Dirichlet character sums

by

CHUNLEI LIU (Zhengzhou)

0. Introduction. Exponential sums have a very long history and many applications. Gauss sums, which appeared already in the work of Lagrange ([10]), are instrumental in proving reciprocity laws ([3], [14]). Jacobi sums are a very convenient tool to determine the number of points on certain varieties ([9], [7], [13]). And trigonometric sums play an important role in Waring’s problem ([4]). Such applications have made exponential sums an interesting topic in number theory.

For some exponential sums in a finite field, Weil’s estimate is established ([12]). For some trigonometric sums in a number field, Hua’s estimate is obtained ([5], [6]). Hua’s estimate is believed by experts to hold also for some character sums. The main result in this paper will confirm this belief.

D. Ismoilov ([8]) had studied some Dirichlet character sums to the modulus of a prime power. He proved

\textbf{Proposition 1 ([8])}. Let $p$ be a prime number, let $\chi$ be a character of conductor $p^n$, and let $f(x) = a_0 + a_1 x + \ldots + a_k x^k$ be an integral polynomial such that $k > 3$ and $(p,a_1,\ldots,a_k) = 1$. If $\chi(f(x))$ is not a constant function, then

$$p^{-n(1-1/k)} \left| \sum_{0 \leq x < p^n} \chi(f(x)) \right| \leq k^{2.5}.$$ 

In this paper we shall establish an iteration for the estimation of some Dirichlet character sums. It is a sharpened analogy of the iteration for the estimation of some trigonometric sums. This iteration enables us to obtain sharper estimates for a more general class of Dirichlet character sums.

\textbf{Theorem 1}. Let $p$ be a prime number, let $\chi$ be a character of conductor $p^n$, and let $f(x) = a_0 + a_1 x + \ldots + a_k x^k$ be an integral polynomial such that $k > 3$ and $(p^n,a_1,\ldots,a_k) = p^n$. Then

1991 \textit{Mathematics Subject Classification}: Primary 11L15.

\textit{Key words and phrases}: exponential sums, Dirichlet characters.

This work was supported by NNSFC and MCSEC.
and for every
where

\[
p^{-\frac{(m-n)(1-1/k)}{p}} \left| \sum_{0 \leq x < p^{n-m}} \chi(f(x)) \right| \leq a(p, k),
\]

where

\[
a(2, k) = \begin{cases} 
(k-1)p^{(k+4)/k-1} & \text{if } k \leq 15, \\
(k-1)p^{(k+1)/k-1} & \text{if } k > 15,
\end{cases}
\]

and for every \( p > 2 \),

\[
a(p, k) = \begin{cases} 
1 & \text{if } (k-1)^{2k/(k-2)} \leq p, \\
(k-1)p^{(k-2)/(2k)} & \text{if } (k-1)^2 \leq p < (k-1)^{2k/(k-2)}, \\
(k-1)p^{1/k} & \text{if } (k-1)^{k/(k-2)} \leq p < (k-1)^2, \\
(k-1)p^{3/(k-1)} & \text{if } (k-1)^{k/(k-1)} < p < (k-1)^{k/(k-2)}, \\
(k-1)p^{(k+2)/k-1} & \text{if } (k-1)^{k/(k+1)} < p \leq (k-1)^{k/(k-1)}, \\
(k-1)p^{(k+1)/k-1} & \text{if } p \leq (k-1)^{k/(k+1)},
\end{cases}
\]

with \( k(p) \) denoting the largest integer not exceeding \( k/\ln p \). In particular,

\[
p^{-\frac{(m-n)(1-1/k)}{p}} \left| \sum_{0 \leq x < p^{n-m}} \chi(f(x)) \right| \leq \begin{cases} 
1 & \text{if } p \geq (k-1)^{2k/(k-2)}, \\
k & \text{otherwise.}
\end{cases}
\]

Theorem 1 enables us to obtain Hua’s estimate in the global case.

**Corollary 1.** Let \( \chi \) be a Dirichlet character of conductor \( q \), and let \( f(x) = a_0 + a_1x + \ldots + a_kx^k \) be an integral polynomial such that \( k > 3 \) and \( (q, a_1, \ldots, a_k) = q/q_1 \). Then

\[
q_1^{-\frac{(1-1/k)}{p}} \left| \sum_{0 \leq x < q_1} \chi(f(x)) \right| \leq e^{F(k)},
\]

where \( F(k) = \sum_p \ln a(p, k) \). In particular \(^{(1)}\),

\[
q_1^{-\frac{(1-1/k)}{p}} \left| \sum_{0 \leq x < q_1} \chi(f(x)) \right| \leq e^{1.8k}.
\]

**1. An iteration.** In this section we shall establish an iteration on which the estimation of character sums will be based.

Let \( p \) be a prime number, and let \( \chi \) be a character of conductor \( p^n \). For every integral polynomial \( f(x) = a_0 + a_1x + \ldots + a_kx^k \), we denote by \( c(f) \) the order at \( p \) of the greatest common divisor \( (a_0, a_1, \ldots, a_k) \). We write \( c_0(f) = c(f - f(0)) \) and \( c_1(f) = \min(n, c_0(f)) \).

For every pair \( (f, l) \), where \( f \) is an integral polynomial and \( l \) is an integer no greater than \( c_1(f) \), we write

\[
S(f, l) = \sum_{0 \leq x < p^{n-l}} \chi(f(x)).
\]

We also write \( S(f) = S(f, c_1(f)) \).

\(^{(1)}\) This can be proved by methods employed in [2].
Lemma 1. If $f$ is an integral polynomial such that
\[\min(c(f') + \operatorname{ord}_p(2), 2c(f') - c_0(f)) < n - 1,\]
then
\[S(f) = \sum_{\xi \in R(f)} p^{c_1(f_\xi) - c_0(f) - 1} S(f_\xi),\]
where $f_\xi(y) = f(\xi + py)$ and
\[R(f) = \{0 \leq \xi < p \mid p^{-c(f')} f'(\xi) \equiv 0 \pmod{p}\}.

Proof. First we observe that, for every $i > 0$, $p^{-c(f')} f^{(i)}(\xi)/(i-1)!$ is an integer since it is the coefficient of $y^{i-1}$ in the integral polynomial $p^{-c(f')} (\xi + y)$. So for every $i > 0$,
\[\operatorname{ord}_p\left(\frac{f^{(i)}(\xi)}{i!} p^f\right) \geq i - \operatorname{ord}_p(i) + c(f') \geq 1 + c(f').\]
Hence $c_0(f_\xi) \geq c(f') + 1 \geq c_0(f) + 1$.

Secondly we observe that
\[S(f) = \sum_{0 < \xi \leq p} S(f_\xi, c_0(f) + 1) = \sum_{0 < \xi \leq p} p^{c_1(f_\xi) - c_0(f) - 1} S(f_\xi).

Therefore it suffices to show that $S(f_\xi)$ vanishes if $\xi \notin R(f)$.

So assume that $\xi \notin R(f)$. We observe that the order at $p$ of $pf'(\xi)$, which is the constant term of the polynomial $(f_\xi)'$, is $c(f') + 1$. So
\[c_0(f_\xi) \leq c((f_\xi)') \leq c(f') + 1,
\]
which along with the inequality $c_0(f_\xi) \geq c(f') + 1$ shows that
\[c((f_\xi)') = c(f') + 1 = c_0(f_\xi).

We now proceed to prove that $S(f_\xi)$ vanishes. It suffices to show that the subsum over every coset of $(p^{n-c(f')-2})$ vanishes. The subsum over the coset $b + (p^{n-c(f')-2})$ is
\[\sum_{0 \leq y < p} \chi(f(\xi + pb + p^{n-c(f')-1}y)).\]
As at the beginning of this proof, we see that, for every $i > 2$,
\[\operatorname{ord}_p\left(\frac{f^{(i)}(\xi + pb)}{i!} p^{(n-c(f')-1)i}\right) \geq i(n - c(f') - 1) - \operatorname{ord}_p(i) + c(f') \geq n.\]
For $i = 2$, we see that
\[\operatorname{ord}_p\left(\frac{f^{(i)}(\xi + pb)}{i!} p^{(n-c(f')-1)i}\right) \geq \max(2n - c(f') - 2 - \operatorname{ord}_p(2), 2n - 2c(f') + c_0(f)) \geq n.

So $f(\xi + pb + p^{n-c(f')-1}y)$ differs from $f(\xi + pb) + p^{n-c(f')-1}f'(\xi + pb)y$ by $p^n$ times an integral polynomial. Hence the subsum over the coset $b + (p^{n-c(f')-2})$ equals

$$\sum_{0 \leq y < p} \chi(f(\xi + pb) + p^{n-c(f')-1}f'(\xi + pb)y).$$

We may assume that $p$ does not divide $f(\xi + pb)$ since otherwise this subsum vanishes trivially. Let $y_0$ be an integer such that $y_0f(\xi + pb)$ is in the unit coset $1 + (p^n)$. The subsum then equals

$$\chi(f(\xi + pb)) \sum_{0 \leq y < p} \chi(1 + p^{n-c(f')-1}f'(\xi + pb)y_0y).$$

Since

$$\text{ord}_p(p^{n-c(f')-1}f'(\xi + pb)) = n - 1 \geq n/2,$$

$\chi(1 + p^{n-c(f')-1}f'(\xi + pb)y_0y)$, as a function in $y$, is a nontrivial additive character to the modulus $p$. Therefore the subsum vanishes as required. The proof of Lemma 1 is complete.

If $f$ is an integral polynomial such that

$$\min(c(f') + \text{ord}_p(2), 2c(f') - c_0(f)) < n - 1,$$

we call $f$ a father and $f_\xi$ a child of $f$ for every $\xi \in R(f)$. We call $(f_1, \ldots, f_r)$ a family chain of height $r$ with ancestor $f_1$ if $f_r$ is a father and for every $1 < i \leq r$, $f_i$ is a child of $f_{i-1}$. The maximum height of family chains with ancestor $f$ is called the height of $f$ and is denoted by $h(f)$. We write $h(f) = 0$ if $f$ is not a father.

**Lemma 2.** Let $f$ be an integral polynomial, and let $\xi \in R(f)$ be of multiplicity $m_\xi$. Then

(i) $2 \leq c_0(f_\xi) - c_0(f) \leq \deg f$.

(ii) $c_0(f_\xi) \geq c(f') + 2 - \text{ord}_p(2)$, and equality holds if $m_\xi = 1$.

(iii) If $m_\xi = 1$, then $f_\xi(y) = b_0 + b_1p^\theta y + b_2p^\theta y^2 + b_3p^\theta y^3 + p^\theta+1y^4g(y),$ where $b_0, b_1, b_2$ and $b_3$ are integers, $p \mid b_1$ if $p = 2$, $p$ does not divide $b_2, p \mid b_3$ if $p \neq 3$, and $g$ is an integral polynomial.

(iv) $c((f_\xi)') \leq c(f') + m_\xi + 1$, and equality holds if $m_\xi = 1$.

(v) Counting multiplicities, the number of roots $\eta$ of the congruence

$$p^{-c((f_\xi)')}(f_\xi)'(\eta) \equiv 0 \pmod{p},$$

does not exceed $m_\xi$.

**Proof.** We first observe that

$$c_0(f(\xi + y)) \geq c(f(\xi + y) - f(0)) = c(f - f(0)) = c_0(f),$$
where \( f(\xi+y) \) is regarded as a polynomial in \( y \). Similarly \( c_0(f) \geq c_0(f(\xi+y)) \). So \( c_0(f) = c_0(f(\xi+y)) \). Therefore, \( p^{c_0(f)} \mid \frac{f^{(i)}(\xi)}{i!} \) if \( i > 0 \), and there exists an integer \( i_0 \) with \( 0 < i_0 \leq \deg f \) such that \( p^{c_0(f)+1} \mid \frac{f^{(i_0)}(\xi)}{i_0!} \).

The coefficient of \( y^i \) in the polynomial \( f_\xi(y) = f(\xi + py) \) is \( \frac{f^{(i)}(\xi)}{i!} p^i \). Trivially \( p^{c_0(f)+2} \mid \frac{f^{(i)}(\xi)}{i!} p^i \) if \( i > 1 \). For \( i = 1 \), since \( \xi \in R(f) \), we also have \( p^{c_0(f)+2} \mid \frac{f^{(i)}(\xi)}{i!} p^i \). So \( c_0(f_\xi) \geq c_0(f) + 2 \). On the other hand, the order at \( p \) of \( \frac{f^{(i)}(\xi)}{i!} p^i \) is no greater than \( i_0 + c_0(f) \). So \( c_0(f_\xi) \leq i_0 + c_0(f) \leq \deg f + c_0(f) \), and (i) is proved.

We secondly observe that, for every \( i > 0 \), \( p^{-c(f')} \frac{f^{(i)}(\xi)}{(i-1)!} \) is an integer since it is the coefficient of \( y^{i-1} \) in the integral polynomial \( p^{-c(f')} f'(\xi + y) \). So

\[
\text{ord}_p \left( \frac{f^{(i)}(\xi)}{i!} p^i \right) \geq i - \text{ord}_p(i) + c(f') \geq c(f') + 2 - \text{ord}_p(2)
\]

if \( i > 1 \), where strict inequality holds if \( i > 2 + \text{ord}_p(3) \) and equality holds if \( i = 2 \) and \( m_\xi = 1 \). For \( i = 1 \), since \( \xi \in R(f) \), we have

\[
\text{ord}_p \left( \frac{f^{(i)}(\xi)}{i!} p^i \right) \geq c(f') + 2.
\]

Therefore we see that \( c_0(f_\xi) \geq c(f') + 2 - \text{ord}_p(2) \), where equality holds if \( m_\xi = 1 \). And if \( m_\xi = 1 \), we also see that

\[
f_\xi(y) = b_0 + b_1 p^\beta y + b_2 p^\beta y^2 + b_3 p^\beta y^3 + p^{\beta+1} y^4 g(y),
\]

where \( b_0, b_1, b_2 \) and \( b_3 \) are integers, \( p \mid b_1 \) if \( p = 2 \), \( p \) does not divide \( b_2, p \mid b_3 \) if \( p \neq 3 \), and \( g \) is an integral polynomial. Thus (ii) and (iii) are proved.

To prove (iv) and (v), we observe that

\[
p^{-c(f')} f'(x) = (x - \xi)^{m_\xi} h(x) + pu(x)
\]

where \( u \) is an integral polynomial of degree less than \( m_\xi \) and \( h \) is an integral polynomial such that \( p \nmid h(\xi) \). So

\[
(f_\xi)'(y) = pf'(\xi + py) = p^{mc} c(f') + 1 y^{m_\xi} h(\xi + py) + p^{2+c(f')} u(\xi + py),
\]

from which (iv) follows. The above equalities also show that the reduction of \( p^{-c(f_\xi)'}(f_\xi)' \) at \( p \) is of degree \( m_\xi \), which implies (v). The proof of Lemma 2 is complete.

2. The case \( p \geq (k-1)^{k/(k-2)} \). In this section we prove the estimate of Theorem 1 by induction on \( h(f) \) in the case \( p \geq (k-1)^{k/(k-2)} \).

We observe that \( 2 < k < p \) and \( c(f') = c_0(f) \) for every integral polynomial \( f \). If \( h(f) = 0 \), then \( c_0(f) \geq n - 1 \). So the desired estimate follows from the trivial estimate and Weil’s estimate ([12]).
If now \( h(f) = h > 0 \) and the desired estimate holds for polynomials of height less than \( h \), then, by Lemma 1, Lemma 2(iv) and the assumed estimate for \( S(f_\xi) \), we have
\[
p^{-\left(n-c_0(f)\right)(1-1/k)}|S(f)| \leq a(p, k) \sum_{\xi \in R(f)} p^{(c_1(f_\xi)-c_0(f))/k-1} \\
\leq a(p, k) \sum_{\xi \in R(f)} p^{(m_\xi+1)/k-1}.
\]

By Lemma 4 of [1], the inequality \( \sum_{\xi \in R(f)} m_\xi \leq k - 1 \), and the fact that \( p \geq (k-1)^{k/(k-2)} \), we have
\[
\sum_{\xi \in R(f)} p^{m_\xi/k} \leq \max((k-1)p^{1/k}, p^{(k-1)/k}) \leq p^{(k-1)/k}.
\]

So
\[
p^{-\left(n-c_0(f)\right)(1-1/k)}|S(f)| \leq a(p, k).
\]
The estimate in Theorem 1 is now proved in the case \( p \geq (k-1)^{k/(k-2)} \).

3. The case \( (k-1)^{k/(k-2)} < p < (k-1)^{k/(k-2)} \). In this section we prove the estimate of Theorem 1 in the case \( (k-1)^{k/(k-2)} < p < (k-1)^{k/(k-2)} \).

Again, \( 2 < k < p \) and \( c(f') = c_0(f) \) for every integral polynomial \( f \). If \( h(f) = 0 \), then the desired estimate follows from the trivial one as well as the fact that \( c_0(f) \geq n - 1 \). If \( h(f) > 0 \), then the estimate follows from Lemmas 1, 2(v) and the following.

**Lemma 3.** Let \( g \) be an integral polynomial of degree \( k > 3 \) which is a child of some polynomial, and let \( p \) be a prime such that \( (k-1)^{k/(k-2)} < p < (k-1)^{k/(k-2)} \). If \( g = f_\xi \) is a child of \( f \), then
\[
p^{-\left(n-c_0(f)\right)(1-1/k)} p^{c_1(f_\xi)-c_0(f)-1} |S(f_\xi)| \leq p^{3/k-1} m_\xi.
\]

**Proof.** First assume that \( h(f_\xi) = 0 \). If \( m_\xi = 1 \), then (1) follows from the trivial estimate for \( S(f_\xi) \) and the fact that \( n \leq 2 + c_0(f) + m_\xi \). If \( m_\xi > 1 \), then (1) follows from the fact that \( n \leq 2 + c_0(f) + m_\xi \), the trivial estimate for \( S(f_\xi) \), and Lemma 2.1 of [11], which says that \( p^{m_\xi/k} \leq m_\xi p^{1/k} \).

If now \( h(f_\xi) = h > 0 \) and (1) holds for polynomials of height less than \( h \) which are children of some polynomials, then (1) follows from Lemma 2(ii), (v). The proof of Lemma 3 is complete.

4. The case \( p > 2 \) and \( (k-1)^{k/(k+1)} < p \leq (k-1)^{k/(k-1)} \). In this case \( c(f') \leq c_0(f) + k(p) \) for every integral polynomial \( f \). If \( h(f) = 0 \), then the estimate of Theorem 1 follows from the trivial one as well as the fact that \( n \leq 1 + c(f') \). If \( h(f) > 0 \), then the estimate follows from Lemmas 1, 2(v) and the following.
**Lemma 4.** Let \( g \) be an integral polynomial of degree \( k > 3 \) which is a child of some polynomial, and let \( p \) be an odd prime such that \( (k-1)^{k/(k+1)} < p \leq (k-1)^{k/(k+1)} \). If \( g = f_\xi \) is a child of \( f \), then
\[
P^{-(n-c_0(f))(1-1/k)}p^{c_1(f_\xi)-c_0(f)-1}|S(f_\xi)| \leq p^{(k(p)+2)/k-1}m_\xi.
\]

**Proof.** First we assume that \( h(f_\xi) = 0 \). We observe that
\[
n \leq 1 + c((f_\xi)' \leq 2 + c(f') + m_\xi.
\]
If \( m_\xi > 1 \), then (2) follows from the trivial estimate for \( S(f_\xi) \) and Lemma 2.1 of [11], which says that \( p^{m_\xi/k} \leq m_\xi \). So we may suppose that \( m_\xi = 1 \). By Lemma 2(ii), (iv), we have \( c((f_\xi)' = c_0(f_\xi) = c(f') + 2 \). If \( n \leq c(f') + 2 \), then (2) follows from the trivial estimate for \( S(f_\xi) \). If \( n = c(f') + 3 \), then by Lemma 2(iii), we have
\[
f_\xi(y) = b_0 + b_1p^{n-1}y + b_2p^{n-1}y^2 + b_3p^{n-1}y^3 + p^n y^4 g(y),
\]
where \( b_0, b_1, b_2 \) and \( b_3 \) are integers, \( p \) does not divide \( b_2, p | b_3 \) if \( p \neq 3 \), and \( g \) is an integral polynomial. Therefore we have
\[
S(f_\xi) = \sum_{0 \leq y < p} \chi(b_0 + b'_1p^{n-1}y + b_2p^{n-1}y^2),
\]
where \( b'_1 = b_1 \) if \( p \neq 3 \) and \( b'_1 = b_1 - b_3 \) if \( p = 3 \). We may assume that \( p \) does not divide \( b_0 \) since otherwise this sum vanishes and (2) is proved. Let \( y_0 \) be an integer such that \( y_0 b_0 \) is in the unit coset \( 1 + (p^n) \). Then
\[
S(f_\xi) = \chi(b_0) \sum_{0 \leq y < p} \chi(1 + p^{n-1}y_0(b'_1y + b_2y^2)).
\]
Since \( n = c(f') + 3 > 1 \), \( \chi(1 + p^{n-1}y_0y) \), as a function in \( y \), is a nontrivial additive character to the modulus \( p \). Therefore \( S(f_\xi) \) is a Gauss sum, and we have \( |S(f_\xi)| \leq \sqrt{p} \). Hence
\[
p^{(n-c_0(f))(1-1/k)}p^{(n-c_1(f_\xi))}|S(f_\xi)| \leq p^{(k(p)+3)/k-1}/\sqrt{p} \leq p^{(k(p)+2)/k-1}m_\xi.
\]

If now \( h(f_\xi) = h > 0 \) and (2) holds for polynomials of height less than \( h \) which are children of some polynomials, then (2) follows from Lemma 2(i), (v). The proof of Lemma 4 is complete.

5. The case \( 2 < p \leq (k-1)^{k/(k+1)} \). In this section, \( c(f') \leq c_0(f) + k(p) \) for every integral polynomial \( f \). If \( h(f) = 0 \), then the estimate of Theorem 1 follows from the trivial one as well as the fact that \( n \leq 1 + c(f') \).

**Lemma 5.** Let \( f \) be an integral polynomial of degree \( k > 3 \), let \( p \) be an odd prime such that \( 2 < p \leq (k-1)^{k/(k+1)} \), and let \( f_\xi \) be a child of \( f \) such that \( h(f_\xi) = 0 \). If \( m_\xi > 1 \) or \( n > c_0(f) \), then
\[
P^{-(n-c_0(f))(1-1/k)}p^{c_1(f_\xi)-c_0(f)-1}|S(f_\xi)| \leq p^{(k(p)+1)/k-1}m_\xi.
\]
Hence is an integral polynomial. As in the proof of Lemma 4 we get

\[ |n| \leq c((f_\xi)' + 1) = c_0(f_\xi) + 1 = c(f') + 3. \]

By Lemma 2(iii), we have

\[ |p| \leq \sqrt{p}. \]

By Lemma 2(iii), we have

\[ f_\xi(y) = b_0 + b_1 p^{n-1} y + b_2 p^{n-1} y^2 + b_3 p^n y^3 + p^n y^4 g(y), \]

where \( b_0, b_1, b_2 \) and \( b_3 \) are integers, \( p \) does not divide \( b_2, p | b_3 \) if \( p \neq 3 \), and \( g \) is an integral polynomial. As in the proof of Lemma 4 we get \( |S(f_\xi)| \leq \sqrt{p}. \)

Hence

\[ p^{(n-c_0(f))\{1-1/k\}p^{c_1(f_\xi)-c_0(f)-1}}|S(f_\xi)| \leq p^{(k(p)+1)/k-1|m_\xi|.} \]

The proof of Lemma 5 is complete.

We now turn back to our main concern. If \( h(f) = 1 \), and there is a child \( f_\xi \) of \( f \) such that \( m_\xi = 1 \) and \( n \leq c_0(f_\xi) \), then the desired estimate follows from the trivial estimate for \( S(f) \) and the fact that \( n \leq c_0(f_\xi) \leq 2 + c(f') \).

If \( h(f) = 1 \) and for every child \( f_\xi \) of \( f \), \( m_\xi = 1 \) or \( n > c_0(f) \), then the desired estimate follows from Lemmas 1, 5 and 2(v). If \( h(f) = 1 \), then the estimate follows from Lemmas 1, 2(v) and the following.

**Lemma 6.** Let \( g \) be an integral polynomial of degree \( k > 3 \) which is a child of some polynomial of height greater than 1, and let \( p \) be an odd prime such that \( 2 < p \leq (k-1)^{k/(k+1)} \). If \( g = f_\xi \) is a child of \( f \) with \( h(f) > 1 \), then

\[ p^{-\{n-c_0(f)\}1-1/k\}p^{c_1(f_\xi)-c_0(f)-1}}|S(f_\xi)| \leq p^{(k(p)+1)/k-1|m_\xi|.} \]

**Proof.** First assume that \( h(f_\xi) = 0 \). If \( m_\xi > 1 \), then (3) follows from Lemma 5. If \( m_\xi = 1 \), then by Lemma 2(ii), we have \( c_0(f_\xi) = c(f') + 2 \leq c_0(f_\eta) < n \), where \( f_\eta \) is a child of \( f \) such that \( h(f_\eta) > 0 \). (3) follows from Lemma 5 again.

Secondly we assume that \( h(f_\xi) = 1 \). If \( m_\xi = k-1 \), then (3) follows from Lemma 2(ii) and the desired estimate for \( S(f_\xi) \). So we may suppose that \( m_\xi < k-1 \). By Lemmas 1 and 2(v), it suffices to prove that, for every child \( f_\xi \) of \( f_\xi \),

\[ p^{-\{n-c_0(f)\}1-1/k\}p^{c_1(f_\xi)-c_0(f)}|S(f_\xi)| \leq p^{(k(p)+1)/k-1|m_\eta|.} \]

If \( m_\eta > 1 \) or \( n > c_0((f_\xi)_\eta) \), then this follows from Lemmas 5 and 2(ii). If \( m_\eta = 1 \) and \( n \leq c_0((f_\xi)_\eta) \), then it follows from the trivial estimate for \( S((f_\xi)_\eta) \) and the fact that \( n \leq c_0((f_\xi)_\eta) \leq 2 + c((f_\xi)') \leq c(f') + k + 1 \).

If now \( h(f_\xi) = h > 1 \) and (3) holds for all polynomials of height less than \( h \) which are children of some polynomials of height greater than 1, then (3) follows from Lemmas 1 and 2(ii). This completes the proof of Lemma 6.
6. The case $p = 2$. By considering this case, we now complete the proof of Theorem 1.

We observe that $c(f') \leq c_0(f) + k(p)$ for every integral polynomial $f$. If $h(f) = 0$, then the desired estimate follows from the trivial one as well as the fact that $n \leq 1 + c(f')$. If $h(f) > 0$, then the estimate follows from Lemmas 1, 2(v) and the following.

**Lemma 7.** Let $p = 2$, and let $g$ be an integral polynomial of degree $k > 3$ which is a child of some polynomial. If $g = f_\xi$ is a child of $f$, then

$$p^{-(n-c_0(f)-(1-1/k))}p^{c_1(f_\xi)-c_0(f)-1}|S(f_\xi)|$$

$$\leq \begin{cases} p^{(k(p)+4)/k-1}m_\xi & \text{if } k \leq 15, \\ p^{(k(p)+1)/k-1}m_\xi & \text{if } k > 15. \end{cases}$$

**Proof.** First assume that $h(f_\xi) = 0$. We observe that

$$n \leq 2 + c((f_\xi)'') \leq 3 + c(f') + m_\xi.$$  

If $m_\xi > 1$, then (4) follows from the trivial estimate for $S(f_\xi)$ and the fact that $p^{(m_\xi+2)/k} \leq m_\xi$. So we may suppose that $m_\xi = 1$. By Lemma 2(ii), (iv), we have $c((f_\xi)') = c(f') + 2 = c_0(f_\xi) + 1$. If $n \leq c(f') + 1$, then (4) follows from the trivial estimate for $S(f_\xi)$.

If $n = c(f') + 2$, then by Lemma 2(iii), we have

$$f_\xi(y) = b_0 + b_1p^{n-1}y + b_2p^{n-1}y^2 + p^ny^3g(y),$$

where $b_0, b_1$ and $b_2$ are integers, $p$ does not divide $b_2$, and $g$ is an integral polynomial. As in the proof of Lemma 4 we get $|S(f_\xi)| \leq \sqrt{p}$, from which (4) follows.

If $n = c(f') + 3 = 3$, then (4) follows from the trivial estimate for $S(f_\xi)$. If $n = c(f') + 3 > 3$, then by Lemma 2(iii), we have

$$f_\xi(y) = b_0 + b_2p^{n-2}y^2 + p^{n-1}yg(y),$$

where $b_0$ and $b_2$ are integers, $p$ does not divide $b_2$, and $g$ is an integral polynomial. Therefore we have

$$S(f_\xi) = \sum_{0 \leq y < p^2} \chi(b_0 + b_2p^{n-2}y^2 + p^{n-1}yg(y))$$

$$= 2 \sum_{0 \leq y < 2} \chi(b_0 + b_2'p^{n-2}y),$$

where $b_2' = b_2 + pg(1)$. We may assume that $p$ does not divide $b_0$ since otherwise this sum vanishes and (4) is proved. Let $y_0$ be an integer such that $y_0b_0$ is in the unit coset $1 + (p^n)$. Then

$$S(f_\xi) = 2\chi(b_0) \sum_{0 \leq y < 2} \chi(1 + p^{n-2}y_0b_2'y).$$
Since \( n > 3 \), \( \chi(1 + p^{n-2}y_0b'_2y) \), as a function in \( y \), is a nontrivial additive character to the modulus \( p^3 \). Therefore \( |S(f_\xi)| \leq 2\sqrt{2} \), from which (4) follows.

If \( n = c(f') + 4 \) and \( k \leq 15 \), then (4) follows from the trivial estimate for \( S(f_\xi) \). If \( n = c(f') + 4 \), \( k > 15 \), and \( c(f') < 2 \), then (4) follows from the trivial estimate for \( S(f_\xi) \). If \( n = c(f') + 4 \), \( k > 15 \), and \( c(f') \geq 2 \), then \( n > 5 \). As in the proof of Lemma 2(iii), we can verify that

\[
f_\xi(y) = b_0 + b'_1p^{n-2}y + b_2p^{n-3}y^2 + b_3p^{n-1}y^3 + b_4p^{n-2}y^4 + p^n y^5 g(y),
\]

where \( b_0, b_1, b_3, b_4, \) and \( b_5 \) are integers, \( p \) does not divide \( b_2 \), and \( g \) is an integral polynomial. We may write

\[
f_\xi(y) = b_0 + b'_1p^{n-2}y + b_2'p^{n-3}y^2 + b_3p^{n-1}(y^3 - y) + b_4p^{n-2}(y^4 - y^2) + p^n y^5 g(y).
\]

Then we have \( p \nmid b'_2 \) and

\[
S(f_\xi) = \sum_{0 \leq y < p^3} \chi(b_0 + b'_1p^{n-2}y + b_2'p^{n-3}y^2).
\]

By a linear transformation, we have

\[
S(f_\xi) = \sum_{0 \leq y < p^3} \chi(b'_0 + b_2'p^{n-3}y^2).
\]

We may assume that \( p \) does not divide \( b'_0 \) since otherwise this sum vanishes and (4) is proved. Let \( y_0 \) be an integer such that \( y_0b'_0 \) is in the unit coset \( 1 + (p^n) \). Then

\[
S(f_\xi) = \chi(b_0) \sum_{0 \leq y < p^3} \chi(1 + y_0b'_2p^{n-3}y^2).
\]

Since \( n > 5 \), \( \chi(1 + p^{n-3}y_0b'_2y) \), as a function in \( y \), is a nontrivial additive character to the modulus \( p^3 \). We write \( \chi(1 + p^{n-3}y_0b'_2) = e^{2\pi ir/8} = \varrho \), where \( r \) is an odd integer. Then we have \( S(f_\xi) = 2\chi(b_0)(1 + 2\varrho + \varrho^4) = 4\varrho\chi(b_0) \), from which (4) follows.

If now \( h(f_\xi) = h > 0 \) and (4) holds for all polynomials of height less than \( h \) which are children of some polynomials, then (4) follows from Lemmas 1 and 2(i). The proof of Lemma 7 is complete.

The author thanks Professor Pan Chengbiao for his help.

References

Dirichlet character sums


P.O. Box 1001-46
Zhengzhou 450002
China
E-mail: zeng@public2.ha.zz.cn

Received on 7.4.1997
and in revised form on 6.7.1998 (3164)