ACTA ARITHMETICA
XCIII.3 (2000)

Estimation of exponential sums of polynomials of higher degrees II

by

YANGBO YE (Iowa City, IA)

1. Introduction. In Ye [10] the author proved the following bounds for an exponential sum. Let p be an odd prime and let b and c be integers relatively prime to p. Set $q = p^a$, $a \geq 1$, and $k \geq 0$. Define the exponential sum

$$S_k(q,b,c) = \sum_{x \bmod q} \mathrm{e}\left(\frac{bx + cx^k}{q}\right)$$

where $\mathrm{e}(x) = e^{2\pi i x}$. Then for $1 < m < p$ we have [10]

$$|S_{\phi(q)-m}(q,b,c)| \leq \begin{cases} (m+1)p^{1/2}+1 & \text{if } m>1,\ m \mid (p-1), \text{ and } a=1,\\ (m+1)q^{1/2} & \text{if } 1<m<p-1 \text{ and } a\geq 2,\\ p^{1/2}q^{1/2} & \text{if } m=p-1 \text{ and } a\geq 5,\\ pq^{1/2} & \text{if } m=p-1 \text{ and } a=4,\\ p^{1/2}q^{1/2} & \text{if } m=p-1 \text{ and } a=3,\\ q^{1/2} & \text{if } m=p-1 \text{ and } a=2. \end{cases}$$

In this article we will prove certain identities between the above exponential sum and hyper-Kloosterman sums, generalize the above estimation for the exponential sum to other cases of m when $a \geq 2$, and establish new bounds for hyper-Kloosterman sums. Write $p^h \parallel n$ if $p^h \mid n$ but $p^{h+1} \nmid n$.

THEOREM 1. *Let p be a prime, $q = p^a$, $a \geq 2$, and k an integer with $a \leq k < \phi(q)$ and $p \nmid k$. We set h by $p^h \parallel (k-1)$. Then for any b and c relatively prime to p we have*

$$|S_k(q,b,c)| \leq \begin{cases} (\phi(q)-k+1)q^{1/2} & \text{if } p\nmid (k-1),\\ (\phi(q)-k+1)p^{-h/2}q^{1/2} & \text{if } h\geq 1 \text{ and } a\geq 3h+2,\\ (k-1,p-1)p^{\min(h,a/2-1)}q^{1/2} & \text{if } h\geq 1 \text{ and } 2\mid a,\\ (k-1,p-1)p^{\min(h+1/2,a/2-1)}q^{1/2} & \text{if } h\geq 1 \text{ and } 2\nmid a, \end{cases}$$

2000 *Mathematics Subject Classification*: Primary 11L07, 11L05.

Supported in part by NSF Grant #DMS 97-01225.

when $p > 2$, *and*

$$|S_k(q,b,c)| \le \begin{cases} (\phi(q)-k+1)p^{1-h/2}q^{1/2} & \text{if } h \ge 1 \text{ and } a \ge 3h+5,\\ p^{\min(h+1,a/2-1)}q^{1/2} & \text{if } h \ge 1 \text{ and } 2\mid a,\\ p^{\min(h+3/2,a/2-1)}q^{1/2} & \text{if } h \ge 1 \text{ and } 2\nmid a,\end{cases}$$

when $p = 2$.

When $a \ge 3h+2$ with $p > 2$ and when $a \ge 3h+5$ with $p = 2$, two bounds are given in Theorem 1; the smaller bound applies. Loxton and Smith [5] proved that

$$|S_k(q,b,c)| \le q^{1/2}d_{k-1}(q)(\Delta,q)^{1/2}$$

when b and c are relatively prime to p, where $d_{k-1}(q)$ is the number of representations of q as a product of $k-1$ positive integers and Δ is the discriminant of the derivative of the polynomial $bx+cx^k$. After an improvement by Loxton and Vaughan [6], Dąbrowski and Fisher established in [1] better bounds for exponential sums of this kind. Under the restriction of $p\nmid k$, which is the case we will deal with in this paper, their Theorem 1.8 implies the following estimates (see Section 4 for details).

THEOREM 2. *Let p be a prime, $a \ge 2$, $q = p^a$, $k \ge 2$, $p\nmid k$, and $p^h \parallel (k-1)$. Then for any integers b and c relatively prime to p we have*

$$|S_k(q,b,c)| \le \begin{cases} (k-1)q^{1/2} & \text{if } p\nmid(k-1) \text{ and } a \ge 2,\\ (k-1)p^{-h/2}q^{1/2} & \text{if } h \ge 1 \text{ and } a \ge 3h+2,\\ (k-1,p-1)p^{\min(h,a/2-1)}q^{1/2} & \text{if } h \ge 1 \text{ and } 2\mid a,\\ (k-1,p-1)p^{\min(h+1/2,a/2-1)}q^{1/2} & \text{if } h \ge 1 \text{ and } 2\nmid a,\end{cases}$$

when $p > 2$, *and*

$$|S_k(q,b,c)| \le \begin{cases} (k-1)p^{1-h/2}q^{1/2} & \text{if } h \ge 1 \text{ and } a \ge 3h+5,\\ p^{\min(h+1,a/2-1)}q^{1/2} & \text{if } h \ge 1 \text{ and } 2\mid a,\\ p^{\min(h+1/2,a/2-1)}q^{1/2} & \text{if } h \ge 1 \text{ and } 2\nmid a,\end{cases}$$

when $p = 2$.

We note that the last two cases here for $p > 2$ and for $p = 2$ are the same as in Theorem 1. In other cases Theorem 1 is effective for large k while Theorem 2 gives better bounds for small k. In particular when $p > 2$ and $p\nmid k(k-1)$, we can combine these two theorems and get

$$|S_k(q,b,c)| \le \min(k-1,\phi(q)-k+1)q^{1/2}.$$

This estimate becomes worse than trivial when $q^{1/2} \le k \le \phi(q)-q^{1/2}$. What kind of non-trivial bounds one can get for k in this middle range is indeed an interesting question. See Vaughan [8] for a history of estimation of this exponential sum. The question of estimating this exponential sum for large k was posed by Loxton and Vaughan [6].

As in [10] our proof of Theorem 1 is based on certain identities between the above exponential sum and hyper-Kloosterman sums (Theorem 3). These identities are in turn deduced from generalized Davenport–Hasse identities of Gauss sums (Theorem 5). Using the new bounds for hyper-Kloosterman sums for prime power moduli obtained by Dąbrowski and Fisher [1] (see (19), (20), and an improved version in (1) and (2)), we then prove Theorem 1.

We denote a hyper-Kloosterman sum by

$$K(q,m+1,z)=\sum_{\substack{x_1,\ldots,x_m \bmod q\\(x_1,p)=\ldots=(x_m,p)=1}}\mathrm{e}\Big(\frac{x_1+\ldots+x_m+z\overline{x}_1\ldots\overline{x}_m}{q}\Big)$$

for $q=p^a$, $m\ge 1$, and $p\nmid z$. Define an exponential sum by

$$I(q,m,z)=\sum_{\substack{x \bmod q\\(x,p)=1}}\mathrm{e}\Big(\frac{mx+z\overline{x}^m}{q}\Big).$$

The identities for hyper-Kloosterman sums are given in the following theorem. Set $\varepsilon_p=1$ if $p\equiv 1 \pmod 4$, and $\varepsilon_p=i$ if $p\equiv 3 \pmod 4$.

Theorem 3. *Let p be a prime, $m\ge 1$, $p\nmid m$, $a\ge 2$, and $q=p^a$. Then for any integer z with $p\nmid z$ we have*

$$K(q,m+1,z)=\begin{cases} q^{(m-1)/2}I(q,m,z) & \text{if } 2\mid a,\\ q^{(m-1)/2}\varepsilon_p^{m-1}\Big(\dfrac{2^{m-1}z^{m-1}m}{p}\Big)I(q,m,z) & \text{if } 2\nmid a,\end{cases}$$

when $p>2$, and

$$K(q,m+1,z)=q^{(m-1)/2}\Big(\frac{2}{m}\Big)^a I(q,m,z)$$

when $p=2$.

For the case of even a these identities were proved by Smith [7]. When $a=1$ a similar identity is indeed the Diophantine manifestation of a geometric isomorphism of sheaves in Katz [4], Theorem 9.2.3. In Section 3 we will thus only consider the case of odd $a\ge 3$.

To see another application of our identities, we note that for any positive integer n,

$$\begin{aligned}I(q,m+n\phi(q),z)&=\sum_{\substack{x \bmod q\\(x,p)=1}}\mathrm{e}\Big(\frac{(m+n\phi(q))x+z\overline{x}^{m+n\phi(q)}}{q}\Big)\\&=\sum_{\substack{y \bmod q\\(y,p)=1}}\mathrm{e}\Big(\frac{my+z(m+n\phi(q))^m\overline{m}^m\overline{y}^m}{q}\Big)\end{aligned}$$

where we set $y \equiv (m+n\phi(q))\overline{m}x \pmod q$, which is still relatively prime to p because $p\nmid m$, $a \ge 2$, and $p \mid \phi(q)$. Since $(m+n\phi(q))^m\overline{m}^m \equiv 1-np^{a-1} \pmod q$, we have

$$I(q, m+n\phi(q), z) = I(q, m, z(1-np^{a-1})).$$

Applying this identity to the exponential sums on the right side in Theorem 3, we can easily deduce the following identity for hyper-Kloosterman sums.

COROLLARY. *Let p be any prime, m and n any positive integer, $p\nmid m$, $a \ge 2$, and $q = p^a$. Then for any integer z relatively prime to p we have*

$$K(q, m+n\phi(q)+1, z) = \begin{cases} q^{n\phi(q)/2}K(q, m+1, z(1-np^{a-1})) \\ \qquad\qquad \textit{if } 2\mid a \textit{ or if } p=2,\ a\ge 5, \textit{ and } 2\nmid a, \\ q^{n\phi(q)/2}\varepsilon_p^{n\phi(q)}K(q, m+1, z(1-np^{a-1})) \\ \qquad\qquad \textit{if } p>2 \textit{ and } 2\nmid a. \end{cases}$$

This Corollary simplifies hyper-Kloosterman sums of prime power moduli with larger m, $p\nmid m$, to hyper-Kloosterman sums with m between 1 and $\phi(q)-1$. Consequently, the bounds for hyper-Kloosterman sums of prime power moduli proved by Dąbrowski and Fisher [1] (see (19) and (20) in Section 4) can be rewritten and improved for large m when $p\nmid m$. These improved bounds may also be proved directly following their Theorem 1.8 and Example 1.17:

$$(1)\quad |K(q, m+1, z)| \le \begin{cases} (r+1)q^{m/2} & \text{if } p\nmid(r+1), \\ (r+1)p^{-h/2}q^{m/2} & \text{if } h\ge 1 \text{ and } a\ge 3h+2, \\ (r+1, p-1)p^{\min(h, a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\mid a, \\ (r+1, p-1)p^{\min(h+1/2, a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\nmid a, \end{cases}$$

when $p>2$, and

$$(2)\quad |K(q, m+1, z)| \le \begin{cases} (r+1)p^{1-h/2}q^{m/2} & \text{if } h\ge 1 \text{ and } a\ge 3h+5, \\ p^{\min(h+1, a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\mid a, \\ p^{\min(h+3/2, a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\nmid a, \end{cases}$$

when $p=2$, where h is given by $p^h \,\|\, (r+1)$ and $m \equiv r \pmod{\phi(q)}$ with $1 \le r < \phi(q)$ and $p\nmid r$.

Using the Corollary and the identities in Theorem 3 backward, we can further deduce new bounds for hyper-Kloosterman sums from the bounds for the exponential sum $S_k(q, b, c)$. These new bounds are sharper than the improved bounds of Dąbrowski and Fisher in (1) and (2) when $m \equiv r \pmod{\phi(q)}$ with r being less than and close to $\phi(q)-a$. Here in order to have

$$\sum_{\substack{x \bmod q\\ p\mid x}} \mathrm{e}\bigg(\frac{bx+cx^{\phi(q)-r}}{q}\bigg)=0$$

we need to assume that $\phi(q)-r\ge a$.

Theorem 4. *Let p be any prime. Assume that $a\ge 2$ when $p>2$ and $a\ge 4$ when $p=2$. Set $q=p^a$ and let m be any positive integer with $p\nmid m$, $m\equiv r \pmod{\phi(q)}$ and $1\le r\le \phi(q)-a$. Define h by $p^h\,\|\,(r+1)$. Then for any integer z relatively prime to p we have*

$$|K(q,m+1,z)| \le \begin{cases} (\phi(q)-r-1)q^{m/2} & \text{if } p\nmid(r+1),\\ (\phi(q)-r-1)p^{-h/2}q^{m/2} & \text{if } h\ge 1 \text{ and } a\ge 3h+2,\\ (r+1,p-1)p^{\min(h,a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\mid a,\\ (r+1,p-1)p^{\min(h+1/2,a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\nmid a,\end{cases}$$

when $p>2$, and

$$|K(q,m+1,z)| \le \begin{cases} (\phi(q)-r-1)p^{1-h/2}q^{m/2} & \text{if } h\ge 1 \text{ and } a\ge 3h+5,\\ p^{\min(h+1,a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\mid a,\\ p^{\min(h+3/2,a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\nmid a,\end{cases}$$

when $p=2$.

Estimation of hyper-Kloosterman sums for prime moduli was proved by Deligne [2] and Katz [3]. It is interesting to see whether bounds like those in Theorem 4 can be established for hyper-Kloosterman sums modulo p.

2. New Davenport–Hasse identities for Gauss sums. Let p be a prime and $m>1$ an integer with $p\nmid m$. Let χ be any ramified multiplicative character on the p-adic field $\mathbb{Q}_p$ with conductor exponent $a(\chi)=a$. Here χ is ramified if it is non-trivial on $R_p^\times$, the group of invertible elements of the ring of integers R_p in $\mathbb{Q}_p$; for a ramified multiplicative character χ its conductor exponent, denoted by $a(\chi)$, is the smallest positive integer a such that χ is trivial on $1+p^aR_p$. Let ψ be an additive character of $\mathbb{Q}_p$ whose order is zero. Here the order of an additive character ψ, denoted by $n(\psi)$, is the largest integer n such that the character ψ is trivial on $p^{-n}R_p$.

For any additive character ϕ we define the *local ε-factor* as

$$\varepsilon(\chi,\phi;dx)=\begin{cases} \chi(p^{n(\phi)})p^{n(\phi)} & \text{if } \chi \text{ is unramified},\\ \displaystyle\int_{p^{-a(\chi)-n(\phi)}R_p^\times} \chi^{-1}(x)\phi(x)\,dx & \text{if } \chi \text{ is ramified},\end{cases}$$

where dx is a Haar measure on $\mathbb{Q}_p$ normalized by $\mathrm{volume}(R_p)=1$. Then the new Davenport–Hasse identities for Gauss sums have the following form.

THEOREM 5. *Let p be a prime and $m > 1$ an integer with $p \nmid m$. Let ψ be a non-trivial additive character of $\mathbb{Q}_p$ of order zero. Then for any ramified multiplicative character χ with conductor exponent $a(\chi) = a \geq 2$ we have*

$$(\varepsilon(\chi,\psi;dx))^m = \begin{cases} q^{(m-1)/2}\chi^m(m)\varepsilon(\chi^m,\psi;dx) & \text{if } 2 \mid a, \\ q^{m-1-[m/p]}\chi^m(m)\varepsilon(\chi^m,\psi;dx) & \\ \times \prod\limits_{\substack{2\le j\le m\\ p\nmid j(j-1)}} \int\limits_{p^{(a-1)/2}R_p} \chi\Big(1+\frac{j-1}{2j}y_j^2\Big)\,dy_j & \text{if } 2\nmid a, \end{cases}$$

when $p > 2$, and

$$(\varepsilon(\chi,\psi;dx))^m = \begin{cases} q^{(m-1)/2}\chi^m(m)\varepsilon(\chi^m,\psi;dx) & \text{if } 2 \mid a, \\ q^{m-1-[(m-1)/4]}\chi^m(m)\varepsilon(\chi^m,\psi;dx) & \\ \times\Big(\int\limits_{u,v\in p^{(a-1)/2}R_p} \chi(1+u^2+uv+v^2)\,du\,dv\Big)^{[(m+1)/4]} & \text{if } 2\nmid a, \end{cases}$$

when $p = 2$, where $q = p^a$.

Proof. Following the computation in Ye [9] and [10] we have

$$(\varepsilon(\chi,\psi;dx))^m = \int\limits_{(q^{-1}R_p^\times)^m} \chi^{-1}(x_1\ldots x_m)\psi(x_1+\ldots+x_m)\,dx_1\,\ldots\,dx_m.$$

Change variables from x_i to $y_i = x_i/x_1$ for $i = 2,\ldots,m$. Since $p\nmid m$, the conductor exponent of χ^m is still a. Consequently, the integral with respect to x_1 vanishes unless $1+y_2+\ldots+y_m \in R_p^\times$. Setting $z = x_1(1+y_2+\ldots+y_m)$ we get

$$(\varepsilon(\chi,\psi;dx))^m = q^{m-1}\varepsilon(\chi^m,\psi;dx) \times \int\limits_{\substack{y_2,\ldots,y_m\in R_p^\times\\ 1+y_2+\ldots+y_m\in R_p^\times}} \chi\Big(\frac{(1+y_2+\ldots+y_m)^m}{y_2\ldots y_m}\Big)\,dy_2\,\ldots\,dy_m.$$

Denote the integral by I_m. Since $a(\chi) = a \geq 2$, for $m \geq 3$ we set $y_m = y_0(1+u)$ where

$$y_0 \in (R_p^\times - (-(1+y_2+\ldots+y_{m-1})+pR_p))/(1+p^{[(a+1)/2]}R_p)$$

and $u \in p^{[(a+1)/2]}R_p$. The integral with respect to u vanishes unless $1+y_2+\ldots+y_{m-1}-(m-1)y_0 \in p^{[a/2]}R_p$. Therefore the variables in I_m satisfy

$$(3)\qquad 1+y_2+\ldots+y_{m-1}-(m-1)y_m \in p^{[a/2]}R_p.$$

If $p\nmid(m-1)$, then we get the case discussed in [10]. Setting $y_m=(1+y_2+\ldots+y_{m-1})/(m-1)+y$ with $y\in p^{[a/2]}R_p$ we get

$$I_m=I_{m-1}\chi\Big(\frac{m^m}{(m-1)^{m-1}}\Big)\int\limits_{p^{[a/2]}R_p}\chi\Big(1+\frac{(m-1)y^2}{2m}\Big)\,dy \tag{4}$$

when $p>2$, $m\geq 3$, and $p\nmid m(m-1)$. When a is even, we can further compute the integral in (4) to get

$$I_m=q^{-1/2}\chi\Big(\frac{m^m}{(m-1)^{m-1}}\Big)I_{m-1} \tag{5}$$

when $p>2$, $m\geq 3$, $p\nmid m(m-1)$, and $2\,|\,a$.

Now we consider the case of $p\,|\,(m-1)$ and $m\geq 4$. Then from (3) we know that $1+y_2+\ldots+y_{m-1}\in pR_p$; hence $1+y_2+\ldots+y_{m-2}\in R_p^\times$ and $y_{m-1}\in-(1+y_2+\ldots+y_{m-2})+(m-1)y_m+p^{[a/2]}R_p$. Set $y_{m-1}=-(1+y_2+\ldots+y_{m-2})+(m-1)y_m+y$ with $y\in p^{[a/2]}R_p$. Then

$$\begin{aligned}(6)\quad & I_m\\ &=\int\limits_{\substack{y\in p^{[a/2]}R_p\\ y_2,\ldots,y_{m-2},y_m\in R_p^\times\\ 1+y_2+\ldots+y_{m-2}\in R_p^\times}}\chi\Big(-\frac{(my_m+y)^m}{y_2\ldots y_{m-2}y_m(1+y_2+\ldots+y_{m-2}-(m-1)y_m-y)}\Big)\\ &\qquad\qquad\times dy\,dy_2\,\ldots\,dy_{m-2}\,dy_m.\end{aligned}$$

When $2\,|\,a$, the integrand above equals

$$\begin{aligned}&\chi\Big(-\frac{m^m y_m^{m-1}}{y_2\ldots y_{m-2}(1+y_2+\ldots+y_{m-2}-(m-1)y_m)}\Big)\\ &\qquad\times\chi\Big(1+\Big(\frac{1}{y_m}+\frac{1}{1+y_2+\ldots+y_{m-2}-(m-1)y_m}\Big)y\Big).\end{aligned}$$

Consequently, in order to have a non-zero integral with respect to y we must have

$$\frac{1}{y_m}+\frac{1}{1+y_2+\ldots+y_{m-2}-(m-1)y_m}\in p^{a/2}R_p,$$

which is equivalent to $1+y_2+\ldots+y_{m-2}-(m-2)y_m\in p^{a/2}R_p$. Note that $p\nmid(m-2)$; hence we can set $y_m=(1+y_2+\ldots+y_{m-2})/(m-2)+z$ with $z\in p^{a/2}R_p$. Integrating with respect to y and substituting the above expression of y_m into

$$\chi\Big(-\frac{m^m y_m^{m-1}}{y_2\ldots y_{m-2}(1+y_2+\ldots+y_{m-2}-(m-1)y_m)}\Big)$$

we can see that the resulting expression is independent of z:

$$\chi\biggl(\frac{m^m}{(m-2)^{m-2}}\biggr)\chi\biggl(\frac{(1+y_2+\ldots+y_{m-2})^{m-2}}{y_2\ldots y_{m-2}}\biggr).$$

Integrating with respect to z we get

$$I_m = q^{-1}\chi\biggl(\frac{m^m}{(m-2)^{m-2}}\biggr)I_{m-2} \tag{7}$$

when $p>2$, $m\ge 4$, $p\nmid m$, $p\,|\,(m-1)$, $a\ge 2$, and $2\,|\,a$.

Now let us turn to the case of $2\nmid a$. Then the integral in (6) becomes

$$\begin{aligned}(8)\quad & I_m \\ &= \int\limits_{\substack{y\in p^{(a-1)/2}R_p\\ y_2,\ldots,y_{m-2},y_m\in R_p^\times\\ 1+y_2+\ldots+y_{m-2}\in R_p^\times}} \chi\biggl(-\frac{m^m y_m^{m-1}}{y_2\ldots y_{m-2}(1+y_2+\ldots+y_{m-2}-(m-1)y_m)}\biggr)\\ &\quad\times\chi\biggl(1+y\biggl(\frac{1}{y_m}+\frac{1}{1+y_2+\ldots+y_{m-2}-(m-1)y_m}\biggr)\\ &\quad+y^2\biggl(\frac{m-1}{2my_m^2}+\frac{\frac{1}{y_m}+\frac{1}{1+y_2+\ldots+y_{m-2}-(m-1)y_m}}{1+y_2+\ldots+y_{m-2}-(m-1)y_m}\biggr)\biggr)\\ &\qquad\qquad\times dy\,dy_2\,\ldots\,dy_{m-2}\,dy_m.\end{aligned}$$

Since we assume in this case that $p>2$, the term $(m-1)/(2my_m^2)\in pR_p$ and hence can be taken out of the above integrand. Setting $y=z+u$ with $z\in p^{(a-1)/2}R_p/p^{(a+1)/2}R_p$ and $u\in p^{(a+1)/2}R_p$, we have $y^2\in z^2+qR_p$. Integrating with respect to u we get a non-zero result only if

$$\frac{1}{y_m}+\frac{1}{1+y_2+\ldots+y_{m-2}-(m-1)y_m}\in p^{(a-1)/2}R_p.$$

Because of this condition, the integrand in (8) can be simplified to

$$\begin{aligned}&\chi\biggl(-\frac{m^m y_m^{m-1}}{y_2\ldots y_{m-2}(1+y_2+\ldots+y_{m-2}-(m-1)y_m)}\biggr)\\ &\qquad\qquad\times\chi\biggl(1+y\biggl(\frac{1}{y_m}+\frac{1}{1+y_2+\ldots+y_{m-2}-(m-1)y_m}\biggr)\biggr).\end{aligned}$$

Then the integral with respect to y is non-zero only when

$$\frac{1}{y_m}+\frac{1}{1+y_2+\ldots+y_{m-2}-(m-1)y_m}\in p^{(a+1)/2}R_p,$$

i.e., only when $1+y_2+\ldots+y_{m-2}-(m-2)y_m\in p^{(a+1)/2}R_p$. Integrate with respect to y and set $y_m=(1+y_2+\ldots+y_{m-2})/(m-2)+z$ with $z\in p^{(a+1)/2}R_p$. If we substitute this expression for y_m, we can see the integrand is indeed independent of z. Integrating with respect to z as before we conclude that

$$I_m = q^{-1}\chi\Big(\frac{m^m}{(m-2)^{m-2}}\Big)I_{m-2} \tag{9}$$

when $p>2$, $m\ge 4$, $p\nmid m$, $p\,|\,(m-1)$, $a\ge 2$, and $2\nmid a$.

Using the same approach as above we can also get

$$I_2 = q^{-1/2}\chi(2^2) \tag{10}$$

when $p>2$, $a\ge 2$, and $2\,|\,a$, and

$$I_2 = \chi(2^2)\int\limits_{p^{(a-1)/2}R_p}\chi\Big(1+\frac{y^2}{4}\Big)\,dy \tag{11}$$

when $p>2$, $a\ge 2$, and $2\nmid a$. Putting all these results from (4), (5), (7), (9), (10), and (11) together we get the following expressions for I_m:

$$I_m = q^{(1-m)/2}\chi(m^m)$$

when $p>2$, $m\ge 2$, $p\nmid m$, $a\ge 2$, and $2\,|\,a$, and

$$I_m = q^{-[m/p]}\chi(m^m)\prod_{\substack{2\le j\le m\\ p\nmid j(j-1)}}\ \int\limits_{p^{(a-1)/2}R_p}\chi\Big(1+\frac{(j-1)y_j^2}{2j}\Big)\,dy_j$$

when $p>2$, $m\ge 2$, $p\nmid m$, $a\ge 2$, and $2\nmid a$. Theorem 5 in the case of $p>2$ then follows.

We now consider the case of $p=2$. Following the same approach as above we set

$$I_m = \int\limits_{\substack{y_2,\dots,y_m\in R_p^\times\\ 1+y_2+\dots+y_m\in R_p^\times}}\chi\Big(\frac{(1+y_2+\dots+y_m)^m}{y_2\cdots y_m}\Big)\,dy_2\,\dots\,dy_m$$

so that

$$(\varepsilon(\chi,\psi;dx))^m = q^{m-1}\varepsilon(\chi^m,\psi;dx)I_m.$$

Since $p=2$ and $2\nmid m$, we always have $p\,|\,(m-1)$. For $m\ge 5$ we get the same expression of I_m as in (6) which implies (7) when a is even. When a is odd, we get (8) again. If $4\,|\,(m-1)$, then we still have $(m-1)/(2my_m^2)\in pR_p$ and hence this term can be taken out of the integrand in (8). By the same computation, we get (9). Therefore

$$I_m = q^{-1}\chi\Big(\frac{m^m}{(m-2)^{m-2}}\Big)I_{m-2} \tag{12}$$

when (i) $p=2$, $m\ge 5$, $2\nmid m$, $a\ge 2$, and $2\,|\,a$, or (ii) $p=2$, $m\ge 5$, $2\nmid m$, $4\,|\,(m-1)$, $a\ge 3$, and $2\nmid a$.

Now we consider the case of $p=2$, $2\nmid m$, $4\nmid(m-1)$, $a\ge 3$, and $2\nmid a$. Then $(m-1)/(2my_m^2)\in R_p^\times$. Consequently, by setting $y=z+u$ with $z\in p^{(a-1)/2}R_p/p^{(a+1)/2}R_p$ and $u\in p^{(a+1)/2}R_p$, we can only get

$$\frac{1}{y_m}+\frac{1}{1+y_2+\ldots+y_{m-2}-(m-1)y_m}\in p^{(a-1)/2}R_p.$$

Set $y_m=(1+y_2+\ldots+y_{m-2})/(m-2)+z$ with $z\in p^{(a-1)/2}R_p$. Then (8) can be simplified to

$$I_m=\int\limits_{\substack{y,z\in p^{(a-1)/2}R_p\\ y_2,\ldots,y_{m-2}\in R_p^\times\\ 1+y_2+\ldots+y_{m-2}\in R_p^\times}}\chi\biggl(\frac{m^m}{(m-2)^{m-2}}\biggr)\chi\biggl(\frac{(1+y_2+\ldots+y_{m-2})^{m-2}}{y_2\cdots y_{m-2}}\biggr)$$
$$\times\chi\biggl(1+\frac{(m-1)z^2}{2(m-2)}\biggr)\chi\biggl(1-yz+\frac{(m-1)y^2}{2m}\biggr)\,dy\,dz\,dy_2\,\ldots\,dy_{m-2}.$$

Since $(m-1)/2$ is an odd integer we can further simplify the integrals with respect to y and z to get

$$I_m=\chi\biggl(\frac{m^m}{(m-2)^{m-2}}\biggr)I_{m-2}\int\limits_{y,z\in p^{(a-1)/2}R_p}\chi(1+y^2+yz+z^2)\,dy\,dz \tag{13}$$

when $p=2$, $m\ge 5$, $2\nmid m$, $4\nmid(m-1)$, $a\ge 3$, and $2\nmid a$.

We can also compute I_3:

$$I_3=q^{-1}\chi(3^3) \tag{14}$$

if $p=2$, $a\ge 2$, and $2\mid a$, and

$$I_3=\chi(3^3)\int\limits_{u,v\in p^{(a-1)/2}R_p}\chi(1+u^2+uv+v^2)\,du\,dv \tag{15}$$

if $p=2$, $a\ge 2$, and $2\nmid a$. Putting the results in (12)–(15) together we prove Theorem 5 for $p=2$.

3. Identities for hyper-Kloosterman sums. In this section we will prove Theorem 3 when $a\ge 3$ is odd. Denote the hyper-Kloosterman sum over p-adic field by

$$K_p(q,m+1,z)=\sum_{x_1,\ldots,x_m\in R_p^\times/(1+qR_p)}\psi\biggl(\frac{1}{q}\biggl(x_1+\ldots+x_m+\frac{z}{x_1\ldots x_m}\biggr)\biggr).$$

Applying the Mellin transform to the p-adic hyper-Kloosterman sum as in [10], we get

$$\int\limits_{R_p^\times}\chi^{-1}(z)K_p(q,m+1,z)\,dz=q^{-1}\chi^{-(m+1)}(q)(\varepsilon(\chi,\psi;dx))^{m+1}$$

when $a(\chi) = a \geq 2$ and $q = p^a$. By Theorem 5 when p is odd and $p \nmid m$ the above becomes

$$q^{m-2-[m/p]}\chi^{-(m+1)}(q)\chi^m(m)\varepsilon(\chi,\psi;dx)\varepsilon(\chi^m,\psi;dx) \times \prod_{\substack{2\leq j\leq m \\ p\nmid j(j-1)}} \int_{p^{(a-1)/2}R_p} \chi\left(1+\frac{j-1}{2j}y_j^2\right) dy_j$$

if a is odd. By the same computation as in [10] we can prove that

$$(16)\quad \int_{R_p^\times} \chi^{-1}(z)K_p(q,m+1,z)\,dz = q^{(m-1)/2}\varepsilon_p^{m-1-2[m/p]} \int_{R_p^\times} \chi^{-1}(z)\,dz \times \sum_{x\in R_p^\times/(1+qR_p)} \psi\left(\frac{1}{q}\left(mx+\frac{z}{x^m}\right)\right) \prod_{\substack{2\leq j\leq m \\ p\nmid j(j-1)}} \left(\frac{2j(j-1)x^m z}{p}\right)$$

when $p > 2$, $p\nmid m$, $2\nmid a$ for any multiplicative character χ. Since the number of factors in the product in (16) is $m-1-2[m/p]$, the product equals

$$\left(\frac{x^m}{p}\right)^{m-1-2[m/p]}\left(\frac{z}{p}\right)^{m-1-2[m/p]} \prod_{\substack{2\leq j\leq m \\ p\nmid j(j-1)}} \left(\frac{j(j-1)}{p}\right) = \left(\frac{x}{p}\right)^{m(m-1)}\left(\frac{2z}{p}\right)^{m-1}\left(\frac{m}{p}\right) \prod_{1\leq k<m/p}\left(\frac{(kp+1)(kp-1)}{p}\right) = \left(\frac{2z}{p}\right)^{m-1}\left(\frac{m}{p}\right)\left(\frac{-1}{p}\right)^{[m/p]}.$$

Consequently, we proved the following identity over the p-adic field:

$$K_p(q,m+1,z) = q^{(m-1)/2}\varepsilon_p^{m-1}\left(\frac{2^{m-1}z^{m-1}m}{p}\right) \times \sum_{x\in R_p^\times/(1+qR_p)} \psi\left(\frac{1}{q}\left(mx+\frac{z}{x^m}\right)\right)$$

when $p > 2$, $p\nmid m$, $2\nmid a$, and $p\nmid z$. This identity is equivalent to Theorem 3 in the case of odd p which is a generalization of a result proved in [10].

Now we turn to the case of $p = 2$ with $2\nmid m$. When $a \geq 3$ is odd, we deduce from Theorem 5 that

$$\int_{R_p^\times} \chi^{-1}(z) K_p(q, m+1, z)\, dz \tag{17}$$
$$= q^{m-2-[(m-1)/4]} \chi^{-(m+1)}(q) \chi^m(m) \varepsilon(\chi, \psi; dx) \varepsilon(\chi^m, \psi; dx)$$
$$\times \Big(\int_{u,v \in p^{(a-1)/2} R_p} \chi(1 + u^2 + uv + v^2)\, du\, dv \Big)^{[(m+1)/4]}.$$

We have

$$q^{-2} \chi^{-(m+1)}(q) \varepsilon(\chi, \psi; dx) \varepsilon(\chi^m, \psi; dx)$$
$$= q^{-2} \chi^{-(m+1)}(q) \int_{(q^{-1} R_p^\times)^2} \chi^{-1}(x_1 x_2^m) \psi(x_1 + x_2)\, dx_1\, dx_2$$
$$= \int_{(R_p^\times)^2} \chi^{-1}(x) \psi\Big(\frac{1}{q}\Big(y + \frac{x}{y^m}\Big)\Big)\, dx\, dy.$$

Rewriting the power in (17) as

$$\prod_{1 \le j \le [(m+1)/4]} \int_{u_j, v_j \in p^{(a-1)/2} R_p} \chi(1 + u_j^2 + u_j v_j + v_j^2)\, du_j\, dv_j$$

we then change variables from x to z via

$$x = z m^m \prod_{1 \le j \le [(m+1)/4]} (1 + u_j^2 + u_j v_j + v_j^2).$$

Then the expression on the right side of (17) becomes

$$q^{m-[(m-1)/4]} \int_{(R_p^\times)^2} \chi^{-1}(z)\, dz\, dy$$
$$\times \int_{\substack{u_j, v_j \in p^{(a-1)/2} R_p \\ 1 \le j \le [(m+1)/4]}} \psi\Big(\frac{1}{q}\Big(y + \frac{z m^m}{y^m} \prod_{1 \le j \le [(m+1)/4]} (1 + u_j^2 + u_j v_j + v_j^2)\Big)\Big)$$
$$\times dz\, dy\, du_1\, dv_1\, \ldots\, du_{[(m+1)/4]}\, dv_{[(m+1)/4]}.$$

Changing variables again and multiplying out the product we get

$$q^{m-1-[(m-1)/4]} \int_{R_p^\times} \chi^{-1}(z)\, dz \sum_{y \in R_p^\times/(1+qR_p)} \psi\Big(\frac{1}{q}\Big(my + \frac{z}{y^m}\Big)\Big)$$
$$\times \Big(\int_{u,v \in p^{(a-1)/2} R_p} \psi\Big(\frac{z}{q y^m}(u^2 + uv + v^2)\Big)\, du\, dv \Big)^{[(m+1)/4]}.$$

In order to compute the integral with respect to u and v we write it as a finite sum

$$\int_{u,v\in p^{(a-1)/2}R_p} \psi\Big(\frac{z}{qy^m}(u^2+uv+v^2)\Big)\,du\,dv$$
$$= p^{-a-1}\sum_{u,v\in p^{(a-1)/2}R_p/p^{(a+1)/2}R_p} \psi\Big(\frac{z}{qy^m}(u^2+uv+v^2)\Big)$$
$$= p^{-a-1}\sum_{u,v\in R_p/pR_p} \psi\Big(\frac{z}{py^m}(u^2+uv+v^2)\Big).$$

Since $p=2$, we can take $u,v=0,1$ and get

$$p^{-a-1}\Big(1+2\psi\Big(\frac{z}{py^m}\Big)+\psi\Big(\frac{3z}{py^m}\Big)\Big).$$

Since the order of ψ is zero and $p^{-1}R_p^\times/R_p$ has only one element, we have

$$\psi\Big(\frac{z}{py^m}\Big)=\psi\Big(\frac{3z}{py^m}\Big)=-1$$

and hence

$$\int_{u,v\in p^{(a-1)/2}R_p} \psi\Big(\frac{z}{qy^m}(u^2+uv+v^2)\Big)\,du\,dv=-q^{-1}.$$

Consequently,

$$\int_{R_p^\times} \chi^{-1}(z)K_p(q,m+1,z)\,dz$$
$$= q^{(m-1)/2}\Big(\frac{2}{m}\Big)\int_{R_p^\times}\chi^{-1}(z)\,dz\sum_{y\in R_p^\times/(1+qR_p)}\psi\Big(\frac{1}{q}\Big(my+\frac{z}{y^m}\Big)\Big)$$

for any ramified character χ with conductor exponent $a(\chi)=a$, where we used the facts that

$$[(m-1)/4]+[(m+1)/4]=(m-1)/2 \quad\text{and}\quad (-1)^{[(m+1)/4]}=\Big(\frac{2}{m}\Big).$$

Since $a>1$ this identity also holds for other multiplicative character χ. Therefore we proved the following identity which is equivalent to Theorem 3 in the case of $p=2$, $p\nmid m$, $a\ge 3$, and $2\nmid a$:

$$K_p(q,m+1,z)=q^{(m-1)/2}\Big(\frac{2}{m}\Big)\sum_{y\in R_p^\times/(1+qR_p)}\psi\Big(\frac{1}{q}\Big(my+\frac{z}{y^m}\Big)\Big) \tag{18}$$

for any $z\in R_p^\times$.

4. Estimation of exponential sums. We first prove Theorem 2 using Theorem 1.8 of Dąbrowski and Fisher [1]. Let $f(x)=bx+cx^k$ be a polynomial with b, c, and k relatively prime to p. For $a\ge 2$ we set $q=p^a$ and $j=[a/2]$. Define the scheme D of critical points of f as zeros of $f'(x)=b+ckx^{k-1}$. Then a point x in D is *étale* if $p\nmid(k-1)$, x is *h-étale* if $p^h\,\|\,(k-1)$, and x is *strictly h-étale* if $p^{h+1}\,\|\,(k-1)$. Theorem 1.8(a) of Dąbrowski and Fisher [1] says that

$$|S_k(q,b,c)|\le\begin{cases}|D(\mathbb{Z}/p^j\mathbb{Z})|q^{1/2} & \text{if } 2\mid a \text{ or if } 2\nmid a \text{ and } p\nmid(k-1),\\ |D(\mathbb{Z}/p^j\mathbb{Z})|p^{1/2}q^{1/2} & \text{if } 2\nmid a \text{ and } p\mid(k-1).\end{cases}$$

Theorem 1.8(b) on the other hand implies that

$$|S_k(q,b,c)|\le|D(\mathbb{Z}_p)|p^{h/2}q^{1/2}$$

if $a\ge 3h+2$ when $p>2$ or $a\ge 3h+5$ when $p=2$, where $h\ge1$ is given by $p^h\,\|\,(k-1)$. Following Example 1.17 of [1] we have

$$|D(\mathbb{Z}/p^j\mathbb{Z})|\le\begin{cases}k-1 & \text{if } p\nmid(k-1),\\ p^{\min(h+1,j-1)} & \text{if } p=2 \text{ and } h\ge1,\\ (k-1,p-1)p^{\min(h,j-1)} & \text{if } p>2 \text{ and } h\ge 1,\end{cases}$$

and

$$|D(\mathbb{Z}_p)|\le\begin{cases}(k-1)p^{-h} & \text{if } p>2,\\ (k-1)p^{1-h} & \text{if } p=2.\end{cases}$$

Substituting these results into the above inequalities for the exponential sum, we get the estimates in Theorem 2.

By similar computation the bounds for the hyper-Kloosterman sum $K(q,m+1,z)$ considered in Example 1.17 of Dąbrowski and Fisher [1] can be written in the following way. Here h is given by $p^h\,\|\,(m+1)$.

$$\text{(19)}\qquad |K(q,m+1,z)|\le\begin{cases}(m+1)q^{m/2} & \text{if } p\nmid(m+1),\\ (m+1)p^{-h/2}q^{m/2} & \text{if } h\ge1 \text{ and } a\ge 3h+2,\\ (m+1,p-1)p^{\min(h,a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\mid a,\\ (m+1,p-1)p^{\min(h+1/2,a/2-1)}q^{m/2} & \text{if } h\ge1 \text{ and } 2\nmid a,\end{cases}$$

when $p>2$, and

$$\text{(20)}\qquad |K(q,m+1,z)|\le\begin{cases}(m+1)p^{1-h/2}q^{m/2} & \text{if } h\ge1 \text{ and } a\ge 3h+5,\\ p^{\min(h+1,a/2-1)}q^{m/2} & \text{if } h\ge 1 \text{ and } 2\mid a,\\ p^{\min(h+3/2,a/2-1)}q^{m/2} & \text{if } h\ge1 \text{ and } 2\nmid a,\end{cases}$$

when $p=2$. As before here we assume that $p\nmid m$. By the identities of hyper-Kloosterman sums in Theorem 3, we get the same bounds as in Theorem 1 but for the exponential sum

$$\sum_{\substack{x \bmod q \\ (x,p)=1}} \mathrm{e}\left(\frac{mx + z\overline{x}^m}{q}\right)$$

if we set $k = \phi(q) - m$. For m in the range of $1 \le m \le \phi(q) - a$, however

$$\sum_{\substack{x \bmod q \\ p \mid x}} \mathrm{e}\left(\frac{mx + zx^{\phi(q)-m}}{q}\right) = 0.$$

This completes the proof of Theorem 1.

Acknowledgements. The author would like to thank the referee for helpful suggestions.

References

[1] R. Dąbrowski 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.

[2] P. Deligne, *Applications de la formule des traces aux sommes trigonométriques*, in: Cohomologie Etale (SGA 4 1/2), Lecture Notes in Math. 569, Springer, Berlin, 1977, 168–232.

[3] N. M. Katz, *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, Ann. of Math. Stud. 116, Princeton Univ. Press, Princeton, 1988.

[4] —, *Exponential Sums and Differential Equations*, Ann. of Math. Stud. 124, Princeton Univ. Press, Princeton, 1990.

[5] J. H. Loxton and R. A. Smith, *On Hua's estimate for exponential sums*, J. London Math. Soc. 26 (1982), 15–20.

[6] J. H. Loxton and R. C. Vaughan, *The estimation of complete exponential sums*, Canad. Math. Bull. 28 (1985), 440–454.

[7] R. A. Smith, *On n-dimensional Kloosterman sums*, J. Number Theory 11 (1979), 324–343.

[8] R. C. Vaughan, *The Hardy–Littlewood Method*, 2nd ed., Cambridge Tracts in Math. 125, Cambridge Univ. Press, Cambridge, 1997.

[9] Y. Ye, *The lifting of an exponential sum to a cyclic algebraic number field of a prime degree*, Trans. Amer. Math. Soc. 350 (1998), 5003–5015.

[10] —, *Hyper-Kloosterman sums and estimation of exponential sums of polynomials of higher degrees*, Acta Arith. 86 (1998), 255–267.

Department of Mathematics
The University of Iowa
Iowa City, IA 52242-1419
U.S.A.
E-mail: yey@math.uiowa.edu

Received on 2.6.1998
and in revised form on 9.11.1999 (3393)