Title

Burgess Inequality In

$${\mathbb {F}_{p^2}}$$

Journal

Geometric and Functional Analysis: GAFA, 19(4)

ISSN

1420-8970

Author

Chang, Mei-Chu

Publication Date

2009-12-01

DOI

10.1007/s00039-009-0031-5

Peer reviewed

Geom. Funct. Anal. Vol. 19 (2009) 1001–1016
DOI 10.1007/s00039-009-0031-5
Published online November 21, 2009

GAFA Geometric And Functional Analysis

BURGESS INEQUALITY IN $\mathbb{F}_{p^2}$

Mei-Chu Chang

Abstract. The purpose of the paper is to present new estimates on incomplete character sums in finite fields that are of the strength of Burgess' celebrated theorem for prime fields. More precisely, an inequality of this type is obtained in F_{p^2} and also for binary quadratic forms, improving on the work of Davenport–Lewis and on several results due to Burgess. The arguments are based on new estimates for the multiplicative energy of certain sets that allow us to improve the amplification step in Burgess' method.

0 Introduction

The paper contributes to two problems on incomplete character sums that go back to the work of Burgess and Davenport–Lewis in the sixties. Incomplete character sums are a challenge in analytic number theory. By incomplete, we mean that the summation is only over an interval I. Typical applications include the problem of the smallest quadratic non-residue $(\mathrm{mod}\, p)$ and the distribution of primitive elements in a finite field. Recall that Burgess' bound [B1] on multiplicative character sums $\sum_{x\in I}\chi(x)$ in a prime field $\mathbb{F}_p$ provides a nontrivial estimate for an interval $I\subset[1,p-1]$ of size $|I|>p^{1/4+\varepsilon}$, with any given $\varepsilon>0$. Burgess' result, which supersedes the Polya–Vinogradov inequality, was a major breakthrough and remains unsurpassed. (It is conjectured that such result should hold as soon as $|I|>p^{\,\varepsilon}$.)

The aim of this paper is to obtain the full generalization of Burgess' theorem in $\mathbb{F}_{p^2}$. Thus

Theorem 5. *Given $\varepsilon>0$, there is $\delta>0$ such that if $\omega\in\mathbb{F}_{p^2}\backslash\mathbb{F}_p$ and I,J are intervals of size $p^{1/4+\varepsilon}$ (p sufficiently large), then*

$$\Big|\sum_{\substack{x\in I\\ y\in J}}\chi(x+\omega y)\Big|<p^{-\delta}\,|I|\,|J| \tag{0.1}$$

for χ a nontrivial multiplicative character.

The importance of the statement is its uniformity in ω. Both Burgess [B2] and Karacuba [K] obtained the above statement under the assumption that ω satisfies a *given* quadratic equation

$$\omega^2+a\omega+b=0\pmod p \tag{0.2}$$

with $a,b\in\mathbb{Q}$.

Keywords and phrases: Character sums, finite fields, multiplicative energy, Burgess, Davenport–Lewis

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

In the generality of Theorem 5, the best known result in $\mathbb{F}_{p^2}$ was due to Davenport and Lewis [DL], under the assumption $|I|, |J| > p^{1/3+\varepsilon}$. More generally, they consider character sums in $\mathbb{F}_{p^n}$ of the form

$$\sum_{x_1 \in I_1, \ldots, x_n \in I_n} \chi(x_1\omega_1 + \cdots + x_n\omega_n)\,, \tag{0.3}$$

where $I_1, \ldots, I_n \subset [1, p-1]$ are intervals. It is shown in [DL] that

$$\sum_{x_1 \in I_1, \ldots, x_n \in I_n} \chi(x_1\omega_1 + \cdots + x_n\omega_n) < p^{-\delta(\varepsilon)}|I_1|\cdots|I_n| \tag{0.4}$$

provided for some $\varepsilon > 0$,

$$|I_i| > p^{\rho+\varepsilon} \ \text{ with } \rho = \rho_n = \frac{n}{2(n+1)}\,. \tag{0.5}$$

In [C2], newly developed sum-product techniques in finite fields were used to establish (0.4) under the hypothesis

$$|I_i| > p^{\frac{2}{5}+\varepsilon} \ \text{ for some } \varepsilon > 0\,. \tag{0.6}$$

Hence [C2] improves upon (0.5) provided $n \geq 5$ and Theorem 5 in this paper provides the optimal result for $n = 2$.

We will briefly recall Burgess' method in the next section. It involves several steps. As in [C2], the novelty in our strategy pertains primarily to new bounds on *multiplicative energy* in finite fields (see section 1 for definition). The other aspects of Burgess technique remain unchanged. We also did not try to optimize the inequality qualitatively, as our concern here was only to obtain a nontrivial estimate under the weakest assumption possible. The new estimates on multiplicative energy are given in Lemma 2 and Lemma 3 in section 1. Contrary to the arguments in [C2] that depend on abstract sum-product theory in finite fields, the input in this paper is more classical. Lemma 2 is based on uniform estimates for the divisor function of an extension of $\mathbb{Q}$ of bounded degree. In Lemma 3, we use multiplicative characters to bound the energy

$$E(A, I) = \left\{(x_1, x_2, t_1, t_2) \in A^2 \times I^2 : x_1 t_1 \equiv x_2 t_2 \mod p\right\}, \tag{0.7}$$

where $A \subset \mathbb{F}_{p^n}$ is an arbitrary set and $I \subset [1, p-1]$ an interval. The underlying principle is actually related to Plunnecke–Ruzsa sum-set theory [TV] (here in its multiplicative version), but in this particular case may be captured in a more classical way.

Closely related to Theorem 5 is the problem of estimating character sums of binary quadratic forms over $\mathbb{F}_p$,

$$\sum_{x \in I, y \in J} \chi(x^2 + axy + by^2)\,, \tag{0.8}$$

where $x^2+axy+by^2 \in \mathbb{F}_p[x, y]$ is not a perfect square and χ a nontrivial multiplicative character of $\mathbb{F}_p$.

Theorem 11. *Given $\varepsilon > 0$, there is $\delta > 0$ such that if $x^2+axy+by^2$ is not a perfect square* $(\mathrm{mod}\, p)$*, and if $I, J \subset [1, p-1]$ are intervals of size*

$$|I|, |J| > p^{\frac{1}{4}+\varepsilon}, \tag{0.9}$$

then for p sufficiently large, we have

$$\Big|\sum_{x\in I,\, y\in J}\chi(x^2+axy+by^2)\Big| < p^{-\delta}|I|\,|J|\,, \tag{0.10}$$

where $\delta=\delta(\varepsilon)>0$ does not depend on the binary form.

This is an improvement upon Burgess' result [B3], requiring the assumption $|I|,|J|>p^{1/3+\varepsilon}$.

We will not discuss in this paper the various classical application of Theorem 1 (to primitive roots, quadratic residues, etc) as the arguments involved are not different from the ones in the literature.

1 Preliminaries and Notation

In what follows we will consider multiplications in $R=\mathbb{F}_{p^d}$ and $R=\mathbb{F}_p\times\mathbb{F}_p$. Denote by R^* the group of invertible elements of R. Let A,B be subsets of R. Denote

(1) $AB:=\{ab : a\in A \text{ and } b\in B\}$.

(2) $aB:=\{a\}B$.

Intervals are intervals of integers.

(3) $[a,b]:=\{n\in\mathbb{Z} : a\le n\le b\}$.

(4) The *multiplicative energy* of $A_1,\dots,A_n\subset R$ is defined as

$$E(A_1,\dots,A_n):=\big|\{(a_1,\dots,a_n,a_1',\dots,a_n') : a_1\cdots a_n=a_1'\cdots a_n'\}\big|$$

with the understanding that all factors a_i,a_i' are in $A_i\cap R^*$.

Using multiplicative characters χ of R , one has

(5) $E(A_1,\dots,A_n)=\frac{1}{|R^*|}\sum_\chi\prod_{i=1}^n\big|\sum_{\xi_i\in A_i}\chi(\xi_i)\big|^2$.

Energy is always multiplicative energy in this paper.

(6) Burgess' method. In this paper we will apply Burgess' method several times. We outline the recipe here, considering intervals in $\mathbb{F}_{p^2}$. For details, see section 2 of [C2].

Suppose we want to bound

$$\Big|\sum_{x\in I,y\in J}\chi(x+\omega y)\Big|, \tag{1.1}$$

where I,J are intervals. We translate (x,y) by $(tu,tv)\in\mathcal{T}M$, where $M=I'\times J'$ is a box in $\mathbb{F}_{p^2}$, and $\mathcal{T}=[1,T]$ such that $T\,|I'|<p^{-\varepsilon}|I|$ and $T\,|J'|<p^{-\varepsilon}|J|$ for some small $\varepsilon>0$. Therefore, it suffices to estimate the following sum

$$\frac{1}{T|M|}\Big|\sum_{\substack{t\in\mathcal{T}\\(u,v)\in M}}\sum_{\substack{x\in I\\y\in J}}\chi(x+tu+(y+tv)\omega)\Big|. \tag{1.2}$$

Let $w(\mu)=\big|\big\{(x,y,u,v)\in I\times J\times M : \mu=\frac{x+\omega y}{u+\omega v}\big\}\big|$.

Then the double sum in (1.2) is bounded by

$$\sum_{\mu\in\mathbb{F}_{p^2}} w(\mu)\Big|\sum_{t\in\mathcal{T}}\chi(t+\mu)\Big| \le \underbrace{\Big(\sum_{\mu\in\mathbb{F}_{p^2.}} w(\mu)^{\frac{2k}{2k-1}}\Big)^{1-\frac{1}{2k}}}_{\alpha}\underbrace{\Big(\sum_{\mu\in\mathbb{F}_{p^2.}}\Big|\sum_{t\in\mathcal{T}}\chi(\mu+t)\Big|^{2k}\Big)^{\frac{1}{2k}}}_{\beta}, \tag{1.3}$$

where k is a large integer to be chosen. By Hölder's inequality and the definition of $w(\mu)$,

$$\alpha \le \Big[\sum w(\mu)\Big]^{1-\frac{1}{k}}\Big[\sum w(\mu)^2\Big]^{\frac{1}{2k}} = \big(|I|\,|J|\,|I'|\,|J'|\big)^{1-\frac{1}{k}} E\big(I+\omega J, I'+\omega J'\big)^{\frac{1}{2k}}.$$

A key idea in Burgess' approach is then to estimate (1.3) using Weil's theorem for multiplicative characters in $\mathbb{F}_{p^n}$ (here $n=2$), leading to the bound,

$$\beta \le k\,T^{1/2}p^{n/2k} + 2Tp^{n/4k}.$$

So the remaining problem to bound the character sum (1.1) is reduced to the bounding of multiplicative energy $E(I+\omega J, I'+\omega J')$. We will describe a new strategy.

2 Multiplicative Energy of Two Intervals in $\mathbb{F}_{p^2}$

The first step in estimating the multiplicative energy is the following:

LEMMA 1. *Let $\omega \in \mathbb{F}_{p^2}\backslash\mathbb{F}_p$ and*

$$Q = \Big\{x+\omega y : x, y \in \Big[1, \tfrac{1}{10}p^{1/4}\Big]\Big\}.$$

Then

$$\max_{\xi\in\mathbb{F}_{p^2}} \big|\{(z_1,z_2)\in Q\times Q : \xi = z_1.z_2\}\big| < \exp\left(c\frac{\log p}{\log\log p}\right).$$

An essential point here is that the bound is uniform in ω. Also, the specific size of Q is important. Note that for our purpose, any estimate of the type $p^{o(1)}$ would do as well.

Proof. For given $\xi \in \mathbb{F}_{p^2}$, assume that ξ can be factored as products of two elements in Q in at least two ways. We consider the set S of polynomials in $\mathbb{Z}[X]$

$$(y_1y_2 - y_1'y_2')X^2 + (x_1y_2 + x_2y_1 - x_1'y_2' - x_2'y_1')X + (x_1x_2 - x_1'x_2'), \tag{2.1}$$

where $x_i+\omega y_i, x_i'+\omega y_i' \in Q$ for $i=1,2$, and

$$(x_1+\omega y_1)(x_2+\omega y_2) = \xi = (x_1'+\omega y_1')(x_2'+\omega y_2') \tag{2.2}$$

in $\mathbb{F}_{p^2}$.

Let $g(X) = X^2 + aX + b \in \mathbb{F}_p[X]$ be the minimal polynomial of ω. Then it is clear that every $f(X)$ in S, when considered as a polynomial in $\mathbb{F}_p[X]$, is a scalar multiple of $g(X)$.

Next, observe that, by definition of Q, the coefficients of (2.1) are integers bounded by $\frac{1}{25}p^{1/2}$. Therefore, since the coefficients of two non-zero polynomials (2.1) are proportional in $\mathbb{F}_p$, they are also proportional in $\mathbb{Q}$. Thus the polynomials

(2.1) are multiples of each other in $\mathbb{Q}[X]$ and therefore have a common root $\tilde{\omega} \in \mathbb{C}$. Since

$$(x_1 + \tilde{\omega} y_1)(x_2 + \tilde{\omega} y_2) = (x_1' + \tilde{\omega} y_1')(x_2' + \tilde{\omega} y_2') \tag{2.3}$$

in $\mathbb{Q}(\tilde{\omega})$ whenever (2.2) holds, it suffices to show that if we fix some $\tilde{\xi} \in \mathbb{Q}(\tilde{\omega})$, then

$$\left|\{(z_1, z_2) \in \tilde{Q} \times \tilde{Q} : \tilde{\xi} = z_1 z_2\}\right| < \exp\left(c \frac{\log p}{\log\log p}\right), \tag{2.4}$$

where

$$\tilde{Q} = \left\{x + \tilde{\omega} y : x, y \in \left[1, \tfrac{1}{10} p^{1/4}\right]\right\}.$$

This is easily derived from a divisor estimate. Let $uX^2 + vX + w$ be a nonzero polynomial in S, then

$$u(\tilde{\omega})^2 + v\tilde{\omega} + w = 0\,.$$

Note that $\eta = u\tilde{\omega}$ is an algebraic integer, since it satisfies

$$\eta^2 + v\eta + uw = 0\,.$$

Thus

$$u^2 \tilde{\xi} = (ux_1 + \eta y_1)(ux_2 + \eta y_2)$$

is a factorization of $u^2\tilde{\xi}$ in the integers of $\mathbb{Q}(\eta)$. Since the height of these integers is obviously bounded by p, (2.4) is implied by the usual divisor bound in a (quadratic) number field (which is uniform for extensions of given degree).

This proves Lemma 1. □

As an immediate consequence of Lemma 1, we have the following:

LEMMA 2. *Let Q be as in Lemma 1. Then the multiplicative energy $E(Q, Q)$ satisfies*

$$E(Q, Q) < \exp\left(c \frac{\log p}{\log\log p}\right) \cdot |Q|^2. \tag{2.5}$$

and

LEMMA 2′. *Let Q be as in Lemma 1 and $z_1, z_2 \in \mathbb{F}_{p^2}$. Then*

$$E(z_1 + Q, z_2 + Q) < \exp\left(c \frac{\log p}{\log\log p}\right) \cdot |Q|^2. \tag{2.6}$$

Proof of Lemma 2′. We have

$$E(z_1 + Q, z_2 + Q) \le |Q|^2 + E(Q + Q, z_2 + Q)$$

and by Cauchy–Schwarz (see [TV, Cor. 2.10])

$$E(Q + Q, z + Q) \le E(Q + Q, Q + Q)^{1/2} E(z + Q, z + Q)^{1/2}.$$

Hence (2.6) follows from (2.5). □

3 Further Amplification

The second ingredient is provided by

LEMMA 3. *Let Q be as in Lemma 1, and let $I = [1, p^{1/k}]$, where $k \in \mathbb{Z}_+$. Let $z_1, z_2 \in \mathbb{F}_{p^2}$. Then*

$$E(I, z_1 + Q, z_2 + Q) < \exp\left(c \frac{\log p}{\log\log p}\right) \cdot p^{1 + \frac{3}{2k}}. \tag{3.1}$$

Proof. Denote χ the multiplicative characters of $\mathbb{F}_{p^2}$. Thus

$$\begin{aligned} &E(I, z_1+Q, z_2+Q) \\ &\quad = \tfrac{1}{p^2}\sum_{\chi} \underbrace{\Big|\sum_{t\in I}\chi(t)\Big|^2}_{A^2}\ \underbrace{\Big|\sum_{\xi\in Q}\chi(\xi+z_1)\Big|^2}_{B^2}\ \underbrace{\Big|\sum_{\xi\in Q}\chi(\xi+z_2)\Big|^2}_{C^2}. \end{aligned} \tag{3.2}$$

Here the sum over $\xi \in Q$ is such that $\xi + z_i \neq 0$, for $i = 1, 2$.

Hence by Hölder's inequality,

$$\begin{aligned} &E(I, z_1+Q, z_2+Q) \\ &\quad \le \Big\{\tfrac{1}{p^2}\sum_{\chi}\big[A^2(BC)^{\frac{2}{k}}\big]^k\Big\}^{\frac{1}{k}}\Big\{\tfrac{1}{p^2}\sum_{\chi}\big[(BC)^{2-\frac{2}{k}}\big]^{\frac{k}{k-1}}\Big\}^{1-\frac{1}{k}} \\ &\quad = \underbrace{\Big\{\tfrac{1}{p^2}\sum_{\chi}A^{2k}B^2C^2\Big\}^{\frac{1}{k}}}_{(3.3)}\Big\{\frac{1}{p^2}\sum_{\chi}B^2C^2\Big\}^{1-\frac{1}{k}}. \end{aligned}$$

Since the second factor is equal to $E(z_1+Q, z_2+Q)^{1-\frac{1}{k}}$, (2.6) applies and we obtain the bound

$$(3.3)\cdot \exp\left(c\frac{\log p}{\log\log p}\right)\cdot |Q|^{2(1-\frac{1}{k})}. \tag{3.4}$$

Estimate (3.3) as

$$\begin{aligned} (3.3) &\le |Q|^{2/k}\Big\{\tfrac{1}{p^2}\sum_{\chi}\Big|\sum_{t\in I}\chi(t)\Big|^{2k}\Big|\sum_{\xi\in Q}\chi(\xi+z_1)\Big|^2\Big\}^{1/k} \\ &< \exp\left(c\frac{\log p}{\log\log p}\right).|Q|^{\frac{2}{k}}\Big\{\tfrac{1}{p^2}\sum_{\chi}\Big|\sum_{t\in\mathbb{F}_p}\chi(t)\Big|^2\Big|\sum_{\xi\in Q}\chi(\xi+z_1)\Big|^2\Big\}^{1/k} \\ &= \exp\left(c\frac{\log p}{\log\log p}\right)\cdot |Q|^{\frac{2}{k}}E(\mathbb{F}_p, Q+z_1)^{\frac{1}{k}}. \end{aligned} \tag{3.5}$$

The second inequality is by definition of I and the divisor bound. Next, let $z = a+\omega b$, with $a, b \in \mathbb{F}_p$ and let $Q = J + \omega J$, with $J = [1, p^{1/4}]$. Then

$$\begin{aligned} &E(\mathbb{F}_p, Q+z) \\ &\quad = \big|\{(t_1,t_2,\xi_1,\xi_2)\in\mathbb{F}_p^2\times Q^2 : t_1(\xi_1+z) = t_2(\xi_2+z)\neq 0\}\big| \\ &\quad = \big|\{(t_1,t_2,x_1,x_2,y_1,y_2)\in\mathbb{F}_p^2\times J^4 : \\ &\qquad t_1((x_1+a)+\omega(y_1+b)) = t_2((x_2+a)+\omega(y_2+b))\neq 0\}\big|. \end{aligned} \tag{3.6}$$

Equating coefficients in (3.6), we have

$$\begin{cases} t_1(x_1+a) = t_2(x_2+a), \\ t_1(y_1+b) = t_2(y_2+b), \end{cases}$$

Therefore,

$$\frac{x_1+a}{y_1+b} = \frac{x_2+a}{y_2+b}.$$

and the number of (x_1, x_2, y_1, y_2) satisfying (3.6) is bounded by $E(a+J, b+J)$, which is bounded by $p^{1/2}\log p$, by [FI]. Hence,

$$E(\mathbb{F}_p, Q+z) \lesssim p^{3/2}\log p\,.$$

By (3.5) and (3.4),

$$(3.3) \le \exp\left(c\frac{\log p}{\log\log p}\right)\cdot |Q|^{2/k} p^{3/2k},$$

and

$$E(I, z_1+Q, z_2+Q) \le \exp\left(c\frac{\log p}{\log\log p}\right)\cdot |Q|^2 p^{3/2k}.$$

This proves Lemma 3. □

LEMMA 4. *Let $I_j = [a_j, b_j]$, where $b_j - a_j \ge p^{1/4}$ for $j = 1, \dots, 4$. Denote*

$$R = I_1 + \omega I_2 \quad \text{and} \quad S = I_3 + \omega I_4\,.$$

Let $I = [1, p^{1/k}]$ with $k \in \mathbb{Z}_+$.

Then

$$E(I, R, S) < \exp\left(c\frac{\log p}{\log\log p}\right)\cdot p^{\frac{3}{2k}-1}\,|R|^2\,|S|^2. \tag{3.7}$$

Proof. Subdivide R and S in translates of Q and apply Lemma 3. Thus the left side of (3.1) needs to be multiplied with $(|R|/|Q|)^2(|S|/|Q|)^2$ which gives (3.7). □

4 Proof of Theorem 5

We now establish the analogue of Burgess for progressions in $\mathbb{F}_{p^2}$.

Theorem 5. *Given $\rho > 1/4$, there is $\delta > 0$ such that if $\omega \in \mathbb{F}_{p^2}\backslash\mathbb{F}_p$ and I, J are intervals of size p^ρ, then*

$$\Big|\sum_{\substack{x\in I\\ y\in J}} \chi(x+\omega y)\Big| < p^{-\delta}\,|I|\,|J| \tag{4.1}$$

for χ a nontrivial multiplicative character. This estimate is uniform in ω.

Proof. Denote $I_0 = [1, p^{1/4}]$ and $K = [1, p^{\,\kappa}]$, where κ is the reciprocal of a positive integer and

$$\rho > \tfrac{1}{4} + 2\kappa\,. \tag{4.2}$$

We translate $I + \omega J$ by $KK(I_0 + \omega I_0)$ and estimate (following the procedure sketched in section 1)

$$\begin{aligned}\frac{1}{|K|^2|I_0|^2}\sum_{\substack{x_1,y_1\in I_0\\ s\in K\\ x\in I,\,y\in J}}\Big|\sum_{t\in K}\chi\big(x+\omega y+st(x_1+\omega y_1)\big)\Big| \\ = \frac{1}{|K|^2|I_0|^2}\sum_{\substack{x\in I,\,y\in J\\ x_1,y_1\in I_0\\ s\in K}}\left|\sum_{t\in K}\chi\left(t+\frac{x+\omega y}{s(x_1+\omega y_1)}\right)\right|.\end{aligned} \tag{4.3}$$

With the notation from section 1, we have

$$\begin{aligned}\alpha &\le \left(|I_0|^2\,|K|\,|I|\,|J|\right)^{1-\frac{1}{k}} E(K, I_0+\omega I_0, I+\omega J)^{\frac{1}{2k}}\\ &\le \exp\left(c\frac{\log p}{\log\log p}\right)\cdot\left(|I_0|^2\,|K|\,|I|\,|J|\right)^{1-\frac{1}{k}}\left(\frac{|K|^{3/2}|I_0|^4|I|^2|J|^2}{p}\right)^{1/2k}\\ &= \exp\left(c\frac{\log p}{\log\log p}\right)\cdot|I_0|^2\,|I|\,|J|\,|K|^{1-\frac{1}{4k}}p^{-\frac{1}{2k}},\end{aligned}$$

by Lemma 4, and

$$\beta \lesssim |K|^{1/2}p^{1/k}+|K|p^{1/2k}.$$

Hence, taking $\kappa = 1/k$, (4.3) is bounded by $|I|\,|J|\,p^{-1/4k^2}$ and the theorem is proved with any $\delta < 1/4k^2$ (taking p large enough). □

REMARK 5.1. In [DL], the result (4.1) was obtained under the assumption that $\rho > 1/3$. In general, it was shown in [DL] that if $\omega_1,\dots,\omega_d$ is a basis in $\mathbb{F}_{p^d}$ then

$$\Big|\sum_{x_i\in I_i}\chi(x_1\omega_1+\cdots+x_d\omega_d)\Big| < p^{-\delta}|I_1|\cdots|I_d|\,, \tag{4.6}$$

provided $I_1,\dots,I_d$ are intervals in $\mathbb{F}_p$ of size at least p^ρ with

$$\rho > \frac{d}{2(d+1)}\,. \tag{4.7}$$

For $d \ge 5$, there is a better (uniform) result in [C2], namely

$$\rho > \tfrac{2}{5}+\varepsilon\,. \tag{4.8}$$

As a consequence of Theorem 5, we have

COROLLARY 6. *Assume $-k \in \mathbb{F}_p$ is not a quadratic residue. Then*

$$\Big|\sum_{\substack{x\in I\\ y\in J}}\chi(x^2+ky^2)\Big| < p^{-\delta}|I|\,|J| \tag{4.9}$$

for χ nontrivial and I, J intervals of size at least $p^{\frac14+\varepsilon}$. Here $\delta=\delta(\varepsilon)>0$ is uniform in k.

Proof. Let $\omega = \sqrt{-k}$. Since x^2+ky^2 is irreducible modulo p, $\chi(x^2+ky^2)$ is a character $(\mathrm{mod}\,p)$ of $x+\omega y$ in the quadratic extension $\mathbb{Q}(\omega)$. □

5 Extension to $\mathbb{F}_{p^d}$

There is the following generalization of Lemma 1.

LEMMA 7. *Let $\omega \in \mathbb{F}_{p^d}$ be a generator over $\mathbb{F}_p$. Given $0<\sigma<1/2$ and let*

$$\begin{aligned}Q &= \left\{x_0+x_1\omega+\cdots+x_{d-1}\omega^{d-1} : x_i\in[1,p^\sigma]\right\}\\ Q_1 &= \left\{y_0+y_1\omega : y_i\in\left[1,p^{\frac12-\sigma}\right]\right\}.\end{aligned}$$

Then

$$\max_{\xi\in\mathbb{F}_{p^d}}\left|\{(z,z_1)\in Q\times Q_1 : \xi = zz_1\}\right| < \exp\left(c_d\frac{\log p}{\log\log p}\right). \tag{5.1}$$

Proof. The proof is similar to that of Lemma 1. It uses the fact that if

$$(x_0 + x_1\omega + \cdots + x_{d-1}\omega^{d-1})(y_0 + y_1\omega) = \xi = (x_0' + \cdots + x_{d-1}'\omega^{d-1})(y_0' + y_1'\omega)$$

then the polynomial

$$(x_0 + x_1X + \cdots + x_{d-1}X^{d-1})(y_0 + y_1X) - (x_0' + x_1'X + \cdots + x_{d-1}'X^{d-1})(y_0' + y_1'X)$$

is irreducible in $\mathbb{F}_p[X]$, or vanishes. □

Hence the analogues of Lemmas 2, 2′ hold. Thus

LEMMA 8. *Let Q, Q_1 be as in Lemma 7 and let $z \in \mathbb{F}_{p^d}$. Then*

$$E(z+Q, Q_1) < \exp\left(c_d \frac{\log p}{\log\log p}\right) \cdot |Q|\,|Q_1| + |Q_1|^2. \tag{5.2}$$

We need the analogue of Lemma 3, but in a slightly more general setting.

LEMMA 9. *Let Q, Q_1 be as in Lemma 7 with $|Q_1| \le |Q|$ and let $I_s = [1, p^{1/k_s}]$ for $s = 1, \dots, r$, with $k_s \in \mathbb{Z}_+$ and $\frac{1}{k_1} + \cdots + \frac{1}{k_r} < 1$. Then*

$$\begin{aligned} E(I_1, \dots, I_r, z+Q, Q_1) &< \exp\left(c_d \frac{\log p}{\log\log p}\right) p^{1+(d-2)\sigma+2(1-\sigma)\sum_{s=1}^r 1/k_s} \\ &= \exp\left(c_d \frac{\log p}{\log\log p}\right) \cdot |Q|\,|Q_1| \prod_s |I_s|^{2(1-\sigma)}. \end{aligned} \tag{5.3}$$

Proof. The left of (5.3) equals

$$\tfrac{1}{p^d} \sum_{\chi} \prod_{s=1}^{r} \Big|\sum_{t\in I_s} \chi(t)\Big|^2 \Big|\sum_{\xi\in Q} \chi(z+\xi)\Big|^2 \Big|\sum_{\xi\in Q_1} \chi(\xi)\Big|^2$$

which we estimate by Hölder's inequality as

$$\prod_{s=1}^{r} \underbrace{\Big\{\frac{1}{p^d}\sum_{\chi}\Big|\sum_{t\in I_s}\chi\Big|^{2k_s}\Big|\sum_{\xi\in Q}\chi\Big|^2\Big|\sum_{\xi\in Q_1}\chi\Big|^2\Big\}^{\frac{1}{k_s}}}_{A_s^{1/k_s}} \underbrace{\Big\{\frac{1}{p^d}\sum_{\chi}\Big|\sum_{\xi\in Q}\chi\Big|^2\Big|\sum_{\xi\in Q_1}\chi\Big|^2\Big\}^{1-\sum\frac{1}{k_s}}}_{B^{1-\sum 1/k_s}}. \tag{5.4}$$

Here we denote $\sum_{t\in I_s}\chi = \sum_{t\in I_s}\chi(t)$, $\sum_{\xi\in Q}\chi = \sum_{\xi\in Q}\chi(z+\xi)$, etc.

By Lemma 8

$$B = E(z+Q, Q_1) < \exp\left(c\frac{\log p}{\log\log p}\right)|Q|\,|Q_1|\,. \tag{5.5}$$

It is clear from the definition of multiplicative energy that

$$\begin{aligned} A_s &\le |Q_1|^2 E(\underbrace{I_s, \dots, I_s}_{k_s}, z+Q) \\ &\le |Q_1|^2 \exp\left(c_{k_s}\frac{\log p}{\log\log p}\right)\cdot E(\mathbb{F}_p, z+Q)\,. \end{aligned}$$

To bound $E(\mathbb{F}_p, z+Q)$, we write $z = a_0 + a_1\omega + \cdots + a_{d-1}\omega^{d-1}$. Hence

$$E(\mathbb{F}_p, z+Q) = \sum_{i=0}^{d-1} \Theta_i\,, \tag{5.6}$$

where

$$\Theta_0 = \Big| \Big\{ (t, t', x_0, \dots, x_{d-1}, x'_0, \dots, x'_{d-1}) \in \mathbb{F}_p^2 \times [1, p^\sigma]^{2(d-1)} : \left(1 + \frac{x_1 + a_1}{x_0 + a_0}\omega + \cdots + \frac{x_{d-1} + a_{d-1}}{x_0 + a_0}\omega^{d-1}\right) \tag{5.7}$$

$$= t' \left(1 + \frac{x'_1 + a_1}{x'_0 + a_0}\omega + \cdots + \frac{x'_{d-1} + a_{d-1}}{x'_0 + a_0}\omega^{d-1}\right) \Big\} \Big| \tag{5.8}$$

and the other Θ_i's are denoted similarly.

Equating the coefficients of (5.7) and (5.8), we have

$$t = t',$$

$$\frac{x_i + a_i}{x_0 + a_0} = \frac{x'_i + a_i}{x'_0 + a_0}, \quad \text{for } i = 1, \dots, d. \tag{5.9}$$

For $i = 1$, the number of solutions (x_0, x'_0, x_1, x'_1) in (5.9) is bounded by $E([1, p^\sigma] + a_0, [1, p^\sigma] + a_1)$, which is bounded by $p^{2\sigma} \log p$. The choices of t and $x_2, \dots, x_{d-1}$ is bounded by $p\, p^{\sigma(d-2)}$. Therefore,

$$E(\mathbb{F}_p, z + Q) \le d p^{1+\sigma d} \log p\,,$$

and

$$A_s \le |Q_1|^2 \exp\left(c_{k_s} \frac{\log p}{\log\log p}\right) \cdot p^{1+\sigma d}. \tag{5.10}$$

Note that $|Q| = p^{d\sigma}$ and $|Q_1| = p^{1-2\sigma}$. Putting (5.4), (5.5) and (5.10) together, we have

$$\begin{aligned} &E(I_1, \dots, I_r, z + Q, Q_1) \\ &\quad \le \exp\left(c_d \frac{\log p}{\log\log p}\right) \cdot |Q_1|^{2\sum 1/k_s} p^{(1+\sigma d)\sum 1/k_s} \big(|Q|\ |Q_1|\big)^{1-\sum 1/k_s} \\ &\quad = \exp\left(c_d \frac{\log p}{\log\log p}\right) \cdot |Q_1|^{1+\sum 1/k_s} |Q|^{1-\sum 1/k_s}\ p^{(1+\sigma d)\sum 1/k_s} \\ &\quad = \exp\left(c_d \frac{\log p}{\log\log p}\right) \cdot p^{(1+\sum 1/k_s)(1-2\sigma) + (1-\sum 1/k_s)d\sigma + (1+\sigma d)\sum 1/k_s}, \end{aligned}$$

which is (5.3). □

We now estimate a character sum over $\mathbb{F}_{p^d}$.

Theorem 10. *Let $\omega \in \mathbb{F}_{p^d}$ be a generator over $\mathbb{F}_p$, and let $J_0, \dots, J_{d-1}$ be intervals of size at least $p^{\rho_d + \varepsilon}$, where*

$$\rho_d = \frac{\sqrt{d^2 + 2d - 7} + 3 - d}{8}. \tag{5.11}$$

Denote

$$Q = \{x_0 + x_1\omega + \cdots + x_{d-1}\omega^{d-1} : x_i \in J_i,\ \text{for } i = 0, \dots, d-1\}.$$

Then

$$\sum_{q \in Q} \chi(q) < p^{-\delta} |J_0| \cdots |J_{d-1}|, \tag{5.12}$$

where $\delta = \delta(\varepsilon) > 0$ is independent of ω.

Proof. First we denote ρ_d by ρ. Note that, by (5.11)

$$\tfrac{1}{4} \le \rho \le \tfrac{1}{2}\,. \tag{5.13}$$

Let

$$Q_0 = \left\{ y_0 + y_1\omega : y_i \in \left[1, c_d\, p^{\frac{1}{2}-\rho}\right] \right\}.$$

Let further $k_1, \dots, k_r \in \mathbb{Z}_+$ satisfy

$$2\rho - \tfrac{1}{2} - 2\varepsilon < \tfrac{1}{k_1} + \cdots + \tfrac{1}{k_r} < 2\rho - \tfrac{1}{2} - \varepsilon\,, \tag{5.14}$$

where $\varepsilon > 0$ will be taken sufficiently small and $r < r(\varepsilon)$.

Let

$$I = \left[1, p^{\varepsilon/2}\right] \quad \text{and} \quad I_s = \left[1, p^{1/k_s}\right]$$

for $s = 1, \dots, r$. We then translate Q by

$$I \cdot \prod_{s=1}^{r} I_s \cdot Q_0$$

and carry out Burgess' argument as outlined in section 1.

The estimate of the left-hand side of (5.12) is

$$\sum_{q \in Q} \chi(q) \le p^{-(\frac{\varepsilon}{2} + \sum \frac{1}{k_s} + 1 - 2\rho)} \alpha\beta\,, \tag{5.15}$$

where

$$\begin{aligned} \alpha &\le \left(|Q|\,|Q_0|\, p^{\sum 1/k_s}\right)^{1-\frac{1}{k}} E(Q, Q_0, I_1, \dots, I_r)^{1/2k} \\ &\le \left(|Q|\,|Q_0|\; p^{\sum 1/k_s}\right)^{1-\frac{1}{k}} \cdot \exp\left(c_d\, \frac{\log p}{\log\log p}\right) \cdot \left(|Q|\,|Q_0|\; p^{2(1-\rho)\sum 1/k_s}\right)^{1/2k}, \end{aligned} \tag{5.16}$$

$$\beta \le k\,|I|^{\frac{1}{2}} p^{\frac{d}{2k}} + 2|I|\; p^{\frac{d}{4k}} < p^{\frac{\varepsilon}{4} + \frac{d}{2k}} + p^{\frac{\varepsilon}{2} + \frac{d}{4k}}, \tag{5.17}$$

and $k \in \mathbb{Z}_+$ to be chosen.

Claim.

$$|Q|\,|Q_0|\, p^{2(1-\rho)\sum \frac{1}{k_s}} < |Q|^2 |Q_0|^2 p^{2\sum \frac{1}{k_s} - \frac{d}{2} - \tau}, \quad \textit{for some } \tau > 0\,. \tag{5.18}$$

Proof of Claim. We will show

$$d\rho + (1-2\rho) + 2(1-\rho)\sum \tfrac{1}{k_s} < 2d\rho + 2(1-2\rho) + 2\sum \tfrac{1}{k_s} - \tfrac{d}{2}\,. \tag{5.19}$$

This is equivalent to

$$d\rho + (1-2\rho) + 2\rho \sum \tfrac{1}{k_s} - \tfrac{d}{2} > 0\,.$$

From (5.14), the choice of $k_1, \dots, k_r$, and taking ε small enough, it suffices to show that

$$d\rho + (1-2\rho) + 2\rho\left(2\rho - \tfrac{1}{2}\right) - \tfrac{d}{2} > 0\,,$$

namely,

$$4\rho^2 + (d-3)\rho - \frac{d-2}{2} > 0\,,$$

which is our assumption (5.11). □

Putting (5.15)–(5.18) together, we have

$$\begin{aligned} \sum_{q \in Q} \chi(q) \le\; & p^{-(\frac{\varepsilon}{2} + \sum \frac{1}{k_s} + 1 - 2\rho)} \left(|Q|\,|Q_0|\; p^{\sum \frac{1}{k_s}}\right)^{1-\frac{1}{k}} \\ & \cdot \left(|Q|^2\,|Q_0|^2\; p^{2\sum \frac{1}{k_s} - \frac{d}{2} - \tau}\right)^{\frac{1}{2k}} \left(p^{\frac{\varepsilon}{4} + \frac{d}{2k}} + p^{\frac{\varepsilon}{2} + \frac{d}{4k}}\right) \end{aligned}$$

$$= |Q|\big(p^{-\frac{\varepsilon}{4}+\frac{1}{2k}(\frac{d}{2}-\tau)} + p^{-\frac{\tau}{2k}}\big)\,.$$

Theorem 10 is proved, if we chose $k > d/\varepsilon$. □

REMARK 10.1. Returning to Remark 1.1, (see (4.7)), we note that

$$\rho_d < \frac{d}{2(d+1)}$$

with $\rho_2 = \frac{1}{4}, \rho_3 = \frac{1}{\sqrt{8}}, \rho_4 = \frac{\sqrt{17}-1}{8}$, and $\rho_5 = \frac{\sqrt{7}-1}{4}$.

6 Character Sums of Binary Quadratic Forms

Following a similar approach, we show the following:

Theorem 11. *Given $\varepsilon > 0$, there is $\delta > 0$ such that the following holds. Let p be a large prime and $f(x,y) = x^2 + axy + by^2$ which is not a perfect square* $(\mathrm{mod}\, p)$. *Let $I, J \subset [1, p-1]$ be intervals of size*

$$|I|, |J| > p^{\frac{1}{4}+\varepsilon}. \tag{6.1}$$

Then

$$\Big|\sum_{x\in I, y\in J} \chi\big(f(x,y)\big)\Big| < p^{-\delta}|I|\,|J| \tag{6.2}$$

for χ a nontrivial multiplicative character $(\mathrm{mod}\, p)$. *This estimate is uniform in f.*

Result was shown by Burgess assuming $|I|, |J| > p^{\frac{1}{3}+\varepsilon}$ instead of (6.1).

Proof. There are two cases.

Case 1. f is irreducible $(\mathrm{mod}\, p)$. Then $\chi(f(x,y))$ is a character $(\mathrm{mod}\, p)$ of $x + \omega y$, with $\omega = \frac{1}{2}a + \frac{1}{2}\sqrt{a^2 - 4b}$, in the quadratic extension $\mathbb{Q}(\omega)$ and the result then follows from Corollary 6 above.

Case 2. $f(x,y)$ is reducible in $\mathbb{F}_p[x,y]$.

$$f(x,y) = (x - \lambda_1 y)(x - \lambda_2 y) \quad \lambda_1 \neq \lambda_2 \ (\mathrm{mod}\, p)\,.$$

We will estimate

$$\sum_{x\in I, y\in J} \chi\big((x - \lambda_1 y)(x - \lambda_2 y)\big)\,.$$

The basis strategy is as in the $\mathbb{F}_{p^2}$-case (cf. Theorem 5), but replacing $\mathbb{F}_{p^2}$ by $\mathbb{F}_p \times \mathbb{F}_p$ (with coordinate-wise multiplication).

Let $I_0 = \big[1, \frac{1}{10}p^{1/4}\big]$ and $K = [1, p^\kappa]$, where $\kappa = \frac{\varepsilon}{4}$.

We translate (x,y) by (stx_1, sty_1) with $x_1, y_1 \in I_0$ and $s, t \in K$ and estimate

$$\frac{1}{|K|^2|I_0|^2} \sum_{\substack{x\in I,\, y\in J \\ x_1, y_1 \in I_0 \\ s\in K}} \left| \sum_{t\in K} \chi\left(\left(t + \frac{x - \lambda_1 y}{s(x_1 - \lambda_1 y_1)}\right)\left(t + \frac{x - \lambda_2 y}{s(x_1 - \lambda_2 y_1)}\right)\right)\right|. \tag{6.3}$$

For $(z_1, z_2) \in \mathbb{F}_p \times \mathbb{F}_p$, denote

$$\omega(z_1, z_2) = \left|\left\{(x, y, x_1, y_1, s) \in I \times J \times I_0 \times I_0 \times K : \right.\right.$$
$$\left.\left. z_1 = \frac{x - \lambda_1 y}{s(x_1 - \lambda_1 y)}, z_2 = \frac{x - \lambda_2 y_1}{s(x_1 - \lambda_2 y_1)}\right\}\right|.$$

Hence

$$(6.3) = \frac{1}{|K|^2|I_0|^2} \sum_{\substack{z_1\in\mathbb{F}_p\\ z_2\in\mathbb{F}_p}} \omega(z_1,z_2)\Big|\sum_{t\in K}\chi\big((t+z_1)(t+z_2)\big)\Big|, \tag{6.4}$$

which we estimate the usual way using Holder's inequality and Weil's theorem. The required property is a bound

$$\sum_{z_1,z_2}\omega(z_1,z_2)^2 < |I|^2|J|^2|K|^2p^{-\tau} \tag{6.5}$$

for some $\tau>0$ (cf. (4.4)).

We may assume $|I|$, $|J|<p$. Let

$$\begin{aligned} R &= \big\{(x-\lambda_1 y, x-\lambda_2 y) : x\in I\,,\ y\in J\big\}\\ T &= \big\{(x_1-\lambda_1y_1, x_1-\lambda_2y_1) : x_1,y_1\in I_0\big\}\\ S &= \big\{(s,s) : s\in K\big\}\,, \end{aligned} \tag{6.6}$$

considered as subsets of $\mathbb{F}_p^*\times\mathbb{F}_p^*$.

Hence (6.5) is equivalent to

$$E(R,T,S) < p^{-\tau}|I|^2|J|^2|K|^2. \tag{6.7}$$

To establish (6.7), we prove the analogues of Lemmas 1–4.

We first estimate $E(R,T)$.

Lemma 12. *Let R and T be defined as in* (6.6). *Then*

$$E(R,T) < \exp\left(c\frac{\log p}{\log\log p}\right)\cdot|R|^2. \tag{6.8}$$

Writing R as a union of translates of T

$$R = \bigcup_{\alpha\lesssim|R|/|T|}(T+\xi_\alpha)$$

we have

$$E(R,T) \le \tfrac{|R|^2}{|T|^2}\max_{\xi\in\mathbb{F}_p\times\mathbb{F}_p}E(T+\xi,T)\,.$$

Thus it will suffice to show that

$$\max_{\zeta,\xi\in\mathbb{F}_p\times\mathbb{F}_p}E(T+\zeta,T+\xi) < \exp\left(c\frac{\log p}{\log\log p}\right)|T|^2. \tag{6.9}$$

Using the same argument as in the proof of Lemma $2'$, it suffices to prove (6.9) for $\zeta=\xi=0$.

Lemma 13. *Let T be defined as in* (6.6). *Then*

$$E(T,T) < \exp\left(c\frac{\log p}{\log\log p}\right)|T|^2. \tag{6.10}$$

There is a stronger statement which is the analogue of Lemma 1.

Lemma 14. *Let T be defined as in* (6.6). *Then*

$$\max_{\rho\in\mathbb{F}_p^*\times\mathbb{F}_p^*}\big|\{(z_1,z_2)\in T\times T : \rho=z_1z_2\}\big| < \exp\left(c\frac{\log p}{\log\log p}\right). \tag{6.11}$$

Proof. Writing $z_1 = (x_1 - \lambda_1 y_1, x_1 - \lambda_2 y_1)$, $z_2 = (x_2 - \lambda_1 y_2, x_2 - \lambda_2 y_2)$ with $x_1, x_2, y_1, y_2 \in I_0$, we want to estimate the number of solutions in $x_1, x_2, y_1, y_2 \in I_0$ of

$$\begin{cases} (x_1 - \lambda_1 y_1)(x_2 - \lambda_1 y_2) = \rho_1 \pmod p \\ (x_1 - \lambda_2 y_1)(x_2 - \lambda_2 y_2) = \rho_2 \pmod p \end{cases} \tag{6.12}$$

Let $\mathcal{F}$ be the set of quadruples $(x_1, x_2, y_1, y_2) \in I_0^4$ such that (6.12) holds. If $(x_1, x_2, y_1, y_2), (x_1', x_2', y_1', y_2') \in \mathcal{F}$, then λ_1, λ_2 are the (distinct) roots $(\mathrm{mod}\, p)$ of the polynomial

$$(y_1 y_1 - y_1' y_2')X^2 + (x_1' y_2' + y_1' x_2' - x_1 y_2 - y_1 x_2)X + (x_1 x_2 - x_1' x_2') = 0\,. \tag{6.13}$$

By the definition of I_0, the coefficients in (6.13) are integers bounded by $\frac{1}{25} p^{1/2}$. Since all non-vanishing polynomials (6.13) are proportional in $\mathbb{F}_p[X]$, they are also proportional in $\mathbb{Z}[X]$. Hence they have common roots $\tilde\lambda_1, \tilde\lambda_2$ and there are conjugate $\tilde\rho_1, \tilde\rho_2 \in \mathbb{Q}(\tilde\lambda_1)$ such that

$$\begin{cases} (x_1 - \tilde\lambda_1 y_1)(x_2 - \tilde\lambda_1 y_2) = \tilde\rho_1 \\ (x_1 - \tilde\lambda_2 y_1)(x_2 - \tilde\lambda_2 y_2) = \tilde\rho_2 \end{cases} \tag{6.14}$$

for all $(x_1, x_2, y_1, y_2) \in \mathcal{F}$.

As in Lemma 1, we use a divisor estimate in the integers of $\mathbb{Q}(\tilde\lambda_1)$ to show that there are at most $\exp\big(c\frac{\log p}{\log\log p}\big)$ solutions of (6.14) in $x_1 - \tilde\lambda_1 y_1, x_2 - \tilde\lambda_1 y_2$, $x_1 - \tilde\lambda_2 y_1, x_2 - \tilde\lambda_2 y_2$. Since $\tilde\lambda_1 \neq \tilde\lambda_2$, these four elements of $\mathbb{Q}(\tilde\lambda_1)$ determine x_1, y_1, x_2, y_2. Therefore, $|\mathcal{F}| < \exp\big(c\frac{\log p}{\log\log p}\big)$. This proves Lemma 14. □

Returning to (6.7), we proceed as in Lemma 3. Let $\kappa = 1/k$ in the definition of K. Thus

$$\begin{aligned} &E(R,T,S) \\ &\quad = \tfrac{1}{p^2} \sum_{\chi = \chi_1\chi_2} \Big|\sum_{z\in S} \chi(z)\Big|^2 \Big|\sum_{z_1\in R} \chi(z_1)\Big|^2 \Big|\sum_{z_2\in T} \chi(z_2)\Big|^2 \\ &\quad \le \underbrace{\Big[\tfrac{1}{p^2}\sum_{\chi} \Big|\sum_{z\in S}\chi(z)\Big|^{2k} \Big|\sum_{R}\cdots\Big|^2 \Big|\sum_{T}\cdots\Big|^2\Big]^{\frac1k}}_{(6.15)^{\frac1k}} \underbrace{\Big[\tfrac{1}{p^2}\sum_{\chi} \Big|\sum_{R}\cdots\Big|^2 \Big|\sum_{T}\cdots\Big|^2\Big]^{1-\frac1k}}_{E(R,T)^{1-\frac1k}} \\ &\quad < (6.15)^{\frac1k} \cdot \exp\Big(c\,\frac{\log p}{\log\log p}\Big) \cdot |R|^{2(1-\frac1k)} \end{aligned} \tag{6.16}$$

(the last inequality is by Lemma 12), where

$$\begin{aligned} (6.15) &= \tfrac{1}{p^2}\sum_{\chi} \Big|\sum_{z\in S}\chi(z)\Big|^{2k} \Big|\sum_{z_1\in R}\chi(z_1)\Big|^2 \Big|\sum_{z_2\in T}\chi(z_2)\Big|^2 \\ &\le \frac{|T|^2}{p^2}\sum_{\chi} \Big|\sum_{z\in S}\chi(z)\Big|^{2k} \Big|\sum_{z_1\in R}\chi(z_1)\Big|^2 \\ &< \exp\left(c_k\frac{\log p}{\log\log p}\right)\cdot\frac{|T|^2}{p^2}\sum_{\chi_1\chi_2} \Big|\sum_{t\in\mathbb{F}_p}\chi_1(t)\chi_2(t)\Big|^2 \Big|\sum_{\substack{x\in I\\ y\in J}}\chi_1(x-\lambda_1 y)\chi_2(x-\lambda_2 y)\Big|^2 \end{aligned}$$

$$= \exp\left(c\frac{\log p}{\log\log p}\right)\cdot |T|^2 E(R,\Delta)\,, \tag{6.17}$$

where $\Delta = \{(t,t) : t \in \mathbb{F}_p\}$. The multiplicative energy $E(R,\Delta)$ in (6.17) equals the number of solutions in $(x,x',y,y',t,t') \in I^2 \times J^2 \times (\mathbb{F}_p^*)^2$ of

$$\begin{cases} t(x-\lambda_1 y) \equiv t'(x'-\lambda_1 y') \pmod p \\ t(x-\lambda_2 y) \equiv t'(x'-\lambda_2 y') \pmod p \end{cases} \tag{6.18}$$

(with the restriction that all factors are nonvanishing).

Rewriting (6.18) as

$$tx - t'x' \equiv \lambda_1(ty - t'y') \equiv \lambda_2(ty - t'y') \pmod p$$

and since $\lambda_1 \neq \lambda_2 \pmod p$

$$\begin{aligned} tx &\equiv t'x' \pmod p \\ ty &= t'y' \pmod p\,. \end{aligned}$$

Hence

$$xy' \equiv x'y \pmod p \tag{6.19}$$

and the number of solutions of (6.19) is bounded by

$$E(I,J) \lesssim (\log p)\cdot |I|\,|J| \tag{6.20}$$

(since $|I|, |J| < p$).

Once x, x', y, y' is specified, the number of solutions of (6.18) in (t,t') is at most $p-1$.

Hence (6.18) has at most

$$p(\log p)\cdot |I|\,|J|$$

solutions and substitution in (6.17) gives the estimate

$$(6.15) < \exp\left(c\,\frac{\log p}{\log\log p}\right)\cdot p\,|R|\,|T|^2. \tag{6.21}$$

Substituting of (6.21) in (6.16) gives

$$E(R,TS) < \exp\left(c\,\frac{\log p}{\log\log p}\right)\cdot p^{\frac{1}{k}}|R|^{2-\frac{1}{k}}|S|^{\frac{2}{k}}. \tag{6.22}$$

Recalling the definition of S, we have $|S| = |I_0|^2 = p^{1/2}$.

Also $\kappa = 1/k$, and $|K| = p^{1/k}$. Hence

$$\begin{aligned} (6.22) &= \exp\left(c\,\frac{\log p}{\log\log p}\right)\cdot p^{\frac{2}{k}}\big(|I|\ \ |J|\big)^{2-\frac{1}{k}} \\ &= \exp\left(c\,\frac{\log p}{\log\log p}\right)\cdot |K|^2\big(|I|\ \ |J|\big)^{2-\kappa} \end{aligned} \tag{6.23}$$

and (6.7) certainly holds.

This proves Theorem 11. □

Acknowledgement. The author would like to thank the referees for helpful comments.

References

[B1] D.A. Burgess, On character sums and primitive roots, Proc. London Math. Soc (3) 12 (1962), 179–192.

[B2] D.A. Burgess, Character sums and primitive roots in finite fields, Proc. London Math. Soc (3) 37 (1967), 11–35.

[B3] D.A. Burgess, A note on character sums of binary quadratic forms, JLMS 43 (1968), 271–274.

[C1] M.-C. Chang, Factorization in generalized arithmetic progressions and applications to the Erdős–Szemerédi sum-product problems, Geom. Funct. Anal. 13 (2003), 720–736.

[C2] 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.

[DL] H. 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. 119:2 (1993), 265–372.

[K] A.A. Karacuba, Estimates of character sums, Math. USSR-Izvestija 4:1 (1970), 19–29.

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

Mei-Chu Chang, Mathematics Department, University of California, Riverside, CA 92521, USA
mcc@math.ucr.edu

Received: September 11, 2008
Revision: October 15, 2008
Accepted: October 23, 2008