

HIGH ORDER MOMENTS OF CHARACTER SUMS

TODD COCHRANE AND ZHIYONG ZHENG

(Communicated by Dennis A. Hejhal)

ABSTRACT. We establish the upper bound

$$\frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll_{\epsilon, k} p^{k-1+\epsilon} + B^k p^\epsilon,$$

with p a prime and k any positive integer, the sum being over all nonprincipal multiplicative characters $(\bmod p)$.

1.

In this paper we obtain upper bounds on the character sum

$$(1) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k},$$

where a, B and k are positive integers, p is a prime, χ runs through the set of multiplicative characters $(\bmod p)$, and χ_o is the principal character. We shall assume that $B < p$ and that the interval $a+1 \leq x \leq a+B$ does not contain a multiple of p . A trivial bound for the sum in (1) that follows directly from the Polya-Vinogradov inequality is

$$\frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll p^k (\log p)^{2k}.$$

Let \mathcal{B} be the cube

$$(2) \quad \mathcal{B} = \{\mathbf{x} \in \mathbb{Z}^{2k} : a+1 \leq x_i \leq a+B, 1 \leq i \leq 2k\}$$

of cardinality $|\mathcal{B}| = B^{2k}$, and let V be the set of integer solutions of the congruence

$$x_1 x_2 \dots x_k \equiv x_{k+1} x_{k+2} \dots x_{2k} \pmod{p}.$$

Then

$$|\mathcal{B} \cap V| = \frac{1}{p-1} \sum_{x_1=a+1}^{a+B} \dots \sum_{x_{2k}=a+1}^{a+B} \sum_{\chi} \chi(x_1 x_2 \dots x_k x_{k+1}^{-1} \dots x_{2k}^{-1})$$

Received by the editors February 25, 1996.

1991 *Mathematics Subject Classification*. Primary 11L40, 11D79.

Key words and phrases. Character sums, congruences.

$$\begin{aligned}
 &= \frac{|\mathcal{B}|}{p-1} + \frac{1}{p-1} \sum_{\chi \neq \chi_o} \sum_{x_1=a+1}^{a+B} \cdots \sum_{x_{2k}=a+1}^{a+B} \chi(x_1 x_2 \cdots x_k x_{k+1}^{-1} \cdots x_{2k}^{-1}) \\
 (3) \quad &= \frac{|\mathcal{B}|}{p-1} + \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k}.
 \end{aligned}$$

Thus, we have

$$(4) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} = |\mathcal{B} \cap V| - \frac{|\mathcal{B}|}{p-1}.$$

For $k = 1$ it is plain that $|\mathcal{B} \cap V| = B$ and so (4) is just

$$(5) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^2 = B - \frac{B^2}{p-1}.$$

In particular, if $B < (p-1)/2$, then

$$(6) \quad \frac{B}{2} \leq \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^2 < B,$$

whence

$$(7) \quad \min_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right| \leq \sqrt{B}$$

and

$$(8) \quad \max_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right| \geq \sqrt{B/2}.$$

For $k = 2$ it was shown in the paper of Ayyad, Cochrane and Zheng ([1], Theorem 2) that

$$(9) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^4 \ll B^2 \log^2 p,$$

and that, for $B < \sqrt{p}$,

$$(10) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^4 \gg B^2 \log B,$$

whence

$$(11) \quad \max_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right| \gg \sqrt{B} (\log B)^{1/4}.$$

For higher moments Montgomery and Vaughan ([4], Theorem 1) established

$$(12) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \max_B \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll p^k,$$

which is sharper, by a power of $\log p$, than what one obtains trivially from the Polya-Vinogradov inequality. The main result of this paper is the following

Theorem. For positive integers k ,

$$(13) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll_{\epsilon,k} p^{k-1+\epsilon} + B^k p^\epsilon.$$

In particular, for intervals of length $B \gg p^{1-\frac{1}{k}}$ we have

$$(14) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll_{\epsilon,k} B^k p^\epsilon.$$

It is significant to note that the validity of (14) for arbitrary k and $B < p$ is equivalent to the upper bound

$$(15) \quad \left| \sum_{x=a+1}^{a+B} \chi(x) \right| \ll_\epsilon B^{1/2} p^\epsilon,$$

for nonprincipal χ , which on the assumption of the Grand Riemann Hypothesis is known to be true; see Montgomery and Vaughan ([3]). We note that for $k = 1$ and $k = 2$ the upper bounds in (5) and (9) are sharper than (13).

For intervals of short length we may improve on (13) by writing

$$(16) \quad \begin{aligned} \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} &\leq \max_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k-4} \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^4 \\ &\ll B^2 \log^2 p \max_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k-4}, \end{aligned}$$

and then inserting the upper bound of Burgess ([2]),

$$\left| \sum_{x=a+1}^{a+B} \chi(x) \right| \ll_\epsilon B^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} \log p,$$

where r is any positive integer ≥ 2 . For intervals of length $\ll p^{1/4}$ we just insert the trivial upper bound $\left| \sum_{x=a+1}^{a+B} \chi(x) \right| \leq B$. In summary, we have for $k \geq 3$,

$$(17) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll_{\epsilon,k} \begin{cases} B^k p^\epsilon, & p^{1-\frac{1}{k}} \leq B < p, \\ p^{k-1+\epsilon}, & p^{\frac{5}{8}-\frac{1}{4k}} \leq B \leq p^{1-\frac{1}{k}}, \\ B^k p^{\frac{3}{8}(k-2)+\epsilon}, & p^{\frac{11}{24}} \leq B \leq p^{\frac{5}{8}-\frac{1}{4k}} \quad (r = 2), \\ B^{\frac{4}{3}k-\frac{2}{3}} p^{\frac{2}{9}(k-2)+\epsilon}, & p^{\frac{19}{48}} \leq B \leq p^{\frac{11}{24}} \quad (r = 3), \\ \vdots \\ B^{2k-2}, & B \leq p^{1/4}. \end{cases}$$

We have indicated (roughly speaking) the best upper bound available on each of the intervals in (17).

2. THE FUNDAMENTAL IDENTITY AND A KEY LEMMA

View \mathcal{B} and V as subsets of \mathbb{F}_p^{2k} , and let α denote the characteristic function of \mathcal{B} with finite Fourier expansion

$$(18) \quad \alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y})e_p(\mathbf{x} \cdot \mathbf{y}),$$

where as usual $e_p(*) = e^{\frac{2\pi i}{p} *}$, $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{2k} x_i y_i$, $\sum_{\mathbf{y}} = \sum_{\mathbf{y} \in \mathbb{F}_p^{2k}}$. The Fourier coefficients are given by

$$(19) \quad a(\mathbf{y}) = p^{-2k} \prod_{i=1}^{2k} e_p\left(-\left(a + \frac{1}{2} + \frac{B}{2}\right)y_i\right) \frac{\sin(\pi B y_i/p)}{\sin(\pi y_i/p)},$$

where a term in the product is taken to be B if $y_i = 0$. We have

$$\begin{aligned} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} &= \sum_{\chi \neq \chi_o} \sum_{x_1 \neq 0} \cdots \sum_{x_{2k} \neq 0} \alpha(\mathbf{x}) \chi(x_1 x_2 \cdots x_k x_k^{-1} \cdots x_{2k}^{-1}) \\ &= \sum_{\mathbf{y}} a(\mathbf{y}) \sum_{\chi \neq \chi_o} \sum_{x_1 \neq 0} \cdots \sum_{x_{2k} \neq 0} \chi(x_1 x_2 \cdots x_k x_{k+1}^{-1} \cdots x_{2k}^{-1}) e_p(\mathbf{x} \cdot \mathbf{y}) \\ (20) \quad &= \sum_{\mathbf{y}} a(\mathbf{y}) \sum_{\chi \neq \chi_o} \prod_{i=1}^k \sum_{x_i \neq 0} \chi(x_i) e_p(x_i y_i) \prod_{i=k+1}^{2k} \sum_{x_i \neq 0} \chi(x_i^{-1}) e_p(x_i y_i). \end{aligned}$$

Now if $y_i = 0$ for some i , then the sum over x_i is zero, since χ is nonprincipal. If all of the y_i are nonzero, then the sum over \mathbf{x} is just

$$(21) \quad \chi\left(\prod_{i=1}^k y_i^{-1} y_{i+k}\right) G(\chi)^k G(\chi^{-1})^k = p^k \chi((-1)^k y_1^{-1} \cdots y_k^{-1} y_{k+1} \cdots y_{2k}),$$

where $G(\chi)$ denotes the Gaussian sum $G(\chi) = \sum_{x \neq 0} \chi(x) e_p(x)$. Here we have used the identities $G(\chi^{-1}) = \chi(-1) \overline{G(\chi)}$ and $|G(\chi)|^2 = p$ for $\chi \neq \chi_o$. Summing over χ and using the identity,

$$(22) \quad \sum_{\substack{y_i \neq 0 \\ \text{for all } i}} a(\mathbf{y}) = p^{-2k} \sum_{\mathbf{x} \in \mathcal{B}} \sum_{\substack{\mathbf{y} \\ y_i \neq 0}} e_p(x_i y_i) = \frac{B^{2k}}{p^{2k}},$$

we obtain the

Fundamental Identity.

$$(23) \quad \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} = p^k \sum_{\substack{y_i \neq 0 \\ y_1 \cdots y_k = (-1)^k y_{k+1} \cdots y_{2k}}} a(\mathbf{y}) - \frac{B^{2k}}{p^k(p-1)}.$$

Lemma. Let $V^\pm \subset \mathbb{Z}^{2k}$ be the set of integer solutions of

$$(24) \quad y_1 \cdots y_k \equiv \pm y_{k+1} \cdots y_{2k} \pmod{p},$$

and let \mathcal{B} be the box of points $0 < |y_i| < B_i$, $1 \leq i \leq 2k$, with the B_i positive integers. Then

$$(25) \quad |\mathcal{B} \cap V^\pm| \ll_{\epsilon,k} \left(\frac{|\mathcal{B}|}{p} + \sqrt{|\mathcal{B}|} \right) p^\epsilon.$$

Proof. We may suppose without loss of generality that $\prod_{i=1}^k B_i \geq \prod_{i=k+1}^{2k} B_i$ and that all of the y_i are positive. Let y_{k+1}, \dots, y_{2k} be any fixed values with $0 < y_i < B_i$, $k+1 \leq i \leq 2k$, and put $c \equiv y_{k+1} \cdots y_{2k} \pmod{p}$ with $0 < c < p$. Then any integer solution y_1, \dots, y_k of (24) with $0 < y_i < B_i$, $1 \leq i \leq k$, must satisfy

$$(26) \quad y_1 \cdots y_k = c + \ell p \quad \text{or} \quad y_1 \cdots y_k = (p - c) + \ell p$$

for some integer ℓ with $0 \leq \ell \leq \prod_{i=1}^k B_i/p$. For each such value ℓ the number of solutions of (26) is $\leq (\tau(c + \ell p))^k + (\tau(p - c + \ell p))^k \ll_\epsilon p^{k^2\epsilon} \ll_{\epsilon,k} p^\epsilon$, where τ is the divisor function. Thus, the total number of solutions of (26) with ℓ in the specified range is

$$\ll_{\epsilon,k} \left(\frac{\prod_{i=1}^k B_i}{p} + 1 \right) p^\epsilon.$$

We obtain the upper bound in (25) on multiplying by the number of choices for y_{k+1}, \dots, y_{2k} . □

3. PROOF OF THE THEOREM

We start by noting that the Fourier coefficients (19) of the characteristic function α admit the upper bound

$$(27) \quad |a(\mathbf{y})| \ll \prod_{i=1}^{2k} \min\left(\frac{B}{p}, \frac{1}{|y_i|}\right) \quad (|y_i| < p/2).$$

Letting the y_i run through the intervals $0 < |y_i| \leq p/B_i$ and $2^{r_i}p/B_i < |y_i| \leq 2^{r_i+1}p/B_i$ for $r_i = 0, 1, 2, \dots$, stopping when $2^{r_i} > B_i/2$, we have

$$\sum_{\substack{y_i \neq 0 \\ y_1 \cdots y_k = (-1)^k y_{k+1} \cdots y_{2k}}} |a(\mathbf{y})| \ll B^{2k} p^{-2k} \sum_{r_1=0} \cdots \sum_{r_{2k}=0} \prod_{i=1}^{2k} 2^{-r_i} \sum_{\substack{0 < |y_i| \leq 2^{r_i} p/B \\ \mathbf{y} \in V^\pm}} 1,$$

where V^\pm is as defined in the Lemma. Inserting the upper bound in (25), the above is

$$\begin{aligned} &\ll_{\epsilon,k} B^{2k} p^{-2k} \sum_{r_1=0} \cdots \sum_{r_{2k}=0} \prod_{i=1}^{2k} 2^{-r_i} \left(\frac{p^{2k-1}}{B^{2k}} \prod_{i=1}^{2k} 2^{r_i} + \frac{p^k}{B^k} \prod_{i=1}^{2k} 2^{r_i/2} \right) p^\epsilon \\ &\ll_{\epsilon,k} p^{-1+\epsilon} + B^k p^{-k+\epsilon}. \end{aligned}$$

The theorem now follows immediately from the Fundamental Identity (23).

REFERENCES

- [1] A. Ayyad, T. Cochrane and Z. Zheng, *The congruence $x_1x_2 \equiv x_3x_4 \pmod{p}$, the equation $x_1x_2 = x_3x_4$ and mean values of character sums*, J. Number Theory **59** (2) (1996), 398–413. MR **97i**:11091
- [2] D.A. Burgess, *On character sums and L-series. II*, Proc. London Math. Soc. (3) **13** (1963), 524–536. MR **26**:6133
- [3] H.L. Montgomery and R.C. Vaughan, *Exponential sums with multiplicative coefficients*, Inventiones Math. **43** (1977), 69–82. MR **56**:15579
- [4] H.L. Montgomery and R.C. Vaughan, *Mean values of character sums*, Canad. J. Math. **31** (3) (1979), 476–587. MR **81c**:10043

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KANSAS 66506
E-mail address: cochrane@math.ksu.edu

DEPARTMENT OF MATHEMATICS, ZHONGSHAN UNIVERSITY, GUANGZHOU 510275, PEOPLE'S REPUBLIC OF CHINA