ACTA ARITHMETICA
LIX.2 (1991)

An improvement to Chalk's estimation of exponential sums

by

PING DING (Burnaby, B.C.)

1. Introduction. Let p be a prime and let

$$f(x) = a_k x^k + \ldots + a_1 x + a_0 \in \mathbf{Z}[x] \tag{1}$$

with $(a_1, \ldots, a_k, p) = 1$.

For any positive integer q we write

$$S(q, f) = \sum_{x=0}^{q-1} e_q(f(x)), \tag{2}$$

where $e_q(t) = \exp(2\pi i t/q)$.

For the case $q = p^n$ $(n \geqslant 1)$, Hua [3] showed that

$$|S(p^n, f)| \leqslant k^3 p^{n(1-1/k)}. \tag{3}$$

In 1985, Loxton and Vaughan [4] worked in a different way and proved that

$$|S(p^n, f)| \leqslant (k-1) p^{\delta/(e+1)} p^{\tau/(e+1)} p^{n[1-1/(e+1)]}, \tag{4}$$

where

$$\tau = \begin{cases} 1 & \text{if } p \leqslant k, \\ 0 & \text{if } p > k, \end{cases} \qquad e = \max_{1 \leqslant i \leqslant s} e_i,$$

e_i satisfies

$$f'(x) = k a_k (x-\xi_1)^{e_1} \ldots (x-\xi_s)^{e_s},$$

ξ_i $(1 \leqslant i \leqslant s)$ are distinct zeros of $f'(x)$ belonging to a fixed finite extension $\boldsymbol{K}_p$ of the p-adic field $\boldsymbol{Q}_p$, and $\delta = \upsilon_p[\theta(f')]$, $\theta(f')$ denoting the different of $f'(x)$ and υ_p the unique extension of the valuation in $\boldsymbol{Q}_p$ and $\boldsymbol{K}_p$.

Define t satisfying $p^t \| (ka_k, \ldots, 2a_2, a_1)$, where the symbol $\|$ means $p^t | (ka_k, \ldots, 2a_2, a_1)$ and $p^{t+1} \nmid (ka_k, \ldots, 2a_2, a_1)$. Let $\mu_1, \ldots, \mu_r$ be the different zeros modulo p of the congruence

$$p^{-t} f'(x) \equiv 0 \pmod{p}, \quad 0 \leqslant x < p, \tag{5}$$

and let $m_1, \ldots, m_r$ be their multiplicities. Put $\max_{1\leqslant i\leqslant r} m_i = M = M(f)$, $m_1+\ldots+m_r = m = m(f)$.

Later, Chalk [1] obtained the following result.

THEOREM 1. *Suppose* $n \geqslant 2$. *If* $r > 0$, *then*

$$|S(p^n, f)| \leqslant mkp^{t/(M+1)} p^{n[1-1/(M+1)]} \tag{6}$$

and if $r = 0$, *then*

$$S(p^n, f) = 0 \quad \text{for all } n \geqslant 2(t+1)$$

and otherwise

$$|S(p^n, f)| \leqslant p^{2t+1}, \quad \text{where } p^t \leqslant k.$$

Since the result for $r = 0$ is trivial, we only consider the case $r > 0$, and so $M \geqslant 1$. In this paper we will show that k can be substituted by $k^{1/2}$ in Theorem 1. That is, we will prove the following

THEOREM. *For* $r > 0$ *we have*

$$|S(p^n, f)| \leqslant mk^{1/2} p^{t/(M+1)} p^{n[1-1/(M+1)]}. \tag{7}$$

2. Some lemmas.

LEMMA 1 ([2]). *Let* σ_j *satisfy* $p^{\sigma_j} \| f(\mu_j+px)-f(\mu_j)$ *and put*

$$g_{\mu_j}(y) = p^{-\sigma_j}\big(f(py+\mu_j)-f(\mu_j)\big).$$

If $p^{t_j} \| g'_{\mu_j}(y)$, *then*

$$\sigma_j \leqslant m_j+t+1-t_j.$$

LEMMA 2 ([3], [2]). *We have*

$$p^t \leqslant k \quad \text{and} \quad p^{t_j} \leqslant k,$$

where t *and* t_j *are defined as above.*

LEMMA 3 (A. Weil [5]).

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

LEMMA 4. *If* $n = 2t+1$, *then*

$$|S(p^n, f)| \leqslant mk^{1/2} p^{t/(M+1)} p^{n[1-1/(M+1)]}. \tag{8}$$

Proof. Since $n \geqslant 2$, we have $t \geqslant 1$. Let $x = y+p^{n-t-1}z$, where y and z run independently through the values

$$y = 1, \ldots, p^{n-t-1}, \quad z = 0, \ldots, p^{t+1}-1.$$

Then

$$S(p^n, f) = \sum_{y=1}^{p^{n-t-1}} e_{p^n}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_p\left(z\frac{f'(y)}{p^t}+\frac{1}{2}z^2 f''(y)\right). \tag{9}$$

Since $p^t | f''(y)$, if either p is an odd prime and $t \geqslant 1$ or $p = 2$ and $t \geqslant 2$, then $2p | f''(y)$ for all $1 \leqslant y \leqslant p^{n-t-1}$. Hence

$$S(p^n, f) = \sum_{y=1}^{p^{n-t-1}} e_{p^n}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_{p^{t+1}}(zf'(y)).$$

If $y \not\equiv \mu_j \pmod p$, $j = 1, \ldots, r$, then

$$\sum_{z=0}^{p^{t+1}-1} e_{p^{t+1}}(zf'(y)) = 0.$$

Therefore

$$\begin{aligned} |S(p^n, f)| &\leqslant p^{t+1} \sum_{j=1}^{r} \Big| \sum_{\substack{y=1 \\ y\equiv\mu_j(\bmod p)}}^{p^{n-t-1}} e_{p^n}(f(y)) \Big| \leqslant rp^{n-1} \\ &= rp^{(2t+1)/(M+1)-1} p^{n[1-1/(M+1)]} \\ &\leqslant rk^{1/2} p^{t/(M+1)} p^{n[1-1/(M+1)]}, \end{aligned} \tag{10}$$

the last inequality here is due to Lemma 2.

Now consider the case $p = 2$ and $t = 1$. This implies $n = 3$ and

$$S(2^3, f) = \sum_{y=1}^{2} e_{2^3}(f(y)) \sum_{z=0}^{2^2-1} e_2\left(z\frac{f'(y)}{2}+\frac{1}{2}z^2 f''(y)\right). \tag{11}$$

If $k \geqslant 4$, then we trivially have

$$\begin{aligned} |S(2^3, f)| &\leqslant 8 = 2^{2/(M+1)} 2^{t/(M+1)} 2^{n[1-1/(M+1)]} \\ &\leqslant k^{1/(M+1)} 2^{t/(M+1)} 2^{n[1-1/(M+1)]}. \end{aligned}$$

If $k = 3$, then $f(x) = a_3x^3+a_2x^2+a_1x+a_0$ with $(a_3, a_2, a_1, 2) = 1$. So $f'(x) = 3a_3x^2+2a_2x+a_1$ and $f''(x) = 6a_3x+2a_2$. The condition $t = 1$ means $2 \| (3a_3, 2a_2, a_1)$ which implies $2|a_3$ and $2|a_1$. For $x = 1$, $f''(1) = 6a_3+2a_2$, and so $f''(1)/2 \not\equiv 0 \pmod 2$ since otherwise $2|a_2$ contradicting $(a_3, a_2, a_1, 2) = 1$. For $x = 2$ we have $f''(2) = 12a_3+2a_2$, and consequently $f''(2)/2 \not\equiv 0 \pmod 2$ with the same reason as in the case of $x = 1$. Thus (11) and Lemma 3 yield

$$\begin{aligned} |S(2^3, f)| &= 2\left|\sum_{y=1}^{2} e_{2^3}(f(y)) \sum_{z=0}^{1} e_2\left(\frac{f'(y)}{2}z+\frac{f''(y)}{2}z^2\right)\right| \\ &\leqslant 4\cdot 2^{1/2} = 2^{3/(M+1)-1/2} 2^{3[1-1/(M+1)]} \\ &\leqslant k^{1/(M+1)} 2^{t/(M+1)} 2^{3[1-1/(M+1)]}. \end{aligned}$$

If $k=2$, then $f(x)=a_2x^2+a_1x+a_0$ with $(a_2,a_1,2)=1$. Thus $f''(x)=2a_2$ but $(a_2,2)=1$ since $t=1$ and $2|a_1$. Clearly $f''(x)/2\not\equiv 0 \pmod 2$ for either $x=1$ or 2 and so using (11) and Lemma 3 again we obtain

$$\begin{aligned}|S(2^3,f)| &= 2\left|\sum_{y=1}^{2} e_{2^3}(f(y)) \sum_{z=0}^{1} e_2\left(\frac{f'(y)}{2}z+\frac{f''(y)}{2}z^2\right)\right| \\ &\leqslant 4\cdot 2^{1/2} = 2^{3/(M+1)-1/2}\,2^{3[1-1/(M+1)]} \\ &\leqslant k^{1/(M+1)}\,2^{t/(M+1)}\,2^{3[1-1/(M+1)]}.\end{aligned}$$

This completes the proof of Lemma 3.

3. Proof of the theorem. For $2\leqslant n\leqslant 2t$, a trivial estimate and Lemma 2 give that

$$|S(p^n,f)|\leqslant p^n\leqslant k^{1/(M+1)}\,p^{t/(M+1)}\,p^{n[1-1/(M+1)]}\leqslant k^{1/2}\,p^{t/(M+1)}\,p^{n[1-1/(M+1)]}.$$

Lemma 3 is for the case $n=2t+1$.

Assume now $n\geqslant 2(t+1)$. By substituting $x=y+p^{n-t-1}z$, $y=1,\ldots,p^{n-t-1}$, $z=0,\ldots,p^{t+1}-1$, we obtain

$$S(p^n,f)=\sum_{y=1}^{p^{n-t-1}} e_{p^n}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_{p^{t+1}}(zf'(y)). \tag{12}$$

So

$$|S(p^n,f)|\leqslant \sum_{j=1}^{r}\Bigg|\sum_{\substack{y=1\\ y\equiv\mu_j \pmod p}}^{p^n} e_{p^n}(f(y))\Bigg| = \sum_{j=1}^{r}|S_{\mu_j}|, \quad \text{say.} \tag{13}$$

Define sets $A_i (i=1,\ldots,4)$ by

$$\begin{aligned}A_1&=\{j:\ n\leqslant\sigma_j\},\\ A_2&=\{j:\ 1\leqslant n-\sigma_j\leqslant 2t_j\},\\ A_3&=\{j:\ n-\sigma_j=2t_j+1\},\\ A_4&=\{j:\ n-\sigma_j\geqslant 2t_j+2\}.\end{aligned}$$

Then

$$\sum_{i=1}^{4}\sum_{j\in A_i} m_j = m. \tag{14}$$

(i) Suppose $j\in A_1$. By Lemmas 1 and 2,

$$\begin{aligned}|S_{\mu_j}| &\leqslant p^{n-1} = p^{n/(M+1)-1}\,p^{n[1-1/(M+1)]}\leqslant p^{\sigma_j/(M+1)-1}\,p^{n[1-1/(M+1)]}\\ &\leqslant p^{(m_j+t+1-t_j)/(M+1)-1}\,p^{n[1-1/(M+1)]}\leqslant p^{t/(M+1)}\,p^{n[1-1/(M+1)]}.\end{aligned}$$

(ii) Suppose $j\in A_2$. Again Lemmas 1 and 2 give that

$$\begin{aligned}|S_{\mu_j}| &\leqslant p^{n-1} = p^{n/(M+1)-1}\,p^{n[1-1/(M+1)]}\leqslant p^{(\sigma_j+2t_j)/(M+1)-1}\,p^{n[1-1/(M+1)]}\\ &\leqslant p^{(m_j+t+1+t_j)/(M+1)-1}\,p^{n[1-1/(M+1)]}\leqslant k^{1/(M+1)}\,p^{t/(M+1)}\,p^{n[1-1/(M+1)]}.\end{aligned}$$

(iii) For $j\in A_3$, we have

$$|S_{\mu_j}| = p^{\sigma_j-1}\,|S(p^{n-\sigma_j}, g_{\mu_j}(y))|. \tag{15}$$

If $t_j=0$, then it follows from Lemmas 1 and 2 that

$$\begin{aligned}|S_{\mu_j}| &\leqslant p^{n-1} = p^{(\sigma_j+1)/(M+1)-1}\,p^{n[1-1/(M+1)]}\\ &\leqslant p^{(m_j+t+2)/(M+1)-1}\,p^{n[1-1/(M+1)]}\leqslant k^{1/(M+1)}\,p^{t/(M+1)}\,p^{n[1-1/(M+1)]}.\end{aligned}$$

Assume now $t_j\geqslant 1$. If either p is an odd prime and $t_j\geqslant 1$ or $p=2$ and $t_j\geqslant 2$, as in the proof of Lemma 3, but using t_j, $n-\sigma_j$ and $g_{\mu_j}(y)$ instead of t, n and $f(x)$ respectively, we obtain

$$|S(p^{n-\sigma_j}, g_{\mu_j}(y))|\leqslant sp^{n-\sigma_j-1}, \tag{16}$$

where s is the number of the different zeros modulo p of the congruence

$$g'_{\mu_j}(y)\equiv 0 \pmod{p^{t_j+1}} \qquad (0\leqslant y<p),$$

and so $s\leqslant m_j$. Hence it follows from (15), (16), Lemmas 1 and 2 that

$$\begin{aligned}|S_{\mu_j}| &\leqslant m_j p^{n-2} = m_j p^{(\sigma_j+2t_j+1)/(M+1)-2}\,p^{n[1-1/(M+1)]}\\ &\leqslant m_j p^{(m_j+t+t_j+2)/(M+1)-2}\,p^{n[1-1/(M+1)]}\\ &\leqslant m_j k^{1/(M+1)}\,p^{t/(M+1)}\,p^{n[1-1/(M+1)]}.\end{aligned}$$

Consider the case $p=2$ and $t_j=1$. If $k\geqslant 4$ then it is easily seen that

$$\begin{aligned}|S_{\mu_j}| &\leqslant 2^{n-1} = 2^{(\sigma_j+3)/(M+1)-1}\,2^{n[1-1/(M+1)]}\\ &\leqslant 2^{(m_j+t+3)/(M+1)-1}\,2^{n[1-1/(M+1)]}\\ &\leqslant 2^{(t+2)/(M+1)}\,2^{n[1-1/(M+1)]}\leqslant k^{1/2}\,2^{t/(M+1)}\,2^{n[1-1/(M+1)]}.\end{aligned}$$

For the case $k=3$ or 2 we note that correspondingly $g_{\mu_j}(y)$ is also a cubic or quadratic polynomial with the same properties as $f(x)$. Hence by the method similar to that in the proof of Lemma 4 for the cases $p=2$, $t=1$, $k=3$ and 2 we obtain

$$\begin{aligned}|S_{\mu_j}| &\leqslant 2^{\sigma_j-1}\,2^{n-\sigma_j-1/2} = 2^{n-3/2} = 2^{(\sigma_j+3)/(M+1)-3/2}\,2^{n[1-1/(M+1)]}\\ &\leqslant 2^{(m_j+t+3)/(M+1)-3/2}\,2^{n[1-1/(M+1)]}\\ &\leqslant 2^{(t+2)/(M+1)-1/2}\,2^{n[1-1/(M+1)]}\leqslant k^{1/2}\,2^{t/(M+1)}\,2^{n[1-1/(M+1)]}.\end{aligned}$$

(iv) Let $j \in A_4$. By induction,

$$|S_{\mu_j}| \leqslant p^{\sigma_j - 1} m(g_j) k^{1/2} p^{t_j/[M(g_j)+1]} p^{(n-\sigma_j)[1-1/(M(g_j)+1)]}$$
$$\leqslant m_j k^{1/2} p^{t_j/(M+1)-1} p^{n[1-1/(M+1)]+\sigma_j/(M+1)}$$
$$\leqslant m_j k^{1/2} p^{(m_j+t+1)/(M+1)-1} p^{n[1-1/(M+1)]} \leqslant m_j k^{1/2} p^{t/(M+1)} p^{n[1-1/(M+1)]},$$

since $n \geqslant 2(t+1)$, $m(g_j) \leqslant m_j$ and $M(g_j) \leqslant M$.

Hence for $n \geqslant 2(t+1)$, it follows from (i)–(iv) that

$$|S(p^n, f)| \leqslant \sum_{i=1}^{4} \sum_{j \in A_i} m_j k^{1/2} p^{t/(M+1)} p^{n[1-1/(M+1)]} = mk^{1/2} p^{t/(M+1)} p^{n[1-1/(M+1)]}.$$

This completes the proof of the theorem.

4. Examples. We give two examples here for comparison purposes.

EXAMPLE 1. Let $p = 2$, $n = 1$, and $f(x) = x^3 - x$. Then

$$S(2, f) = \sum_{x=0}^{1} e_2(x^3 - x) = 2 = 2^{1/2} 2^{1/2}. \tag{17}$$

We have $f'(x) = 3x^2 - 1$ and so $t = 0$. Since $f'(0) = -1 \not\equiv 0 \pmod 2$ and $f'(1) = 2 \equiv 0 \pmod 2$, we have $r = m = M = 1$. Our theorem gives that

$$|S(2, f)| \leqslant 3^{1/2} 2^{1/2}. \tag{18}$$

I think, in general, one could expect to obtain the sharp estimation

$$|S(p^n, f)| \leqslant mp^{1/(M+1)} p^{t/(M+1)} p^{n[1-1/(M+1)]}. \tag{19}$$

EXAMPLE 2. This example is qouted by Chalk [1]. Let $p > k > 2$ and

$$f(x) = k!(px - 1)^{k-1} x.$$

Then $r = m = M = 1$ and $t = 0$. Since $\xi_1 = p^{-1}$, $\xi_2 = 0$, $e = k - 1 > M = 1$ and $\delta = k - 2$, the estimation (4) is

$$(k-1) p^{(k-2)/(k-1)} p^{n[1-(1/k)]}$$

whereas (6) yields

$$kp^{n/2}$$

and (7) gives

$$k^{1/2} p^{n/2}.$$

Acknowledgement. I appreciate the referee's valuable suggestions and comments.

References

[1] J. H. H. Chalk, *On Hua's estimates for exponential sums*, Mathematika 34 (2) (1987), 115–123.
[2] P. Ding and M. G. Qi, *Further estimate of complete trigonometric sums*, J. Tsinghua Univ. (1990), to appear.
[3] L. K. Hua, *Additive Theory of Prime Numbers*, A.M.S., Providence 1965.
[4] J. H. Loxton and R. C. Vaughan, *The estimation of complete exponential sums*, Canad. Math. Bull. 28 (1985), 440–454.
[5] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.

DEPARTMENT OF MATHEMATICS AND STATISTICS
SIMON FRASER UNIVERSITY
Burnaby, B. C., Canada V5A 1S6

Received on 4.5.1990
and in revised form on 21.8.1990 (2042)