Записки научных
семинаров ПОМИ
Том 322, 2005 г.

Ping Ding

ON AN EXPONENTIAL SUM

1. Introduction. Let p be a prime, n a positive integer, and $f(x) = ax^k + bx$. In this paper we are concerned with the exponential sum

$$S(f, p^n) = \sum_{x=1}^{p^n} e\big(\frac{f(x)}{p^n}\big), \tag{1.1}$$

where $e(t) = \exp(2\pi it)$.

Pioneered by the work of Hardy and Littlewood this special case was widely studied in connection with Waring's Problem. Davenport and Heilbronn [5] showed that

$$S(f, q) <<_\varepsilon q^{\eta+\varepsilon}(q, b) \quad ((a, q) = 1) \tag{1.2}$$

where $\eta = 2/3$ when $k = 3$ and $\eta = 3/4$ when$k \geqslant 4$. A well-known work of Weil [13] implies that

$$S(f, p) \leqslant (k-1)p^{1/2}, \quad \text{if} \quad p \nmid a. \tag{1.3}$$

By making use of (1.3), Hua [7] was able to reduce η to $1/2$ for all $k \geqslant 2$.

Improving the work of Loxton and Smith [9], Loxton and Vaughan [10] showed

$$|S(f, p^n)| \leqslant (k-1)p^{\frac{n+\tau_0}{2}}(D, p^n)^{1/2}, \tag{1.4}$$

where D is the different of $f(x)$, and $\tau_0 = 1$ or 0 according to $p \leqslant k$ or $p > k$.

Let $\mathrm{ord}_p(Y)$ denote the normalized exponent valuation on the p-adic field. For any positive integer Y, $\mathrm{ord}_p(Y)$ is the largest integer v such that $p^v | Y$. For convenience, we write $\theta = \mathrm{ord}_p(b)$, $\alpha = \mathrm{ord}_p(k)$, $\beta = \mathrm{ord}_p(k-1)$, $k = p^\alpha k_1$, $b = p^\theta b_1$, and $k - 1 = p^\beta k_0$. Then $(p, k_1) = (p, b_1) = (p, k_0) = 1$.

Recently, Dabrowkski and Fisher [4] established the following estimates under the conditions $(p,b)=(p,k)=1$. If $p>2$, then

$$|S(f,p^n)|\leqslant\begin{cases}(k-1)p^{1/2}, & \text{if } \beta=0,\\ (k-1)p^{-\beta/2}p^{n/2}, & \text{if } \beta\geqslant 1 \text{ and } n\geqslant 3\beta+2,\\ (k-1,p-1)^{\min(\beta,\frac{n}{2}-1)}p^{n/2}. & \text{if } n \text{ is even},\\ (k-1,p-1)p^{\min(\beta,\frac{n-1}{2}-1)}p^{(n+1)/2}, & \text{if } n \text{ is odd}.\end{cases} \tag{1.5}$$

Similar results hold for $p=2$.

For relatively large k, Ye [15] modified (1.5) when $\beta=0$ and when $1\leqslant\beta\leqslant(k-2)/3$ by using $(\varphi(p^n)-k+1)$ instead of $(k-1)$. This supersedes (1.5) when k is close to $\varphi(p^n)$ for $\beta=0$ and for $1\leqslant\beta\leqslant(k-2)/3$; specifically, when k lies in the interval $(\frac{1}{2}\varphi(p^n)+1,\varphi(p^n))$.

Cochrane and Zheng [3] proved the following general result.

Let $k\geqslant 2$, $n\geqslant 2$, and $\gamma=\mathrm{ord}_p(a)\leqslant n-2$. Then for odd prime p,

$$|S(f,p^n)|\leqslant(k-1,p-1)p^{\frac{1}{2}\min(1,\alpha)}p^{\frac{1}{2}\min(\beta,n-2-\gamma)}p^{\frac{n}{2}}(b,p^n)^{\frac{1}{2}}, \tag{1.6}$$

and for $p=2$,

$$|S(f,2^n)|\leqslant 2\cdot 2^{\frac{1}{2}\min(\beta,n-2-\gamma)}2^{\frac{n}{2}}(b,2^n)^{\frac{1}{2}}. \tag{1.7}$$

We write $n=Qk+r$ with $0\leqslant r\leqslant k-1$ and $Q\geqslant 0$. Let

$$\zeta=\begin{cases}\frac{\theta-\alpha}{k-1}, & \text{if } \theta\geqslant\alpha,\\ 0, & \text{otherwise},\end{cases}$$

and $J=[\zeta]$. Moreover we write $V=\min(Q,J)$. Define

$$\theta_j=\theta+j-jk, \text{ for } j=0,1,2,\dots,V. \tag{1.8}$$

Let $t=\mathrm{ord}_p(f'(x))$, μ a root of the underlying congruence

$$p^{-t}f'(x)=0(\mathrm{mod}\,p) \tag{1.9}$$

with multiplicity m_μ, and $\mathcal{A}$ the set of roots of (1.8). Write $M=\max_{\mu\in A}m_\mu$ and $m=\sum_{\mu\in A}m_\mu$.

Define further $\sigma_\mu=\mathrm{ord}_p(f(px+\mu)-f(\mu))$). For convenience we write $d=(k-1,p-1)$. We define a sequence of polynomials f_j as follows. Let $f_0=f$. For $j=1,\dots,V$, let $f_j=ax^k+p^{\theta_j}b_1x$. For each f_j, $j\geqslant 1$, we define $t_j,\mu_j,m_{\mu_j},\mathcal{A}_j$, and σ_{μ_j} corresponding to $t,\mu,m_\mu,\mathcal{A}$, and σ_μ, respectively.

The aim of this paper is to improve the above results by establishing the following

Theorem. *Let $k \geqslant 2$ and $n \geqslant 2$. If $p > 2$, then*

$$|S(f, p^n)| \leqslant$$

$$\begin{cases} p^{\frac{1-V}{2}} p^{\frac{n}{2}} (b, p^n)^{\frac{1}{2}}, & \text{if } n \equiv 1 (\operatorname{mod} k), \quad (1.10) \\ (k-1, p-1) p^{-\frac{V}{2}} p^{\frac{\min(\alpha,1)}{2}} p^{\min(\frac{\beta}{2}, \frac{n}{2}-1)} p^{\frac{n}{2}} (b, p^n)^{\frac{1}{2}}, & \text{if } n \not\equiv 1 (\operatorname{mod} k). (1.11) \end{cases}$$

The outcome of the theorem is best possible by examining an example at Section 4 and some discussions are also provided at the end of this paper.

2. Preliminary results.

Lemma 1 ([3]). *If $p > 2$ and $n \geqslant t+2$, or $p = 2$ and $n \geqslant t+3$, or $p = 2$ and $t = 0$, then if $\mathcal{A} = \phi$ then $S(f, p^n) = 0$; if $\mathcal{A}$ is not empty, we have*

$$S(f, p^n) = \sum_{\mu \in A} e\left(\frac{f(\mu)}{p^n}\right) p^{\sigma_\mu - 1} S(g_\mu, p^{n-\sigma_\mu}),$$

where

$$S(g_\mu, p^{n-\sigma_\mu}) = \begin{cases} p^{n-\sigma_\mu}, & \text{if } n < \sigma_\mu, \\ \sum\limits_{m \operatorname{mod} p^{n-\sigma_\mu}} e\left(\frac{g_\mu(x)}{p^{n-\sigma_\mu}}\right), & \text{if } n \geqslant \sigma_\mu. \end{cases}$$

Lemma 2 ([6] [2]). $|S(f, p^n)| \leqslant m p^{\frac{t}{M+1}} p^{n\left(1 - \frac{1}{M+1}\right)}$.

We call a polynomial mod_ p_polynomial of degree l if l is the largest integer i such that $(a_i, p) = 1$, where a_i are integer coefficients of the polynomial. Let $f(x)$ be a mod_ p_polynomial of degree l, then we may write

$$f(x) = a_l x^l + a_{l-1} x^{l-1} + \ldots + a_1 x + a_0 + pH(x),$$

where $H(x) \in \mathbf{Z}[x]$.

Lemma 3. *Let $f(x)$ be a* mod_ *p_polynomial of degree l. If $(a_l, p) = 1$ when $2 \leqslant l < p$, or if $(a_l, p) = (a_{l-1}, p) = 1$ when $l = p$, then*

$$|S(f, p^n)| \leqslant \begin{cases} (l-2) p^{n\left(1 - \frac{1}{l-1}\right)}, & \text{when } l = p > 2; \\ (l-1) p^{n\left(1 - \frac{1}{l}\right)}, & \text{when } 2 \leqslant l < p. \end{cases}$$

When $l = p = 2$ and $(a_l, 2) = 1$, $S(f, 2^n) = 0$.

Proof. If $l = p$, then

$$f'(x) = (l-1)a_{l-1}x^{l-2} + \ldots + a_1 + p(H'(x) + a_l x^{l-1}).$$

Let $Q(x) = a_{l-1}x^{l-1} + \ldots + a_1 x + a_0$, then

$$f'(x) \equiv Q'(x) \equiv 0 (\operatorname{mod} p).$$

It is easily seen that the zeros of the congruence

$$f'(x) \equiv 0 (\operatorname{mod} p)$$

and

$$Q'(x) \equiv 0 (\operatorname{mod} p)$$

are exactly the same. Hence $M \leqslant m \leqslant l-2$. Since $(a_{l-1}, p) = 1$, we have $t = 0$. By Lemma 2

$$|S(f, p^n)| \leqslant m p^{n\left(1-\frac{1}{M+1}\right)} \leqslant (l-2) p^{n\left(1-\frac{1}{l-1}\right)},$$

as required.

The case of $2 \leqslant l < p$ follows directly from Lemma 2 and the above arguments.

When $l = p = 2$ and $(a_1, 2) = 1$ we may write

$$f(x) = a_2 x^2 + a_1 x + a_0 + 2H(x).$$

Then $f'(x) = a_1 + 2(H'(x) + a_2 x)$. This implies that the congruence $f'(x) \equiv 0 (\operatorname{mod} 2)$ has no solution when $(a_1, 2) = 1$. Thus $\mathcal{A} = \phi$. Since $t = 0$ and $n \geqslant 2 = t + 2$, it follows from Lemma 1 that $S(f, 2^n) = 0$.

Lemma 4. *If $\theta = \alpha$ and $n \geqslant 2$, then for $p \geqslant 3$,*

$$|S(f, p^n)| \leqslant (k-1, p-1) p^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{\frac{n}{2}} p^{\frac{\theta}{2}}.$$

Proof. If $\theta = \alpha$, then $t = \min(\theta, \alpha) = \theta = \alpha$. If $\beta = \operatorname{ord}_p(k-1) = 0$, the congruence $p^{-t}(akx^{k-1} + b) \equiv 0 (\operatorname{mod} p)$ has at most $(k-1, p-1)$ distinct solutions, each of multiplicity one. In view of Lemma 2 with $M = 1$, we have

$$|S(f, p^n)| \leqslant (k-1, p-1) p^{\frac{n}{2}} p^{\frac{\theta}{2}}.$$

Suppose now $\beta \geqslant 1$ which implies $\operatorname{ord}_p(k) = 0$, whence $t = \theta = \alpha = \operatorname{ord}_p(k) = 0$. Write $k - 1 = p^{\beta} k_0$ with $(k_0, p) = 1$. The congruence

$p^{-t}(akx^{k-1}+b)\equiv 0(\bmod p)$ has at most $(k_0, p-1)$ solutions. Since $n \geqslant 2 = t+2$, by Lemma 1 one has, when $n \geqslant \sigma_\mu + 1$,

$$S(f,p^n) = \sum_{\mu\in A} e\left(\frac{f(\mu)}{p^n}\right) p^{\sigma_\mu - 1} \sum_{x \bmod p^{n-\sigma_\mu}} e\left(\frac{g_\mu(x)}{p^{n-\sigma_\mu}}\right), \tag{2.1}$$

where

$$g_\mu(x) = p^{-\sigma_\mu}(f(px+\mu) - f(\mu)) \tag{2.2}$$

and

$$\sigma_\mu = \mathrm{ord}_p(f(px+\mu)-f(\mu)). \tag{2.3}$$

First we have trivially

$$S(f,p^n)| \leqslant (k-1,p-1)p^{\frac{n}{2}-1}p^{\frac{n}{2}}.$$

By Taylor's expansion,

$$f(px+\mu)-f(\mu) = f'(\mu)px + \frac{f''(\mu)}{2!}p^2x^2 + \frac{f'''(\mu)}{3!}p^3x^3 + \ldots \tag{2.4}$$

Write $\nu_i = \mathrm{ord}_p\left(\frac{f^{(i)}(\mu)}{i!}\right) + i$. A simple calculation reveals that for $i \geqslant 2$, $\frac{f^{(i)}(\mu)}{i!} = a\binom{k}{i}\mu^{k-i}$. Recall that μ is a root of the congruence $p^{-t}(akx^{k-1}+b) \equiv 0(\bmod p)$, that is, a root of the congruence $ak_1\mu^{k-1} + b_1 \equiv 0(\bmod p)$, as $t=\theta=\alpha=0$. Thus $p \nmid \mu$. Since $p \nmid a$ and $p \nmid \mu$, we have $\mathrm{ord}_p\left(\frac{f^{(i)}(\mu)}{i!}\right) = \mathrm{ord}_p\left(\binom{k}{i}\right)$. Furthermore since $\binom{k}{i} = \frac{(k-i+1)}{i}\binom{k}{i-1}$, we obtain a recursive relation for $i \geqslant 3$

$$\begin{aligned}\nu_i &= \mathrm{ord}_p(k-i+1) - \mathrm{ord}_p(i) + \mathrm{ord}_p\left(\binom{k}{i-1}\right) + i \\ &= \mathrm{ord}_p(k-i+1) - \mathrm{ord}_p(i) + \nu_{i-1} + 1. \end{aligned}\tag{2.5}$$

Thus

$$\nu_i \geqslant -\mathrm{ord}_p(i) + \nu_{i-1} + 1.$$

When $i \geqslant 2$, we have

$$\nu_i \geqslant -\mathrm{ord}_p(i!) + \nu_2 + i - 2.$$

The first term on the right hand side is

$$\mathrm{ord}_p(i!) \leqslant \sum_{j=1}^{\infty}\left[\frac{i}{p^j}\right] \leqslant i\sum_{j=1}^{\infty}\frac{1}{p^j} = \frac{i}{p-1},$$

thus

$$\nu_i \geqslant -\frac{i}{p-1} + \nu_2 + i - 2. \tag{2.6}$$

If $p > 3$ and $i \geqslant 3$ we have

$$\nu_i \geqslant -\frac{i}{p-1} + \nu_2 + i - 2 \geqslant -\frac{i}{4} + \nu_2 + i - 2 \geqslant \nu_2 + 1.$$

This implies, in view of (2.4), that

$$\sigma_\mu = \min(\nu_1, \nu_2),$$

where $\nu_1 = \mathrm{ord}_p(ak_1\mu^{k-1} + b_1) + 1$ and $\nu_2 = \mathrm{ord}_p\left(\frac{k(k-1)}{2}\right) + 2 = \beta + 2$.

If $n \leqslant \sigma_\mu$, then by Lemma 1 we have trivially

$$|S(f, p^n)| \leqslant \sum_{\mu \in A} p^{n-1} \leqslant (k_0, p-1) p^{\frac{\sigma_\mu}{2} - 1} p^{\frac{n}{2}} \leqslant (k, p-1) p^{\frac{\beta}{2}} p^{\frac{n}{2}}.$$

If $n \geqslant \sigma_\mu + 1$, it then follows from (2.1) that

$$|S(f, p^n)| \leqslant \sum_{\mu \in A} p^{\sigma_\mu - 1} |S(g_\mu, p^{n-\sigma_\mu})|.$$

If $\nu_1 < \nu_2$, then $\sigma_\mu = \nu_1$ and $\deg(g_\mu) = 1$. By Lemma 2, noting that $m \leqslant k-1$ we have $S(f, p^n) = 0$. If $\nu_1 \geqslant \nu_2$, then $\sigma_\mu = \nu_2$ and $\deg(g_\mu) = 2$. Thus

$$|S(g_\mu, p^{n-\sigma_\mu})| \leqslant p^{\frac{n-\sigma_\mu}{2}},$$

therefore

$$|S(f, p^n)| \leqslant (k_0, p-1) p^{\frac{n}{2}} p^{\frac{\sigma_\mu}{2} - 1} = (k, p-1) p^{\frac{\beta}{2}} p^{\frac{n}{2}}.$$

If $p = 3$ and $i \geqslant 5$ we have

$$\nu_i \geqslant -\frac{i}{p-1} + \nu_2 + i - 2 = -\frac{i}{2} + \nu_2 + i - 2 \geqslant \nu_2 + 1;$$

moreover, in view of (2.5), we obtain

$$\nu_4 = \mathrm{ord}_3(k-3) - \mathrm{ord}_3(4) + \mathrm{ord}_3(k-2) - \mathrm{ord}_3(3) + \nu_2 + 2 = \nu_2 + 1,$$

and

$$\nu_3 = \mathrm{ord}_3(k-2) - \mathrm{ord}_3(3) + \nu_2 + 1 = \nu_2.$$

Hence we may write

$$f(x) = b_3 x^3 + b_2 x^2 + b_1 x + b_0 + 3h(x),$$

where $(b_3, 3) = (b_2, 3) = 1$ and $h(x) \in \mathbf{Z}[x]$. It then follows from Lemma 3 that

$$|S(f, 3^n)| \leqslant 3^{\frac{n}{2}}.$$

This completes the proof.

Lemma 5. *If $\lambda \geqslant 1$ and $f(x) = ap^{\lambda}x^k + bx$ with $(a, p) = (b, p) = 1$, then*

$$S(f, p^n) = 0.$$

Proof. If $n = 1$, then

$$S(f, p^n) = \sum_{x=1}^{p} e\left(\frac{ap^{\lambda}x^k + bx}{p}\right) = \sum_{x=1}^{p} e\left(\frac{bx}{p}\right) = 0.$$

Suppose that $n \geqslant 2$ and $p > 2$. Since $t = 0$, we deduce that $n \geqslant t + 2$. Noting that the congruence $f'(x) \equiv 0 (\operatorname{mod} p)$ has no solution, we obtain that $\mathcal{A}$ is empty. It thus follows from Lemma 1 that $S(f, p^n) = 0$, as required.

3. Proof of the theorem. Let p be a prime $\geqslant 3$. Write $a = p^{\lambda}a_1$ with $(a_1, p) = 1$. If $\lambda > \theta$, it follows from Lemma 5 that $S(f, p^n) = 0$. Thus we only consider $\lambda \leqslant \theta$. If $\lambda > 0$,

$$S(f, p^n) = \sum_{x=1}^{p^n} e\left(\frac{a_1 p^{\lambda} x^k + b_1 p^{\theta} x}{p^n}\right) = p^{\lambda} \sum_{x=1}^{p^{n-\lambda}} e\left(\frac{a_1 x^k + b_1 p^{\theta-\lambda} x}{p^{n-\lambda}}\right).$$

Thus we may assume, without loss of generality, that $(a, p) = 1$.

Suppose that $n \leqslant t + 1$. Since $t = \min(\alpha, \theta)$, the condition $n \geqslant 2$ ensures $\alpha \geqslant 1$ and $\theta \geqslant 1$. Now a trivial estimate reveals

$$|S(f, p^n)| \leqslant p^n \leqslant p^{\frac{t+1}{2}} p^{\frac{n}{2}} \leqslant p^{\frac{\min(\alpha,1)}{2}} p^{\frac{\theta}{2}} p^{\frac{n}{2}}.$$

We claim that $V = 0$. Actually, $n \leqslant t + 1 = \min(\theta, \alpha) + 1 \leqslant \left[\frac{\log k}{\log p}\right] + 1$. When $p > k$, we deduce that $n \leqslant 1$ which violates the condition $n \geqslant 2$. Thus we may assume that $p \leqslant k$.

When $p \geqslant 3$, $\left[\frac{\log k}{\log p}\right] + 1 \leqslant k - 1$ which ensures $Q = 0$, and consequently the theorem holds for $V = 0$.

We may now assume that $n \geqslant t + 2$. By Lemma 1 we have

$$S(f, p^n) = \sum_{\mu \in A} e\left(\frac{f(\mu)}{p^n}\right) p^{\sigma_{\mu}-1} S(g_{\mu}, p^{n-\sigma_{\mu}}), \tag{3.1}$$

where

$$S(g_\mu, p^{n-\sigma_\mu}) = \begin{cases} p^{n-\sigma_\mu}, & \text{if } n \leqslant \sigma_\mu, \\ \sum\limits_{x \bmod p^{n-\sigma_\mu}} e\left(\frac{g_\mu(x)}{p^{n-\sigma_\mu}}\right), & \text{if } n > \sigma_\mu, \end{cases} \tag{3.2}$$

and

$$g_\mu(x) = p^{-\sigma_\mu}(f(px+\mu) - f(\mu)). \tag{3.3}$$

If $\alpha > \theta$, we have $t = \theta$. The underlying congruence

$$p^{-t}(akx^{k-1} + b) \equiv 0 (\bmod p) \tag{3.4}$$

has no solution, and so $\mathcal{A}$ is empty, which implies $S(f, p^n) = 0$, by Lemma 1.

If $\alpha = \theta$, it follows from Lemma 3 that

$$|S(f, p^n)| \leqslant (k-1, p-1) p^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{\frac{n}{2}} p^{\frac{\theta}{2}}.$$

In this case $J = 0$ so that the theorem holds.

We now consider the case of $\alpha < \theta$. In this case the underlying congruence (3.4) has only one root, $x = 0$, with multiplicity $k-1$. By (3.1),

$$S(f, p^n) = \sum_{x=1}^{p^{n-1}} e\left(\frac{f(px)}{p^n}\right). \tag{3.5}$$

Obviously $\sigma_0 = \min(k, \theta+1)$. If $k > \theta + 1$, in view of Lemma 5, we obtain

$$S(f, p^n) = p^\theta \sum_{x=1}^{p^{n-\theta-1}} e\left(\frac{ap^{k-\theta-1}x^k + b_1 x}{p^{n-\theta-1}}\right) = 0.$$

Thus we may suppose that $k \leqslant \theta + 1$. If $k = \theta + 1$, then when $2 \leqslant n \leqslant \theta + 1 = k$, we have $|S(f, p^n)| \leqslant p^{n-1} \leqslant p^{-\frac{1}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}}$, verifying (1.11) with $V \leqslant 1$. When $n \geqslant \theta + 2 = k + 1$, we obtain

$$S(f, p^n) = p^\theta \sum_{x=1}^{p^{n-k}} e\left(\frac{ax^k + b_1 x}{p^{n-k}}\right).$$

If $\alpha > 0 = ord_p(b_1)$, then $S(f, p^n) = 0$. Suppose $\alpha = 0 = \mathrm{ord}_p(b_1)$. If $n = k + 1$, we obtain trivially

$$|S(f, p^n)| \leqslant p^{n-1} \leqslant p^{\frac{n}{2}} p^{\frac{\theta}{2}},$$

verifying (1.10) for $V=1$. If $n-k\geqslant 2$, it follows from Lemma 3 that

$$|S(f,p^n)|\leqslant dp^{\min\left(\frac{\beta}{2},\frac{n}{2}-1\right)}p^{\frac{n-k}{2}+\theta}=dp^{-\frac{1}{2}}p^{\min\left(\frac{\beta}{2},\frac{n}{2}-1\right)}p^{\frac{n}{2}}p^{\frac{\theta}{2}}.$$

In this case, $J=1$, and so $V=1$, as required.

Consider $k<\theta+1$. If $n\leqslant k+1$, then by (3.5)

$$|S(f,p^n)|\leqslant p^{n-1}\leqslant p^{\frac{n}{2}}p^{\frac{k+1}{2}-1}\leqslant p^{-\frac{1}{2}}p^{\frac{n}{2}}p^{\frac{\theta}{2}}.$$

Note that here $Q\leqslant 1$ and $V\leqslant 1$.

If $n\geqslant k+2$, then again by (3.5)

$$S(f,p^n)=p^{k-1}\sum_{x=1}^{p^{n-k}}e\left(\frac{ax^k+p^{\theta+1-k}b_1x}{p^{n-k}}\right). \tag{3.7}$$

We may rewrite (3.7) as

$$S(f,p^n)=p^{n-k}\sum_{x=1}^{p^{n-k}}e\left(\frac{f_1(x)}{p^{n-k}}\right)=p^{k-1}S(f_1,p^{n-k}), \tag{3.8}$$

with $n-k\geqslant 2$. We have shown that the theorem holds for $V=j=0$. We now turn our attention to $V\geqslant 1$. Suppose that $V>j-1$ with $j\geqslant 1$. In view of the above arguments and (3.8) we should have $\alpha<\theta_j$, $n-jk\geqslant 2$, and

$$S(f,p^n)=p^{j(k-1)}\sum_{x=1}^{p^{n-jk}}e\left(\frac{ax^k+p^{\theta_j}b_1x}{p^{n-jk}}\right)=p^{j(k-1)}S(f_j,p^{n-jk}). \tag{3.9}$$

We proceed from here.

First suppose that $n-jk\leqslant t_j+1$. If $\alpha=0$, then $t_j=\min(\alpha,\theta_j)=0$ and $n-jk\leqslant 1$, violating the fact of $n-jk\geqslant 2$. Thus $\alpha\geqslant 1$ in this case. By a trivial estimate and (3.9) we have

$$\begin{aligned}|S(f,p^n)|&\leqslant p^{j(k-1)}p^{n-jk}\leqslant p^{\frac{n}{2}-1}p^{\frac{jk+t_j+1}{2}}\leqslant p^{\frac{n}{2}-j}p^{\frac{jk+\theta_j+1}{2}}\\&=p^{-j}p^{\frac{n}{2}}p^{\frac{jk+\theta+j-jk+1}{2}}=p^{-\frac{j}{2}}p^{\frac{\min(\alpha,1)}{2}}p^{\frac{n}{2}}p^{\frac{\theta}{2}}.\end{aligned}$$

We now secure our theorem by checking V. In fact, $n-jk\leqslant t_j+1\leqslant\alpha+1\leqslant\left[\frac{\log k}{\log p}\right]+1\leqslant k-1$, and therefore, $Q=j$, verifying the theorem for this case.

Next we assume that $n-jk\geqslant t_j+2$.

If $\alpha > \theta_j$, we have as before that $S(f_j, p^{n-jk}) = 0$.

If $\alpha = \theta_j$, then Lemma 3 yields

$$|S(f_j, p^{n-jk})| \leqslant dp^{\min\left(\frac{\beta}{2}, \frac{n-jk}{2}-1\right)} p^{\frac{n-jk}{2}} p^{\frac{\theta_j}{2}},$$

combining with (3.9),

$$|S(f, p^n)| \leqslant dp^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{\frac{n-jk}{2}} p^{\frac{\theta_j}{2}} p^{jk-j} = dp^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{-\frac{j}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}}.$$

The condition $\alpha = \theta_j$ implies that $\zeta = j$ so that $V \leqslant j$ and the theorem holds.

Finally we consider $\alpha < \theta_j$. Again the underlying congruence $p^{-t_j}(akx^{k-1} + p^{\theta_j} b_1) \equiv 0 (\operatorname{mod} p)$ has only one root, $x = 0$. It follows from Lemma 1 that

$$S(f_j, p^{n-jk}) = \sum_{x=1}^{p^{n-jk-1}} e\left(\frac{f_j(px)}{p^{n-jk}}\right) = \sum_{x=1}^{p^{n-jk-1}} e\left(\frac{ap^k x^k + p^{\theta_j+1} b_j x}{p^{n-jk}}\right). \tag{3.10}$$

If $k > \theta_j + 1$, then by Lemma 5, $S(f_j, p^{n-jk}) = 0$, and the theorem is an immediate. If $k = \theta_j + 1$, then $\theta = (j+1)(k-1)$, so

$$j + 1 = \frac{\theta}{k-1} \geqslant \frac{\theta - \alpha}{k-1} = \zeta \geqslant J. \tag{3.11}$$

We divide into cases. When $jk + 2 \leqslant n \leqslant (j+1)k$, we have trivially

$$|S(f_j, p^{n-jk})| \leqslant p^{n-jk-1}, \tag{3.12}$$

thus by (3.9),

$$\begin{aligned} |S(f, p^n)| &\leqslant p^{n-j-1} \leqslant p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+k}{2}} = p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+\theta_j+1}{2}} \\ &= p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+\theta+j-jk+1}{2}} = p^{-\frac{j+1}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}} \leqslant p^{-\frac{V}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}}, \end{aligned}$$

proving that (1.11) holds.

When $n = (j+1)k + 1$, we have $n \equiv 1 (\operatorname{mod} k)$. By a trivial estimate again and (3.9) we obtain

$$|S(f, p^n)| \leqslant p^{n-j-1} = p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+k+1}{2}}$$

$$= p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+\theta_j+2}{2}} = p^{-\frac{j}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}} \leqslant p^{-\frac{j}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}} \leqslant p^{\frac{1-V}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}},$$

verifying (1.10) for this case. When $n \geqslant (j+1)k+2$, we have

$$S(f_j, p^{n-jk}) = p^{k-1} \sum_{x=1}^{p^{n-(j+1)k}} e\left(\frac{ax^k + b_1 x}{p^{n-(j+1)k}}\right).$$

If $\alpha > 0$, the above sum equals 0 and the theorem is an immediate.

If $\alpha = 0 = \mathrm{ord}_p(b_1)$, since $n-(j+1)k \geqslant 2$, we can apply Lemma 3 to the above sum to deduce

$$|S(f_j, p^{n-jk})| \leqslant dp^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{k-1} p^{\frac{n-(j+1)k}{2}},$$

and by (3.10),

$$\begin{aligned} |S(f, p^n)| &\leqslant dp^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{j(k-1)} p^{k-1} p^{\frac{n-(j+1)k}{2}} \\ &= dp^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+k}{2}} \\ &= dp^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+\theta_j+1}{2}} \\ &= dp^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+\theta+j-jk+1}{2}} \\ &= dp^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{-\frac{j+1}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}} \\ &\leqslant dp^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{-\frac{V}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}}. \end{aligned}$$

Suppose that $k \leqslant \theta_j$. If $n \leqslant (j+1)k+1$, then by a trivial estimate (3.12) and (3.9) we have

$$\begin{aligned} |S(f, p^n)| &\leqslant p^{n-j-1} \leqslant p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+k+1}{2}} \leqslant p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+\theta_j+1}{2}} \\ &= p^{-j-1} p^{\frac{n}{2}} p^{\frac{jk+\theta+j-jk+1}{2}} = p^{-\frac{j+1}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}} \leqslant p^{-\frac{V}{2}} p^{\frac{n}{2}} p^{\frac{\theta}{2}}, \end{aligned}$$

as required. If $n \geqslant (j+1)k+2$, by repeating the above arguments, at most $(V+1)$ times, we can conclude the proof of the theorem.

4. Example. The following example shows that our result is best possible.

Example. Let p be a prime > 3, $f(x) = x^3 + p^2 x$, and $n = 3$. We now consider the exponential sum $S(f, p^3)$. Writing $x = y + p^2 z$ with $1 \leqslant y \leqslant p^2$ and $1 \leqslant z \leqslant p$, we have

$$S(f, p^3) = \sum_{y=1}^{p^2} \sum_{z=1}^{p} e\left(\frac{(y^3 + p^2 y) + (3y^2 + p^2) p^2 z}{p^3}\right)$$

$$= \sum_{y=1}^{p^2} e\left(\frac{y^3+p^2y}{p^3}\right) \sum_{z=1}^{p} e\left(\frac{3y^2z}{p}\right).$$

The sum over z is zero unless $y = wp$, where $w = 1, 2, \dots, p$. Thus

$$S(f, p^3) = p \sum_{w=1}^{p} e\left(\frac{w^3p^3+p^3w}{p^3}\right) = p^2. \tag{4.1}$$

On the other hand, for this function $f(x)$, $n = k = 3$. Thus $Q = 1$. By observation we have $\theta = 2$, $\alpha = 0$, and $J = \left[\frac{\theta-\alpha}{k-1}\right] = \left[\frac{2-0}{3-1}\right] = 1$. Hence $V = \min(J, Q) = 1$. Also $d = 1$, $r = 0$, and $(p^3, b) = p^2$. Moreover, $\min\left(\frac{\beta}{2}, \frac{n}{2} - 1\right) = 0$ and $\frac{\min(\alpha,1)}{2} = 0$. Our upper bound is therefore

$$dp^{\frac{\min(\alpha,1)}{2}} p^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)} p^{-\frac{V}{2}} p^{\frac{n}{2}} (p^n, b)^{\frac{1}{2}} = p^2,$$

which is coincident with (4.1).

5. Remarks. Though our example shows that the theorem is best possible, it is based on the case of both $\min(\frac{\beta}{2}, \frac{n}{2} - 1) = 0$ and $\frac{\min(\alpha,1)}{2} = 0$. It therefore still leaves room to remove either $p^{\frac{\min(\alpha,1)}{2}}$ or $p^{\min\left(\frac{\beta}{2}, \frac{n}{2}-1\right)}$, or both. To achieve this, one needs to get a nontrivial upper bound for $S(f, p^n)$ when $n \equiv 1 (\bmod k)$ and $n \equiv 1 (\bmod t_j)$ for $j = 0, 1, \dots, V$. Since this type of exponential sum is of particular interest, I would make the following conjecture.

Conjecture. $|S(f, p^n)| \leqslant p^{-\frac{V}{2}} p^{\frac{n}{2}} (p^n, b)^{\frac{1}{2}}$.

References

1. J. H. H. Chalk, *On Hua's estimate for exponential sums.* — Mathematika **14** (1987), 115–123.
2. T. Cochrane and Z. Zheng, *Pure and mixed exponential sums.* — Acta Arith. **91** (1999), 249–278.
3. T. Cochrane and Z. Zheng, *Bounds for certain exponential sums.* — Asian J. Math. **4** (2000), 757–774.
4. R. Dabrowski and B. Fisher, *A stationary phase formula for exponential sums over Z/Z and applications to GL(3)-kloosterman sums.* — Acta Arith. **80** (1997), 1–48.
5. H. Davenport and H. Heilbronn, *On an exponential sum.* — Proc. London Math. Soc. **41** (1936), 449–453.
6. P. Ding, *On a conjecture of Chalk.* — J. Number Theory **65** (1997), 116–129.
7. L. K. Hua, *On exponential sums.* — Sci. Record (Peking)(N.S.) **1** (1957), 1–4.
8. W. K. A. Loh, *Hua's Lemma.* — Bull. Australian Math. Soc. **50** (1994), 451–458.

9. J. H. Loxton and R. A. Smith, *On Hua's estimate for exponential sums.* — J. London Math. Soc. **26** (1982), 15–20.
10. J. H. Loxton and R. C. Vaughan, *The estimate for complete exponential sums.* — Canada Math. Bull. **28** (1985(4)), 442–454.
11. R. A. Smith, *Estimate for exponential sums.* — Proc. Amer. Math. Soc. **79** (1980), 365–368.
12. R. C. Vaughan, *The Hardy-Littlewood method.* 2nd ed. Cambridge Tracts in Math. 125, Cambridge Univ. Press, Cambridge, 1997.
13. A. Weil, *On some exponential sums.* — Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207.
14. Y. Ye, *Hyper-Kloosterman sums and estimation of exponential sums of polynomials of higher degree.* — Acta Arith. **86** (1998), 255–267.
15. Y. Ye, *Estimation of exponential sums of polynomials of higher degree II.* — Acta Arith. **93** (2000), 221–235.

Simon Fraser University at Kamloops
Kamloops, British Columbia V2H 1H1
Canada

Поступило 3 февраля 2005 г.