HIGH ORDER MOMENTS OF CHARACTER SUMS

TODD COCHRANE AND ZHIYONG ZHENG

(Communicated by Dennis A. Hejhal)

Abstract. We establish the upper bound

\[
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll e^{\epsilon k} p^{k-1+\epsilon} + B^k p^\epsilon,
\]

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

1.

In this paper we obtain upper bounds on the character sum

\[
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k},
\]

where \( a, B \) and \( k \) are positive integers, \( p \) is a prime, \( \chi \) runs through the set of multiplicative characters \( \mod p \), and \( \chi_0 \) 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

\[
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll p^k (\log p)^{2k}.
\]

Let \( B \) be the cube

\[
B = \{ x \in \mathbb{Z}^{2k} : a + 1 \leq x_i \leq a + B, 1 \leq i \leq 2k \}
\]

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

\[
x_1x_2 \ldots x_k \equiv x_{k+1}x_{k+2} \ldots x_{2k} \pmod{p}.
\]

Then

\[
|B \cap V| = \frac{1}{p-1} \sum_{x_1=a+1}^{a+B} \cdots \sum_{x_{2k}=a+1}^{a+B} \sum_{\chi} \chi(x_1x_2 \ldots x_kx_{k+1}^{-1} \ldots x_{2k}^{-1})
\]

Received by the editors February 25, 1996.
1991 Mathematics Subject Classification. Primary 11L40, 11D79.
Key words and phrases. Character sums, congruences.

©1998 American Mathematical Society
\[ = \frac{|B|}{p-1} + \frac{1}{p-1} \sum_{\chi \neq \chi_o} \sum_{x_1=a+1}^{a+B} \cdots \sum_{x_{2k}=a+1}^{a+B} \chi(x_1 x_2 \cdots x_k x_{k+1} \cdots x_{2k}) \]

\[ = \frac{|B|}{p-1} + \frac{1}{p-1} \sum_{\chi \neq \chi_o} \sum_{x=a+1}^{a+B} \chi(x)|^{2k}. \]

(3)

Thus, we have

\[ \frac{1}{p-1} \sum_{\chi \neq \chi_o} \sum_{x=a+1}^{a+B} \chi(x)|^{2k} = |B \cap V| - \frac{|B|}{p-1} \]

(4)

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

\[ \frac{1}{p-1} \sum_{\chi \neq \chi_o} \sum_{x=a+1}^{a+B} \chi(x)|^{2} = B - \frac{B^2}{p-1}. \]

(5)

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

\[ \frac{B}{2} \leq \frac{1}{p-1} \sum_{\chi \neq \chi_o} \sum_{x=a+1}^{a+B} \chi(x)|^{2} < B, \]

whence

\[ \min_{\chi \neq \chi_o} \sum_{x=a+1}^{a+B} \chi(x) \leq \sqrt{B} \]

(7)

and

\[ \max_{\chi \neq \chi_o} \sum_{x=a+1}^{a+B} \chi(x) \geq \sqrt{B/2}. \]

(8)

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

\[ \frac{1}{p-1} \sum_{\chi \neq \chi_o} \sum_{x=a+1}^{a+B} \chi(x)|^{4} \ll B^2 \log^2 p, \]

(9)

and that, for \( B < \sqrt{p} \),

\[ \frac{1}{p-1} \sum_{\chi \neq \chi_o} \sum_{x=a+1}^{a+B} \chi(x)|^{4} \gg B^2 \log B, \]

(10)

whence

\[ \max_{\chi \neq \chi_o} \sum_{x=a+1}^{a+B} \chi(x) \gg \sqrt{B} (\log B)^{1/4}. \]

(11)

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

\[ \frac{1}{p-1} \sum_{\chi \neq \chi_o} \max_{B} \sum_{x=a+1}^{a+B} \chi(x)|^{2k} \ll p^k, \]

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 $k$,

\begin{equation}
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll_{\epsilon,k} p^{k-1+\epsilon} + B^k p^\epsilon.
\end{equation}

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

\begin{equation}
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \ll_{\epsilon,k} B^k p^\epsilon.
\end{equation}

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

\begin{equation}
| \sum_{x=a+1}^{a+B} \chi(x) | \ll \epsilon B^{1/2} p^\epsilon,
\end{equation}

for nonprincipal $\chi$, 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

\begin{equation}
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k} \leq \max_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k-4} \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{4}
\end{equation}

\begin{equation}
\ll B^2 \log^2 p \max_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^{2k-4},
\end{equation}

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

\begin{equation}
| \sum_{x=a+1}^{a+B} \chi(x) | \ll \epsilon B^{1-\frac{1}{r}} p^{\frac{r+1}{r+2}} \log p,
\end{equation}

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

\begin{equation}
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \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{2}{k}} \leq B \leq p^{1-\frac{1}{k}}, \\
B^k p^{\frac{k(k-2)}{2}+\epsilon}, & p^{\frac{4}{k}} \leq B \leq p^{\frac{2}{k}} (r = 2), \\
B^{\frac{k}{r}} p^{\frac{k(k-2)}{2}+\epsilon}, & p^{\frac{4}{k}} \leq B \leq p^{\frac{2}{k}} (r = 3), \\
\vdots \\
B^{2k-2}, & B \leq p^{1/4}.
\end{cases}
\end{equation}

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

$$\alpha(x) = \sum_y a(y)e_p(x \cdot y),$$

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

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

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

$$\sum_{\chi \neq \chi_0} a(y) \sum_{x = a+1}^{a+B} \chi(x)^{2k} = \sum_{\chi \neq \chi_0} \sum_{x_k \neq 0} \cdots \sum_{x_{2k} \neq 0} a(x) \chi(x_1 x_2 \ldots x_k x_{k+1} \ldots x_{2k})$$

$$= \sum_y a(y) \sum_{\chi \neq \chi_0} \sum_{x_k \neq 0} \cdots \sum_{x_{2k} \neq 0} \chi(x_1 x_2 \ldots x_k x_{k+1} \ldots x_{2k}) e_p(x \cdot y)$$

$$= \sum_y a(y) \prod_{i=1}^{k} \sum_{\chi \neq \chi_0} \chi(x_i) e_p(x_i y_i) \prod_{i=k+1}^{2k} \sum_{x_i \neq 0} \chi(x_i^{-1}) e_p(x_i y_i).$$

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

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

where $G(\chi)$ denotes the Gaussian sum $G(\chi) = \sum_{x \neq 0} \chi(x) e_p(x)$. Here we have used the identities $G(\chi^{-1}) = \chi(-1) G(\chi)$ and $|G(\chi)|^2 = p$ for $\chi \neq \chi_0$. Summing over $\chi$ and using the identity,

$$\sum_{y_i \neq 0} a(y) = p^{-2k} \sum_{x \in B} \sum_{y \neq 0} e_p(x \cdot y_i) = \frac{B^{2k}}{p^{2k}},$$

we obtain the

**Fundamental Identity.**

$$\frac{1}{p - 1} \sum_{\chi \neq \chi_0} a(y) \sum_{x = a+1}^{a+B} \chi(x)^{2k} = p^k \sum_{y_i \neq 0} a(y) - \frac{B^{2k}}{p^{2k}(p - 1)}.$$

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

$$y_1 \ldots y_k \equiv \pm y_{k+1} \ldots y_{2k} \pmod{p},$$

and let $\sum_{\chi \neq \chi_0} a(y) \sum_{x = a+1}^{a+B} \chi(x)^{2k} = p^k \sum_{y_i \neq 0} a(y) - \frac{B^{2k}}{p^{2k}(p - 1)}.$
and let $B$ be the box of points $0 < |y_i| < B_i$, $1 \leq i \leq 2k$, with the $B_i$ positive integers. Then

\begin{equation}
|B \cap V^\pm| \ll_{\epsilon,k} \left( \frac{|B|}{p} + \sqrt{|B|} \right) p^\epsilon.
\end{equation}

**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 $y_{k+1}, \ldots, y_{2k}$ 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 $y_1, \ldots, y_k$ of (24) with $0 < y_i < B_i$, $1 \leq i \leq k$, must satisfy

\begin{equation}
y_1 \cdots y_k = c + \ell p \quad \text{or} \quad y_1 \cdots y_k = (p - c) + \ell p
\end{equation}

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

\begin{equation}
\ll_{\epsilon,k} \left( \prod_{i=1}^{k} B_i / p + 1 \right) p^\epsilon.
\end{equation}

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

3. **Proof of the theorem**

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

\begin{equation}
|a(y)| \ll \prod_{i=1}^{2k} \min \left( \frac{B}{p}, \frac{1}{|y_i|} \right) \left( |y_i| < p/2 \right)
\end{equation}

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

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

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

\[
\ll_{\epsilon,k} B^{2k} p^{-2k} \sum_{r_1=0}^{2k} \cdots \sum_{r_{2k}=0}^{2k} \prod_{i=1}^{2k} 2^{-r_i} \left( \frac{p^{2k-1}}{B^{2k}} \prod_{i=1}^{2k} 2^{r_i} + \frac{p^k}{B^k} \prod_{i=1}^{2k} 2^{r_i/2} \right) p^\epsilon
\]

\[
\ll_{\epsilon,k} p^{-1+\epsilon} + B^k p^{-k+\epsilon}.
\]

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


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