ASIAN J. MATH.
Vol. 4, No. 4, pp. 757–774, December 2000

003

BOUNDS FOR CERTAIN EXPONENTIAL SUMS*

TODD COCHRANE† AND ZHIYONG ZHENG‡

1. Introduction.

In this paper we consider exponential sums of the type

$$S(ax^n + bx, p^m) = \sum_{x \bmod p^m} e(ax^n + bx/p^m), \tag{1.1}$$

and

$$S(ax^n + bx, \chi, p^m) = \sum_{x \bmod p^m} \chi(x) e(ax^n + bx/p^m), \tag{1.2}$$

where p^m is a prime power , $\chi \bmod p^m$ is a Dirichlet character, a, b, n are integers with $n \geq 2$.

The first sum was studied in connection with Waring's problem and we have a classical result due to professor Hua [10]. The second sum has not been studied before as far as the authors know. We hope it can be used in the work of generalizing Waring's problem. In [6], Davenport and Heilbronn showed that

$$S(ax^n + bx, p^m) \ll_n p^{\theta m}(b, p^m), \quad \text{if } p \nmid a, \tag{1.3}$$

where $\theta = 2/3$ if $n = 3$, and $\theta = 3/4$ if $n \geq 3$. Hua [10] showed that $\theta = 1/2$ for all $n \geq 2$ (also see Lemma 4.1 of Vaughan [19]). Hua's proof depends on Weil's estimate for exponential sums over finite fields (see Bombieri [1] or Schmidt [15]). In this case we have

$$|S(ax^n + bx, p)| \leq (n-1)p^{\frac{1}{2}}, \quad \text{if } p \nmid a. \tag{1.4}$$

For $m \geq 2$, following the work of Loxton and Smith [13], and Smith [17], one has that

$$|S(ax^n + bx, p^m)| \leq d_{n-1}(p^m) p^{\frac{m}{2}} (\Delta, p^m)^{\frac{1}{2}}, \tag{1.5}$$

where $d_{n-1}(p^m)$ is the number of representations of p^m as a product of $n-1$ positive integers and Δ is the discriminant of the derivative of the polynomial $ax^n + bx$. After an improvement by Loxton and Vaughan, Theorem 1 of [14] implies the following estimate

$$|S(ax^n + bx, p^m)| \leq (n-1)p^{\frac{m+\tau_0}{2}} (D, p^m)^{\frac{1}{2}}, \tag{1.6}$$

where D is the different of the derivative of the polynomial $ax^n + bx$, and $\tau_0 = 1$ if $p \leq n$, and $\tau_0 = 0$ if $p > n$. Very recently, Dabrowski and Fisher established better bounds for exponential sums of this kind. Under the restriction $p \nmid ab$, $p \nmid n$, and

*Received September 11, 2000; accepted for publication October 20, 2000.
†Department of Mathematics, Kansas State University, Manhattan, KS 66506 (cochrane@math.ksu.edu).
‡Department of Mathematics, Tsinghua University, Beijing 100084, P.R. China (zzheng@math.tsinghua.edu.cn). Supported by NNSF of China (19625102) and partially by "973" project.

$n \geq 2$, their work implies the following bounds (see Theorem 1.8 of [5] or Theorem 2 of Ye [21]): If $p > 2$, then

(1.7)
$$|S(ax^n + bx, p^m)| \leq \begin{cases} (n-1)p^{\frac{m}{2}}, & \text{if } p \nmid n-1, \\ (n-1)p^{\frac{-h}{2}}p^{\frac{m}{2}}, & \text{if } p^h \| n-1, h \geq 1 \text{ and } m \geq 3h+2, \\ (n-1, p-1)p^{\min(h, \frac{m}{2}-1)}p^{\frac{m}{2}}, & \text{if } m \text{ is even}, \\ (n-1, p-1)p^{\min(h, \frac{m-1}{2}-1)}p^{\frac{m+1}{2}}, & \text{if } m \text{ is odd}. \end{cases}$$

There is a similar estimate for $p = 2$.

The purpose of this paper is to improve the above estimate by showing the following quite general result. To state our theorem conveniently, let $ord_p(x)$ denote the normal exponent valuation on the p-adic field. In particular, for $x \in \mathbb{Z}, x \neq 0, p^{ord_p(x)} \| x$.

THEOREM 1.1. *Let $n \geq 2$, $m \geq 2$, $h = ord_p(n-1)$, $\beta = ord_p(n)$, and $a, b \in \mathbb{Z}$ be any integers with $\tau = ord_p(a) \leq m-2$. If $p > 2$ we have*

$$|S(ax^n + bx, p^m)| \leq (n-1, p-1)p^{\frac{1}{2}\min(1,\beta)}p^{\frac{1}{2}\min(h, m-2-\tau)}p^{\frac{m}{2}}(b, p^m)^{\frac{1}{2}}, \tag{1.8}$$

and if $p = 2$, then

$$|S(ax^n + bx, p^m)| \leq 2p^{\frac{1}{2}\min(h, m-2-\tau)}p^{\frac{m}{2}}(b, p^m)^{\frac{1}{2}}, \tag{1.9}$$

where (i, j) denotes the greatest common divisor of two integers i and j.

COROLLARY 1. *If $m \geq 2, n \geq 2$ and $p \nmid n(n-1)$, $(n-1, p-1) = 1$ and $p \nmid b$, then for any integer a, we have the following sharp bound that*

$$|S(ax^n + bx, p^m)| \leq p^{\frac{m}{2}}. \tag{1.10}$$

The condition $\tau \leq m-2$ in the above theorem is natural since we can deal with the case $\tau \geq m-1$ in a trivial manner. If $\tau = ord_p(a) \geq m-1$, then $S(ax^n + bx, p^m) = 0$ when $ord_p(b) = \delta < \tau$. If $ord_p(b) \geq ord_p(a) \geq m$, then $S(ax^n + bx, p^m) = p^m$. If $ord_p(b) \geq ord_p(a) = m-1$, we have $|S(ax^n + bx, p^m)| \leq (n-1)p^{m-\frac{1}{2}}$, by Weil's estimate (1.4).

It also is of interest to compare this result with Theorem 5 of [21], in which Ye considered the special case of very large n, and showed that if $p > 2$, $p \nmid ab$, $n = \varphi(p^m) - k$ with $1 < k \leq p-1$, where $\varphi(p^m) = p^{m-1}(p-1)$ is the Euler function, then one has

$$|S(ax^{\varphi(p^m)-k} + bx, p^m)| \leq \begin{cases} (k+1)p^{\frac{1}{2}} + 1, & \text{if } k > 1, k \mid p-1, \text{ and } m = 1, \\ (k+1)p^{\frac{m}{2}}, & \text{if } 1 < k < p-1, \text{ and } m \geq 2, \\ p^{\frac{m+1}{2}}, & \text{if } k = p-1, \text{ and } m = 3, \text{ or } m \geq 5, \\ p \cdot p^{\frac{m}{2}}, & \text{if } k = p-1, \text{ and } m = 4, \\ p^{\frac{m}{2}}, & \text{if } k = p-1, \text{ and } m = 2. \end{cases}$$

Since $m \geq 2$, if $1 \leq k \leq p-1$, then $p \nmid \varphi(p^m) - k = n$ and we have $\beta = ord_p(n) = 0$. If $1 \leq k \leq p-2$, then $h = ord_p(n-1) = 0$, and $(n-1, p-1) = (k+1, p-1)$. If

$k = p-1$, then $h = 1$, and $(n-1, p-1) = 1$. Thus by (1. 8), if $m \geq 2$, and $p \nmid ab$, we have

$$|S(ax^{\varphi(p^m)-k} + bx, p^m)| \leq \begin{cases} (k+1, p-1)p^{\frac{m}{2}}, & \text{if } 1 \leq k \leq p-2, \\ p^{\frac{m}{2}}, & \text{if } k = p-1, m = 2, \\ p^{\frac{m+1}{2}}, & \text{if } k = p-1, m \geq 3, \end{cases} \tag{1.11}$$

which is better than Ye's result when $1 \leq k \leq p-1$. This improvement allows us to establish a new bound for hyper-Kloosterman sums. We state this result as follows.

Estimation of Kloosterman Sums. The classical Kloosterman sum is defined by

$$K(a, b, p^m) = \sum_{\substack{x \bmod p^m \\ p \nmid x}} e(\frac{a\overline{x} + bx}{p^m}), \quad \text{where } \overline{x}x \equiv 1 (\mathrm{mod} p^m). \tag{1.12}$$

If $m = 1$ we have the well known bound due to Weil [20],

$$|K(a, b, p)| \leq 2p^{\frac{1}{2}}, \qquad \text{if } p \nmid (a, b). \tag{1.13}$$

If $m \geq 2$, Salie [16] showed that there exists an absolute constant C such that

$$|K(a, b, p^m)| \leq Cp^{\frac{m}{2}}, \quad \text{if } p \nmid (a, b) \text{ and } m \geq 2. \tag{1.14}$$

Estermann [8] showed that $C = 2$ for $p > 2$ and $p \nmid (a, b)$, (see Lemma 4 and Lemma 8 of [8]). As a direct corollary of Theorem 1.1, we have Estermann's result immediately.

COROLLARY 2. *If $p > 2$, $m \geq 2$, and $p \nmid (a, b)$, then we have*

$$|K(a, b, p^m)| \leq 2p^{\frac{m}{2}}. \tag{1.15}$$

Proof. If $m \geq 2$, then $K(a, b, p^m) = 0$ if $p|a$, and $p \nmid b$, or $p \nmid a$ and $p|b$. Thus we may assume that $p \nmid ab$. Since $x^{\varphi(p^m)} \equiv 1 (\mathrm{mod} p^m)$ when $p \nmid x$, it follows that

$$K(a, b, p^m) = S(ax^{\varphi(p^m)-1} + bx, p^m). \tag{1.16}$$

The corollary follows by (1.11) immediately. □

We turn now to a discussion of the hyper-Kloosterman sum. For any $a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}$ we define an n-dimensional Kloosterman sum by

$$K_n(a_1, a_2, \cdots a_{n+1}, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{x_n=1}^{p^m} e(\frac{a_1x_1 + \cdots + a_nx_n + a_{n+1}\overline{x_1 \cdots x_n}}{p^m}),$$

where, in the sum, it is understood that the values x_i are restricted to nonzero residue classes (mod p). If $m = 1$, we have a deep estimate due to Deligne,

$$|K_n(a_1, a_2, \cdots a_{n+1}, p^m)| \leq (n+1)p^{\frac{m}{2}}, \quad \text{if } p \nmid a_1a_2 \cdots a_{n+1}. \tag{1.17}$$

If $m \geq 2$, we have $K_n(a_1, a_2, \cdots a_{n+1}, p^m) = 0$ if $p \mid a_i$ for some a_i, and $p \nmid a_j$ for some a_j (see Theorem 3 of [18]). Thus we may assume $p \nmid a_1 a_2 \cdots a_{n+1}$ and restrict our attention to the sum,

$$K_n(a, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{x_n=1}^{p^m} e\left(\frac{x_1 + \cdots + x_n + a\overline{x_1 \cdots x_n}}{p^m}\right). \tag{1.18}$$

In [21], [22] Ye generalized the identity (1.16) to any $n > 1$. If $p > 2$, $p \nmid n$ and $p \nmid a$, he showed that

$$K_n(a, p^m) = \begin{cases} p^{\frac{m}{2}(n-1)} S(ax^{\varphi(p^m)-n} + nx, p^m), & \text{if } m \text{ is even,} \\ \left(\frac{2^{n-1}a^{n-1}n}{p}\right)\varepsilon_p^{n-1} p^{\frac{m}{2}} S(ax^{\varphi(p^m)-n} + nx, p^m), & \text{if } m \text{ is odd,} \end{cases} \tag{1.19}$$

where $(\frac{x}{p})$ is the Legendre symbol and $|\varepsilon_p| = 1$.

By (1.11) and (1.19), we obtain

COROLLARY 3.[1] *Let $p > 2$, $m \geq 2$, $1 \leq n \leq p-1$, and $p \nmid a$, then we have*

$$|K_n(a, p^m)| \leq \begin{cases} (n+1, p-1) p^{\frac{mn}{2}}, & \text{if } 1 \leq n \leq p-2, \\ p^{\frac{mn}{2}}, & \text{if } n = p-1, m = 2, \\ p^{\frac{1}{2}} \cdot p^{\frac{mn}{2}}, & \text{if } n = p-1, m \geq 3. \end{cases} \tag{1.20}$$

The result of this corollary was obtained earlier by R. A. Smith [18, Theorem 6], and by Dabrowski and Fisher [5, Theorem 1.8, Example 1.7].

Mixed Exponential Sums. Another purpose of this paper is to establish an estimate for the mixed exponential sum, $S(ax^n + bx, \chi, p^m)$. If $m = 1$, it follows from Weil's work [17] that for all $\chi \bmod p$, and $p \nmid a$

$$|S(ax^n + bx, \chi, p^m)| \leq np^{\frac{1}{2}}. \tag{1.21}$$

Using the method the authors established in [3] and [4], we obtain the following bound for $S(ax^n + bx, \chi, p^m)$.

THEOREM 1.2. *Let $n \geq 2$, $m \geq 1$ and a, b be any integers with $p \nmid a$. If $p > 2$, then for all $\chi \bmod p^m$, we have*

$$|S(ax^n + bx, \chi, p^m)| \leq np^{\frac{2}{3}m}(b, p^m)^{\frac{1}{3}}. \tag{1.22}$$

If $p = 2$, then for all $\chi \bmod 2^m$, we have

$$|S(ax^n + bx, \chi, 2^m)| \leq 2n2^{\frac{2}{3}m}(b, 2^m)^{\frac{1}{3}}. \tag{1.23}$$

The following example shows that the exponent $\frac{2}{3}m$ in (1.22) is best possible.

EXAMPLE 1.3. For any $a, b \in \mathbb{Z}$ with $p \nmid ab$, and $p \geq 5$, there exists at least one character χ such that

$$|S(ax^2 + bx, \chi, p^3)| = p^2. \tag{1.24}$$

The proof is given at the end of the paper.

[1] A more general result on n-dimensional Kloosterman sums was obtained in a recent work of Todd Cochrane, Ming-Chit Liu and Zhiyong Zheng, "Upper bounds for n-dimensional Kloosterman sums"; preprint.

2. Preliminaries. To prove the above theorems, we first consider exponential sums in general and state some sharp estimates given in the author's works [3] and [4]. Let $f(x)$ be a polynomial with integral coefficients, and let

$$S(f,p^m)=\sum_{x \bmod p^m} e(f(x)/p^m), \quad S(f,\chi,p^m)=\sum_{x \bmod p^m} \chi(x)e(f(x)/p^m). \tag{2.1}$$

Let $d=d(f)$ denote the ordinary degree of $f(x)$, and $d_p(f)$ denote the degree of f read (mod$p$). For $f(x)=a_0+a_1x+\cdots+a_dx^d \in \mathbb{Z}[x]$, we define

$$ord_p(f)=\min_{0\le i\le d}\{ord_p(a_i)\}. \tag{2.2}$$

If $m=1$, it is a well known consequence of the work of Weil [17] on the Riemann hypothesis for curves over a finite field (also see for example Bombieri [1] and Schmidt [14]) that if $d_p(f)\ge 1$ and p is an odd prime, then for all f and all $\chi \bmod p$,

$$|S(f,p)|\le (d_p(f)-1)p^{\frac{1}{2}} \quad \text{and} \quad |S(f,\chi,p)|\le d_p(f)p^{\frac{1}{2}}. \tag{2.3}$$

If $m\ge 2$, Hua [8] and [10] showed that if $d_p(f)\ge 1$, then

$$|S(f,p^m)|\le d^3p^{m(1-\frac{1}{d})}. \tag{2.4}$$

In [2], Chalk considered the zeros of $f'(x)$ modulo p and showed that if $m\ge 2t+2$ then

$$|S(f,p^m)|\le d(\sum_{\alpha\in\mathcal{A}}\mu_\alpha)p^{\frac{t}{M+1}}\cdot p^{m(1-\frac{1}{M+1})}, \tag{2.5}$$

where $t=ord_p(f'(x))$, $\mathcal{A}=\mathcal{A}(f,p)$ is the set of distinct zeros of the related congruence

$$p^{-t}f'(x)\equiv 0 \pmod p, \tag{2.6}$$

μ_α is the multiplicity of each $\alpha\in\mathcal{A}$ and $M=max\{\mu_\alpha\}$ is the maximum multiplicity. In [3] and [4], we improved Chalk's result by proving the following theorem (see Theorem 2.1 of [3]).

THEOREM 2.1. *Let p be an odd prime and f be any nonconstant polynomial defined over $\mathbb{Z}$, $t=ord_p(f'(x))$, $m\ge 2$. Then if $0\le t\le m-2$, we have*
(i) If $\mathcal{A}$ is empty, then $S(f,p^m)=0$.
(ii) If $\mathcal{A}$ is not empty, then

$$|S(f,p^m)|\le (\sum_{\alpha\in\mathcal{A}}\mu_\alpha)p^{\frac{t}{M+1}}p^{m(1-\frac{1}{M+1})}. \tag{2.7}$$

(iii) If $p=2$, then for $m\ge t+3$, or $m=2$, $t=0$, if $\mathcal{A}$ is empty then $S(f,2^m)=0$. Also, for any $m\ge 1$, $t\ge 0$, we have

$$|S(f,2^m)|\le (\sum_{\alpha\in\mathcal{A}}\mu_\alpha)2^{\frac{t}{M+1}}2^{m(1-\frac{1}{M+1})}. \tag{2.8}$$

The estimate (2.7), known as Chalk's conjecture (see [7]), provides a local upper bound for $S(f,p^m)$. Similar upper bounds were obtained by Ding [7] and Loh [12].

Exponential sums with a Dirichlet character χ denoted by $S(f,\chi,p^m)$, are called mixed type exponential sums. Several authors, including E. Bombieri, M. C. Liu and W. M. Schmidt, posed the problem of how to generalize the classical bound of Hua (2.4) to $S(f,\chi,p^m)$. In [3] and [4], we succeeded in establishing a sharp estimate for this sum. To state this result, let p be odd prime and $\chi \bmod p^m$ be a Dirichlet character. Let g be a primitive root $(\mathrm{mod} p^m)$ such that $g > 0$, and

$$g^{p-1} = 1 + rp, \quad \text{with } p \nmid r. \tag{2.9}$$

Then we can find a unique integer $c = c(\chi, g)$ with $0 < c \leq p^{m-1}(p-1)$, such that for all k

$$\chi(g^k) = e(ck/p^{m-1}(p-1)). \tag{2.10}$$

Let

$$t = ord_p(f'(x)) \quad \text{and} \quad t_1 = ord_p(rxf'(x) + c). \tag{2.11}$$

Since $p \nmid r$, it is plain that $t_1 = \min\{t, ord_p(c)\} \leq m-1$. Let $\mathcal{A}_1$ be the set of distinct nonzero solutions of the related congruence

$$p^{-t_1}\{rxf'(x) + c\} \equiv 0 \pmod{p}. \tag{2.12}$$

THEOREM 2.2 (Theorem 1.1 of [3]). *If $0 \leq t_1 \leq m-2$, we have*
(i) If $\mathcal{A}_1$ is empty, then $S(f,\chi,p^m) = 0$.
(ii) If $\mathcal{A}_1$ is not empty, then $t = t_1$, and we have

$$|S(f,\chi,p^m)| \leq (\sum_{\alpha \in \mathcal{A}_1} \mu_\alpha) p^{\frac{t}{M+1}} p^{m(1-\frac{1}{M+1})}, \tag{2.13}$$

where μ_α is the multiplicity of each $\alpha \in \mathcal{A}$ and $M = max\{\mu_\alpha\}$.

Since $M \leq d$, it follows that

$$|S(f,\chi,p^m)| \leq 6dp^{m(1-\frac{1}{d+1})}, \tag{2.14}$$

uniformly for any prime p, polynomial f with $d_p(f) \geq 1$, and $m \geq 1$. We also showed that the exponent $m(1-\frac{1}{d+1})$ is best possible for $m \geq 2$; see Example 9.2 of [3] and Example 1.3 of this paper.

3. Lemmas. To prove Theorem 1.1, we first state a recursion relationship which was established in [3]. Let

$$\sigma_\alpha = ord_p\{f(px+\alpha) - f(\alpha)\}, \quad g_\alpha(x) = p^{-\sigma_\alpha}\{f(px+\alpha) - f(\alpha)\} \tag{3.1}$$

where $\alpha \in \mathcal{A}$ is a solution of congruence (2.6).

LEMMA 1 (Proposition 3.1 of [3]). *If $p > 2$ and $m \geq t+2$, or $p = 2$, $m \geq t+3$, or $p = 2$, $m = 2$, and $t = 0$, then if $\mathcal{A}$ is not empty, we have*

$$S(f,p^m) = \sum_{\alpha \in \mathcal{A}} e(f(\alpha)/p^m) p^{\sigma_\alpha - 1} S(g_\alpha, p^{m-\sigma_\alpha}), \tag{3.2}$$

where $S(g_\alpha, p^{m-\sigma_\alpha}) = p^{m-\sigma_\alpha}$, if $m < \sigma_\alpha$, and

$$S(g_\alpha, p^{m-\sigma_\alpha}) = \sum_{x \bmod p^{m-\sigma_\alpha}} e(g_\alpha(x)/p^{m-\sigma_\alpha}), \quad \text{if } m \geq \sigma_\alpha. \tag{3.3}$$

Trivially, we have $|S(g_\alpha, p^{m-\sigma_\alpha})| \le p^{m-\sigma_\alpha}$, and so we deduce from this lemma the nontrivial estimate for $S(f, p^m)$,

$$|S(f,p^m)| \le (\sum_{\alpha\in\mathcal{A}} 1)p^{m-1}, \quad (0 \le t \le m-2). \tag{3.4}$$

LEMMA 2. *Let p be an odd prime, $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree d and $d_p = d_p(f)$ be the degree of $f(x)$ read modulo p. If $1 \le d_p \le p-1$, we have*

$$|S(f,p^m)| \le (d_p - 1)p^{m(1-\frac{1}{d_p})}. \tag{3.5}$$

Proof. Write $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0 + pH(x)$, where $H(x) \in \mathbb{Z}[x]$, $k = d_p(f)$ with $1 \le k \le p-1$, and $p \nmid a_k$. If $m = 1$, the lemma follows from Weil's estimate. Let $m \ge 2$. Since $f'(x) = ka_k x^{k-1} + \cdots + a_1 + pH'(x)$ and $p \nmid k$, we have $t = 0$. By Theorem 2.1, we have

$$|S(f,p^m)| \le (\sum_{\alpha\in\mathcal{A}} \mu_\alpha)p^{m(1-\frac{1}{M+1})} \le (k-1)p^{m(1-\frac{1}{k})}, \tag{3.6}$$

and the lemma follows. □

LEMMA 3. *Let n be a positive integer with $n \equiv 1 (mod p)$ and $\tau_j = j + ord_p\{\binom{n}{j}\}$ for $1 \le j \le n$. Then if $p > 3$, we have $\tau_j \ge 1 + \tau_2$ for all $j \ge 3$. If $p = 3$, then $\tau_3 = \tau_2$, and $\tau_j \ge 1 + \tau_2$ for all $j \ge 4$. If $p = 2$, then $\tau_4 \ge \tau_3 = 1 + \tau_2$, and $\tau_j \ge 2 + \tau_2$ for all $j \ge 5$.*

Proof. Since $j\binom{n}{j} = (n-j+1)\binom{n}{j-1}$, then for $1 \le j \le n$, we have

$$\tau_j = 1 + ord_p(n-j+1) - ord_p(j) + \tau_{j-1}. \tag{3.7}$$

If $p > 2$, we have

$$ord_p(j!) = \sum_{k=1}^{\infty}[j/p^k] < \frac{j}{p-1} \le \frac{j}{2}. \tag{3.8}$$

Thus if $j \ge 4$, we have

$$\tau_j \ge j - 2 - ord_p(j!) + \tau_2 \ge 1 + \tau_2.$$

If $p > 3$, then $\tau_3 = 1 + \tau_2$ by (3.6), and for all $j \ge 3$, we have $\tau_j \ge 1 + \tau_2$. If $p = 3$, then $\tau_3 = \tau_2$, and $\tau_4 = 1 + \tau_3$. Now we consider $p = 2$. It is easy to see that

$$\tau_{2\delta} \ge 2 - ord_2(\delta) + \tau_{2(\delta-1)} \quad \text{and} \quad \tau_j = 1 + \tau_{j-1}, \quad \text{if } j \text{ is odd.}$$

In particular, $\tau_3 = 1 + \tau_2, \tau_5 = 1 + \tau_4 \ge 2 + \tau_2, \tau_4 \ge \tau_3 = 1 + \tau_2, \tau_6 \ge 2 + \tau_4 \ge 3 + \tau_2$, and $\tau_7 \ge 1 + \tau_6 \ge 4 + \tau_2$. If $j \ge 8$, $j = 2\delta$ with $\delta \ge 4$, we have

$$\tau_{2\delta} \ge 2(\delta - 2) + 1 - ord_2(\delta!) + \tau_4.$$

Since

$$ord_2(\delta!) = \sum_{k=1}^{\infty}[\delta/2^k] < \delta, \tag{3.9}$$

we have

$$\tau_{2\delta} > \delta - 3 + \tau_4 \geq 2 + \tau_2,$$

and the lemma follows immediately. □

LEMMA 4. *Let $\theta_j = j - ord_p(j!)$. If $p > 3$, then $\theta_3 = 1 + \theta_2$ and $\theta_j \geq 1 + \theta_3$ for all $j \geq 4$. If $p = 3$, then $\theta_3 = \theta_2$, and $\theta_j \geq 1 + \theta_3$ for all $j \geq 4$.*

Proof. We have

$$\theta_j = 1 - ord_p(j) + \theta_{j-1}, \quad \text{for } j \geq 2.$$

It follows that

$$\theta_j \geq j - 3 - ord_p(j!) + ord_p(6) + \theta_3. \tag{3.10}$$

If $p \geq 3$, then $ord_p(j!) < \frac{1}{2}j$, and $\theta_j \geq \frac{j}{2} - 3 + ord_p(6) + \theta_3 \geq 1 + \theta_3$, if $j \geq 8$. Now if $p > 3$, then $\theta_3 = 1 + \theta_2$ and $\theta_4 = 1 + \theta_3, \theta_5 \geq \theta_4 \geq 1 + \theta_3, \theta_6 = 1 + \theta_5 \geq 2 + \theta_3, \theta_7 \geq \theta_6 \geq 2 + \theta_3$. If $p = 3$, then $\theta_3 = \theta_2, \theta_4 = \theta_3 + 1, \theta_5 = 1 + \theta_4 = 2 + \theta_3, \theta_6 = \theta_5 = 2 + \theta_3$, and $\theta_7 = 1 + \theta_6 = 3 + \theta_3$. The lemma follows. □

To prove Theorem 1.2, we need to untwist the sum $S(f, \chi, p)$ using the method established in [3]. Let $p > 2$ be an odd prime, $\chi \bmod p^m$ be a Dirichlet character, r and c be defined by (2.9) and (2.10) with $p \nmid r$, and $0 < c \leq p^{m-1}(p-1)$, t and t_1 be defined by (2.11), and $\mathcal{A}_1$ be defined by (2.12).

LEMMA 5. *If $m \geq t_1 + 2$, then for any polynomial f and multiplicative character $\chi \bmod p^m$, we have*
(i) If $\mathcal{A}_1$ is empty, then $S(f, \chi, p^m) = 0$.
(ii) If $\mathcal{A}_1$ is not empty, then $t = t_1$, and

$$S(f, p^m) = \sum_{\alpha \in \mathcal{A}_1} \chi(\alpha) e(f(\alpha)/p^m) \sum_{y \bmod p^{m-1}} e(F_\alpha(y)/p^m), \tag{3.11}$$

where $F_\alpha(y)$ is an integral-valued function given by

$$F_\alpha(y) = f(\alpha(1 + rp)^y) - f(\alpha) + pcy. \tag{3.12}$$

Proof. See formula (6.3) of [3]. □

This lemma also gives a nontrivial estimate for $S(f, \chi, p^m)$, namely,

$$|S(f, \chi, p^m)| \leq (\sum_{\alpha \in \mathcal{A}_1} 1) p^{m-1}, \quad \text{if } 0 \leq t_1 \leq m - 2. \tag{3.13}$$

4. Proof of Theorem 1.1. Let $p > 2$, $m \geq 2$, $n \geq 2$, $a, b \in \mathbb{Z}$, and $f(x) = ax^n + bx$. Put

$$ord_p(b) = \delta, \quad ord_p(n) = \beta \quad \text{and} \quad ord_p(n-1) = h. \tag{4.1}$$

We will prove that if $ord_p(a) = \tau \leq m - 2$, then

$$|S(ax^n + bx, p^m)| \leq (n - 1, p - 1) p^{\frac{1}{2}\min\{1,\beta\}} p^{\frac{1}{2}\min\{h, m-2-\tau\}} p^{\frac{m}{2}} p^{\frac{\delta}{2}}. \tag{4.2}$$

If we have (4.2) when $\tau = 0$ then we claim it is true for any τ with $1 \le \tau \le m-2$. To see this, first note that $S(ax^n + bx, p^m) = 0$ if $\delta < \tau$ and so we may assume $\delta \ge \tau$. Then we have

$$\begin{aligned}|S(ax^n + bx, p^m)| &= p^\tau |\sum_{x \bmod p^{m-\tau}} e(\frac{ap^{-\tau}x^n + bp^{-\tau}x}{p^{m-\tau}})| \\ &\le p^\tau (n-1, p-1) p^{\frac{1}{2}\min\{h, m-2-\tau\}} p^{\frac{\delta-\tau}{2}} p^{\frac{1}{2}\min\{1,\beta\}} p^{\frac{m-\tau}{2}} \\ &\le (n-1, p-1) p^{\frac{1}{2}\min\{1,\beta\}} p^{\frac{1}{2}\min\{h, m-2-\tau\}} p^{\frac{m}{2}} p^{\frac{\delta}{2}}.\end{aligned}$$

Thus without loss of generality, we may let $\tau = 0$, and prove the following inequality,

$$|S(ax^n + bx, p^m)| \le (n-1, p-1) p^{\frac{1}{2}\min\{1,\beta\}} p^{\frac{1}{2}\min\{h, m-2\}} p^{\frac{m}{2}} p^{\frac{\delta}{2}}, \tag{4.3}$$

for all $m \ge 2$, and $p \nmid a$. We use induction on m. If $m = 2$, we consider the two cases $\beta \ge 1$ and $\beta = 0$. If $\beta \ge 1$ and $\delta = 0$, then $\tau = 0$ and the related congruence $p^{-t}\{anx^{n-1} + b\} \equiv 0 (\bmod p)$ has no solution, thus $S(ax^n + bx, p^m) = 0$. If $\beta \ge 1$, and $\delta \ge 1$, then (4.3) is trivial. Let $\beta = 0$, then $t = \beta = 0$, and the related congruence has a t most $(n-1, p-1)$ distinct solutions. It follows from (3.4) that

$$|S(ax^n + bx, p^2)| = (\sum_{\alpha \in \mathcal{A}} 1)p \le (n-1, p-1)p. \tag{4.4}$$

Next we consider $m \ge 3$, and suppose (4.3) holds for smaller m with $m \ge 2$. If $\delta \ge m$, then (4.3) is trivial. If $\delta = m-1$ and $\beta \ge 1$, then (4.3) is trivial again. We consider $\delta = m-1$ and $\beta = 0$, or $\delta = m-2$, then $t = \min(\delta, \beta) \le m-2$. By (3.4) we have

$$|S(ax^n + bx, p^m)| \le (\sum_{\alpha \in \mathcal{A}} 1)p^{m-1} \le (n-1, p-1) p^{\frac{m}{2}} p^{\frac{\delta}{2}}. \tag{4.5}$$

Therefore we may let $0 \le \delta \le m-3$, and then $t = \min(\beta, \delta) \le m-3$. We consider three cases $\beta > \delta$, $\beta < \delta$, and $\beta = \delta$.

Case (i). $\beta > \delta$. In this case $t = \delta$, and the related congruence $p^{-t}(anx^{n-1} + b) \equiv 0 \pmod p$ has no solution, so $S(ax^n + bx, p^m) = 0$.

Case (ii). $\beta < \delta$. In this case the related congruence has only one solution, $x = 0$, with multiplicity $n-1$. By Lemma 1, we have

$$S(ax^n + bx, p^m) = \sum_{x=1}^{p^{m-1}} e(f(px)/p^m) = \sum_{x=1}^{p^{m-1}} e(g(x)/p^m), \tag{4.6}$$

where

$$g(x) = f(px) = ap^n x^n + pbx. \tag{4.7}$$

Let $b = p^\delta b_1$, and $n = p^\beta n_1$ with $p \nmid b_1 n_1$, then

$$g(x) = ap^n x^n + b_1 p^{\delta+1} x, \qquad \sigma := ord_p(g(x)) = min(n, \delta+1).$$

If $n > \delta + 1$, then

$$S(ax^n + bx, p^m) = p^\delta \sum_{x=1}^{p^{m-\delta-1}} e(\frac{ap^{n-\delta-1}x^n + b_1 x}{p^{m-\delta-1}}) = 0. \tag{4.8}$$

If $n \le \delta + 1$, since $\delta \le m - 3$, then $m - n \ge 2$, and we have

$$S(ax^n + bx, p^m) = p^{n-1} \sum_{x=1}^{p^{m-n}} e(\frac{ax^n + p^{\delta+1-n}b_1 x}{p^{m-n}}) = p^{n-1} S(g_1, p^{m-n}),$$

where $g_1(x) = ax^n + p^{\delta+1-n}b_1 x$. By the induction supposition (note that $m - n \ge 2$) we obtain

$$|S(g_1, p^{m-n})| \le (n-1, p-1) p^{\frac{1}{2}\min(h, m-n-2)} p^{\frac{m-n}{2}} p^{\frac{\delta+1-n}{2}} p^{\frac{1}{2}\min(1,\beta)}.$$

It follows that

$$|S(ax^n + bx, p^m)| \le (n-1, p-1) p^{\frac{1}{2}\min(h, m-2)} p^{\frac{m}{2}} p^{\frac{\delta}{2}} p^{\frac{1}{2}\min(1,\beta)}.$$

Case (iii). $\beta = \delta$. In this case we have $t = \beta = \delta$. If $h = ord_p(n-1) = 0$, then the related congruence $p^{-t}\{anx^{n-1} + b\} \equiv 0 \pmod p$ has at most $(n-1, p-1)$ distinct solutions, each of multiplicity one, and so by (2.7) we have

$$|S(ax^n + bx, p^m)| \le (n-1, p-1) p^{\frac{m}{2}} p^{\frac{t}{2}} = (n-1, p-1) p^{\frac{m}{2}} p^{\frac{\delta}{2}}. \tag{4.9}$$

Thus (4.3) is true for $h = 0$. If $h \ge 1$, then $t = \delta = \beta = ord_p(n) = 0$. We may let $1 \le h \le m - 3$, otherwise (4.3) follows from (3.4). Let $n = p^h n_1 + 1$, where $p \nmid n_1$, and $1 \le h \le m - 3$. The related congruence $anx^{n-1} + b \equiv 0 (\mathrm{mod} p)$ has at most $(n_1, p-1)$ solutions and each solution has multiplicity p^h. Let $\alpha \in \mathcal{A}$, since $p \nmid b$, then $p \nmid a$. By Lemma 1 and (3.1)

$$\begin{aligned} g_\alpha(x) &= p^{-\sigma_\alpha}(f(px + \alpha) - f(\alpha)) \\ &= p^{-\sigma_\alpha}\{\sum_{j=2}^{n} \binom{n}{j} a_j p^j x^j + (an\alpha^{n-1} + b)px\}, \end{aligned} \tag{4.10}$$

where $a_j = a\alpha^{n-j}$ with $p \nmid a_j$, and $\sigma_\alpha = ord_p\{f(px + \alpha) - f(\alpha)\}$. Let

$$\tau_j = j + ord_p\{\binom{n}{j}\} \quad \text{and} \quad v = ord_p\{an\alpha^{n-1} + b\} + 1. \tag{4.11}$$

By Lemma 3, we have

$$\sigma_\alpha = \min(\tau_2, \nu) \quad \text{and} \quad \tau_2 = ord_p\{\frac{1}{2}n(n-1)\} + 2 = h + 2. \tag{4.12}$$

It follows from Lemma 1 that

$$S(ax^n + bx, p^m) = \sum_{\alpha \in \mathcal{A}} e(f(\alpha)/p^m) p^{\sigma_\alpha - 1} \sum_{x \bmod p^{m-\sigma_\alpha}} e(\frac{g_\alpha(x)}{p^{m-\sigma_\alpha}}). \tag{4.13}$$

If $\nu < \tau_2$, then $\sigma_\alpha = \nu$, and we have $d_p(g_\alpha(x)) = 1$, that is, $g_\alpha(x)$ is a linear polynomial over F_p. By Lemma 2, it follows that $S(ax^n + bx, p^m) = 0$. Let $\tau_2 \le \nu$, then $\sigma_\alpha = \tau_2 = h + 2 \le m - 1$, for $h \le m - 3$. If $p > 3$, by Lemma 3, we have $d_p(g_\alpha(x)) = 2$. By Lemma 2, we have

$$|\sum_{x \bmod p^{m-\sigma_\alpha}} e(\frac{g_\alpha(x)}{p^{m-\sigma_\alpha}})| \le p^{\frac{m-\sigma_\alpha}{2}}.$$

It follows from (4.13) that

$$|S(ax^n+bx,p^m)| \le (n_1,p-1)p^{\sigma_\alpha-1}p^{\frac{m-\sigma_\alpha}{2}} = (n-1,p-1)p^{\frac{h}{2}}p^{\frac{m}{2}}, \tag{4.14}$$

and so (4.3) is true. If $p=3$, by Lemma 3 we have $\tau_3=\tau_2=h+2$, then $d_p(g_\alpha(x))=3$, and we can write $g_\alpha(x)=Ax^3+Bx^2+Cx+pH(x)$, with $p\nmid AB$. It is easy to see that for all $m\ge 1$, we have

$$|\sum_{x \bmod 3^m} e(g_\alpha(x)/3^m)| = |\sum_{x \bmod 3^m} e(\frac{Ax^3+Bx^2+Cx+3H(x)}{3^m})| \le 3^{\frac{m}{2}}. \tag{4.15}$$

So (4.14) follows for $p=3$. This completes the proof of Theorem 1.1 when $p>2$.

Now if $p=2$, and (1.9) is true when $\tau=ord_2(a)=0$, then it is easily extended to all $1\le\tau\le m-2$. Since if $\delta\le\tau\le m-2$, then $S(ax^n+bx,2^m)=0$. So we only consider $\delta\ge\tau$. If $\delta\ge\tau=m-2$, then (1.9) is trivial. Let $\delta\ge\tau$ and $1\le\tau\le m-3$, then

$$\begin{aligned}|S(ax^n+bx,2^m)| &= 2^\tau|\sum_{x=1}^{2^{m-\tau}} e(\frac{a2^{-\tau}x^n+b2^{-\tau}x}{2^{m-\tau}})| \\ &\le 2^\tau 2\cdot 2^{\frac{1}{2}\min(h,m-\tau-2)}2^{\frac{m-\tau}{2}}2^{\frac{\delta-\tau}{2}} \\ &\le 2\cdot 2^{\frac{1}{2}\min(h,m-\tau-2)}2^{\frac{m}{2}}2^{\frac{\delta}{2}}.\end{aligned}$$

Let $\tau=0$, $\delta=ord_2(b)$, $\beta=ord_2(n)$, $h=ord_2(n-1)$. We are to show that

$$|S(ax^n+bx,2^m)| \le 2\cdot 2^{\frac{1}{2}\min(h,m-2)}2^{\frac{m}{2}}2^{\frac{\delta}{2}}. \tag{4.16}$$

We may suppose $m\ge 3$ and $0\le\delta\le m-3$, otherwise it is trivial. In this case we have $t=\min(\beta,\delta)\le m-3$. We consider three cases $\beta>\delta$ and $\beta<\delta$ and $\beta=\delta$.

If $\beta>\delta$, then the related congruece $2^{-\delta}(anx^{n-1}+b)\equiv 0 \pmod 2$ has no solution and we have $S(ax^n+bx,2^m)=0$ by Lemma 1.

If $\beta<\delta$, then $t=\beta$ and the related congruence has only one solution, $x=0$. Let $b=2^\delta b_1$. By Lemma 1, if $2\nmid b_1$ then

$$S(ax^n+bx,2^m) = \sum_{x=1}^{2^{m-1}} e(\frac{a2^nx^n+2^{\delta+1}b_1x}{2^m}). \tag{4.17}$$

If $n>\delta+1$, then $S(ax^n+bx,2^m)=0$. If $n\le\delta+1$, then $m-n\ge 2$ for $\delta\le m-3$. By the induction assumption we have

$$\begin{aligned}|S(ax^n+bx,2^m)| &\le 2\cdot 2^{n-1}2^{\frac{1}{2}\min(h,m-n-2)}2^{\frac{m-n}{2}}2^{\frac{\delta+1-n}{2}} \\ &\le 2\cdot 2^{\frac{1}{2}\min(h,m-2)}2^{\frac{m}{2}}2^{\frac{\delta}{2}}.\end{aligned}$$

Finally, we consider $\beta=\delta$. In this case if $h=0$, then the related congruence $2^{-t}\{anx^{n-1}+b\}\equiv 0 \pmod 2$ has one solution, $x=1$, of multiplicity one. By (2.8) of Theorem 2.1, we have

$$|S(ax^n+bx,p^m)| \le 2^{\frac{m}{2}}2^{\frac{t}{2}} = 2^{\frac{m}{2}}2^{\frac{\delta}{2}}.$$

If $h \geq m-2$, then the result is trivial, so we only consider $1 \leq h \leq m-3$. In this case we have $\beta = 0$, and then $t = \delta = \beta = 0$. Let $n = 2^h n_1 + 1$ with $2 \nmid n_1$, then the related congruence $anx^{n-1} + b \equiv 0 \pmod 2$ has one solution, $x = 1$. Let

$$g_1(x) = 2^{-\sigma}\{f(2x+1) - f(1)\} = 2^{-\sigma}\{\sum_{j=2}^{n} \binom{n}{j} a2^j x^j + (an+b)2x\}, \tag{4.18}$$

where $\sigma = ord_2(f(2x+1) - f(1))$. Let

$$\tau_j = j + ord_2\{\binom{n}{j}\}, \quad v = 1 + ord_2(an+b). \tag{4.19}$$

By Lemma 1, we have

$$S(ax^n + bx, 2^m) = e(\frac{a+b}{2^m})2^{\sigma-1}S(g_1, 2^{m-\sigma}). \tag{4.20}$$

By Lemma 3, we have

$$\sigma = \min\{\tau_2, v\} \leq \tau_2 = h+1 \leq m-2. \tag{4.21}$$

If $v < \tau_2$, then $\sigma = v$, and we have $S(ax^n + bx, 2^m) = 0$. Let $\tau_2 \leq v$, then $\sigma = \tau_2 = h+1$. By Lemma 3, $\tau_3 = 1 + \tau_2$, $\tau_4 \geq 1 + \tau_2$, and $\tau_j \geq 2 + \tau_2$ when $j \geq 5$, then $g_1(x)$ may be written as follows

$$g_1(x) = 2Ax^4 + 2Bx^3 + Cx^2 + Dx + 4H(x), \quad H(x) \in \mathbb{Z}[x], \tag{4.22}$$

where $2 \nmid BC$. As a simple application of Theorem 2.1, one may get for all $m \geq 1$ that

$$|\sum_{x=1}^{2^m} e(\frac{2Ax^4 + 2Bx^3 + Cx^2 + Dx + 4H(x)}{2^m})| \leq 2 \cdot 2^{\frac{m+1}{2}}. \tag{4.23}$$

It follows that

$$|S(ax^n + bx, 2^m)| \leq 2^{\sigma-1}2 \cdot 2^{\frac{m-\sigma+1}{2}} \leq 2 \cdot 2^{\frac{\sigma-1}{2}}2^{\frac{m}{2}} = 2 \cdot 2^{\frac{h}{2}}2^{\frac{m}{2}},$$

which completes the proof of Theorem 1.1 when $p = 2$.

5. Proof of Theorem 1.2. We first prove (1.22). Let $p > 2$, $n \geq 2$, $m \geq 1$, $\delta = ord_p(b)$, and $\beta = ord_p(n)$. We will show that for all $\chi \bmod p^m$, and $a, b \in \mathbb{Z}$ with $p \nmid a$ that

$$|S(ax^n + bx, \chi, p^m)| \leq np^{\frac{2}{3}m}(b, p^m)^{\frac{1}{3}}. \tag{5.1}$$

If $m = 1$, the result follows from Weil's upper bound (1.21). Let $m \geq 2$, and consider $\delta \geq m-3$. If $\delta \geq m$, then (5.1) is trivial. If $\delta \geq m-3$, and $\beta > 0$, then $p|n$, so (5.1) is trivial again. If $\delta \geq m-3$, and $\beta = 0$, then by (3.13), it follows that $t_1 = 0$ and that

$$|S(ax^n + bx, \chi, p^m)| \leq (\sum_{\alpha \in \mathcal{A}_1} 1)p^{m-1} \leq np^{m-1} \leq np^{\frac{2m}{3}}p^{\frac{\delta}{3}}.$$

Therefore, we may let $m \geq 4$, and $0 \leq \delta \leq m-4$. In particular $t_1 = \min\{\delta, \beta, ord_p(c)\} \leq m-4$, and so the conditions of Theorem 2.2 and Lemma 5 hold. By Lemma 5, if $\mathcal{A}_1$ is not empty, then

$$S(ax^n + bx, \chi, p^m) = \sum_{\alpha \in \mathcal{A}_1} \chi(\alpha) e\left(\frac{a\alpha^n + b\alpha}{p^m}\right) \sum_{y \bmod p^{m-1}} e\left(\frac{F_\alpha(y)}{p^m}\right), \tag{5.2}$$

where $f(x) = ax^n + bx$, and

$$F_\alpha(y) = f(\alpha(1+rp)^y) - f(\alpha) + pcy. \tag{5.3}$$

To express the integral valued function $F_\alpha(y)$ as a polynomial over $\mathbb{Z}/p^m\mathbb{Z}$, we let $\theta_j = j - ord_p(j!)$, $j! = p^{ord_p(j!)}\omega_j$, $p \nmid \omega_j$ and $\overline{\omega_j}\omega_j \equiv 1 (\mathrm{mod} p^m)$. Let N be a positive integer such that

$$\theta_j = j - ord_p(j!) \geq m, \quad \text{for all } j > N. \tag{5.4}$$

It is easy to see that for any integer y, we have

$$(1+rp)^y = 1 + \sum_{j=1}^{N} C_j(y)\overline{\omega_j} r^j p^{\theta_j} \pmod{p^m}, \tag{5.5}$$

where $C_j(y)$ is a polynomial of degree j in the variable y defined by

$$C_j(y) = y(y-1)\cdots(y-j+1). \tag{5.6}$$

It follows that we can take

$$F_\alpha(y) = (ran\alpha^n + rb\alpha + c)py + \sum_{j=2}^{N} (a\alpha^n C_j(ny) + b\alpha C_j(y))\overline{\omega_j} r^j p^{\theta_j}. \tag{5.7}$$

We let

$$\sigma_\alpha = ord_p(F_\alpha(y)), \qquad g_\alpha(y) = p^{-\sigma_\alpha} F_\alpha(y). \tag{5.8}$$

Then $g_\alpha(y)$ is a nonzero polynomial read (mod$p$). To prove (5.1), we consider three cases, $\beta > \delta$ and $\beta < \delta$ and $\beta = \delta$.

Case (i). $\beta > \delta$. In this case, we have $t_1 = \delta$, and $ord_p(c) = \delta$. The related congruence $p^{-\delta}\{brx + c\} \equiv 0 (\mathrm{mod} p)$ has one solution with multiplicity one. By Theorem 2.2 and (2.13), we get

$$|S(ax^n + bx, \chi, p^m)| \leq p^{\frac{m}{2}} p^{\frac{t}{2}} = p^{\frac{m}{2}} p^{\frac{\delta}{2}} \leq p^{\frac{2}{3}m} p^{\frac{\delta}{2}},$$

and (5.1) follows immediately.

Case (ii). $\beta < \delta$. If $ord_p(c) < \beta$, then the related congruence has no solution. If $ord_p(c) > \beta$, then the congruence has only one solution $x = 0$. In both cases we have $S(ax^n + bx, \chi, p^m) = 0$. Thus we let $ord_p(c) = \beta < \delta$. Then $t = t_1 = \beta$, and the related congruence

$$p^{-\beta}(arnx^n + c) \equiv 0 \pmod{p} \tag{5.9}$$

has at most $(n,p-1)$ distinct solutions. If $\beta = 0$, we see that each solution has multiplicity one. By Theorem 2.2 and (2.13),

$$|S(ax^n + bx, \chi, p^m)| \leq (n,p-1)p^{\frac{m}{2}}p^{\frac{t}{2}} \leq np^{\frac{2}{3}m}p^{\frac{\delta}{3}}.$$

Hence, we may let $1 \leq ord_p(c) = \beta < \delta$.

LEMMA 6. *Let p be an odd prime. Let $\alpha \in \mathcal{A}_1$ be a solution of (5.9), and $F_\alpha(y)$, σ_α and $g_\alpha(y)$ be defined by (5.7) and (5.8). Let $d_p(g_\alpha)$ be the degree of $g_\alpha(y)$ read modulo p. Then we have $\sigma_\alpha \leq \delta + 3$, and $d_p(g_\alpha) \leq 3$.*

Proof. Let $C_j(y) = \sum_{i=1}^{j} \pi_i(j)y^i$ with $\pi_i(j) \in \mathbb{Z}$. We have

$$a\alpha^n C_j(ny) + b\alpha C_j(y) = (an\alpha^n + b\alpha)\pi_1(j)y + \sum_{i=2}^{j}(an^i\alpha^n + b\alpha)\pi_i(j)y^i.$$

In particular,

$$a\alpha^n C_2(ny) + b\alpha C_2(y) = (an^2\alpha^n + b\alpha)y^2 - (an\alpha^n + b\alpha)y,$$

and

$$a\alpha^n C_3(ny) + b\alpha C_3(y) = (an^3\alpha^n + b\alpha)y^3 - 3(an^2\alpha^n + b\alpha)y^2 + 2(an\alpha^n + b\alpha)y.$$

By (5.7), we have if $p \geq 3$,

$$F_\alpha(y) = A_\alpha y^3 + B_\alpha y^2 + D_\alpha y + \sum_{j\geq 4}^{N}(\sum_{i=2}^{j}(an^i\alpha^n + b\alpha)\pi_i(j)y^i)\overline{\omega_j}r^j p^{\theta_j}, \tag{5.10}$$

where $D_\alpha \in \mathbb{Z}$ and

$$A_\alpha = \overline{\omega_3}r^3 p^{\theta_3}(an^3\alpha^n + b\alpha), \quad B_\alpha = r^2 p^{\theta_2}(an\alpha^n + b\alpha)(\overline{\omega_2} - 3\overline{\omega_3}rp^{\theta_3 - \theta_2}). \tag{5.11}$$

We consider three cases, $\delta < 2\beta, \delta = 2\beta$ and $\delta > 2\beta$.

If $\delta < 2\beta$, then $ord_p(B_\alpha) = \delta + 2$, and for all $i \geq 2$, we have

$$ord_p(an^i\alpha^n + b\alpha) \geq \min(i\beta, \delta) = \delta.$$

So $ord_p(A_\alpha) \geq \delta + 3$, by Lemma 4 and (5.10). It follows that $\sigma_\alpha \leq \delta + 2$ and that $d_p(g_\alpha) \leq 2$.

If $\delta = 2\beta$, then $ord_p(B_\alpha) \geq \delta + 2$ and $ord_p(A_\alpha) = \delta + 3$. For all $i \geq 3$, we have

$$ord_p(an^i\alpha^n + b\alpha) \geq \min(i\beta, \delta) = \delta.$$

By Lemma 4 and (5.10), we have $\sigma_\alpha \leq \delta + 3$, and $d_p(g_\alpha) \leq 3$.

If $\delta > 2\beta$, then $ord_p(B_\alpha) = 2\beta + 2$ and for all $i \geq 3$, we have

$$ord_p(an^i\alpha^n + b\alpha) \geq \min(3\beta, \delta) > 2\beta.$$

Then we have $\sigma_\alpha \leq 2\beta + 2 < \delta + 2$, and $d_p(g_\alpha) \leq 2$. There is a similar discussion for $p = 3$. This completes the proof of Lemma 6. □

We now use Lemma 6 and Lemma 2 to complete the proof of the theorem when $\beta < \delta$. For each $\alpha \in \mathcal{A}_1$, by Lemma 6 we have $\sigma_\alpha \leq \delta + 3$ and $d_p(g_\alpha) \leq 3$. Then $m - \sigma_\alpha \geq 1$ since $\delta \leq m - 4$, and so by Lemma 2

$$|\sum_{y \bmod p^{m-\sigma_\alpha}} e(\frac{g_\alpha(y)}{p^{m-\sigma_\alpha}})| \leq 2p^{\frac{2}{3}(m-\sigma_\alpha)}.$$

It follows from Lemma 5 and (5.2) that

$$\begin{aligned} |S(ax^n + bx, \chi, p^m)| &\leq \sum_{\alpha \in \mathcal{A}_1} p^{\sigma_\alpha - 1} p^{\frac{2}{3}(m-\sigma_\alpha)} \\ &\leq 2(n, p-1) p^{\frac{2}{3}m} p^{\frac{\delta}{3}} \\ &\leq n p^{\frac{2}{3}m} p^{\frac{\delta}{3}}. \end{aligned}$$

The last inequality follows from $\sigma_\alpha \leq \delta + 3$ and the fact that $2(n, p-1) \leq n$, since $p|n$.

Case (iii). $\beta = \delta$. In this case, if $\mathcal{A}_1$ is not empty, then we must have $\gamma = ord_p(c) \geq \beta = \delta$. Thus $t = t_1 = \delta$ and the related congruence is

$$p^{-\delta}[anrx^n + brx + c] \equiv 0 (\mathrm{mod} p).$$

If $\delta > 0$, then $\gamma > 0$, where we define $\gamma = ord_p(c)$. We show that each $\alpha \in \mathcal{A}_1$ has multiplicity one. To prove this conclusion, first let $\gamma > \delta$. Then α is a solution of $p^{-\delta}(anx^{n-1} + b) \equiv 0 (\mathrm{mod} p)$. Since $\beta = \delta > 0$, then $p|n$, and $p \nmid n - 1$, and so α just has multiplicity one. If $\gamma = \delta > 0$, and $\alpha \in \mathcal{A}_1$ has multiplicity greater than one, then

$$p^{-\delta}(an^2 r\alpha^{n-1} + br) \equiv 0 \pmod{p}.$$

But this is impossible since $\beta = \delta > 0$. This proves that if $\beta = \delta > 0$, then each $\alpha \in \mathcal{A}_1$ has multiplicity one. The result now follows from Theorem 2.2.

We consider next $\delta = \beta = 0$ and discuss the two cases $\gamma = 0$ and $\gamma > 0$. If $\gamma = 0$, let $f(x) = anrx^n + brx + c$, $f'(x) = an^2 rx^{n-1} + br$. If $n \equiv 1 (\mathrm{mod} p)$, then each $\alpha \in \mathcal{A}_1$ has multiplicity one. For if $f(\alpha) \equiv f'(\alpha) \equiv 0 \pmod{p}$ and $n \equiv 1 \pmod{p}$, then $p|c$, a contradiction. If $\gamma = 0$ and $n \not\equiv 1 (\mathrm{mod} p)$, then each $\alpha \in \mathcal{A}_1$ has at most multiplicity two. By Theorem 2.2 and (2.13), we have

$$|S(ax^n + bx, \chi, p^m)| \leq (\sum_{\alpha \in \mathcal{A}_1} \mu_\alpha) p^{\frac{2}{3}m} \leq n p^{\frac{2}{3}m}.$$

Next we discuss $\delta = \beta = 0$, and $\gamma > 0$. In this case the related congruence is $anx^{n-1} + b \equiv 0 (\mathrm{mod} p)$. If $n \not\equiv 1 (\mathrm{mod} p)$, then each $\alpha \in \mathcal{A}_1$ has multiplicity one, and the conclusion follows. If $n \equiv 1 (\mathrm{mod} p)$, we let

$$n = p^h n_1 + 1, \quad \text{with} \quad p \nmid n_1 \quad \text{and} \quad h \geq 1.$$

So the congruence has at most $(n_1, p-1)$ distinct solutions, each of multiplicity p^h. Without loss of generality, we may let $1 \leq h \leq m - 3$. Since if $h \geq m - 2$, then $np^{\frac{2m}{3}} \geq p^m$ for $n \geq p^{m-2}$ and $m \geq 3$. Now for each $\alpha \in \mathcal{A}_1$,

$$an\alpha^{n-1} + b \equiv 0 (\mathrm{mod} p), \quad n = p^h n_1 + 1 \quad \text{and} \quad 1 \leq h \leq m - 3. \tag{5.12}$$

Let $F_\alpha(y)$ and $g_\alpha(y)$ be as defined by (5.7) and (5.8).

LEMMA 7. *Under the above assumptions, we have* $\sigma_\alpha \le h+3$, *and* $d_p(g_\alpha) \le 3$.

Proof. The proof is similar to Lemma 6. Let $\rho = ord_p(an^2\alpha^n + b\alpha)$. We consider the two cases $\rho > h$ and $\rho \le h$.
If $\rho \le h$, then for all $i \ge 3$, we have

$$\begin{aligned} ord_p(an^i\alpha^n + b\alpha) &= ord_p(an^2\alpha^n + b\alpha + an^2\alpha^n(n^{i-2}-1)) \\ &\ge \min(\rho, h) \ge \rho. \end{aligned}$$

It follows that $\sigma_\alpha \le \rho + 2 \le h+2$ and $d_p(g_\alpha) \le 2$.
If $\rho > h$, then $ord_p(A_\alpha) = 3+h$, and for all $i \ge 3$, we have

$$ord_p(an^i\alpha^n + b\alpha) = h.$$

It follows that $\sigma_\alpha \le 3+h$, and $d_p(g_\alpha) \le 3$. This completes the proof of Lemma 7. □

By Lemma 7, Lemma 2 and the same discussion as in case (ii), we have

$$|S(ax^n + bx, \chi, p^m)| \le 2(n_1, p-1)p^{\frac{2}{3}m}p^{\frac{\delta}{3}} \le np^{\frac{2}{3}m}p^{\frac{\delta}{3}},$$

which completes the proof of Theorem 1.2 when $p > 2$. If $p = 2$, then following the method of section 8 of [3], we obtain the result. Here we omit the details of the proof.

Proof of (1.24) in Example 1.3. Let $p \ge 5$, $n = 2$, $m = 3$, $a, b \in \mathbb{Z}$ with $p \nmid ab$, and $f(x) = ax^2 + bx$. We will select a character χ mod p^3 such that the related congruence $2arx^2 + brx + c \equiv 0 \pmod p$ has only one solution with multiplicity two, where r and c defined by (2.9) and (2.10) when $m = 3$. Let $1 \le \alpha \le p-1$, and $1 \le \delta_\alpha \le p-1$, be defined by the congruences,

$$4a\alpha + b \equiv 0 \pmod p, \quad \alpha r^2(a\alpha + \overline{2}b) \equiv \delta_\alpha \pmod p. \tag{5.13}$$

Now we pick up c by setting

$$c \equiv p\delta_\alpha - r\alpha(2a\alpha + b) \pmod{p^2}. \tag{5.14}$$

It is easy to see that $p \nmid c$, and so the corresponding character χ mod p^3 is a primitive character. By the above definition, then α is the unique solution of $2arx^2 + brx + c \equiv 0 \pmod p$ with multiplicity two. By (5.2), and (5.7), we have

$$S(ax^2 + bx, \chi, p^3) = \chi(\alpha)e\left(\frac{a\alpha^2 + b\alpha}{p^3}\right) \sum_{y \bmod p^2} e\left(\frac{F_\alpha(y)}{p^3}\right), \tag{5.15}$$

where

$$\begin{aligned} F_\alpha(y) &\equiv (2ar\alpha^2 + rb\alpha + c)py + (a\alpha^2 C_2(2y) + b\alpha C_2(y))\overline{2}r^2p^2 \\ &\equiv Ay^2 + By \pmod{p^3}, \end{aligned} \tag{5.16}$$

and

$$A = \overline{2}r^2p^2(4a\alpha^2 + b\alpha), \quad B = p[(2ra\alpha^2 + rb\alpha + c) - pr^2(a\alpha^2 + \overline{2}b\alpha)]. \tag{5.17}$$

By (5.13) and (5.14), we have $p^3 | A$ and $p^3 | B$. It follows that

$$|S(ax^2 + bx, \chi, p^3)| = p^2, \tag{5.18}$$

which completes the proof.

ACKNOWLEDGMENTS. The authors would like to thank Professor Wang Yuan for his kind help.

REFERENCES

[1] E. BOMBIERI, *On exponential sums in finite field*, Amer. J. Math., 88 (1966), pp. 71–105.

[2] J. H. H. CHALK, *On Hua's estimate for exponential sums*, Mathematika, 14 (1987), pp. 115–123.

[3] T. COCHRANE AND Z. ZHENG, *Pure and mixed exponential sums*, Acta Arith., 91:3 (1999), pp. 249–278.

[4] ———, *Exponential sums with rational function entries*, to appear in Acta Arith..

[5] R. DABROWSKI AND B. FISHER, *A stationary phase formula for exponential sums over Z/p^mZ and applications to $GL(3)$-Kloosterman sums*, Acta Arith., 80 (1997), pp. 1–48.

[6] H. DAVENPORT AND H. HEILBRONN, *On an exponential sum*, Proc. Lond. Math. Soc., 41:2 (1936), pp. 449–453.

[7] P. DING, *On a conjecture of Chalk*, J. Number Theory, 65 (1997), pp. 116–129.

[8] T. ESTERMANN, *On Kloosterman's sum*, Mathematika, 8 (1961), pp. 83–86.

[9] L. K. HUA, *On exponential sums*, J. Chinese Math. Soc., 20 (1940), pp. 301–312.

[10] ———, *On exponential sums*, Sci Record (Peking) (N.S), 1 (1957), pp. 1–4.

[11] ———, *Additive primzahltheorie*, Teubner Leipzing, 1959, pp. 2–7.

[12] W. K. A. LOH, *Hua's lemma*, Bull. Australian Math. Soc. (3), 50 (1994), pp. 451–458.

[13] J. H. LOXTON AND R. A. SMITH, *On Hua's estimate for exponential sums*, J. London Math. Soc. (2), 26 (1982), pp. 15–20.

[14] J. H. LOXTON AND R. C. VAUGHAN, *The estimate for complete exponential sums*, Canada. Math. Bull. (4), 28 (1995), pp. 442–454.

[15] W. M. SCHMIDT, *Equations over Finite Fields*, L. N. M. 536, Springer-Verlag, Berlin, 1976.

[16] H. SALIÉ, *Über die Kloosterman summen S(u, u; q)*, Math. Zeit., 34 (1931), pp. 91–109.

[17] R. A. SMITH, *Estimate for exponential sums*, Proc. Amer. Math. Soc., 79 (1980), pp. 365–368.

[18] ———, *On n-dimensional Kloosterman sums*, J. Number Theory, 11 (1979), pp. 324–343.

[19] R. C. VAUGHAN, *The Hardy-Littlewood Method*, 2nd ed. Cambridge Tracts in Math. 125, Cambridge Univ. press, Cambridge, 1997.

[20] A. WEIL, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A., 34 (1948), pp. 204–207.

[21] Y. YE, *Hyper-Kloosterman sums and estimation of exponential sums of polynomials of higher degree*, Acta Arith., 86 (1998), pp. 255–267.

[22] ———, *Estimation of exponential sums of polynomials of higher degree II*, Acta Arith., 93 (2000), pp. 221–235.