{B}| \le |\mathcal{B}_1| \le e^{C(K)}|\mathcal{B}| \ \text{ and } \ |\mathcal{B}_2| = 2|\mathcal{B}_1| - 1. \tag{4.14}$$

Estimate

$$\begin{aligned}\Big|\sum_{x\in A, y\in B} \chi(x+y)\Big| \le & \sum_{y\in B}\Big|\sum_{x\in A}\chi(x+y)\Big| \\ \le & |\mathcal{B}_0|^{-1}|I|^{-1} \sum_{\substack{y\in\mathcal{B}_2\\ z\in\mathcal{B}_0, t\in I}} \Big|\sum_{x\in A}\chi(x+y+zt)\Big|.\end{aligned} \tag{4.15}$$

The second inequality is by (4.13). Write

$$\sum_{\substack{y\in\mathcal{B}_2\\ z\in\mathcal{B}_0, t\in I}} \Big|\sum_{x\in A}\chi(x+y+zt)\Big| \le (|\mathcal{B}_2|\,|\mathcal{B}_0|\,|I|)^{\frac{1}{2}} \ \Bigg|\sum_{\substack{y\in\mathcal{B}_2, z\in\mathcal{B}_0, t\in I\\ x_1,x_2\in A}} \chi\Big(\frac{(x_1+y)z^{-1}+t}{(x_2+y)z^{-1}+t}\Big)\Bigg|^{\frac{1}{2}}. \tag{4.16}$$

The sum on the right-hand side of (4.16) equals

$$\Big|\sum_{u_1,u_2\in\mathbb{F}_p}\nu(u_1,u_2)\sum_{t\in I}\chi\Big(\frac{u_1+t}{u_2+t}\Big)\Big|$$
$$\leq\Big[\sum_{u_1,u_2}\nu(u_1,u_2)^{\frac{2r}{2r-1}}\Big]^{1-\frac{1}{2r}}\Big[\sum_{u_1,u_2}\Big|\sum_{t\in I}\chi\Big(\frac{u_1+t}{u_2+t}\Big)\Big|^{2r}\Big]^{\frac{1}{2r}} \tag{4.17}$$

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

$$\nu(u_1,u_2)=|\{(x_1,x_2,y,z)\in A\times A\times\mathcal{B}_2\times\mathcal{B}_0:\frac{x_1+y}{z}=u_1\text{ and }\frac{x_2+y}{z}=u_2\}|. \tag{4.18}$$

Hence

$$\sum_{u_1,u_2}v(u_1,u_2)=|A|^2|\mathcal{B}_2|\;|\mathcal{B}_0| \tag{4.19}$$

and

$$\sum_{u_1,u_2}\nu(u_1,u_2)^2$$
$$=\Big|\{(x_1,x_2,x_1',x_2',y,y',z,z')\in A^4\times\mathcal{B}_2^2\times\mathcal{B}_0^2:\frac{x_i+y}{z}=\frac{x_i'+y'}{z'}\text{ for }i=1,2\}\Big|$$
$$\leq\;|A|^3\max_{x_1,x_1'}\Big|\Big\{(y,y',z,z')\in\mathcal{B}_2^2\times\mathcal{B}_0^2:\frac{x_1+y}{z}=\frac{x_1'+y'}{z'}\Big\}\Big|$$
$$\leq\;|A|^3E(\mathcal{B}_0,\mathcal{B}_0)^{\frac12}\max_x E(x+\mathcal{B}_2,x+\mathcal{B}_2)^{\frac12}$$
$$<\;|A|^3\log p\;|\mathcal{B}_0|^{\frac{11}{8}}|\mathcal{B}_2|^{\frac{11}{8}}$$
$$<\;C|A|^3\;|\mathcal{B}_2|^{\frac{11}{4}} \tag{4.20}$$

by Proposition 1, Fact 1 and several applications of the Cauchy-Schwarz inequality. Therefore, by Fact 5 (after (2.12)), (4,19) and (4.20) , the first factor of (4.17) is bounded by

$$\Big[\sum\nu(u_1,u_2)\Big]^{1-\frac{1}{r}}\Big[\sum\nu(u_1,u_2)^2\Big]^{\frac{1}{2r}}$$
$$\leq C|A|^2|\mathcal{B}_2|\;|\mathcal{B}_0|(|A|^{-\frac12}|\mathcal{B}_2|^{-\frac58}p^{2d\delta}\Big)^{\frac1r}. \tag{4.21}$$

Next, write using Weil's inequality (2.14)

$$\sum_{u_1,u_2\in\mathbb{F}_p}\Big|\sum_{t\in I}\chi\Big(\frac{u_1+t}{u_2+t}\Big)\Big|^{2r}\leq\sum_{t_1,\dots,t_{2r}\in I}\Big|\sum_{u\in\mathbb{F}_p}\chi\Big(\frac{(u+t_1)\cdots(u+t_r)}{(u+t_{r+1})\cdots(u+t_{2r})}\Big|^2$$

$$\leq p^2\;|I|^r\;r^{2r}+Cr^2p\;|I|^{2r}, \tag{4.22}$$

so that the second factor in (4.17) is bounded by

$$Crp^{\frac{1}{r}}\ |I|^{\frac{1}{2}} + Cp^{\frac{1}{2r}}\ |I|. \tag{4.23}$$

Applying (4.14) and collecting estimates (4.16), (4.17), (4.21), (4.23) and assumption (a), we bound (4.15) by

$$\begin{aligned}\Big|\sum_{x\in A, y\in B}\chi(x+y)\Big| &< C|A|\ |B|\ |I|^{-\frac{1}{2}}(|A|^{-\frac{1}{2}}|B|^{-\frac{5}{8}}p^{2d\delta})^{\frac{1}{2r}}(\sqrt{r}\ p^{\frac{1}{2r}}\ |I|^{\frac{1}{4}} + p^{\frac{1}{4r}}\ |I|^{\frac{1}{2}})\\ &< C\sqrt{r}\ |A|\ |B|\ (p^{-(\frac{4}{9}+\varepsilon)\frac{9}{8}+2d\delta})^{\frac{1}{2r}}(p^{\frac{1}{2r}-\frac{\delta}{4}} + p^{\frac{1}{4r}})\\ &< C\sqrt{r}\ |A|\ |B|\ (p^{\frac{1}{2}-\frac{9}{8}\varepsilon+2d\delta-\frac{\delta}{2}r} + p^{-\frac{9}{8}\varepsilon+2d\delta})^{\frac{1}{2r}}.\end{aligned} \tag{4.24}$$

Recall (4.12). The theorem follows by taking $\tau(\varepsilon) = \frac{\varepsilon^2}{128K}$ $\square$.

Next, we consider the special case $A \subset \mathbb{F}_p$ and $I \subset \mathbb{F}_p$ an interval. First, we begin with the following technical lemma.

**Lemma 7.** *Let $A \subset \mathbb{F}_p^*$ and let $I_1, \dots, I_s$ be intervals such that $I_i \subset [1, p^{\frac{1}{k_i}}]$. Denote*

$$w(u) = \Big|\big\{(y, z_1, \dots, z_s) \in A \times I_1 \times \cdots \times I_s :\ y \equiv uz_1 \dots z_s\ \ (mod\ p)\big\}\Big| \tag{4.25}$$

*and*

$$\gamma = \frac{1}{k_1} + \cdots + \frac{1}{k_s}. \tag{4.26}$$

*Then*

$$\sum w(u)^2 < |A|^{1+\gamma}p^{\gamma + \frac{s}{\log\log p}}.$$

*Proof.* Using multiplicative characters and Plancherel, we have

$$\sum w(u)^2 = \frac{1}{p-1}\sum_\chi \langle w, \chi\rangle^2, \tag{4.27}$$

where

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

Hence

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

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

$$\sum w(u)^2 = \frac{1}{p-1}\sum_\chi \Big|\sum_{y\in A}\chi(y)\Big|^2 \prod_i \Big|\sum_{z_i\in I_i}\chi(z_i)\Big|^2$$
$$\leq \frac{1}{p-1}\Big(\sum_\chi\Big|\sum_{y\in A}\chi(y)\Big|^{\frac{2}{1-\gamma}}\Big)^{1-\gamma} \prod_i\Big(\sum_\chi\Big|\sum_{z_i\in I_i}\chi(z_i)\Big|^{2k_i}\Big)^{\frac{1}{k_i}}. \tag{4.28}$$

Now we estimate different factors. Writing the exponent as $\frac{2}{1-\gamma}=\frac{2\gamma}{1-\gamma}+2$ and using the trivial bound, we have

$$\sum_\chi\Big|\sum_{y\in A}\chi(y)\Big|^{\frac{2}{1-\gamma}} \leq |A|^{\frac{2\gamma}{1-\gamma}}\sum_\chi\Big|\sum_{y\in A}\chi(y)\Big|^2 = |A|^{\frac{2\gamma}{1-\gamma}}\sum_{y,z\in A}\sum_\chi \chi(yz^{-1}) = p|A|^{\frac{1+\gamma}{1-\gamma}}. \tag{4.29}$$

For an interval $I\subset[1,p^{\frac{1}{k}}]$, we define

$$\eta(u)=\Big|\{(z_1,\ldots,z_k)\in I\times\cdots\times I:\ z_1\ldots z_k\equiv u \pmod p\}\Big|.$$

Since $z_1\ldots z_k\equiv z_1'\ldots z_k' \pmod p$ implies $z_1\ldots z_k=z_1'\ldots z_k'$ in $\mathbb{Z}$, $\eta(u)<\big(\exp(\frac{\log p}{\log\log p})\big)^k$. On the other hand $\sum\eta(u)<(p^{\frac{1}{k}})^k=p$. Therefore,

$$\sum_\chi\Big|\sum_{z\in I}\chi(z)\Big|^{2k} = \sum_\chi\Big(\sum_u \eta(u)\chi(u)\Big)^2 = \sum_\chi\langle\eta,\chi\rangle^2 = (p-1)\sum\eta(u)^2 < p^{2+\frac{k}{\log\log p}}. \tag{4.30}$$

Putting (4.28)-(4.30) together, we have the lemma. $\square$

**Theorem 8.** *Let $A\subset\mathbb{F}_p$ be a subset with $|A|=p^\alpha$ and let $I\subset[1,p]$ be an arbitrary interval with $|I|=p^\beta$, where*

$$\alpha(1-\beta)+\beta>\frac{1}{2}+\delta \tag{4.31}$$

*and $\beta>\delta>0$. Then for a non-principal multiplicative character $\chi$, we have*

$$\Big|\sum_{\substack{x\in I\\ y\in A}}\chi(x+y)\Big| < p^{-\frac{\delta^2}{13}}|A|\,|I|.$$

*Proof.* Let

$$\tau=\frac{\delta}{6} \tag{4.32}$$

and

$$R = \left\lceil \frac{1}{2\tau} \right\rceil. \tag{4.33}$$

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

$$2\tau < \beta - \sum_i \frac{1}{k_i} < 3\tau. \tag{4.34}$$

Denote

$$I_0 = \big[1, p^\tau\big], \quad I_i = \big[1, p^{\frac{1}{k_i}}\big] \qquad (1 \le i \le s).$$

We perform the Burgess amplification as follows. First, for any $z_0 \in I_0, \dots, z_s \in I_s$,

$$\sum_{\substack{x \in I \\ y \in A}} \chi(x+y) = \sum_{\substack{x \in I \\ y \in A}} \chi(x + y + z_0 z_1 \dots z_s) + O(|A| p^{\beta - \tau}).$$

Letting $\gamma = \sum_i \frac{1}{k_i}$, we have

$$\begin{aligned}
\Big| \sum_{\substack{x \in I \\ y \in A}} \chi(x+y+z_0 z_1 \dots z_s) \Big| &= p^{-\gamma-\tau} \Big| \sum_{\substack{x \in I,\, y \in A \\ z_0 \in I_0, \dots, z_s \in I_s}} \chi(x+y+z_0 z_1 \dots z_s) \Big| \\
&\le p^{-\gamma-\tau} \sum_{\substack{x \in I,\, y \in A \\ z_1 \in I_1, \dots, z_s \in I_s}} \Big| \sum_{z_0 \in I_0} \chi(x+y+z_0 z_1 \dots z_s) \Big| \\
&\le p^{\beta-\gamma-\tau} \max_{x \in I} \sum_{\substack{y \in A \\ z_1 \in I_1, \dots, z_s \in I_s}} \Big| \sum_{z_0 \in I_0} \chi\Big( \frac{x+y}{z_1 \dots z_s} + z_0 \Big) \Big|. 
\end{aligned} \tag{4.35}$$

Fix $x \in I$ achieving maximum in (4.35), and replace $A$ by $A_1 = A + x$. Denote $w(u)$ the function (4.25) with $A$ replaced by $A_1$. Hence (4.35) is

$$p^{\beta-\gamma-\tau} \sum_u w(u) \Big| \sum_{z \in I_0} \chi(u+z) \Big|. \tag{4.36}$$

By (4.36), Hölder inequality, Fact 5 and Weil estimate $\big($cf (2.16)$\big)$, (4.35) is bounded by

$$\begin{aligned}
&p^{\beta-\gamma-\tau} \Big( \sum_u w(u)^{\frac{2R}{2R-1}} \Big)^{1-\frac{1}{2R}} \Big( \sum_u \Big| \sum_{z \in I_0} \chi(u+z) \Big|^{2R} \Big)^{\frac{1}{2R}} \\
\le& p^{\beta-\gamma-\tau} \Big[ \sum w(u) \Big]^{1-\frac{1}{R}} \Big[ \sum w(u)^2 \Big]^{\frac{1}{2R}} \Big( R|I_0|^{\frac{1}{2}} p^{\frac{1}{2R}} + 2|I_0| p^{\frac{1}{4R}} \Big) \\
\ll& p^{\alpha+\beta-\frac{1}{2R}(\delta-3\tau-\frac{1}{\log\log p})} < |A||I| p^{-\frac{\delta^2}{13}}.
\end{aligned}$$

In the last inequalities, we use $|\sum w(u)| = |A|p^\gamma$, (4.31)-(4.34) and Lemma 7. $\square$

*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 referee for many helpful comments. The author would also like to thank J. Bourgain and Nick Katz for communication on Propositions K1-K3, 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 MS.

[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).

[Kar]. A.A. Karacuba, *Estimates of character sums*, Math. USSR-Izvestija Vol. 4 (1970), No. 1 , 19-29.

[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).

[K1]. Nick Katz, *An estimate for character sums*, JAMS Vol 2, No 2 (1989), 197-200.

[K2]. ———, *Private communication.*

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