C. R. Acad. Sci. Paris, Ser. I 348 (2010) 115–120

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number Theory

On a multilinear character sum of Burgess

Sur les sommes de caractères multi-linéaires de Burgess

Jean Bourgain [a], Mei-Chu Chang [b]

[a] *School of Mathematics, Institute for Advanced Study, Olden lane, Princeton, NJ 08540, USA*
[b] *Department of Mathematics, University of California, Riverside, 900 University Avenue, Riverside, CA 92521, USA*

ARTICLE INFO

Article history:
Received 29 November 2009
Accepted 10 December 2009
Available online 20 January 2010

Presented by Jean Bourgain

ABSTRACT

Let p be a sufficiently large prime and $(L_i)_{1\leqslant i\leqslant n}$ a nondegenerate system of linear forms in n variables over $\mathbb{F}_p$. We establish a nontrivial estimate on the incomplete character sum

$$\sum_{x\in\prod_{i=1}^n [a_i,a_i+H]} \mathcal{X}\left(\prod_{j=1}^n L_j(x)\right),$$

provided $H > p^{\frac{1}{4}+\varepsilon}$.

RÉSUMÉ

Soit p un nombre premier suffisamment grand et $(L_i)_{1\leqslant i\leqslant n}$ un système non-dégénéré de formes linéaires sur $\mathbb{F}_p$ en n variables. Nous obtenons une estimée non-triviale de la somme incomplète

$$\sum_{x\in\prod_{i=1}^n [a_i,a_i+H]} \mathcal{X}\left(\prod_{j=1}^n L_j(x)\right),$$

où $\mathcal{X}\neq 1$ est un caractère multiplicatif $(\mathrm{mod}\, p)$ et $H > p^{\frac{1}{4}+\varepsilon}$.

Version française abrégée

Soit p un nombre premier et $(L_i)_{1\leqslant i\leqslant n}$ un système non-dégénéré de formes linéaires en $x_1,\ldots,x_n\in\mathbb{F}_p$. Soit $\mathcal{X}\neq 1$ un caractère multiplicatif $(\mathrm{mod}\, p)$ et

$$S = \sum_{x\in\prod_{i=1}^n [a_i,a_i+H]} \mathcal{X}\left(\prod_{j=1}^n L_j(x)\right).$$

E-mail address: bourgain@ias.edu (J. Bourgain).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2009.12.013

Nous établissons une estimation non-triviale de S sous l'hypothèse $H > p^{\frac{1}{4}+\varepsilon}$. Ceci généralise l'inégalité classique de Burgess [1] pour $n = 1$, le résultat obtenu dans [4] pour $n = 2$ et améliore la condition $H > p^{\frac{1}{2}-\frac{1}{2(n+1)}+\varepsilon}$ de [2]. L'outil principal de la démonstration est la géométrie des nombres et une approche initiée dans [5].

1. Introduction

Let p be a large prime and let $(L_i)_{1\leqslant i\leqslant n}$ be n linearly independent forms in $x_1, \dots, x_n \in \mathbb{F}_p$.
For $\mathcal{X}$ a nontrivial multiplicative character $(\bmod p)$, we consider incomplete sums of the form

$$S = \sum_{x\in\prod_{i=1}^n [a_i, a_i+H]} \mathcal{X}\left(\prod_{j=1}^n L_j(x)\right). \tag{1}$$

For $n = 1$, Burgess' classical inequality provides an estimate

$$|S| < p^{-\delta} H \tag{2}$$

if $H > p^{\frac{1}{4}+\varepsilon}$, where $\delta = \delta(\varepsilon) > 0$ (see [1]).

In [2] an estimate of the form (2) is established for $n = 2$ and $H > p^{\frac{1}{3}+\varepsilon}$ and in the general case for $H > p^{\frac{1}{2}-\frac{1}{2(n+1)}+\varepsilon}$. (See also [3].) If $n = 2$, a result of the same strength as Burgess theorem for $n = 1$ (i.e. assuming $H > p^{\frac{1}{4}+\varepsilon}$) was obtained in [4]. Here we extend that result to the general dimension n.

Theorem. *Assume $H > p^{\frac{1}{4}+\varepsilon}$. Then*

$$|S| < p^{-\delta} H^n \tag{3}$$

with $\delta = \delta_n(\varepsilon) > 0$.

Let us emphasize that the estimate (3) (as well as [4]) is uniform in $(L_i)_{1\leqslant i\leqslant n}$.

The approach is based on the 'shifted product' technique (standard in this type of problem) and an estimate on 'multiplicative energy' which is the new ingredient. Compared with [4] for $n = 2$, the technique involved here is quite different. In [4], the problem is reduced to uniform estimates for divisor functions in quadratic number fields while here we rely on methods from geometry of numbers. This approach to the multiplicative energy originates from recent work of S. Konyagin [5] and [3,4] on the Davenport–Lewis problem on incomplete character sums over boxes in fields $\mathbb{F}_{p^n}$.

2. Burgess method

For $i = 1, \dots, n$, let

$$L_i = (\ell_{i,1}, \dots, \ell_{i,n}) \in \mathbb{Z}^n$$

and assume

$$\det(L_i, \dots, L_n) \not\equiv 0 \ (\bmod p). \tag{4}$$

Our aim is to bound nontrivially

$$\sum_{x\in B_H} \mathcal{X}\left(\prod_{i=1}^n L_i x\right) \tag{5}$$

where

$$B_H = B_H^{(n)} = \big\{x \in [1, p]^n \colon a_i \leqslant x_i \leqslant a_i + H \ (1 \leqslant i \leqslant n)\big\},$$

and clearly, $L_i x$ is the inner product $\langle L_i, x\rangle$.

Following Burgess' method, first we replace x by $x + ty$ with $1 \leqslant t < p^{\frac{\varepsilon}{2}}$, $y \in B_{p^{-\varepsilon}H}$ and estimate

$$(5) \leqslant \big(p^{-\varepsilon} H\big)^{-n} p^{-\frac{\varepsilon}{2}} \sum_{\substack{x\in B_H,\ y\in B_{p^{-\varepsilon}H}\\ t<p^{\varepsilon/2}}} \mathcal{X}\Big(\prod (L_i x + tL_i y)\Big) + Cp^{-\frac{\varepsilon}{2}} H^n.$$

In the sum we may restrict x, y requiring $L_i x \not\equiv 0, L_i y \not\equiv 0 \ (\bmod p)$ for $i = 1, \dots, n$.

Estimate the sum by

$$\sum_{x\in B_H,\, y\in B_{p^{-\varepsilon}H}} \left| \sum_{t<p^{\varepsilon/2}} \mathcal{X}\left(\prod_{i=1}^{n}\left(t+\frac{L_i x}{L_i y}\right)\right)\right| = \sum_{z\in\mathbb{F}_p^n} \eta(z_1,\dots,z_n) \left| \sum_{t<p^{\varepsilon/2}} \mathcal{X}\left(\prod_{i=1}^{n}(t+z_i)\right)\right| \tag{6}$$

and denoting

$$\eta(z_1,\dots,z_n) = \left|\left\{(x,y)\in B_H\times B_{p^{-\varepsilon}H}\colon\ L_i x \equiv z_i L_i y \pmod p \text{ for } i=1,\dots,n\right\}\right| \tag{7}$$

where, from the preceding, $z_1,\dots,z_n \not\equiv 0 \pmod p$.

Applying Burgess' technique, it then suffices to establish a bound

$$\sum_{z\in\mathbb{F}_p^n} \eta^2(z) < p^{-\frac{n}{2}} |B_H|^2 |B_{p^{-\varepsilon}H}|^2 p^{-\delta} \tag{8}$$

for some $\delta>0$.

Thus we need H to satisfy

$$\left|\left\{(x,y,x',y')\in B_H^4\colon\ L_i x, L_i x', L_i y, L_i y' \not\equiv 0 \pmod p,\ \text{and } L_i x L_i y \equiv L_i x' L_i y' \pmod p \text{ for } i=1,\dots,n\right\}\right| < p^{-\frac{n}{2}-\delta} H^{4n} \tag{9}$$

for some $\delta>0$.

Note that in the definition of B_H, it suffices to consider the case where $a_i = 0$ $(1\leqslant i\leqslant n)$.

3. Lattices and geometry of numbers

Fix $z=(z_1,\dots,z_n)\in(\mathbb{F}_p^*)^n$ and introduce the lattice $\mathcal{L}_z\subset\mathbb{Z}^{2n}$

$$\mathcal{L}_z = \left\{(x,y)\in\mathbb{Z}^{2n}\colon\ L_i y \equiv z_i L_i x \pmod p \text{ for } i=1,\dots,n\right\}. \tag{10}$$

Let $\lambda_1\leqslant\lambda_2\leqslant\cdots\leqslant\lambda_{2n}$ be the successive minima of $B=[-1,1]^{2n}$ with respect to $\mathcal{L}_z$. By Minkowski's second theorem

$$\lambda_1\dots\lambda_{2n} \sim \operatorname{Vol}\mathcal{L}_z = p^n \tag{11}$$

where $\sim$ involves factors that are dependent on n.

Define $1\leqslant s\leqslant 2n$ by

$$\lambda_1,\dots,\lambda_s < H, \qquad \lambda_{s+1} > H. \tag{12}$$

If $u_1,\dots,u_{2n}\in\mathcal{L}_z$, $|u_i|=\lambda_i$, and $E_s=\operatorname{span}(u_1,\dots,u_s)$ in $\mathbb{R}^{2n}$, one has

$$\left|(B_H\times B_H)\cap\mathcal{L}_z\right| \sim \left|(B_H\times B_H)\cap\mathcal{L}_z\cap E_s\right| \sim \prod_{i=1}^{s}\left(\frac{H}{\lambda_i}\right). \tag{13}$$

The dual lattice $\mathcal{L}_z^*$ is defined as

$$\mathcal{L}_z^* = \left\{x\in\mathbb{R}^{2n}\colon\ \langle x,y\rangle\in\mathbb{Z} \text{ for all } y\in\mathcal{L}_z\right\}.$$

Obviously $p\mathbb{Z}^{2n}\subset\mathcal{L}_z$. It follows that for $x=(x_1,\dots,x_{2n})\in\mathcal{L}_z^*$, $\langle x,\mathbb{Z}^{2n}\rangle\subset\frac{1}{p}\mathbb{Z}$, and hence $x_i\in\frac{1}{p}\mathbb{Z}$ $(1\leqslant i\leqslant 2n)$. Denote

$$\mathcal{L}_z' = p\mathcal{L}_z^*.$$

Hence $\mathcal{L}_z'\subset Z^{2n}$ and

$$\mathcal{L}_z' = \left\{x\in\mathbb{Z}^{2n}\colon\ \langle x,y\rangle\equiv 0 \pmod p \text{ for all } y\in\mathcal{L}_z\right\}.$$

Denoting A the $(n\times n)=$ matrix $(L_i)_{1\leqslant i\leqslant n}$, we have

$$\mathcal{L}_z = \left\{(u,v)\in\mathbb{Z}^{2n}\colon\ Au\equiv z\cdot Av \pmod p\right\} \tag{14}$$

and

$$\mathcal{L}_z' = \left\{(x,y)\in\mathbb{Z}^{2n}\colon\ \left(A^{-1}\right)^* x \equiv -z\cdot\left(A^{-1}\right)^* y \pmod p\right\}. \tag{15}$$

Here $\cdot$ indicates the product in the ring $\mathbb{F}_p\times\cdots\times\mathbb{F}_p$. We will omit it, when there is no ambiguity.

The successive minima $\lambda_1^* \leqslant \cdots \leqslant \lambda_{2n}^*$ of $\mathcal{L}_z^*$ satisfy for $1 \leqslant i \leqslant 2n$

$$\lambda_i \lambda_{2n+1-i}^* \sim 1 \tag{16}$$

(cf. [6]). Denoting $\mu_i = p\lambda_i^*$ the successive minima of $\mathcal{L}_z'$, it follows

$$\lambda_i \mu_{2n+1-i} \sim p \quad (1 \leqslant i \leqslant 2n). \tag{17}$$

From (13), (11) and (17),

$$\big|(B_H \times B_H) \cap \mathcal{L}_z\big| \sim \frac{H^s}{p^n} \lambda_{s+1} \cdots \lambda_{2n} \sim \frac{H^s}{p^{s-n}} \frac{1}{\mu_1 \cdots \mu_{2n-s}} \tag{18}$$

and if $s = 2n$

$$\big|(B_H \times B_H) \cap \mathcal{L}_z\big| \sim \frac{H^{2n}}{p^n}. \tag{19}$$

Let $u_1', \ldots, u_{2n}' \in \mathcal{L}_z'$, $|u_i'| = \mu_i$. Note that by (12), (17) we get

$$\mu_1, \ldots, \mu_{2n-s} \lesssim \frac{p}{H}, \qquad \mu_{2n-s+1} \gtrsim \frac{p}{H}. \tag{20}$$

Denoting $E_{2n-s}' = \operatorname{span}(u_1', \ldots, u_{2n-s}')$, it follows that

$$\big|(B_{\frac{p}{H}} \times B_{\frac{p}{H}}) \cap \mathcal{L}_z'\big| \sim \big|(B_{\frac{p}{H}} \times B_{\frac{p}{H}}) \cap \mathcal{L}_z' \cap E_{2n-s}'\big| \sim \prod_{i=1}^{2n-s} \left(\frac{p}{H\mu_i}\right)$$

and recalling (18)

$$\big|(B_{\frac{p}{H}} \times B_{\frac{p}{H}}) \cap \mathcal{L}_z'\big| \sim \frac{p^n}{H^{2n}} \big|(B_H \times B_H) \cap \mathcal{L}_z\big|. \tag{21}$$

We emphasize that

$$\big|(B_H \times B_H) \cap \mathcal{L}_z\big| \sim \big|(B_H \times B_H) \cap \mathcal{L}_z \cap E_s\big| \tag{22}$$

and

$$\big|(B_{\frac{p}{H}} \times B_{\frac{p}{H}}) \cap \mathcal{L}_z'\big| \sim \big|(B_{\frac{p}{H}} \times B_{\frac{p}{H}}) \cap \mathcal{L}_z' \cap E_{2n-s}'\big| \tag{23}$$

where E_s (resp. E_{2n-s}') is an s-dim (resp. $(2n-s)$-dim) subspace of $\mathbb{R}^{2n}$. Clearly either $s \leqslant n$ or $2n - s \leqslant n$ holds. It will be exploited later on.

4. Some inequalities

Returning to (9) and with $A = (L_i)_{1 \leqslant i \leqslant n}$ as above, we need to bound

$$\big|\big\{(x, y, x', y') \in B_H^4 \colon\ Ax \cdot Ay \equiv Ax' \cdot Ay' \ (\mathrm{mod}\ p)\big\}\big|. \tag{24}$$

It will be useful to generalize the setting a bit. We consider sets of the form

$$\big\{(x, y, x', y') \in B_H^4 \colon\ A_1 x \cdot A_2 y \equiv A_3 x' \cdot A_4 y' \ (\mathrm{mod}\ p)\big\} \tag{25}$$

with $A_1, A_2, A_3, A_4 \in \mathrm{Mat}_{n \times n}(\mathbb{Z})$ satisfying

$$\det A_j \not\equiv 0 \ (\mathrm{mod}\ p) \quad \text{for } j = 1, 2, 3, 4. \tag{26}$$

Let $C(n, H)$ denote an upperbound on (25) with the A_j satisfying (26).

Let us use the notation $\overline{A}$ to indicate restriction of A on $x \in \mathbb{Z}^n$ such that $L_i x \not\equiv 0 \ (\mathrm{mod}\ p)$ for $i = 1, \ldots, n$.

By elimination of variables, one easily sees that

$$\big|(25)\big| \leqslant \big|\big\{(x, y, x', y') \in B_H^4 : \overline{A}_1 x \cdot \overline{A}_2 y \equiv \overline{A}_3 x' \cdot \overline{A}_4 y' \ (\mathrm{mod}\ p)\big\}\big| + C \max_{m<n} H^{2(n-m)} C(m, H). \tag{27}$$

Further

$$(27) = \sum_{z\in\mathbb{F}_p^n} \big|\big\{(x,x')\in B_H^2\colon\ \overline{A}_1 x \equiv z\cdot \overline{A}_3 x'\big\}\big| \cdot \big|\big\{(y,y')\in B_H^2\colon\ \overline{A}_4 y' \equiv z\cdot \overline{A}_2 y\big\}\big|$$
$$\leqslant \sum_{z\in\mathbb{F}_p^n} \big|B_H^2\cap \mathcal{L}_z\big|\cdot\big|B_H^2\cap \mathcal{M}_z\big| \tag{28}$$

where

$$\mathcal{L}_z = \big\{(x,x')\in\mathbb{Z}^{2n}\colon\ A_1 x \equiv z\cdot A_3 x' \ (\mathrm{mod}\ p)\big\} \tag{29}$$

and the lattice $\mathcal{M}_z$ is defined similarly.

More generally, for $1\leqslant H, K < p$

$$\sum_{z\in\mathbb{F}_p^n} \big|\big\{(x,x')\in B_H^2\colon\ \overline{A}_1 x \equiv z\cdot \overline{A}_3 x'\big\}\big| \cdot \big|\big\{(y,y')\in B_K^2\colon\ A_4 y' \equiv z\cdot A_2 y\big\}\big|$$
$$= \big|\big\{(x,x',y,y')\in B_H^2\times B_K^2\colon\ \overline{A}_1 x\cdot A_2 y \equiv \overline{A}_3 x'\cdot A_4 y' \ (\mathrm{mod}\ p)\big\}\big|$$
$$\leqslant \big|\big\{(x,x',y,y')\in B_H^2\times B_K^2\colon\ \overline{A}_1 x\cdot \overline{A}_2 y \equiv \overline{A}_3 x'\cdot \overline{A}_4 y' \ (\mathrm{mod}\ p)\big\}\big| \tag{30}$$
$$+ C\max_{m<n} H^{2(n-m)}\cdot C(m,H)^{1/2}\cdot C(m,K)^{\frac{1}{2}} \tag{31}$$
$$\leqslant C\max_{m\leqslant n} H^{2(n-m)}\cdot C(m,H)^{\frac{1}{2}}\cdot C(m,K)^{\frac{1}{2}} \tag{32}$$

where in (31), (32) we used the Cauchy–Schwarz inequality.

If $s = s(z)$ is defined as in (12), the pigeonhole inequality implies

$$\big|(B_H\times B_H)\cap\mathcal{L}_z\big| \lesssim \left(\frac{H}{H_1}\right)^s \big|(B_{H_1}\times B_{H_1})\cap\mathcal{L}_z\big| \quad \text{for } H_1\leqslant H. \tag{33}$$

Finally recall also (21).

5. The recursive inequality

We establish a recursive inequality on the $C(n,H)$, $H<\sqrt{p}$.

Considering (25), let $\mathcal{L}_z$ be defined by (29). Either $s(z)\leqslant n$ or $2n-s(z)\leqslant n$.

Consider first the contribution of $z\in(\mathbb{F}_p^*)^n$ with $s(z)\leqslant n$.

Following previous section, estimate (28) by

$$\sum_{\substack{z\in\mathbb{F}_p^n\\ s(z)\leqslant n}} \big|\big\{(y,y')\in B_H^2\colon\ \overline{A}_4 y'\equiv z\cdot\overline{A}_2 y\big\}\big|\cdot\big|B_H^2\cap\mathcal{L}_z\big| \leqslant \sum_{z\in\mathbb{F}_p^n}\left(\frac{H}{H_1}\right)^n \big|\big\{(y,y')\in B_H^2\colon\ \overline{A}_4 y'\equiv z\cdot\overline{A}_2 y\big\}\big|\big|B_{H_1}^2\cap\mathcal{L}_z\big| \tag{34}$$

by (33) and choosing $H_1 = p^{-\kappa}H$ for some small $\kappa>0$ to be specified later. We distinguish two cases. Either

$$\big|B_{H_1}^2\cap\mathcal{L}_z\big| \sim \big|\big\{(x,x')\in B_{H_1}^2\colon\ \overline{A}_1 x\equiv z\cdot\overline{A}_3 x'\big\}\big|. \tag{35}$$

Using Cauchy–Schwarz, the corresponding contribution to (34) may be bounded by

$$H^{2n}\big[H^{-2n}C(n,H)\big]^{\frac{1}{2}}\big[H_1^{-2n}C(n,H_1)\big]^{\frac{1}{2}}. \tag{36}$$

If (35) fails, elimination of variables give, for some $m<n$

$$\big|\big(B_{H_1}^{(n)}\times B_{H_1}^{(n)}\big)\cap\mathcal{L}_z\big| < C\big|\big(B_{H_1}^{(m)}\times B_{H_1}^{(m)}\big)\cap\tilde{\mathcal{L}}_z\big| \tag{37}$$

with $\tilde{\mathcal{L}}_z$ obtained from $\mathcal{L}_z$ by eliminating $2(n-m)$ variables.

Substituting (37) in (34) and following the calculation leading to (32) gives the bound

$$H^{2n}\max_{m<n}\left(\frac{H}{H_1}\right)^{n-m}\big[H^{-2m}C(m,H)\big]^{\frac{1}{2}}\big[H_1^{-2m}C(m,H_1)\big]^{\frac{1}{2}} < p^{C\kappa}H^{2n}\max_{\substack{m<n\\ H'\leqslant H}}\big[(H')^{-2m}C(m,H')\big]. \tag{38}$$

Thus the contribution to (28) for $s(z)\leqslant n$ is bounded by (36) + (38).

Next, consider the case $s(z)>n$. Then certainly $2n-s\leqslant n$. We use the dual lattice $\mathcal{L}_z'$ and (21).

Thus

$$\sum_{\substack{z\in\mathbb{F}_p^n\\ s(z)\geqslant n}} \big|\big\{(y,y')\in B_H^2\colon\ \overline{A}_4 y'\equiv z\cdot\overline{A}_2 y\big\}\big|\big|B_H^2\cap\mathcal{L}_z\big|$$

may be estimated (up to factors depending on n) by

$$\frac{H^{2n}}{p^n}\sum_{\substack{z\in\mathbb{F}_p^n\\ s(z)\geqslant n}} \big|\big\{(y,y')\in B_H^2\colon\ \overline{A}_4 y'\equiv z\cdot\overline{A}_2 y\big\}\big|\big|B_{\frac{p}{H}}^2\cap\mathcal{L}'_z\big| \tag{39}$$

and since $2n-s\leqslant n$ in (23), application of (33) with $\mathcal{L}'_z$ give

$$\big|B_{\frac{p}{H}}^2\cap\mathcal{L}'_z\big|\leqslant\left(\frac{p}{KH}\right)^n\big|B_K^2\cap\mathcal{L}'_z\big|\quad\text{for } K\leqslant\frac{p}{H}$$

and

$$(39)\leqslant\sum_{z\in\mathbb{F}_p^n}\left(\frac{H}{K}\right)^n\big|\big\{(y,y')\in B_H^2\colon\ \overline{A}_4 y'\equiv z\cdot\overline{A}_2 y\big\}\big|\big|B_K^2\cap\mathcal{L}'_z\big|. \tag{40}$$

Since $H\leqslant\sqrt{p}$, we may take $K=H_1$ as above. The expression (40) may be estimated as (34).

From the preceding, it follows that

$$H^{-2n}C(n,H)<C\big[H^{-2n}C(n,H)\big]^{\frac12}\big[H_1^{-2n}C(n,H_1)\big]^{\frac12}+p^{C\kappa}\max_{\substack{m<n\\ H'\leqslant H}}\big[(H')^{-2m}C\big(m,H'\big)\big]. \tag{41}$$

Iterating (41) easily leads to an estimate

$$\begin{aligned}\max_{H<\sqrt{p}} H^{-2n}C(n,H)&<C^{\frac{1}{\kappa}}p^{C\kappa}\quad(C\text{ depending on }n)\\ &<C^{\sqrt{\log p}}\end{aligned} \tag{42}$$

choosing κ appropriately.

Hence we proved in particular

Lemma. *For $H<\sqrt{p}$,*

$$\big|\big\{(x,y,x',y')\in B_H^4\colon\ Ax\cdot Ay\equiv Ax'\cdot Ay'\ (\mathrm{mod}\ p)\big\}\big|\ll p^{\varepsilon}H^{2n}.$$

It follows that (9) will hold for $H>p^{\frac14+\varepsilon}$, proving the theorem.

6. Remark

One expects the analogue of the theorem to remain valid when summing over arbitrary boxes $B_{H_1,\dots,H_n}=\{a_i\leqslant x_i\leqslant a+i+H_i\ (1\leqslant i\leqslant n)\}$ where $0<H_i<p$ and $\prod_{i=1}^n H_i>p^{\frac{n}{4}+\varepsilon}$ (it is easily seen that it suffices to consider the case $H_i\leqslant\sqrt{p}$). The methods described above permit to prove such statement for small values of n, but the general case remains to be settled.

Acknowledgement

The authors are grateful to S. Konyagin for making his preprint available.

References

[1] D.A. Burgess, The distribution of quadratic residues and non-residues, Mathematica 4 (1957) 106–112.
[2] D.A. Burgess, A note on character sums for binary quadratic forms, J. London Math. Soc. 43 (1968) 271–274.
[3] M.-C. Chang, On a question of Davenport and Lewis and new character sum bounds in finite fields, Duke Math. J. 145 (3) (2008) 409–442.
[4] M.-C. Chang, Character sums in $\mathbb{F}_{p^2}$, GAFA, in press.
[5] S.V. Konyagin, Estimates of character sums in finite fields, Matematicheskie Zametki (in Russian), in press.
[6] C. Lekkerkerker, Geometry of Numbers, North-Holland Mathematical Library, vol. 37, 1987.