

An improvement to Chalk's estimation of exponential sums

by

PING DING (Burnaby, B.C.)

1. Introduction. Let p be a prime and let

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

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

For any positive integer q we write

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

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

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

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

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

$$(4) \quad |S(p^n, f)| \leq (k-1) p^{\delta/(e+1)} p^{\tau/(e+1)} p^{n(1-1/(e+1))},$$

where

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

e_i satisfies

$$f'(x) = ka_k(x - \zeta_1)^{e_1} \dots (x - \zeta_s)^{e_s},$$

ζ_i ($1 \leq i \leq s$) are distinct zeros of $f'(x)$ belonging to a fixed finite extension K_p of the p -adic field \mathbf{Q}_p , and $\delta = v_p[\theta(f')]$, $\theta(f')$ denoting the different of $f'(x)$ and v_p the unique extension of the valuation in \mathbf{Q}_p and K_p .

Define t satisfying $p^t \parallel (ka_k, \dots, 2a_2, a_1)$, where the symbol \parallel means $p^t \mid (ka_k, \dots, 2a_2, a_1)$ and $p^{t+1} \nmid (ka_k, \dots, 2a_2, a_1)$. Let μ_1, \dots, μ_r be the different zeros modulo p of the congruence

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

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

Later, Chalk [1] obtained the following result.

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

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

and if $r = 0$, then

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

and otherwise

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

Since the result for $r = 0$ is trivial, we only consider the case $r > 0$, and so $M \geq 1$. 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*

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

2. Some lemmas.

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

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

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

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

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

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

where t and t_j are defined as above.

LEMMA 3 (A. Weil [5]).

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

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

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

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

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

Then

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

Since $p^t |f''(y)|$, if either p is an odd prime and $t \geq 1$ or $p = 2$ and $t \geq 2$, then $2p |f''(y)|$ for all $1 \leq y \leq p^{n-t-1}$. 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 $y \not\equiv \mu_j \pmod{p}$, $j = 1, \dots, r$, then

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

Therefore

$$(10) \quad |S(p^n, f)| \leq p^{t+1} \sum_{j=1}^r \left| \sum_{\substack{y=1 \\ y \equiv \mu_j \pmod{p}}}^{p^{n-t-1}} e_{p^n}(f(y)) \right| \leq rp^{n-1} \\ = rp^{(2t+1)/(M+1)-1} p^{n[1-1/(M+1)]} \\ \leq rk^{1/2} p^{t/(M+1)} p^{n[1-1/(M+1)]},$$

the last inequality here is due to Lemma 2.

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

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

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

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

If $k = 3$, then $f(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$ with $(a_3, a_2, a_1, 2) = 1$. So $f'(x) = 3a_3 x^2 + 2a_2 x + a_1$ and $f''(x) = 6a_3 x + 2a_2$. The condition $t = 1$ means $2 \parallel (3a_3, 2a_2, a_1)$ 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

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

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

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

This completes the proof of Lemma 3.

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

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

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

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

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

So

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

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

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

Then

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

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

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

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

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

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

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

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

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

Assume now $t_j \geq 1$. If either p is an odd prime and $t_j \geq 1$ or $p = 2$ and $t_j \geq 2$, 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

$$(16) \quad |S(p^{n-\sigma_j}, g_{\mu_j}(y))| \leq s p^{n-\sigma_j-1},$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EXAMPLE 2. This example is quoted 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)