ACTA ARITHMETICA
LXXXVIII.4 (1999)

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

Proposition 1 ([8]). *Let p be a prime number, let χ be a character of conductor p^n, and let $f(x)=a_0+a_1x+\ldots+a_kx^k$ 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*
$$p^{-n(1-1/k)}\Big|\sum_{0\le x<p^n}\chi(f(x))\Big|\le k^{2.5}.$$

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.

Theorem 1. *Let p be a prime number, let χ be a character of conductor p^n, and let $f(x)=a_0+a_1x+\ldots+a_kx^k$ be an integral polynomial such that $k>3$ and $(p^n,a_1,\ldots,a_k)=p^m$. Then*

1991 *Mathematics Subject Classification*: Primary 11L15.
Key words and phrases: exponential sums, Dirichlet characters.
This work was supported by NNSFC and MCSEC.

$$p^{-(n-m)(1-1/k)}\Big|\sum_{0\le x<p^{n-m}}\chi(f(x))\Big|\le a(p,k),$$

where

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

and for every $p>2$,

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

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

$$p^{-(n-m)(1-1/k)}\Big|\sum_{0\le x<p^{n-m}}\chi(f(x))\Big|\le\begin{cases}1 & \text{if } p\ge(k-1)^{2k/(k-2)},\\ k & \text{otherwise.}\end{cases}$$

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

Corollary 1. *Let* χ *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*

$$q_1^{-(1-1/k)}\Big|\sum_{0\le x<q_1}\chi(f(x))\Big|\le e^{F(k)},$$

where $F(k)=\sum_p\ln a(p,k)$. *In particular* ([1]),

$$q_1^{-(1-1/k)}\Big|\sum_{0\le x<q_1}\chi(f(x))\Big|\le e^{1.8k}.$$

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 χ 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

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

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

$$R(f) = \{0 \le \xi < p \mid p^{-c(f')} f'(\xi) \equiv 0 \pmod p\}.$$

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 $p^{-c(f')} f'(\xi + y)$. So for every $i > 0$,

$$\operatorname{ord}_p\left(\frac{f^{(i)}(\xi)}{i!} p^i\right) \ge i - \operatorname{ord}_p(i) + c(f') \ge 1 + c(f').$$

Hence $c_0(f_\xi) \ge c(f') + 1 \ge c_0(f) + 1$.

Secondly we observe that

$$S(f) = \sum_{0 < \xi \le p} S(f_\xi, c_0(f) + 1) = \sum_{0 < \xi \le p} p^{c_1(f_\xi) - c_0(f) - 1} S(f_\xi).$$

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

$$c_0(f_\xi) \le c((f_\xi)') \le c(f') + 1,$$

which along with the inequality $c_0(f_\xi) \ge c(f') + 1$ 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

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

As at the beginning of this proof, we see that, for every $i > 2$,

$$\operatorname{ord}_p\left(\frac{f^{(i)}(\xi + pb)}{i!} p^{(n - c(f') - 1)i}\right) \ge i(n - c(f') - 1) - \operatorname{ord}_p(i) + c(f') \ge n.$$

For $i = 2$, we see that

$$\operatorname{ord}_p\left(\frac{f^{(i)}(\xi + pb)}{i!} p^{(n - c(f') - 1)i}\right) \\ \ge \max(2n - c(f') - 2 - \operatorname{ord}_p(2), 2n - 2c(f') + c_0(f)) \ge n.$$

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

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

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

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

Since

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

$\chi(1+p^{n-c(f')-1}f'(\xi+pb)y_0y)$, 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

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

we call f a *father* and f_ξ 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 $1<i\le r$, 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_ξ. Then*

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

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

(iii) *If* $m_\xi=1$, *then* $f_\xi(y)=b_0+b_1p^\theta y+b_2p^\theta y^2+b_3p^\theta y^3+p^{\theta+1}y^4g(y)$, *where* b_0,b_1,b_2 *and* b_3 *are integers*, $p\,|\,b_1$ *if* $p=2$, p *does not divide* b_2, $p\,|\,b_3$ *if* $p\ne3$, *and* g *is an integral polynomial.*

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

(v) *Counting multiplicities*, *the number of roots* η *of the congruence*

$$p^{-c((f_\xi)')}(f_\xi)'(\eta)\equiv0\pmod p,$$

does not exceed m_ξ.

Proof. We first observe that

$$c_0(f(\xi+y))\ge c(f(\xi+y)-f(0))=c(f-f(0))=c_0(f),$$

where $f(\xi+y)$ is regarded as a polynomial in y. Similarly $c_0(f)\ge c_0(f(\xi+y))$. 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 $0<i_0\le\deg f$ such that $p^{c_0(f)+1}\nmid \frac{f^{(i_0)}(\xi)}{i_0!}$.

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 $c_0(f_\xi)\ge c_0(f)+2$. On the other hand, the order at p of $\frac{f^{(i_0)}(\xi)}{i_0!}p^{i_0}$ is no greater than $i_0+c_0(f)$. So $c_0(f_\xi)\le i_0+c_0(f)\le\deg f+c_0(f)$, 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

$$\operatorname{ord}_p\left(\frac{f^{(i)}(\xi)}{i!}p^i\right)\ge i-\operatorname{ord}_p(i)+c(f')\ge c(f')+2-\operatorname{ord}_p(2)$$

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

$$\operatorname{ord}_p\left(\frac{f^{(i)}(\xi)}{i!}p^i\right)\ge c(f')+2.$$

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

$$f_\xi(y)=b_0+b_1p^\theta y+b_2p^\theta y^2+b_3p^\theta y^3+p^{\theta+1}y^4g(y),$$

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 $p\ne3$, 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_ξ and h is an integral polynomial such that $p\nmid h(\xi)$. So

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

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_ξ, which implies (v). The proof of Lemma 2 is complete.

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

We observe that $2<k<p$ and $c(f')=c_0(f)$ for every integral polynomial f. If $h(f)=0$, then $c_0(f)\ge n-1$. 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

$$p^{-(n-c_0(f))(1-1/k)}|S(f)| \le a(p,k) \sum_{\xi\in R(f)} p^{(c_1(f_\xi)-c_0(f))/k-1} \le a(p,k) \sum_{\xi\in R(f)} p^{(m_\xi+1)/k-1}.$$

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

$$\sum_{\xi\in R(f)} p^{m_\xi/k} \le \max((k-1)p^{1/k}, p^{(k-1)/k}) \le p^{(k-1)/k}.$$

So

$$p^{-(n-c_0(f))(1-1/k)}|S(f)| \le a(p,k).$$

The estimate in Theorem 1 is now proved in the case $p \ge (k-1)^{k/(k-2)}$.

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

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 $c_0(f) \ge n-1$. 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 $(k-1)^{k/(k-1)} < p < (k-1)^{k/(k-2)}$. If $g = f_\xi$ is a child of f, then*

$$p^{-(n-c_0(f))(1-1/k)} p^{c_1(f_\xi)-c_0(f)-1}|S(f_\xi)| \le p^{3/k-1} m_\xi. \tag{1}$$

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

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(i), (v). The proof of Lemma 3 is complete.

4. The case $p > 2$ and $(k-1)^{k/(k+1)} < p \le (k-1)^{k/(k-1)}$. In this case $c(f') \le c_0(f) + k(p)$ 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 $n \le 1 + c(f')$. 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 $(k-1)^{k/(k+1)} < p \le (k-1)^{k/(k-1)}$. If $g = f_\xi$ is a child of f, then*

$$p^{-(n-c_0(f))(1-1/k)} p^{c_1(f_\xi)-c_0(f)-1} |S(f_\xi)| \le p^{(k(p)+2)/k-1} m_\xi. \tag{2}$$

P r o o f. First we assume that $h(f_\xi) = 0$. We observe that

$$n \le 1 + c((f_\xi)') \le 2 + c(f') + m_\xi.$$

If $m_\xi > 1$, then (2) follows from the trivial estimate for $S(f_\xi)$ and Lemma 2.1 of [11], which says that $p^{m_\xi/k} \le m_\xi$. 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 $n \le c(f') + 2$, then (2) follows from the trivial estimate for $S(f_\xi)$. If $n = c(f') + 3$, then by Lemma 2(iii), we have

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

where b_0, b_1, b_2 and b_3 are integers, p does not divide b_2, $p \mid b_3$ if $p \ne 3$, and g is an integral polynomial. Therefore we have

$$S(f_\xi) = \sum_{0 \le y < p} \chi(b_0 + b_1' p^{n-1} y + b_2 p^{n-1} y^2),$$

where $b_1' = b_1$ if $p \ne 3$ 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

$$S(f_\xi) = \chi(b_0) \sum_{0 \le y < p} \chi(1 + p^{n-1} y_0 (b_1' y + b_2 y^2)).$$

Since $n = c(f') + 3 > 1$, $\chi(1 + p^{n-1} y_0 y)$, 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 $|S(f_\xi)| \le \sqrt{p}$. Hence

$$p^{(n-c_0(f))/k-1} p^{-(n-c_1(f_\xi))} |S(f_\xi)| \le p^{(k(p)+3)/k-1}/\sqrt{p} \le p^{(k(p)+2)/k-1} m_\xi.$$

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 $2 < p \le (k-1)^{k/(k+1)}$**.** In this section, $c(f') \le c_0(f) + k(p)$ 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 $n \le 1 + c(f')$.

LEMMA 5. *Let f be an integral polynomial of degree $k > 3$, let p be an odd prime such that $2 < p \le (k-1)^{k/(k+1)}$, and let f_ξ be a child of f such that $h(f_\xi) = 0$. If $m_\xi > 1$ or $n > c_0(f)$, then*

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

Proof. If $m_\xi > 1$, this follows from the trivial estimate for $S(f_\xi)$, the fact that $n \le 1 + c((f_\xi)') \le 2 + c(f') + m_\xi$ and Lemma 2.1 of [2], which says that $p^{(m_\xi+1)/k} \le m_\xi$.

If $m_\xi = 1$, then by Lemma 2(ii), (iv) we have

$$n = c((f_\xi)') + 1 = c_0(f_\xi) + 1 = c(f') + 3.$$

By Lemma 2(iii), we have

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

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

$$p^{(n-c_0(f))/k-1} p^{-(n-c_1(f_\xi))} |S(f_\xi)| \le p^{(k(p)+3)/k-1}/\sqrt{p} \le p^{(k(p)+1)/k-1} m_\xi.$$

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_ξ of f such that $m_\xi = 1$ and $n \le c_0(f_\xi)$, then the desired estimate follows from the trivial estimate for $S(f)$ and the fact that $n \le c_0(f_\xi) \le 2 + c(f')$. If $h(f) = 1$ and for every child f_ξ 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* $2 < p \le (k-1)^{k/(k+1)}$. *If $g = f_\xi$ is a child of f with $h(f) > 1$, then*

$$(3) \qquad p^{-(n-c_0(f))(1-1/k)} p^{c_1(f_\xi)-c_0(f)-1} |S(f_\xi)| \le p^{(k(p)+1)/k-1} m_\xi.$$

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 $c_0(f_\xi) = c(f') + 2 \le c_0(f_\eta) < n$, where f_η 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(i) 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 $(f_\xi)_\eta$ of f_ξ,

$$p^{-(n-c_0(f))(1-1/k)} p^{c_1((f_\xi)_\eta)-c_0(f)-2} |S((f_\xi)_\eta)| \le p^{(k(p)+1)/k-1} m_\eta.$$

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

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(i). 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 $c(f') \le c_0(f) + k(p)$ for every integral polynomial f. If $h(f) = 0$, then the desired estimate follows from the trivial one as well as the fact that $n \le 1 + c(f')$. 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*

$$p^{-(n-c_0(f))(1-1/k)} p^{c_1(f_\xi)-c_0(f)-1} |S(f_\xi)| \le \begin{cases} p^{(k(p)+4)/k-1} m_\xi & \text{if } k \le 15, \\ p^{(k(p)+1)/k-1} m_\xi & \text{if } k > 15. \end{cases} \tag{4}$$

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

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

If $m_\xi > 1$, then (4) follows from the trivial estimate for $S(f_\xi)$ and the fact that $p^{(m_\xi+2)/k} \le m_\xi$. 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 $n \le c(f') + 1$, then (4) follows from the trivial estimate for $S(f_\xi)$.

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

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

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 $|S(f_\xi)| \le \sqrt{p}$, 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

$$f_\xi(y) = b_0 + b_2 p^{n-2} y^2 + p^{n-1} y g(y),$$

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

$$\begin{aligned} S(f_\xi) &= \sum_{0 \le y < p^2} \chi(b_0 + b_2 p^{n-2} y^2 + p^{n-1} y g(y)) \\ &= 2 \sum_{0 \le y < 2} \chi(b_0 + b_2' p^{n-2} y), \end{aligned}$$

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 $y_0 b_0$ is in the unit coset $1 + (p^n)$. Then

$$S(f_\xi) = 2\chi(b_0) \sum_{0 \le y < 2} \chi(1 + p^{n-2} y_0 b_2' y).$$

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

If $n=c(f')+4$ and $k\le 15$, 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 $c(f')\ge 2$, then $n>5$. As in the proof of Lemma 2(iii), we can verify that

$$f_\xi(y)=b_0+b_1p^{n-2}y+b_2p^{n-3}y^2+b_3p^{n-1}y^3+b_4p^{n-2}y^4+p^ny^5g(y),$$

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

$$\begin{aligned}f_\xi(y)=b_0+b_1'p^{n-2}y+b_2'p^{n-3}y^2+b_3p^{n-1}(y^3-y)\\+b_4p^{n-2}(y^4-y^2)+p^ny^5g(y).\end{aligned}$$

Then we have $p\nmid b_2'$ and

$$S(f_\xi)=\sum_{0\le y<p^3}\chi(b_0+b_1'p^{n-2}y+b_2'p^{n-3}y^2).$$

By a linear transformation, we have

$$S(f_\xi)=\sum_{0\le y<p^3}\chi(b_0'+b_2'p^{n-3}y^2).$$

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

$$S(f_\xi)=\chi(b_0)\sum_{0\le y<p^3}\chi(1+y_0b_2'p^{n-3}y^2).$$

Since $n>5$, $\chi(1+p^{n-3}y_0b_2'y)$, 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

[1] J.-R. Chen, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711–719.

[2] P. Ding and M.-G. Qi, *Further estimate of complete trigonometric sums*, J. Tsinghua Univ. 29 (1989), no. 6, 74–85.
[3] C. F. Gauss, *Summatio quarumdam serierum singularium*, Comment. Soc. Reg. Sci. Gottingensis 1 (1811); Werke, Vol. 2, Königl. Gesellschaft der Wissenschaften, Göttingen, 1876, 9–45.
[4] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum': IV. The singular series in Waring's Problem and the value of the number $G(k)$*, Math. Z. 12 (1922), 161–188.
[5] L.-K. Hua, *On exponential sums*, J. Chinese Math. Soc. 2 (1940), 301–312.
[6] —, *On exponential sums over an algebraic number field*, Canad. J. Math. 3 (1951), 44–51.
[7] L.-K. Hua and H. S. Vandiver, *On the existence of solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. 35 (1949), 481–487.
[8] D. Ismoilov, *Estimates of complete character sums of polynomials*, Trudy Mat. Inst. Steklov. 200 (1991), 171–184 (in Russian).
[9] C. G. J. Jacobi, *Brief an Gauss vom 8. Februar 1827*, Gesammelte Werke, Vol. 7, Reimer, Berlin, 1891, 393–400.
[10] J.-L. Lagrange, *Réflexions sur la résolution algébrique des équations*, Nouv. Mémoires Acad. Roy. Berlin 1770, 134–215; ibid. 1771, 138–254; Oeuvres, Vol. 3, Gauthier-Villars, Paris, 1869, 205–421.
[11] M.-G. Lu, *Estimate of a complete trigonometric sum*, Sci. Sinica 28 (1985), 561–578.
[12] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.
[13] —, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), 497–508.
[14] —, *La cyclotomie jadis et naguère*, Enseign. Math. (2) 20 (1974), 247–263.

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)