Title	Upper bounds on n-dimensional Kloosterman sums
Author(s)	Cochrane, T; Liu, MC; Zheng, Z
Citation	Journal of Number Theory, 2004, v. 106 n. 2, p. 259-274
Issued Date	2004
URL	http://hdl.handle.net/10722/48609
Rights	Creative Commons: Attribution 3.0 Hong Kong License

UPPER BOUNDS ON N-DIMENSIONAL KLOOSTERMAN SUMS

TODD COCHRANE, MING-CHIT LIU, AND ZHIYONG ZHENG

ABSTRACT. Let p^m be any prime power and $K_n(a,p^m)$ be the n-dimensional Kloosterman sum

$$K_n(a,p^m)=\sum_{x_1=1}^{p^m}\cdots\sum_{x_n=1}^{p^m} e_{p^m}(x_1+\cdots+x_n+a\overline{x_1x_2\dots x_n}),$$

where the x_i are restricted to values not divisible by p. Let m,n be positive integers with $m\geq 2$ and suppose that $p^\gamma\|(n+1)$. We obtain the upper bound $|K_n(a,p^m)|\leq (n+1,p-1)p^{\frac{1}{2}\min(\gamma,m-2)}p^{mn/2}$, for odd p. For $p=2$ we obtain the same bound, with an extra factor of 2 inserted.

1. INTRODUCTION

Let p be a prime, m,n be positive integers, a be any integer and $K_n(a,p^m)$ be the n-dimensional Kloosterman sum

$$K_n(a,p^m)=\sum_{\substack{x_1=1\\ p\nmid x_1x_2\dots x_n}}^{p^m}\cdots\sum_{x_n=1}^{p^m} e_{p^m}(x_1+\cdots+x_n+a\overline{x_1x_2\dots x_n}), \tag{1.1}$$

where the overline denotes multiplicative inverse $(\mathrm{mod}\ p^m)$. If $p|a$ it is easily seen that $K_n(a,p)=(-1)^n$ and that $K_n(a,p^m)=0$ for $m\geq 2$ (see Theorem 3 of [9]), and so we may always assume that $p\nmid a$. Deligne [4], appealing to his deep work on the Weil conjectures established in the case $m=1$ that

$$|K_n(a,p)|\leq (n+1)p^{n/2}. \tag{1.2}$$

There is also an elementary upper bound,

$$|K_n(a,p)|\leq p^{\frac{n+1}{2}}, \tag{1.3}$$

due to Mordell [7] and Smith [9], which is sharper than (1.2) for $n>\sqrt{p}$. The reader is referred to the paper of Smith for a historical discussion on the estimation of the Kloosterman sum.

For a general value of $m\geq 1$ Smith [9] proved that for odd p we have

$$|K_n(a,p^m)|\leq (n+1)p^{\frac{nm}{2}}. \tag{1.4}$$

The same argument that was used by Smith to prove (1.3) can also be used to obtain the upper bound

$$|K_n(a,p^m)|\leq p^{\frac{(n+1)m}{2}}. \tag{1.5}$$

Date: January 11, 2000.

1991 *Mathematics Subject Classification.* 11L07;11L03.

Key words and phrases. kloosterman sums.

Research of the third author was supported by the National Science Fund of The Peoples Republic of China for Distinguished Young Scholars.

Dabrowski and Fisher [3] (Example 1.17) obtained an extra savings in the special case that $p = n+1$:

$$|K_n(a,p^m)| \le \begin{cases} p^{\frac{nm}{2}}, & \text{if } m=2; \\ p^{1/2}p^{\frac{nm}{2}}, & \text{if } m=3 \text{ or } m\ge 5; \\ p\cdot p^{\frac{nm}{2}}, & \text{if } m=4. \end{cases} \tag{1.6}$$

See also the work of Ye [10] for an application of (1.6).

Here, we take the work of Smith one step further and establish an upper bound that sharpens (1.4), (1.5) and (1.6).

Theorem 1.1. *Let p be a prime, n be a positive integer and suppose that $p^\gamma \| (n+1)$.*

(a) If p is odd then for $m \ge 2$,

$$|K_n(a,p^m)| \le (n+1, p-1)\ p^{\frac{1}{2}\min(\gamma, m-2)} p^{nm/2}. \tag{1.7}$$

(b) If $p=2$ then for $m \ge 2$,

$$|K_n(a,2^m)| \le 2\cdot 2^{\frac{1}{2}\min(\gamma,m-2)} 2^{nm/2}. \tag{1.8}$$

In Proposition 2.1 we state a more precise version of this theorem for the case of odd p. When $(n+1, p-1)$ is bounded by a constant we deduce from (1.7) the upper bound

$$|K_n(a,p^m)| \ll \sqrt{n}\ p^{nm/2}, \tag{1.9}$$

which is a best possible type of upper bound. Indeed, by Proposition 2.1, it follows that if $n+1 = p^\gamma$ then for any $m \ge \gamma+2$ we have

$$|K_n(1,p^m)| = \sqrt{n+1}\ p^{nm/2}.$$

It is reasonable to conjecture that (1.9) holds in general, even when $m=1$, but this is no doubt a very difficult problem.

2. Proof of Theorem 1.1

We take up the case of odd p in this section and deal with $p=2$ in section 3. The theorem is deduced from the following result of Smith [9].

Theorem 2.1. *Let p be an odd prime and a an integer not divisible by p.*
(i) Suppose that m is even. Then by Theorem 4 of [9] we have

$$K_n(a,p^m) = p^{nm/2} \sum_{\substack{u=1 \\ u^{n+1}\equiv a \pmod{p^{m/2}}}}^{p^{m/2}} e_{p^m}(nu + a\overline{u}^n). \tag{2.1}$$

(ii) Suppose that $m \ge 3$ is odd. Let $\beta = (m-1)/2$. If $p \nmid (n+1)$ we have by Theorem 5 (i) of [9] that $K_n(a,p^m)$ is a sum of $(n+1, p-1)$ complex numbers of modulus $p^{nm/2}$ and so

$$|K_n(a,p^m)| \le (n+1, p-1) p^{nm/2}. \tag{2.2}$$

If $p|(n+1)$ then by Theorem 5 (ii) of [9],

$$K_n(a,p^m) = p^{(nm+1)/2}\theta \sum_{\substack{u=1 \\ u^{n+1}\equiv a \pmod{p^{\beta+1}}}}^{p^\beta} e_{p^m}(nu + a\overline{u}^n), \tag{2.3}$$

where θ is a complex number of modulus one.

(We note that the value of θ in Smith's paper should be corrected to read $\theta = \epsilon_{n-1}(p)\chi_p(gN(a))$.)

In the course of proving Theorem 1.1 we actually establish the more precise result,

Proposition 2.1. *Let n be a positive integer, p an odd prime and suppose that $p^\gamma || (n+1)$.*

(i) If a is not an $(n+1)$-th power $\pmod{p^{\gamma+1}}$ *and $m \geq \gamma+2$ then $K_n(a, p^m) = 0$.*

(ii) If a is an $(n+1)$-th power $\pmod{p^{\gamma+1}}$ *and $m \geq 2$ then $K_n(a, p^m)$ is a sum of $(n+1, p-1)$ complex numbers, each of modulus $p^{nm/2} p^{\frac{1}{2}\min\{\gamma, m-2\}}$.*

The values of the complex numbers in part (ii) may be calculated explicitly using the method here together with the results of Smith [9]. This may give one hope of making a further savings in the constant $(n+1, p-1)$ on the right-hand side of (1.7).

We start with the following elementary lemma, which follows from the standard criterion for an element to be an $(n+1)$-th power in a cyclic group.

Lemma 2.1. *Suppose that p is an odd prime with $p^\gamma || (n+1)$ and $p \nmid a$. If a is an $(n+1)$-th power* $\pmod{p^{\gamma+1}}$ *then a is an $(n+1)$-th power modulo any power of p.*

The next lemma is an easy application of the method of critical points for estimating exponential sums. If $f(x)$ is a polynomial over $\mathbb{Z}$ and p^t is the largest power of p dividing all of the coefficients of $f'(x)$ then the set critical points $\mathcal{A}$ associated with the sum $S := \sum_{x=1}^{p^m} e_{p^m}(f(x))$ is just the set of zeros of the congruence $p^{-t} f'(x) \equiv 0 \pmod{p}$. The basic result we need here is that if $m \geq t+2$ then

$$S = \sum_{\alpha \in \mathcal{A}} S_\alpha, \tag{2.4}$$

where S_α is the same sum as S with x restricted to the residue class $\alpha \pmod{p}$; see eg. Theorem 2.1 of [2] or Loh [6] or Ding [5]. Also, if α is a zero of multiplicity one then

$$|S_\alpha| = p^{\frac{m+t}{2}}. \tag{2.5}$$

When $p = 2$ the same result holds provided that $m \geq t+3$.

Lemma 2.2. *(a) Let p be an odd prime, a, b be integers with $p \nmid b$ and $f(x)$ be a polynomial with integer coefficients. Then for $m \geq 1$ we have*

$$|\sum_{x=1}^{p^m} e_{p^m}(bx^2 + cx + pf(x))| = p^{m/2}. \tag{2.6}$$

(b) If $p = 3$ and $3 \nmid b$ then for any $a, f(x)$ and $m \geq 1$ we have

$$|\sum_{x=1}^{p^m} e_{p^m}(ax^3 + bx^2 + cx + pf(x))| = p^{m/2}. \tag{2.7}$$

Proof. When $m = 1$, the two sums are just quadratic Gauss sums (replacing x^3 with x in part (b).) For $m \geq 2$ the critical point congruence associated with each of the sums is just $2bx + c \equiv 0 \pmod{p}$, and thus there is a single critical point of multiplicity one. The result follows from (2.4) and (2.5). □

The case of even m. We proceed now to the proof of the Theorem 1.1 and Proposition 2.1. Suppose first that m is even. Let $n+1 = p^\gamma d$ with $p \nmid d$ and let U be the set of residues $u \pmod{p^{m/2}}$ satisfying $u^{n+1} \equiv a \pmod{p^{m/2}}$. Then by (2.1) we have the immediate upper bound

$$|K_n(a,p^m)| \le p^{mn/2}|U| \le p^{mn/2}(p^{\frac{m}{2}-1}(p-1), n+1). \tag{2.8}$$

If $\gamma = 0$ or $\gamma \ge m-2$ then (1.7) follows immediately from (2.8). Also, if $\gamma = 0$ we see by (2.1) that $K_n(a,p^m) = 0$ if a is not an $(n+1)$-th power $\pmod p$ and that $K_n(a,p^m)$ is a sum of $(n+1, p-1)$ complex numbers of modulus $p^{nm/2}$ if a is an $(n+1)$-th power $\pmod p$. Here we have used Lemma 2.1.

Suppose next that $1 \le \gamma < \frac{m}{2}$. If a is not an $(n+1)$-th power $\pmod{p^{\gamma+1}}$ then by (2.1) it follows that $K_n(a,p^m) = 0$. Suppose now that a is an $(n+1)$-th power $\pmod{p^{\gamma+1}}$. Then by Lemma 2.1 a is an $(n+1)$-th power modulo any power of p. We first note that (2.1) may be written in the manner

$$K_n(a,p^m) = p^{nm/2} \sum_{u \in U} e_{p^m}(nu + a\overline{u}^n), \tag{2.9}$$

since, for $u \in U$, the value of $nu + a\overline{u}^n \pmod{p^m}$ depends only on the value of $u \pmod{p^{m/2}}$. To see this, let

$$k := (\phi(p^m) - 1)n. \tag{2.10}$$

In particular,

$$p^{m-1} \| (n+k). \tag{2.11}$$

Let u be any integer satisfying $u^{n+1} \equiv a \pmod{p^{m/2}}$, and let $\overline{u}$ denote a multiplicative inverse of $u \pmod{p^m}$. Then

$$a\overline{u}^{n+1}p^{m/2} \equiv p^{m/2} \pmod{p^m},$$

and so

$$\begin{aligned} n(u+p^{m/2}) + a\overline{(u+p^{m/2})}^n &\equiv nu + np^{m/2} + a\overline{u}^n(1+\overline{u}p^{m/2})^k \pmod{p^m} \\ &\equiv nu + np^{m/2} + a\overline{u}^n(1 + k\overline{u}p^{m/2} + \binom{k}{2}\overline{u}^2p^m + \dots) \pmod{p^m} \\ &\equiv nu + a\overline{u}^n \pmod{p^m}. \end{aligned}$$

We partition U into $(d, p-1)$ subsets as follows. Start by observing that the congruence $x^{n+1} \equiv a \pmod p$ has $(d, p-1)$ distinct solutions $\alpha_1, \dots, \alpha_{(d,p-1)} \pmod p$, each of which can be lifted to a solution $\pmod{p^m}$. We may assume that representatives have been chosen so that each α_i satisfies the congruence $x^{n+1} \equiv a \pmod{p^m}$. Put $j = \frac{m}{2} - \gamma$. In particular $j \ge 1$. For $i = 1, 2, \dots, (d, p-1)$, let

$$U_i = \{\alpha_i + p^j t : t = 1, 2, \dots p^\gamma\}.$$

Then (viewing the elements of U, U_i as residue classes $\pmod{p^{m/2}}$) U is the disjoint union of the sets U_i and we have by (2.9)

$$K_n(a,p^m) = p^{nm/2} \sum_{i=1}^{(p-1,d)} S_i,$$

where

$$S_i = \sum_{t=1}^{p^\gamma} e_{p^m}\left(n(\alpha_i + p^j t) + a(\overline{\alpha_i + p^j t})^n\right).$$

In what follows let $\alpha = \alpha_i$ and $S_\alpha = S_i$ for a typical value i, and let k be as defined in (2.10). Thus

$$S_\alpha = \sum_{t=1}^{p^\gamma} e_{p^m}(f_\alpha(t)), \tag{2.12}$$

where

$$f_\alpha(t) := n(\alpha + p^j t) + a(\overline{\alpha + p^j t})^n. \tag{2.13}$$

The theorem will be proved if we can show that $|S_\alpha| = p^{\gamma/2}$.

Now for any integer t,

$$(\overline{1 + \overline{\alpha} p^j t})^n \equiv (1 + \overline{\alpha} p^j t)^k \pmod{p^m}.$$

Also,

$$p^\gamma \| (k-1), \tag{2.14}$$

and $a\overline{\alpha}^n \equiv \alpha \pmod{p^m}$. Thus,

$$\begin{aligned} f_\alpha(t) &\equiv n\alpha + np^j t + \alpha(\overline{1 + \overline{\alpha} p^j t})^n \pmod{p^m} \\ &\equiv n\alpha + np^j t + \alpha(1 + \overline{\alpha} p^j t)^k \pmod{p^m} \\ &\equiv n\alpha + np^j t + \alpha(1 + k\overline{\alpha} p^j t + \binom{k}{2}\overline{\alpha}^2 p^{2j} t^2 + \binom{k}{3}\overline{\alpha}^3 p^{3j} t^3 + \dots) \pmod{p^m}. \end{aligned}$$

Using (2.11) we obtain

$$f_\alpha(t) \equiv (n+1)\alpha + \overline{\alpha}\binom{k}{2} p^{2j} t^2 + \overline{\alpha}^2 \binom{k}{3} p^{3j} t^3 + \cdots := \sum_{r=0}^{\infty} a_r t^r, \pmod{p^m} \tag{2.15}$$

say. Put

$$\sigma_\alpha = \min_{r \geq 1} \operatorname{ord}_p(a_r), \quad g_\alpha(t) = p^{-\sigma_\alpha} f_\alpha(t). \tag{2.16}$$

Now, since $p^\gamma \| (k-1)$ we have $\operatorname{ord}_p(a_2) = 2j + \gamma$ and for any $r \geq 3$

$$\operatorname{ord}_p(a_r) = \operatorname{ord}_p \binom{k}{r} p^{rj} \geq \gamma + rj - \operatorname{ord}_p(r!) > \gamma + rj - \tfrac{r}{p-1}$$

If $p > 3$ or $p = 3$ and $j > 1$ it follows that $\operatorname{ord}_p(a_r) > 2j + \gamma$ for $r \geq 3$. Thus $\sigma_\alpha = 2j + \gamma$, and since $m - (2j + \gamma) = \gamma$, we can write

$$S_\alpha = \sum_{t=1}^{p^\gamma} e_{p^{m-\sigma_\alpha}}(g_\alpha(t)) = e_{p^m}((n+1)\alpha) \sum_{t=1}^{p^\gamma} e_{p^\gamma}(\overline{2\alpha} k \frac{k-1}{p^\gamma} t^2 + ph(t)),$$

for some polynomial $h(t) \in \mathbb{Z}[t]$. By Lemma 2.2 (a) we have $|S_\alpha| = p^{\gamma/2}$, and the result follows. If $p = 3$ and $j = 1$ then the same conclusion can be made using Lemma 2.2 (b).

Suppose finally that $\frac{m}{2} \leq \gamma$. If a is not an $(n+1)$-th power $\pmod{p^{m/2}}$ then by (2.1), $K_n(a, p^m) = 0$. Suppose that a is an $(n+1)$-th power $\pmod{p^{m/2}}$.

Let $\alpha_1, \ldots, \alpha_{(d,p-1)}$ be distinct values $\pmod p$, each satisfying the congruence $x^{n+1} \equiv a \pmod{p^{m/2}}$. Then U can be written as a disjoint union of the sets

$$U_i = \{\alpha_i + pt : t = 1, 2, \ldots, p^{\frac{m}{2}-1}\},$$

and we have

$$K_n(a, p^m) = \sum_{i=1}^{(p-1,d)} S_i,$$

where $S_i := \sum_{u \in U_i} e_{p^m}(nu + a\overline{u}^n)$. Let $\alpha = \alpha_i$, $S_\alpha = S_i$ for a typical value i. Now, since $a\overline{\alpha}^n \equiv \alpha \pmod{p^{m/2}}$ we can write

$$a\overline{\alpha}^n = \alpha + \rho p^{m/2},$$

for some integer ρ. Then

$$S_\alpha = \sum_{t=1}^{p^{\frac{m}{2}-1}} e_{p^m}(f_\alpha(t)),$$

where

$$\begin{aligned} f_\alpha(t) &\equiv n\alpha + npt + (\alpha + \rho p^{m/2})(\overline{1 + \overline{\alpha}pt})^n \pmod{p^m} \\ &\equiv n\alpha + npt + (\alpha + \rho p^{m/2})(1 + \overline{\alpha}p^j t)^k \pmod{p^m} \\ &\equiv (n+1)\alpha + \rho p^{m/2} + k\rho\overline{\alpha}p^{\frac{m}{2}+1}t + (\alpha + \rho p^{\frac{m}{2}})\overline{\alpha}^2\tbinom{k}{2}p^2t^2 \\ &\qquad + (\alpha + \rho p^{\frac{m}{2}})\overline{\alpha}^3\tbinom{k}{3}p^3t^3 + \ldots \pmod{p^m} \\ &:= \sum_{r=0}^{\infty} a_r t^r. \end{aligned} \tag{2.17}$$

We consider two cases. If a is not an $(n+1)$-th power $\pmod{p^{\gamma+1}}$ then $\mathrm{ord}_p(\rho) + m/2 < \gamma + 1$ and so

$$\mathrm{ord}_p(a_1) = \mathrm{ord}_p(\rho) + 1 + m/2 < \gamma + 2 = \mathrm{ord}_p(a_2).$$

It follows that $\sigma_\alpha = \mathrm{ord}_p(a_1)$ and that g_α is linear $\pmod p$, where σ_α and g_α are as defined in (2.16). Thus for any $p > 2$ and $m \geq \gamma + 2$, $S_\alpha = 0$. If a is an $(n+1)$-th power $\pmod{p^{\gamma+1}}$ then $\sigma_\alpha = \gamma + 2$ and we may assume (by Lemma 2.1) that $\alpha^{n+1} \equiv a \pmod{p^m}$. If $\gamma \geq m-2$ then we just get $|S_\alpha| = p^{\frac{m}{2}-1}$. If $p \geq 3$ and $\gamma < m - 2$ then

$$S_\alpha = e_{p^m}((n+1)\alpha)p^{\gamma+1-\frac{m}{2}} \sum_{t=1}^{p^{m-\gamma-2}} e_{p^{m-\gamma-2}}(\overline{2\alpha}k\frac{k-1}{p^\gamma}t^2 + ph(t)),$$

for some polynomial $h(t) \in \mathbb{Z}[t]$. It follows from Lemma 2.2 that $|S_\alpha| = p^{\gamma/2}$. The case $p = 3$ can be dealt with in a similar manner using Lemma 2.2 (b).

The case of odd m. Suppose now that $m \geq 3$ is odd, say $m = 2\beta + 1$. Again write $n + 1 = p^\gamma d$ with $p \nmid d$. If $\gamma = 0$ then (1.7) is an immediate consequence of (2.2) . Indeed, if a is not an $(n+1)$-th power $\pmod p$ then by Theorem 3 of [9], $K_n(a, p^m) = 0$, and if a is an $(n+1)$-th power $\pmod p$ then by Theorem 1.2 (ii), $K_n(a, p^m)$ is a sum of $(n+1, p-1)$ complex numbers of modulus $p^{nm/2}$.

Suppose that $\gamma \geq 1$. Set

$$U = \{u : 1 \leq u \leq p^\beta, u^{n+1} \equiv a \pmod{p^{\beta+1}}\}.$$

By (2.3) we have the immediate upper bound

$$|K_n(a,p^m)| \le p^{(nm+1)/2}|U| = p^{(nm-1)/2}(p^\beta(p-1),n+1). \tag{2.18}$$

If $\gamma \ge m-2$ or $\gamma = 1$ then (1.7) follows from (2.18). Moreover, if $\gamma = 1$, then Proposition 2.1 also follows immediately from (2.3).

Suppose now that $2 \le \gamma \le \beta$. If a is not an $(n+1)$-th power $\pmod{p^\gamma}$, then U is empty and $K_n(a,p^m) = 0$. If a is an $(n+1)$-th power $\pmod{p^\gamma}$ then we proceed as above. Let $\alpha_1,\dots,\alpha_{(d,p-1)}$ be distinct $(n+1)$-th roots of a chosen so that each α_i satisfies $\alpha_i^{n+1} \equiv a \pmod{p^m}$. The trick for dealing with the sum in (2.3) is to note that for $u \in U$, the value of $nu + a\overline{u}^n \pmod{p^m}$ depends only on the value of $u \pmod{p^\beta}$. Indeed, if $u^{n+1} \equiv a \pmod{p^\beta}$ then setting $k = n(p^{m-1}(p-1)-1)$ we have

$$\begin{aligned}
n(u+p^\beta) + a(\overline{u+p^\beta})^n &\\
&\equiv n(u+p^\beta) + a(u+p^\beta)^k \pmod{p^m}\\
&\equiv nu + np^\beta + a(u^k + ku^{k-1}p^\beta) \pmod{p^m}, \quad (\text{since } p|(k-1))\\
&\equiv nu + au^k + p^\beta n(1-au^{k-1}) \pmod{p^m}\\
&\equiv nu + au^k + p^\beta n(1-u^{n+k}) \pmod{p^m}\\
&\equiv nu + au^k \pmod{p^m}.
\end{aligned}$$

Set $j = \frac{m+1}{2} - \gamma \ge 1$. For $i = 1,\dots,(d,p-1)$, let

$$U_i = \{\alpha_i + p^j t : t = 1,2,\dots,p^{\gamma-1}\}.$$

Then viewing the sets U, U_i as residue classes $\pmod{p^\beta}$, we see that U is a disjoint union of the sets U_i. Thus by (2.3) we have

$$|K_n(a,p^m)| = p^{(nm+1)/2}\Big|\sum_{i=1}^{(d,p-1)} S_i\Big|, \tag{2.19}$$

where

$$S_i = \sum_{t=1}^{p^{\gamma-1}} e_{p^m}(n(\alpha_i + p^j t) + a(\overline{\alpha_i + p^j t})^n).$$

Let $\alpha = \alpha_i$, $S_\alpha = S_i$. Now,

$$\begin{aligned}
f_\alpha(t) &:= n\alpha + np^j t + a\overline{\alpha}^n(\overline{1+\overline{\alpha}p^j t})^n\\
&\equiv (n+1)\alpha + (n+k)p^j t + \overline{2\alpha}(k-1)kp^{2j}t^2 + \dots.
\end{aligned}$$

This time the multiplicity of p dividing the t^2 coefficient is $2j+\gamma$. Since $m-(2j+\gamma) = \gamma - 1$ it follows as above that $|S_\alpha| = p^{\frac{\gamma-1}{2}}$, and the theorem follows.

Finally, suppose that $\beta + 1 \le \gamma$. If a is not an $(n+1)$-th power $\pmod{p^{\beta+1}}$ then U is empty and $K_n(a,p^m) = 0$. If a is an $(n+1)$-th power $\pmod{p^{\beta+1}}$ then we set

$$U_i = \{\alpha_i + pt : t = 1,2,\dots,p^{\beta-1}\},$$

where the α_i are distinct $(n+1)$-th roots of a, $\pmod p$. Then U (viewed as residue classes $\pmod{p^\beta}$) is the disjoint union of the sets U_i. Let $\alpha = \alpha_i$ and

$$S_\alpha = \sum_{t=1}^{\beta-1} e_{p^m}(f_\alpha(t)),$$

where

$$f_\alpha(t) := (n(\alpha+pt) + a(\overline{\alpha+pt})^n.$$

Write

$$a\overline{\alpha}^n = \alpha + \rho p^{\beta+1},$$

for some integer ρ. If a is not an $(n+1)$-th power $\pmod{p^{\gamma+1}}$ then $\mathrm{ord}_p(\rho)+\beta+1 < \gamma+1$ and so

$$\mathrm{ord}_p(a_1) < \gamma+2 = \mathrm{ord}_p(a_2) < \mathrm{ord}_p(a_i), \quad \text{for } i \geq 3.$$

It follows that $\sigma_\alpha = \mathrm{ord}_p(a_1)$, and that g_α is linear $\pmod p$. If $\sigma_\alpha \geq \gamma-1$ then $|S_\alpha| = p^{\beta-1}$ and $p^{1/2}|S_\alpha| = p^{\frac{m}{2}-1}$. If $\sigma_\alpha < \gamma-1$ then $S_\alpha = 0$. If a is an $(n+1)$-th power $\pmod{p^{\gamma+1}}$ then as above we obtain that $|S_\alpha| = p^{\frac{\gamma}{2}}$.

3. The case $p = 2$

Theorem 1.1 (b) is deduced from the following result of Smith [9], his Theorem 4 and Lemma 5 combined.

Theorem 3.1. *Let m, n be positive integers with $m \geq 2$ and suppose that $2^\gamma \| (n+1)$. Then*

(i) If m is even then

$$K_n(a, 2^m) = 2^{\frac{mn}{2}} \sum_{\substack{u=1 \\ u^{n+1} \equiv a \pmod{2^{m/2}}}}^{2^{m/2}} e_{2^m}(nu + a\overline{u}^n). \tag{3.1}$$

(ii) If m is odd and $\gamma = 0$ then $|K_n(a, 2^m)| = 2^{mn/2}$.

(iii) If m is odd and $\gamma = 1$ then, letting $\beta = (m-1)/2$,

$$|K_n(a, 2^m)| = 2^{\frac{mn+1}{2}} \Big| \sum_{\substack{u=1 \\ 2^\beta \| (u^{n+1}-a)}}^{2^\beta} e_{2^m}(nu + a\overline{u}^n) \Big|. \tag{3.2}$$

(iv) If m is odd and $\gamma \geq 2$ then, letting $\beta = (m-1)/2$,

$$|K_n(a, 2^m)| = 2^{\frac{mn+1}{2}} \Big| \sum_{\substack{u=1 \\ 2^{\beta+1} | (u^{n+1}-a)}}^{2^\beta} e_{2^m}(nu + a\overline{u}^n) \Big|. \tag{3.3}$$

We need also the following lemmas. For any odd integer a and positive integers s, λ let $N_s(a, \lambda)$ denote the number of solutions of the congruence $u^s \equiv a \pmod{2^\lambda}$. The first lemma is elementary; see eg. [8] Corollary 2.44.

Lemma 3.1. *Suppose that a is odd and $\lambda \geq 1$.*

(i) If s is odd then $N_s(a, \lambda) = 1$.

(ii) If s is even then $N_s(a, \lambda) = (2s, 2^{\lambda-1})$ if $a \equiv 1 \pmod{2(2s, 2^{\lambda-1})}$, and equal to zero otherwise.

We deduce easily the following analogue of Lemma 2.1.

Lemma 3.2. *Let a be odd and suppose that $2^\gamma \| (n+1)$. If a is an $(n+1)$-th power $\pmod{2^{\gamma+2}}$ then a is an $(n+1)$-th power modulo any power of 2.*

Lemma 3.3. *Let a be an odd integer and $H(x)$ be any polynomial over $\mathbb{Z}$. Then for any $m \geq 1$ we have*

$$|\sum_{x=1}^{2^m} e_{2^m}(ax^2 + 2^2 H(x))| \leq 2^{\frac{m+1}{2}}, \tag{3.4}$$

and consequently

$$|\sum_{x=1}^{2^m} e_{2^{m+1}}(ax^2 + 2^2 H(x))| \leq 2^{m/2}. \tag{3.5}$$

Proof. We note that if $x \equiv y \pmod{2^m}$ then

$$ax^2 + 2^2 H(x) \equiv ay^2 + 2^2 H(y) \pmod{2^{m+1}},$$

and thus (3.5) is an immediate consequence of (3.4). The critical point congruence for the sum in (3.4) is just $x \equiv 0 \pmod 2$ and thus there is a single critical point, of multiplicity 1. The inequality in (3.4) then follows from (2.4) and (2.5) for $m \geq 4$. For $m = 1$ the inequality is trivial. For $m = 2$ it is well known that $\sum_{x=1}^{4} e_4(ax^2) = 2(1 + i^a)$, while for $m = 3$ we have

$$\sum_{x=1}^{8} e_8(ax^2 + 4H(x)) = 4(-1)^{H(1)} e_8(a).$$

□

Lemma 3.4. *Let a be any integer, b, c, d be odd integers and $H(x)$ be any polynomial over $\mathbb{Z}$. Then for any $m \geq 1$ we have*

$$|\sum_{x=1}^{2^m} e_{2^m}(ax + bx^2 + 2cx^3 + 2dx^4 + 2^2 H(x))| \leq 2^{\frac{m+3}{2}}. \tag{3.6}$$

Consequently, if a is even then

$$|\sum_{x=1}^{2^m} e_{2^{m+1}}(ax + bx^2 + 2cx^3 + 2dx^4 + 2^2 H(x))| \leq 2^{\frac{m+2}{2}}. \tag{3.7}$$

Proof. We note that the inequality in (3.6) is trivial for $m = 1, 2, 3$. If $4 \nmid a$ then there are no critical points associated with the sum and so the sum is zero for $m \geq 4$. If $4|a$ then the critical point congruence for the sum in (3.6) is just $x(x+1) \equiv 0 \pmod 2$, and thus there are two critical points, each of multiplicity one. The result follows from (2.4) and (2.5) for $m \geq 4$. □

We turn now to the proof of Theorem 1.1 when $p = 2$. Suppose first that $\gamma = 0$, that is, $n + 1$ is odd. Then for any λ, the congruence $u^{n+1} \equiv a \pmod{2^\lambda}$ has a unique solution. It follows from parts (i) and (ii) of Theorem 3.1 that $|K_n(a, 2^m)| = 2^{m/2}$. Henceforth we may assume that $\gamma \geq 1$.

The case of even m. Suppose first that m is even. By Lemma 3.1 and Theorem 3.1 (i) we have the immediate upper bound

$$|K_n(a, 2^m)| \leq 2^{\min(\gamma+1, \frac{m}{2}-1)} \cdot 2^{mn/2}. \tag{3.8}$$

The upper bound in (1.8) follows trivially if $\gamma \geq m - 4$. Thus we may assume that $1 \leq \gamma \leq m - 5$ and that $m \geq 6$. We first consider the case that $1 \leq \gamma \leq \frac{m}{2} - 2$. Then by Lemma 3.1, the congruence $u^{n+1} \equiv a \pmod{2^{m/2}}$ has either no solution,

in which case $|K_n(a,2^m)| = 0$, or $2^{\gamma+1}$ solutions. Suppose that the latter holds. Then by Lemma 3.2 a is also an $(n+1)$-th power $\pmod{2^m}$. Let α be a fixed value satisfying $\alpha^{n+1} \equiv a \pmod{2^m}$. Then the set of solutions of the congruence $u^{n+1} \equiv a \pmod{2^{m/2}}$ (regarded as residue classes $\pmod{2^{m/2}}$) may be written

$$\{2^{\frac{m}{2}-\gamma}t \pm \alpha : 1 \le t \le 2^\gamma\}.$$

Since the value of $nu + a\overline{u}^n \pmod{2^m}$ in the sum (3.1) depends only on the value of $u \pmod{2^{m/2}}$ we may write

$$K_n(a,2^m) = 2^{mn/2}(S^+ + S^-), \tag{3.9}$$

where, setting $j = \frac{m}{2} - \gamma$,

$$S^{\pm} = \sum_{t=1}^{2^\gamma} e_{2^m}\left(n(2^j t \pm \alpha) + a\overline{(2^j t \pm \alpha)}^n\right). \tag{3.10}$$

Set $k = (2^{m-1}-1)n$ and $f(t) = n(2^j t+\alpha) + a\overline{(2^j t+\alpha)}^n$. Then, since $2^\gamma \| (k-1)$ and $a\overline{\alpha}^n \equiv \alpha \pmod{2^m}$ we have for any value of t,

$$f(t) \equiv n(2^j t+\alpha) + \alpha(1+2^j\overline{\alpha}t)^k \pmod{2^m} \tag{3.11}$$

$$\equiv (n+1)\alpha + a_2 2^{m-\gamma-1}t^2 + \sum_{r\ge 3} a_r t^r \pmod{2^m}, \tag{3.12}$$

say, where $a_2 = k\frac{k-1}{2^\gamma}\overline{\alpha}$ and the coefficients a_r satisfy

$$\mathrm{ord}_2(a_r) = \mathrm{ord}_2\binom{k}{r} + rj, \quad \text{for } r \ge 3. \tag{3.13}$$

Now $\mathrm{ord}_2(a_3) = \gamma - 1 + 3j \ge 2j + \gamma + 1$ (since $j \ge 2$) and for $r \ge 4$,

$$\mathrm{ord}_2(a_r) \ge \gamma + 1 - \mathrm{ord}_2(r!) + rj > \gamma + 1 - r + rj > 2j + \gamma + 1 = m - \gamma + 1.$$

Therefore we may write

$$f(t) \equiv (n+1)\alpha + a_2 2^{m-\gamma-1}t^2 + 2^{m-\gamma+1}H(t) \pmod{2^m}$$

for some polynomial $H(t)$ with integer coefficients. It follows from Lemma 3.3 that,

$$|S^+| = |\sum_{t=1}^{2^\gamma} e_{2^{\gamma+1}}(a_2 t^2 + 2^2 H(t))| \le 2^{\gamma/2}.$$

The same upper bound holds for S^- and the theorem follows.

Next we consider the case that $\frac{m}{2} - 1 \le \gamma \le m-5$. Then, assuming that a is an $(n+1)$-th power $\pmod{2^{m/2}}$, we may write the set of solutions of the congruence $u^{n+1} \equiv a \pmod{2^{m/2}}$ as

$$\{2t + \alpha : 1 \le t \le 2^{\frac{m}{2}-1}\},$$

where α is a fixed value satisfying $\alpha^{n+1} \equiv a \pmod{2^{m/2}}$.

As with the case of odd p we write

$$a\overline{\alpha}^n = \alpha + \rho 2^{m/2},$$

for some integer ρ. Letting $f(t) = n(2t+\alpha) + a\overline{(2t+\alpha)}^n$, we have by Theorem 3.1 (i) that

$$K_n(a,2^m) = 2^{mn/2}\sum_{t=1}^{\frac{m}{2}-1} e_{2^m}(f(t)).$$

Now, expanding $f(t)$ as above, we see that

$$f(t) \equiv a_0 + a_1 2^{\frac{m}{2}+1} t + a_2 2^{\gamma+1} t^2 + a_3 2^{\gamma+2} t^3 + a_4 2^{\gamma+2} t^4 + 2^{\gamma+3} H(t) \pmod{2^m},$$

for some integers a_r, $0 \le r \le 4$, with a_2, a_3, a_4 odd, and polynomial $H(t)$ over $\mathbb{Z}$. Let δ denote the multiplicity of 2 dividing the coefficient of t. Note, $\delta \ge \frac{m}{2} + 1$. If $\delta < \gamma + 1$ then $K_n(a, 2^m) = 0$. If $\delta \ge \gamma + 1$ then we obtain

$$|K_n(a, 2^m)| = 2^{mn/2} \Big| \sum_{t=1}^{2^{\frac{m}{2}-1}} e_{2^{m-\gamma-1}}(a_1' t + a_2 t^2 + 2a_3 t^3 + 2a_4 t^4 + 4H(t)) \Big|,$$

for some integer a_1'. If $\gamma = \frac{m}{2} - 1$ then a_1' is even and so by inequality (3.7) of Lemma 3.4 we obtain

$$|K_n(a, 2^m)| \le 2 \cdot 2^{\gamma/2} 2^{mn/2}.$$

If $\gamma \ge \frac{m}{2}$ then, by (3.6) we obtain

$$|K_n(a, 2^m)| \le 2^{\frac{mn}{2}} 2^{\gamma - \frac{m}{2}} 2^{\frac{m-\gamma+2}{2}} = 2 \cdot 2^{\frac{\gamma}{2}} 2^{mn/2}.$$

This completes the proof of the theorem for the case of even m.

The case of odd m. Suppose that $m \ge 3$ is odd. If $\gamma = 1$ then we trivially have from Theorem 3.1 (iii) that $|K_n(a, 2^m)| \le 2^{\frac{mn+3}{2}}$, for there are at most two values of u satisfying the constraints on the sum. Indeed, if a is not an $(n+1)$-th power (mod 2^β) then the sum is zero, and if a is such a power then, provided $\beta \ge 3$, there are precisely four distinct $(n+1)$-th roots of $a \pmod{2^\beta}$ of which exactly two are roots $\pmod{2^{\beta+1}}$. If $\beta = 1$ or 2 the assertion is also trivial.

Suppose now that $\gamma \ge 2$. By Theorem 3.1 (iv) we have

$$|K_n(a, 2^m)| = 2^{\frac{mn-1}{2}} \Big| \sum_{\substack{u=1 \\ 2^{\beta+1} | (u^{n+1} - a)}}^{2^\beta} e_{2^m}(nu + a\overline{u}^n) \Big|. \tag{3.14}$$

If $\gamma \ge m - 2$ then by Lemma 3.1,

$$|K_n(a, 2^m)| \le 2^{\beta-1} 2^{\frac{mn+1}{2}} \le 2^{\frac{m}{2}-1} 2^{mn/2} = 2^{\frac{1}{2}\min(\gamma, m-2)} 2^{mn/2}.$$

Suppose now that $2 \le \gamma \le m-3$ and that a is an $(n+1)$-th power $\pmod{2^{\beta+1}}$. If $2 \le \gamma \le \beta - 1$ then by Lemma 3.2, a is also an $(n+1)$-th power $\pmod{2^m}$ and the set of solutions of the congruence $u^{n+1} \equiv a \pmod{2^{\beta+1}}$ is given by

$$\{2^{\beta+1-\gamma} t \pm \alpha : 1 \le t \le 2^\gamma\},$$

where α satisfies $\alpha^{n+1} \equiv a \pmod{2^m}$. By Theorem 3.1 (iv) we can write

$$|K_n(a, 2^m)| = 2^{\frac{mn+1}{2}} |S^+ + S^-|,$$

where $S^\pm$ are as given in (3.10) with $j = \beta + 1 - \gamma$. The proof of the theorem follows as above. If $\gamma \ge \beta$ then the set of solutions is given similarly by

$$\{2t + \alpha : 1 \le t \le 2^{\beta-1}\},$$

where α is a fixed value satisfying $\alpha^{n+1} \equiv a \pmod{2^{\beta+1}}$. The theorem again follows as above.

References

[1] T. Cochrane and Z. Zheng, *Bounds for certain exponential sums*, preprint.
[2] T. Cochrane and Z. Zheng, *Pure and mixed exponential sums*, to appear in Acta Arithmetica.
[3] R. Dabrowski and B. Fisher, *A stationary phase formula for exponential sums over $\mathbb{Z}/p^m\mathbb{Z}$ and applications to $GL(3)$-Kloosterman sums*, Acta Arith. 80 (1997), 1-48.
[4] P. Deligne, *Applications de la formula des traces aux sommes trigonométriques*, in Cohomologie Etale SGA $4\frac{1}{2}$, Lecture Notes in Mathematics, No. 569, Springer Verlag, New York, (1977), 168-232.
[5] P. Ding, *On a conjecture of Chalk*, J. Number Theory 65, no. 2 (1997), 116-129.
[6] W.K.A. Loh, *Hua's Lemma*, Bull. Australian Math. Soc. (3) 50 (1994), 451-458.
[7] L.J. Mordell, *On a special polynomial congruence and exponential sums*, in Calcutta Math. Soc. Golden Jubilee Commemoration Volume, Part I, (1958/59),29-32.
[8] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers, fifth edition*, Wiley, New York, (1991).
[9] R. A. Smith, *On n-dimensional Kloosterman sums*, J. Number Theory 11, (1979), 324-343.
[10] Y. Ye, *Hyper-Kloosterman sums and estimation of exponential sums of polynomials of higher degrees*, Acta Arith. 86, no. 3, (1998), 255-267.

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: cochrane@math.ksu.edu

Department of Mathematics, University of Hong Kong, Pokfulam, Hong Kong
E-mail address: matmcliu@hkucc.hku.hk

Department of Mathematics, Tsinghua University, Beijing 100084, P.R. China
E-mail address: zzheng@math.tsinghua.edu.cn