ACTA ARITHMETICA
101.2 (2002)

Exponential sums modulo prime powers

by

TODD COCHRANE (Manhattan, KS)

1. Introduction. In this paper we develop a method for evaluating and estimating a very general mixed exponential sum of the type

$$S(\chi,g,f,p^m)=\sum_{x=1}^{p^m}\chi(g(x))e_{p^m}(f(x)), \tag{1.1}$$

where p^m is a prime power with $m\ge 2$, χ is a multiplicative character (mod p^m), $e_{p^m}(\cdot)$ is the additive character, $e_{p^m}(x)=e^{2\pi ix/p^m}$, and f,g are rational functions with integer coefficients. It is understood that the sum is only over values of x for which g and f are both defined as functions on $\mathbb{Z}/(p^m)$, and g is nonzero (mod p). The sum is trivial if f and g are both constants, so we shall always assume that either f or g is nonconstant.

The case $m=1$, a classical sum over a finite field, has been thoroughly studied. In this case it follows from the rationality of the L-function associated with the sum and the accompanying Riemann Hypothesis that under very general conditions $S(\chi,g,f,p)$ can be expressed as a sum of a certain number of complex numbers of modulus $\sqrt{p}$. If f and g are polynomials of degrees d_1, d_2 then this number is exactly d_1+d_2-1, provided that $p\nmid d_1$ and $(\operatorname{ord}(\chi),d_2)=1$, and so we obtain the upper bound

$$|S(\chi,g,f,p)|\le(d_1+d_2-1)\sqrt{p}. \tag{1.2}$$

For the case of polynomials we refer the reader to the works of Schmidt [29] and Stepanov [30] for elementary proofs of this result. For rational functions see Bombieri [1] and Perelmuter [26].

For values of $m\ge 2$, much attention has been given to the study of pure exponential sums $S(f,p^m)$ $(g=1)$, but little has been said about the general sum. Ismoilov [9]–[16] and Liu [18]–[20] obtained estimates for pure character sums $(f=0)$. In our work with Zheng, [3], [4] we dealt with the case of mixed exponential sums with $g(x)=x$. In this paper we obtain formulae

2000 *Mathematics Subject Classification*: 11L07, 11L03.
Key words and phrases: exponential sums.

and estimates for a general sum of the type (1.1). In order to succeed with the evaluation of a general sum we were forced to greatly simplify the proofs of our earlier work. The main new idea of this paper that allows such a generalization (Lemma 2.2) is the use of the p-adic logarithm to describe the behavior of χ on the subgroup of residues (mod p^m) congruent to 1 (mod p).

We restrict our attention to odd p in this section and take up the case $p = 2$ in Sections 6 and 7. Let a denote a fixed primitive root (mod p^2) and r the value defined by

$$a^{p-1} = 1 + rp. \tag{1.3}$$

In particular, $p \nmid r$ and a is a primitive root (mod p^m) for any exponent m. Let R be the p-adic integer

$$R := p^{-1}\log(1+rp) = p^{-1}\sum_{i=1}^{\infty}\frac{(-1)^{i+1}(rp)^i}{i} \equiv r \ (\operatorname{mod} p). \tag{1.4}$$

For any multiplicative character χ (mod p^m) let $c = c(\chi, a)$ be the unique integer with $0 < c \le p^{m-1}(p-1)$ and

$$\chi(a^k) = e^{2\pi i ck/(p^{m-1}(p-1))}, \tag{1.5}$$

for every integer k.

Let $\operatorname{ord}_p(x)$ denote the normal exponent valuation on the p-adic field $\mathbb{Q}_p$, extended to the field of rational functions over $\mathbb{Q}_p$. Thus for a polynomial f over $\mathbb{Z}$, $\operatorname{ord}_p(f)$ is the largest power of p dividing all of the coefficients of f, and for rational functions f_1/f_2, $\operatorname{ord}_p(f_1/f_2) = \operatorname{ord}_p(f_1) - \operatorname{ord}_p(f_2)$. Also, for any polynomial f we let $d_p(f)$ denote the degree of f read (mod p).

Put

$$t = t_p(\chi, g, f) := \operatorname{ord}_p(Rgf' + cg'). \tag{1.6}$$

We may assume that $\operatorname{ord}_p(g) = 0$ for otherwise the sum in (1.1) is empty. In Lemma 2.1 we show that

$$t = \min\{\operatorname{ord}_p(f'), \operatorname{ord}_p(cg')\}, \tag{1.7}$$

a fact that plays an important role in our proof. We define the set of critical points $\mathcal{A} \subset \mathbb{F}_p$ associated with the sum $S(\chi, g, f, p^m)$ to be the set of solutions of the

Critical Point Congruence:

$$\mathcal{C}(x) := p^{-t}(Rg(x)f'(x) + cg'(x)) \equiv 0 \ (\operatorname{mod} p), \tag{1.8}$$

for which the summand in $S(\chi, g, f, p^m)$ is defined. Thus,

$$\mathcal{A} := \{\alpha \in \mathbb{F}_p : \mathcal{C}(\alpha) \equiv 0 \ (\operatorname{mod} p) \text{ and } g(\alpha) \not\equiv 0 \ (\operatorname{mod} p)\}.$$

One may check that this congruence does not depend on the choice of the primitive root.

Write $S(\chi,g,f,p^m)=\sum_{\alpha=1}^{p} S_\alpha$ with

$$S_\alpha = S_\alpha(\chi,g,f,p^m) := \sum_{\substack{x=1\\ x\equiv\alpha \,(\mathrm{mod}\, p)}}^{p^m} \chi(g(x))e_{p^m}(f(x)). \tag{1.9}$$

THEOREM 1.1. *Let f,g be rational functions over $\mathbb{Z}$, not both constant, p be an odd prime, χ a multiplicative character* (*mod* p^m) *and m an integer with $m\ge t+2$.*

(i) *If $\alpha\notin\mathcal{A}$, then $S_\alpha(\chi,g,f,p^m)=0$.*

(ii) *If α is a critical point of multiplicity one then*

$$S_\alpha(\chi,g,f,p^m) = \begin{cases} \chi(g(\alpha^*))e_{p^m}(f(\alpha^*))p^{(m+t)/2} & \text{if } m-t \text{ is even},\\ \chi(g(\alpha^*))e_{p^m}(f(\alpha^*))\left(\dfrac{A_\alpha}{p}\right)\mathcal{G}_p p^{(m+t-1)/2} & \text{if } m-t \text{ is odd}, \end{cases}$$

where α^* is the unique lifting of α to a solution of the congruence

$$\mathcal{C}(x)\equiv 0 \pmod{p^{[(m-t+1)/2]}} \quad \text{and} \quad A_\alpha \equiv 2r(\mathcal{C}/g)'(\alpha) \pmod{p}.$$

Here $\mathcal{G}_p$ is the quadratic Gauss sum,

$$\mathcal{G}_p := \sum_{x=0}^{p-1} e_p(x^2) = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e_p(x) = \begin{cases} \sqrt{p} & \text{if } p\equiv 1 \pmod 4,\\ i\sqrt{p} & \text{if } p\equiv 3 \pmod 4,\end{cases} \tag{1.10}$$

and $\left(\frac{A_\alpha}{p}\right)$ is the Legendre symbol. Thus, if all of the critical points are of multiplicity one then we obtain the formula

$$S(\chi,g,f,p^m) = \begin{cases} \sum_{\alpha\in\mathcal{A}} \chi(g(\alpha^*))e_{p^m}(f(\alpha^*))p^{(m+t)/2}, & m-t \text{ even},\\ \sum_{\alpha\in\mathcal{A}} \chi(g(\alpha^*))e_{p^m}(f(\alpha^*))\left(\dfrac{A_\alpha}{p}\right)\mathcal{G}_p p^{(m+t-1)/2}, & m-t \text{ odd}. \end{cases} \tag{1.11}$$

This generalizes the formulae we obtained in [3] and [4] for the cases of pure exponential sums and mixed sums with $g(x)=x$. The formula of Salié [28] for the Kloosterman sum, and of Mauclaire [23], [24] and Odoni [25] for the Gauss sum $\sum_{x=1}^{p^m}\chi(x)e_{p^m}(x)$ are variations of (1.11), as are the stationary phase formulae of Katz [17, p. 110] and Dąbrowski and Fisher [6, Theorem 1.8] for the case of pure exponential sums having only critical points of multiplicity 1.

From (1.11) we see that the sum $S(\chi,g,f,p^m)$ can be expressed as a sum of a certain number of complex numbers of modulus $p^{(m+t)/2}$. Moreover, if f and g are both polynomials, then this number is at most one less than the sum of the degrees of f and g. This striking analogy with the case $m=1$

leads us to ask whether there is a unified treatment of exponential sums that can yield both the $m = 1$ and the $m \geq 2$ results all at once.

If α is a critical point of multiplicity greater than one, then in general we are not able to obtain an explicit formula for S_α. However, we are able to convert S_α into a pure exponential sum (Proposition 4.1) via the formula

$$S_\alpha(\chi, g, f, p^m) = p^{\sigma-1}\chi(g(\alpha))e_{p^m}(f(\alpha))S(G_\alpha, p^{m-\sigma}),$$

where σ and G_α are as defined in (4.4) and (4.5). Using known upper bounds on pure exponential sums we are then able to deduce the following upper bound on S_α.

Theorem 1.2. *Suppose that p is odd, f, g are rational functions over $\mathbb{Z}$, not both constant, χ is any multiplicative character* (*mod* p^m), *and $m \geq t+2$. Put $\lambda = (5/4)^5 = 3.05\ldots$ If α is a critical point of multiplicity $\nu_\alpha \geq 1$ then*

$$|S_\alpha(\chi, g, f, p^m)| \leq \lambda_\alpha p^{t/(\nu_\alpha+1)} p^{m(1-1/(\nu_\alpha+1))}, \tag{1.12}$$

where $\lambda_\alpha = \min(\nu_\alpha, \lambda)$.

It follows immediately that under the hypotheses of the theorem

$$|S(\chi, g, f, p^m)| \leq \Big(\sum_{\alpha\in\mathcal{A}} \lambda_\alpha\Big) p^{t/(M+1)} p^{m(1-1/(M+1))}, \tag{1.13}$$

where M is the maximum multiplicity of the critical points. Also, it follows from (1.12) and the proof of [5, Theorem 2.1] that

$$|S(\chi, g, f, p^m)| \leq \lambda p^{t/(d_p(\mathcal{C})+1)} p^{m(1-1/(d_p(\mathcal{C})+1))}. \tag{1.14}$$

The result obtained here generalizes the upper bound for pure exponential sums obtained in [5], which was a sharpening of earlier bounds of Chalk [2], Ding [7], [8], Loh [21] and Cochrane and Zheng [3] for pure exponential sums. It also sharpens slightly the upper bound of Cochrane and Zheng [3] for the case of mixed exponential sums with $g(x) = x$. There we had ν_α in (1.12) instead of λ_α.

We deduce from Theorem 1.2 the following uniform upper bound for mixed exponential sums with polynomial entries.

Corollary 1.1. *Suppose that f, g are polynomials over $\mathbb{Z}$ of degrees d_1, d_2 respectively, p is an odd prime, $m \geq 1$, and χ is a multiplicative character* (*mod* p^m). *If $m = 1$ suppose that $\chi(g)e_p(f)$ is not constant on $\mathbb{F}_p$* (*wherever it is defined*), *and if $m \geq 2$ suppose that the sum $S(\chi, g, f, p^m)$ does not degenerate to one of smaller modulus. Then*

$$|S(\chi, g, f, p^m)| \leq 4.41 p^{m(1-1/(d_1+d_2))}. \tag{1.15}$$

If $p = 2$ the same bound holds with constant 8.82 *on the right-hand side.*

We note that the sum degenerates to one of smaller modulus if $d_p(f) = 0$ and either χ is not primitive ($p \mid c$), or $d_p(g) = 0$. The exponent on the right-hand side of (1.15) is best possible, as can be seen by constructing f and g such that there is a single critical point of multiplicity $d_1 + d_2 - 1$; see e.g. [3, Example 9.2].

As an application consider the case of a pure character sum

$$S(\chi, g, 0, p^m) = \sum_{x=1}^{p^m} \chi(g(x)),$$

with χ a primitive character (mod p^m) ($p \nmid c$) and g a polynomial of degree d with $d_p(g) \geq 1$, and $\chi(g)$ nonconstant. The critical point congruence in this case is $p^{-t}g'(x) \equiv 0 \pmod{p}$. Thus $M \leq d-1$ and we deduce from the corollary above that for any odd p and $m \geq 1$,

$$\Big|\sum_{x=1}^{p^m} \chi(g(x))\Big| \leq 4.41 p^{m(1-1/d)},$$

which sharpens the result of [19] for the case $p < d$.

For the prime $p = 2$, analogues of Theorems 1.1 and 1.2 are given in Sections 6 and 7. The proofs are complicated by the fact that the group of units (mod 2^m) is not cyclic for $m \geq 3$. Combining the results for p odd and $p = 2$ one can then obtain evaluations or estimates of mixed exponential sum to an arbitrary modulus using the multiplicative property of such sums.

2. Some p-adic background.

Let p be an odd prime and $\mathbb{Z}_p$ denote the ring of p-adic integers. Let f, g, R, χ, c and t be as defined above. Throughout the paper, for any $y \in \mathbb{Z}_p$, we let the overbar $\overline{y}$ denote the multiplicative inverse of y in $\mathbb{Z}_p$. (For most purposes, it could also denote a multiplicative inverse of y (mod p^m).)

The first lemma we state embodies the key idea for untwisting a mixed exponential sum and converting it into a pure exponential sum. In order to make sense of the lemma we extend the characters χ and $e_{p^m}(\cdot)$ to the ring of p-adic integers by setting for any $x \in \mathbb{Z}_p$,

$$\chi(x) = \chi(\widetilde{x}), \qquad e_{p^m}(x) = e_{p^m}(\widetilde{x}),$$

where $\widetilde{x}$ denotes the residue class of x in $\mathbb{Z}_p/(p^m) \simeq \mathbb{Z}/(p^m)$. The p-adic logarithm and p-adic exponential functions, defined for $y \in \mathbb{Z}_p$ by

$$\log(1+py) = \sum_{j=1}^{\infty} (-1)^{j+1} \frac{(py)^j}{j}, \qquad e^{py} = \sum_{j=0}^{\infty} \frac{(py)^j}{j!},$$

enjoy the usual inverse function relationship $e^{\log(1+py)} = 1 + py$.

Lemma 2.1. *For any multiplicative character χ (mod p^m) and p-adic integer y,*

$$\chi(1+py) = e_{p^m}(\overline{R}c \log(1+py)).$$

Proof. We start by defining the exponential function $a^{(p-1)\lambda}$ for any p-adic integer λ by

$$a^{(p-1)\lambda} = (1+rp)^{\lambda} = e^{\lambda Rp}.$$

If λ' is an ordinary integer with $\lambda' \equiv \lambda \pmod{p^{m-1}}$ then it follows that $a^{(p-1)\lambda'} \equiv a^{(p-1)\lambda} \pmod{p^m}$, since $e^{(\lambda-\lambda')Rp} \equiv 1 \pmod{p^m}$. Thus, for the extended characters χ and $e_{p^m}(\cdot)$ we have by (1.5),

$$\chi(a^{(p-1)\lambda}) = e^{2\pi i\lambda' c/p^{m-1}} = e_{p^m}(p\lambda c).$$

Now for any $y \in \mathbb{Z}_p$,

$$1+py = e^{\log(1+py)} = a^{(p-1)\overline{R}p^{-1}\log(1+py)}.$$

If we put $\lambda = \overline{R}p^{-1}\log(1+py)$, the lemma follows. ■

This lemma describes how χ behaves on the multiplicative subgroup H of $\mathbb{Z}/(p^m)$ of residue classes congruent to 1 (mod p), a cyclic subgroup of order p^{m-1}. A related lemma can be found in the work of Postnikov [27].

Lemma 2.2. *For any rational functions* f, g *over* $\mathbb{Z}$ *with* $\operatorname{ord}_p(g) = 0$ *we have*

$$t = \min\{\operatorname{ord}_p(f'), \operatorname{ord}_p(cg')\}.$$

Proof. In view of the definition (1.6), it suffices to prove that $\operatorname{ord}_p(cg') \ge t$. Let K_p be a splitting field for g over $\mathbb{Q}_p$ and say

$$g(X) = g_0(X-r_1)^{d_1}(X-r_2)^{d_2}\ldots(X-r_k)^{d_k},$$

for some nonzero integers d_i (possibly negative) and values $g_0, r_i \in K_p$. Let ν_p be an extension of the valuation $\operatorname{ord}_p(\cdot)$ to K such that $\operatorname{ord}_p(x) = e\cdot\nu_p(x)$ for $x \in \mathbb{Q}_p$, where e is the ramification index. Fix i with $1 \le i \le k$ and work in the field of formal Laurent series in $X - r_i$ with valuation

$$\nu_p\Big(\sum_{j=-l}^{\infty} c_j(X-r_i)^j\Big) = \min_{j\ge -l}\{\nu_p(c_j)\}.$$

Write

$$f(X) = \sum_{j=-l}^{\infty} a_j(X-r_i)^j, \qquad \frac{g'(X)}{g(X)} = \frac{d_i}{X-r_i} + \sum_{j=0}^{\infty} b_j(X-r_i)^j,$$

for some coefficients a_j, b_j in K_p. Thus

$$Rf'(X) + c\frac{g'(X)}{g(X)} = R\sum_{j=-l}^{\infty} ja_j(X-r_i)^{j-1} + \frac{cd_i}{X-r_i} + c\sum_{j=0}^{\infty} b_j(X-r_i)^j.$$

The coefficient of $(X-r_i)^{-1}$ is cd_i. Thus for $1 \le i \le k$,

$$t = e\nu_p\bigg(Rf'(X) + c\frac{g'(X)}{g(X)}\bigg) \le e\nu_p(cd_i) = \operatorname{ord}_p(cd_i)$$

and

$$\operatorname{ord}_p(cg'(X)) = \operatorname{ord}_p\biggl(g(X)\sum_{i=1}^{k}\frac{cd_i}{X-r_i}\biggr) \ge t. \ \blacksquare$$

3. Proof of Theorem 1.1. Critical points of multiplicity one. Let p be an odd prime, f, g rational functions over $\mathbb{Z}$, not both constant and χ a multiplicative character (mod p^m). Suppose first that $m-t \ge 2$ is even. Let α be any integer for which $f(\alpha)$, $g(\alpha)$ are both defined (mod p^m) and $g(\alpha) \not\equiv 0 \pmod{p}$. Set $x = u + p^{(m-t)/2}v$ with u running from 1 to $p^{(m-t)/2}$, subject to the constraint $u \equiv \alpha \pmod{p}$, and v running from 1 to $p^{(m+t)/2}$. Then

$$S_\alpha = \sum_{u\equiv\alpha \,(\mathrm{mod}\, p)}^{p^{(m-t)/2}} \sum_{v=1}^{p^{(m+t)/2}} \chi(g(u+p^{(m-t)/2}v))e_{p^m}(f(u+p^{(m-t)/2}v)). \tag{3.1}$$

To proceed, we develop f and g into Taylor series about α as follows. Let $t_1 = \operatorname{ord}_p(g')$. For any integers u, v there exists a p-adic integer $w(u,v)$ such that

$$g(u+p^{(m-t)/2}v) = g(u) + g'(u)p^{(m-t)/2}v + p^{m-t+t_1}w(u,v),$$

since $\operatorname{ord}_p(g^{(j)}(u)) \ge t_1$ for $j \ge 1$, and the power of p dividing $j!$ is dominated by the increasing power of $p^{(m-t)/2}$. Writing $g = g(u)$, $g' = g'(u)$, $w = w(u,v)$ (for the moment) we see by Lemma 2.1 that

$$\begin{aligned}\chi(g(u+p^{(m-t)/2}v)) &= \chi(g)\chi(1+\overline{g}g'p^{(m-t)/2}v + \overline{g}p^{m-t+t_1}w)\\ &= \chi(g)e_{p^m}(\overline{R}c\log(1+\overline{g}g'p^{(m-t)/2}v+\overline{g}p^{m-t+t_1}w)).\end{aligned}$$

Now, by Lemma 2.2,

$$m - t + t_1 + \operatorname{ord}_p(c) \ge m,$$

and so

$$c\log(1+\overline{g}g'p^{(m-t)/2}v + \overline{g}p^{m-t+t_1}w) \equiv c\overline{g}g'p^{(m-t)/2}v \pmod{p^m}.$$

Thus, we obtain

$$\begin{aligned}\chi(g(u+p^{(m-t)/2}v)) &= \chi(g)e_{p^m}(\overline{R}c\overline{g}g'p^{(m-t)/2}v)\\ &= \chi(g)e_{p^{(m+t)/2}}(\overline{R}c\overline{g}g'v).\end{aligned} \tag{3.2}$$

By Lemma 2.2 we also have $t \le \operatorname{ord}_p(f'(X))$. It follows that for any $j \ge 1$, $\operatorname{ord}_p(f^{(j)}(u)) \ge t$ and thus

$$f(u+p^{(m-t)/2}v) \equiv f(u) + f'(u)p^{(m-t)/2}v \pmod{p^m} \tag{3.3}$$

and

$$e_{p^m}(f(u+p^{(m-t)/2}v)) = e_{p^m}(f(u))e_{p^{(m+t)/2}}(f'(u)v). \tag{3.4}$$

It follows from (3.2), (3.4) and (3.1) that

$$S_\alpha = \sum_{u\equiv\alpha\,(\mathrm{mod}\,p)} \chi(g(u))e_{p^m}(f(u)) \times \sum_{v=1}^{p^{(m+t)/2}} e_{p^{(m+t)/2}}(\overline{R}c\overline{g(u)}g'(u)v + f'(u)v). \tag{3.5}$$

Recalling the definition of $\mathcal{C}(u)$ in (1.8) we see that the inner sum vanishes unless $p^{(m-t)/2}\,|\,\mathcal{C}(u)$ in which case it equals $p^{(m+t)/2}$, and so we obtain

$$S_\alpha(\chi, g, f, p^m) = p^{(m+t)/2} \sum_{\substack{u\equiv\alpha\,(\mathrm{mod}\,p)\\ p^{(m-t)/2}|\mathcal{C}(u)}} \chi(g(u))e_{p^m}(f(u)). \tag{3.6}$$

In particular, $S_\alpha = 0$ unless α is a critical point. Moreover, if α is a critical point of multiplicity one then it has a unique lifting to a solution of the congruence $\mathcal{C}(x) \equiv 0 \pmod{p^{(m-t)/2}}$ and we obtain the result of part (ii) of the theorem.

Suppose next that $m - t \ge 3$ is odd. The argument proceeds as before. Write $x = u + p^{(m-t+1)/2}v$ with u running from 1 to $p^{(m-t+1)/2}$, subject to the constraint $u \equiv \alpha \pmod{p}$, and v running from 1 to $p^{(m+t-1)/2}$. We obtain

$$\begin{aligned} S_\alpha &= \sum_{u\equiv\alpha\,(\mathrm{mod}\,p)}^{p^{(m-t+1)/2}} \sum_{v=1}^{p^{(m+t-1)/2}} \chi(g(u + p^{(m-t+1)/2}v))e_{p^m}(f(u + p^{(m-t+1)/2}v)) \\ &= \sum_u \sum_v \chi(g(u) + g'(u)p^{(m-t+1)/2}v + \ldots) \\ &\quad \times e_{p^m}(f(u) + f'(u)p^{(m-t+1)/2}v + \ldots) \\ &= \sum_u \sum_v \chi(g(u))\chi(1 + \overline{g(u)}g'(u)p^{(m-t+1)/2}v + \ldots) \\ &\quad \times e_{p^m}(f(u))e_{p^m}(f'(u)p^{(m-t+1)/2}v) \\ &= \sum_u \chi(g(u))e_{p^m}(f(u)) \sum_{v=1}^{p^{(m+t-1)/2}} e_{p^{(m+t-1)/2}}(\overline{R}c\overline{g(u)}g'(u)v + f'(u)v), \end{aligned}$$

and thus

$$S_\alpha = p^{(m+t-1)/2} \sum_{p^{(m-t-1)/2}|\mathcal{C}(u)} \chi(g(u))e_{p^m}(f(u)). \tag{3.7}$$

We see again that $S_\alpha = 0$ unless α is a critical point.

Suppose now that α is a critical point of multiplicity one. Let α^* be a solution of the congruence $\mathcal{C}(x) \equiv 0 \pmod{p^{(m-t+1)/2}}$. The values u occurring in the sum in (3.7) may then be written $u = \alpha^* + yp^{(m-t-1)/2}$, with y

running from 1 to p, and so

$$S_\alpha = p^{(m+t-1)/2}\sum_{y=1}^{p}\chi(g(\alpha^* + yp^{(m-t-1)/2}))e_{p^m}(f(\alpha^* + yp^{(m-t-1)/2})).$$

Writing (for the moment) $g = g(\alpha^*)$, $g' = g'(\alpha^*)$, $g'' = g''(\alpha^*)$, $f = f(\alpha^*)$, $f' = f'(\alpha^*)$, $f'' = f''(\alpha^*)$, we have

$$\begin{aligned} S_\alpha &= p^{(m+t-1)/2}\sum_{y=1}^{p}\chi(g)e_{p^m}(f)\chi(1 + \overline{g}g'yp^{(m-t-1)/2} + \overline{g}g''\overline{2}y^2p^{m-t-1}) \\ &\qquad \times e_{p^m}(f'yp^{(m-t-1)/2} + f''\overline{2}y^2p^{(m-t-1)/2}) \\ &= p^{(m+t-1)/2}\chi(g)e_{p^m}(f)\sum_{y=1}^{p}e_{p^{(m-t+1)/2}}(\overline{R}c(\overline{g}g'y + \overline{g}g''\overline{2}y^2p^{(m-t-1)/2}) \\ &\qquad - \overline{R}c\overline{2}p^{(m-t-1)/2}(\overline{g}g'y)^2 + f'y + f''\overline{2}y^2p^{(m-t-1)/2}). \end{aligned}$$

Now, by our choice of α^* the coefficient on y vanishes, and so we obtain

$$\begin{aligned} S_\alpha &= \chi(g(\alpha^*))e_{p^m}(f(\alpha^*))p^{(m+t-1)/2}\sum_{y=1}^{p}e_p(Ay^2) \\ &= \chi(g(\alpha^*))e_{p^m}(f(\alpha^*))\left(\frac{A}{p}\right)\mathcal{G}_p p^{(m+t-1)/2}, \end{aligned}$$

where

$$A = p^{-t}\overline{2}(\overline{R}c\overline{g}g'' - \overline{R}c\overline{g}^2(g')^2 + f'') = \overline{2R}\left(\frac{\mathcal{C}}{g}\right)'(\alpha^*).$$

4. Critical points of higher multiplicity. If α is a critical point of multiplicity greater than one, then in general it is not possible to obtain a concise formula for S_α due to our inability to evaluate exponential sums modulo p. However, we are able to convert the mixed sum to a pure exponential sum as we shall demonstrate in this section. The formula we obtain (in Proposition 4.1) is analogous to the well known recursion formula for pure exponential sums, which we now recall. Let α be a critical point associated with the pure exponential sum $S(f, p^m)$ and define

$$\sigma := \mathrm{ord}_p(f(\alpha + pY) - f(\alpha)), \qquad g_\alpha(Y) := p^{-\sigma}(f(\alpha + pY) - f(\alpha)).$$

Then for $m \ge \sigma$,

$$S_\alpha(f, p^m) = p^{\sigma-1}e_{p^m}(f(\alpha))S(g_\alpha, p^{m-\sigma}) \tag{4.1}$$

(see e.g. [3]). The recursion formula reduces the original sum to a sum with smaller modulus. The difficulty in evaluating S_α arises when $m - \sigma = 1$, leaving us with an exponential sum over a finite field.

We return now to a general sum of the type $S(\chi,g,f,p^m)$. Suppose that α is a critical point of multiplicity $\nu\ge 1$. Write $x=u+p^{m-t-1}v$ with u running from 1 to p^{m-t-1}, subject to the constraint $u\equiv\alpha\ (\operatorname{mod} p)$ and v running from 1 to p^{t+1}. Then proceeding as in the previous section, we have

$$\begin{aligned}
S_\alpha &= p^{t+1}\sum_{u\equiv\alpha\,(\operatorname{mod} p)}\chi(g(u))e_{p^m}(f(u))\\
&= p^{t+1}\sum_{y=1}^{p^{m-t-2}}\chi(g(\alpha+py))e_{p^m}(f(\alpha+py))\\
&= p^{t+1}\chi(g(\alpha))e_{p^m}(f(\alpha))\sum_y\chi(\overline{g}g(\alpha+py))e_{p^m}(f(\alpha+py)-f(\alpha))\\
&= p^{t+1}\chi(g(\alpha))e_{p^m}(f(\alpha))\sum_{y=1}^{p^{m-t-2}}e_{p^m}(F_\alpha(y)),
\end{aligned}$$

say where (by Lemma 2.2),

$$F_\alpha(Y):=c\overline{R}\log(\overline{g(\alpha)}g(\alpha+pY))+f(\alpha+pY)-f(\alpha). \tag{4.2}$$

$F_\alpha(Y)$ may be expanded into a formal power series of the type

$$F_\alpha(Y)=\sum_{j=1}^{\infty}a_jY^j, \tag{4.3}$$

with p-adic integer coefficients a_j. Define

$$\sigma:=\operatorname{ord}_p(F_\alpha(Y))=\min_{j\ge1}\{\operatorname{ord}_p(a_j)\}, \tag{4.4}$$

and

$$G_\alpha(Y):=p^{-\sigma}F_\alpha(Y). \tag{4.5}$$

Then we have the following conversion of S_α to a pure exponential sum.

Proposition 4.1. *If $m\ge\sigma$ then*

$$S_\alpha(\chi,g,f,p^m)=p^{\sigma-1}\chi(g(\alpha))e_{p^m}(f(\alpha))S(G_\alpha,p^{m-\sigma}), \tag{4.6}$$

where $S(G_\alpha,p^{m-\sigma})=\sum_{y=1}^{p^{m-\sigma}}e_{p^{m-\sigma}}(G_\alpha(y))$.

The function G_α, defined a priori as an infinite series with p-adic coefficients, may be viewed as a polynomial over $\mathbb{Z}$ in the exponential sum $S(G_\alpha,p^{m-\sigma})$, since its coefficients are p-adic integers and the high order coefficients all vanish modulo $p^{m-\sigma}$. Thus $S(G_\alpha,p^{m-\sigma})$ is just an ordinary pure exponential sum.

We proceed now to obtain a relationship between G_α and the critical point function $\mathcal{C}$. Note

$$F'_\alpha(Y)=c\overline{R}p\,\frac{g'(\alpha+pY)}{g(\alpha+pY)}+pf'(\alpha+pY)=p^{t+1}\overline{R}\,\frac{\mathcal{C}(\alpha+pY)}{g(\alpha+pY)}. \tag{4.7}$$

Develop $\overline{R}\mathcal{C}/g$ into a Taylor expansion about α,

$$\overline{R}\frac{\mathcal{C}(X)}{g(X)}=\sum_{j=0}^{\infty}c_j(X-\alpha)^j, \tag{4.8}$$

with p-adic integer coefficients c_j, and note that since α is a zero of $\mathcal{C}$ of multiplicity ν,

$$\mathrm{ord}_p(c_j)>0 \quad \text{for } 0\le j<\nu \quad \text{and} \quad \mathrm{ord}_p(c_\nu)=0.$$

It follows from (4.7) that

$$F_\alpha(Y)=p^{t+1}\sum_{j=0}^{\infty}c_jp^j\frac{Y^{j+1}}{j+1}, \tag{4.9}$$

and that

$$G_\alpha(Y)=p^{-\sigma}F_\alpha(Y)=p^{-\sigma}\sum_{j=1}^{\infty}a_jY^j=p^{t-\sigma}\sum_{j=1}^{\infty}\frac{c_{j-1}}{j}p^jY^j. \tag{4.10}$$

5. Proof of Theorem 1.2. Many kinds of upper bounds are available for pure exponential sums of the type appearing in (4.6). We shall make use of the following bound of Theorem 2.1 of [5]. Let f be a nonconstant (mod p) polynomial over $\mathbb{Z}$, $t=\mathrm{ord}_p(f')$ and $f_1=p^{-t}f'$. Let $d_p(f_1)$ denote the degree of f_1 viewed as a polynomial (mod p). Then if p is odd and $m\ge t+2$ or $p=2$ and $m\ge t+3$,

$$\Big|\sum_{x=1}^{p^m}e_{p^m}(f(x))\Big|\le\min(\lambda,d_p(f_1))p^{t/(d_p(f_1)+1)}p^{m(1-1/(d_p(f_1)+1))}, \tag{5.1}$$

where $\lambda=(5/4)^5$. See also [3], [5], [8], [21] and [22] for related bounds. For the case that S_α is converted to a (mod p) exponential sum we need the following upper bound, which is an easy consequence of Weil's bound (see [5, Lemma 3.1]): For any nonconstant (mod p) polynomial f of degree d,

$$\Big|\sum_{x=1}^{p}e_p(f(x))\Big|\le 1.75p^{1-1/d}. \tag{5.2}$$

In order to apply these bounds to the sum $S(G_\alpha,p^{m-\sigma})$ define

$$\tau:=\mathrm{ord}_p(G'_\alpha(Y)), \tag{5.3}$$

$$H_\alpha(Y):=p^{-\tau}G'_\alpha(Y)=p^{-\tau-\sigma}\sum_{j=1}^{\infty}a_jjY^{j-1}=p^{t-\tau-\sigma}\sum_{j=1}^{\infty}c_{j-1}p^jY^{j-1}. \tag{5.4}$$

Noting that the series $G_\alpha(Y)$ and $H_\alpha(Y)$ have p-adic integer coefficients we readily obtain the following relationships:

$$\sigma \geq t+2, \tag{5.5}$$

$$\sigma \leq \nu+1+t-\tau, \tag{5.6}$$

$$d_p(G_\alpha) \leq \sigma - t + \mathrm{ord}_p(d_p(G_\alpha)), \tag{5.7}$$

$$d_p(H_\alpha) \leq \sigma+\tau-t-1 \leq \nu, \tag{5.8}$$

$$\tau \leq \mathrm{ord}_p(d_p(G_\alpha)). \tag{5.9}$$

The first inequality (5.5) follows from (4.9) and the fact that $p \mid c_0$. Inequalities (5.6) and (5.8) follow from the second series expansion of H_α in (5.4), setting $j=\nu+1$ and $j=d_p(H_\alpha)$ respectively, while inequality (5.7) follows from the second series expansions of G_α in (4.10), setting $j=d_p(G_\alpha)$. Finally, to obtain (5.9) we set $j=d_p(G_\alpha)$ and note that by definition $\mathrm{ord}_p(a_j)=\sigma$. Then, by the definition of τ,

$$\tau \leq \mathrm{ord}_p(a_j j) - \sigma = \mathrm{ord}_p(j).$$

Proof of Theorem 1.2. Having established the inequalities in (5.5) to (5.9) the proof of Theorem 1.2 is almost identical to the proof given in [5] for pure exponential sums. We repeat here the argument for the convenience of the reader. Suppose that $m \geq t+2$ and that α is a critical point of multiplicity $\nu \geq 1$. If $\nu=1$ then (1.12) follows immediately from Theorem 1.1, and so we suppose henceforth that $\nu \geq 2$. Let σ be as defined in (4.4).

Case (i). Suppose first that $\sigma \geq m$. Then we have the trivial upper bound

$$|S_\alpha| \leq p^{m-1} = p^{(m-\nu-1)/(\nu+1)} p^{m(1-1/(\nu+1))} \leq p^{t/(\nu+1)} p^{m(1-1/(\nu+1))},$$

the last inequality following from (5.6).

Case (ii). Suppose next that $\sigma = m-1$. By (5.6) we have trivially

$$|S_\alpha| \leq p^{m-1} \leq 2p^{t/(\nu+1)} p^{m(1-1/(\nu+1))},$$

unless $\tau=0$ and $p>2^{\nu+1}$, and so we may assume that $p>2^{\nu+1}$. Let $d_p = d_p(G_\alpha)$. By (5.7) we have

$$d_p \leq \nu+1+\mathrm{ord}_p(d_p). \tag{5.10}$$

Suppose that $\mathrm{ord}_p(d_p) \geq 1$. If $d_p = p$ then by (5.10) $p \leq \nu+2$, contradicting our assumptions that $p > 2^{\nu+1}$ and $\nu \geq 2$. Otherwise $d_p \geq 2p$ and thus since $\mathrm{ord}_p(d_p) \leq d_p/2$ we see by (5.10) that

$$p \leq \tfrac{1}{2} d_p \leq d_p - \mathrm{ord}_p(d_p) \leq \nu+1,$$

again contradicting our assumptions.

Thus we must have $\mathrm{ord}_p(d_p) = 0$ and so by (5.10), $d_p \le \nu + 1$. It follows from Proposition 4.1 and the upper bound of (5.2) that

$$\begin{aligned}|S_\alpha| &= p^{\sigma-1}|S(G_\alpha, p)| \le 2p^{\sigma-1/d_p} \le 2p^{m-1-1/(\nu+1)}\\ &= 2p^{t/(\nu+1)}p^{m(1-1/(\nu+1))}p^{(\sigma-\nu-1-t)/(\nu+1)}.\end{aligned}$$

By (5.6) we then obtain (1.12).

Case (iii). Suppose that $m - 1 - \tau \le \sigma \le m - 2$. In particular, we must have $\tau \ge 1$. Then we have the trivial estimate

$$\begin{aligned}|S_\alpha| &\le p^{m-1} = p^{(m-\nu-1)/(\nu+1)}p^{m(1-1/(\nu+1))}\\ &\le p^{1/(\nu+1)}p^{(\sigma+\tau-\nu-1)/(\nu+1)}p^{m(1-1/(\nu+1))}\\ &\le p^{1/(\nu+1)}p^{t/(\nu+1)}p^{m(1-1/(\nu+1))},\end{aligned} \tag{5.11}$$

the latter inequality following from (5.6). Now, by (5.9), $p^\tau \mid d_p(G_\alpha)$. Since $\tau \ge 1$ and $d_p(G_\alpha) \ge 1$, it follows from (5.7) that

$$p - 1 \le p^\tau - \tau \le d_p(G_\alpha) - \mathrm{ord}_p(d_p(G_\alpha)) \le \nu + 1 - \tau \le \nu.$$

Thus $p^{1/(\nu+1)} \le p^{1/p} \le 3^{1/3} \le 2$, and so (1.12) follows from (5.11).

Case (iv). Suppose finally that $\sigma \le m - 2 - \tau$. In this case we can apply inequality (5.1) to $S(G_\alpha, p^{m-\sigma})$ and conclude from Proposition 4.1 that

$$\begin{aligned}|S_\alpha| &= p^{\sigma-1}|S(G_\alpha, p^{m-\sigma})|\\ &\le \min(\lambda, d_p(H_\alpha))p^{\sigma-1}p^{\tau/(d_p(H_\alpha)+1)}p^{(m-\sigma)(1-1/(d_p(H_\alpha)+1))}.\end{aligned}$$

Now by (5.8), $d_p(H_\alpha) \le \nu$ and thus since $m - \sigma - \tau > 0$ we obtain

$$\begin{aligned}|S_\alpha| &\le \min(\lambda, \nu)p^{\sigma-1}p^{\tau/(\nu+1)}p^{(m-\sigma)(1-1/(\nu+1))}\\ &\le \min(\lambda, \nu)p^{(\tau+\sigma-\nu-1)/(\nu+1)}p^{m(1-1/(\nu+1))}.\end{aligned}$$

The theorem follows from (5.6).

6. The prime $p = 2$**.** Suppose that $m \ge 3$. Let χ be a multiplicative character (mod 2^m) defined by the relations

$$\chi(5) = e_{2^{m-2}}(c), \qquad \chi(-1) = (-1)^\kappa, \tag{6.1}$$

for some integer c with $1 \le c \le 2^{m-2}$ and $\kappa = 0$ or 1. Let R be the 2-adic integer

$$R := \frac{1}{4}\log(5) = \sum_{j=1}^{\infty}\frac{(-1)^{j-1}4^{j-1}}{j} \equiv -1 \pmod{16}. \tag{6.2}$$

Let f, g be rational functions over $\mathbb{Z}$, not both constant and $S(\chi, g, f, 2^m)$ be the exponential sum in (1.1). The value t and the critical point congruence associated with the sum are defined as before,

$$\mathcal{C}(x) := 2^{-t}(Rg(x)f'(x) + cg'(x)) \equiv 0 \pmod 2. \tag{6.3}$$

To untwist the mixed exponential sum we use the following analogue of Lemma 2.1, valid for any 2-adic integer y:

$$\chi(1+4y) = e_{2^m}(c\overline{R}\log(1+4y)). \tag{6.4}$$

We also observe that Lemma 2.2 holds identically for $p=2$.

Theorem 6.1. *If $m \ge t+5$ and α is a critical point of multiplicity one then we have for $m-t$ even and $m-t$ odd respectively,*

$$S_\alpha(\chi, g, f, 2^m) = \begin{cases} \chi(g(\alpha^*))e_{2^m}(f(\alpha^*))e_8(-(\mathcal{C}/g)'(\alpha^*))2^{(m+t)/2}, \\ \chi(g(\alpha^*))e_{2^m}(f(\alpha^*))[1+e_4(-(\mathcal{C}/g)'(\alpha^*))]2^{(m+t-1)/2}, \end{cases}$$

where α^* is the unique lifting of α to a solution of the congruence $\mathcal{C}(x) \equiv 0 \pmod{2^m}$. In particular $|S_\alpha| = 2^{(m+t)/2}$. If $m = t+3$ then $|S_\alpha| \le 2^{(m+t+1)/2}$. If $m = t+4$ then $|S_\alpha| \le 2^{(m+t)/2}$.

Proof. Let $\alpha = 0$ or 1. If $m-t \ge 4$ is even then setting $x = u + 2^{(m-t+2)/2}v$, with u running from 1 to $2^{(m-t+2)/2}$ subject to the constraint $u \equiv \alpha \pmod 2$ and v running from 1 to $2^{(m+t-2)/2}$ we have

$$\begin{aligned} S_\alpha &= \sum_{u\equiv\alpha \,(\mathrm{mod}\, 2)} \sum_v \chi(g(u+2^{(m-t+2)/2}v))e_{2^m}(f(u+2^{(m-t+2)/2}v)) \\ &= \sum_u \chi(g(u))e_{2^m}(f(u)) \\ &\quad \times \sum_v e_{2^m}(\overline{R}c\overline{g(u)}g'(u)2^{(m-t+2)/2}v + f'(u)2^{(m-t+2)/2}v) \\ &= 2^{(m+t-2)/2} \sum_{2^{(m-t-2)/2}|\mathcal{C}(u)} \chi(g(u))e_{2^m}(f(u)). \end{aligned}$$

Thus the sum is zero unless α is a critical point.

Suppose now that α is a critical point of multiplicity one. Let α^* be the unique lifting of α to a solution of the congruence $\mathcal{C}(x) \equiv 0 \pmod{2^m}$. Put $g = g(\alpha^*)$, $g' = g'(\alpha^*)$, $g'' = g''(\alpha^*)$, $f = f(\alpha^*)$, $f' = f'(\alpha^*)$, $f'' = f''(\alpha^*)$, for the moment. Then we have

$$\begin{aligned} S_\alpha = 2^{(m+t-2)/2}\chi(g)e_{2^m}(f)\sum_{y=1}^{4}\chi(\overline{g}g(\alpha^*+2^{(m-t-2)/2}y)) \\ \times e_{2^m}(f(\alpha^*+2^{(m-t-2)/2}y) - f(\alpha^*)). \end{aligned}$$

We split the latter sum into two pieces, the first corresponding to the terms $y = 2,4$ and the second to the terms $y = 1,3$. For the first part we set $y = 2z$ and apply (6.4) to obtain

$$\sum_{z=1}^{2} e_2(2^{-t}(c\overline{R}\overline{g}g'' - c\overline{R}\overline{g}^2(g')^2 + f'')z^2) = \sum_{z=1}^{2} e_2(-(\mathcal{C}/g)'(\alpha)z) = 0,$$

since α is a zero of $\mathcal{C}/g$ of multiplicity one.

For the terms $y = 1, 3$ we consider two cases. Suppose first that $m-t \geq 6$ or that $m - t = 4$ and $g' + g''$ is even. In this case we can apply (6.4) again and obtain the sum

$$\sum_{y=1,3} e_8(2^{-t}(c\overline{R}\overline{g}g'' - c\overline{R}\overline{g}^2(g')^2 + f'')y^2) = 2e_8(-(\mathcal{C}/g)'(\alpha^*)).$$

Suppose now that $m - t = 4$ and that $g' + g''$ is odd, that is, g' is odd. In this case we settle for an upper bound of 2.

Next assume that $m - t \geq 3$ is odd. Put $x = u + 2^{(m-t+1)/2}v$ with u running from 1 to $2^{(m-t+1)/2}$, subject to the constraint $u \equiv \alpha \pmod 2$, and v running from 1 to $2^{(m+t-1)/2}$. Then we obtain

$$\begin{aligned} S_\alpha &= \sum_u \chi(g(u))e_{2^m}(f(u)) \sum_v \chi(1 + \overline{g(u)}g'(u)2^{(m-t+1)/2}v + \ldots) \\ &\quad \times e_{2^m}(f'(u)2^{(m-t+1)/2}v + \ldots) \\ &= \sum_u \chi(g(u))e_{2^m}(f(u)) \\ &\quad \times \sum_v e_{2^m}(\overline{R}c\overline{g(u)}g'(u)2^{(m-t+1)/2}v + f'(u)2^{(m-t+1)/2}v) \\ &= 2^{(m+t-1)/2} \sum_{2^{(m-t-1)/2} \mid \mathcal{C}(u)} \chi(g(u))e_{2^m}(f(u)). \end{aligned}$$

Again we see that the sum is zero unless α is a critical point.

Suppose that α is a critical point of multiplicity one and let α^* be a lifting of α to a solution of the congruence $\mathcal{C}(x) \equiv 0 \pmod{2^m}$. Using the same abbreviations as above we have, if $m - t \geq 5$,

$$\begin{aligned} S_\alpha = 2^{(m+t-1)/2}\chi(g)e_{2^m}(f) &\sum_{y=0}^{1} \chi(1 + \overline{g}g'2^{(m-t-1)/2}y + \overline{g}g''2^{m-t-2}y^2) \\ &\times e_{2^m}(f'2^{(m-t-1)/2}y + f''2^{m-t-2}y^2). \end{aligned}$$

The $y = 1$ term of the latter sum is just

$$\begin{aligned} e_{2^m}((c\overline{R}\overline{g}g' + f')2^{(m-t-1)/2} + (c\overline{R}\overline{g}g'' - c\overline{R}\overline{g}^2(g')^2 + f'')2^{m-t-2}) \\ = e_4(-(\mathcal{C}/g)'(\alpha^*)), \end{aligned}$$

and thus

$$S_\alpha = 2^{(m+t-1)/2}\chi(g(\alpha^*))e_{2^m}(f(\alpha^*))[1 + e_4(-(\mathcal{C}/g)'(\alpha^*))].$$

If $m - t = 3$ then further terms need to be accounted for in the Taylor expansions. We settle for an upper bound of 2 in this case. This completes the proof of Theorem 6.1. ■

7. Upper bounds for the case $p = 2$. Let $\alpha = 0$ or 1 be a critical point of multiplicity ν. Write $x = u + 2^{m-t-1}v$ with u running from 1 to 2^{m-t-1} subject to the constraint $u \equiv \alpha \pmod 2$ and v running from 1 to 2^{t+1}. We then have for $m - t \geq 3$,

$$S_\alpha(\chi, g, f, 2^m) = 2^{t+1} \sum_{2 | \mathcal{C}(u)} \chi(g(u)) e_{2^m}(f(u)) = T_1 + T_2,$$

say, where

$$T_1 = 2^{t+1} \sum_{y=1}^{2^{m-t-3}} \chi(g(\alpha + 4y)) e_{2^m}(f(\alpha + 4y)),$$

and T_2 is the same sum with α replaced by $\alpha + 2$. By (6.4) we have

$$T_1 = 2^{t+1} \chi(g(\alpha)) e_{2^m}(f(\alpha)) \sum_{y=1}^{2^{m-t-3}} e_{2^m}(F_\alpha(y)), \tag{7.1}$$

with F_α as defined in (4.2) with the value p replaced by 4. In particular,

$$F_\alpha(Y) = \sum_{j=1}^{\infty} a_j Y^j = 2^t \sum_{j=1}^{\infty} c_{j-1} 4^j \frac{Y^j}{j},$$

for some 2-adic integers a_j, c_j as defined in (4.3), (4.8).

Define σ, τ, G_α and H_α identically as in Section 4, so that

$$G_\alpha(Y) = 2^{-\sigma} \sum_{j=1}^{\infty} a_j Y^j = 2^{t-\sigma} \sum_{j=1}^{\infty} \frac{c_{j-1}}{j} 4^j Y^j, \tag{7.2}$$

$$H_\alpha(Y) = 2^{-\tau-\sigma} \sum_{j=1}^{\infty} a_j j Y^{j-1} = 2^{t-\tau-\sigma} \sum_{j=1}^{\infty} c_{j-1} 4^j Y^{j-1}, \tag{7.3}$$

and

$$T_1 = 2^{\sigma-2} \chi(g(\alpha)) e_{2^m}(f(\alpha)) S(G_\alpha, 2^{m-\sigma}). \tag{7.4}$$

Arguing as above for the case of odd p, we have the following relations for the prime $p = 2$:

$$\sigma \geq t + 3, \tag{7.5}$$

$$\sigma \leq 2\nu + 2 + t - \tau, \tag{7.6}$$

$$d_p(G_\alpha) \leq \tfrac{1}{2}[\sigma - t + \mathrm{ord}_2(d_p(G_\alpha))], \tag{7.7}$$

$$d_p(H_\alpha) \leq \tfrac{1}{2}(\sigma + \tau - t) - 1 \leq \nu, \tag{7.8}$$

$$\tau \leq \mathrm{ord}_2(d_p(G_\alpha)). \tag{7.9}$$

Exactly the same relations hold for the sum T_2.

THEOREM 7.1. *For any rational functions f and g over $\mathbb{Z}$, not both constant, multiplicative character χ (mod 2^m) and critical point α of multiplicity $\nu = \nu_\alpha$ we have for $m \ge t+3$,*

$$|S_\alpha(\chi, g, f, 2^m)| \le 2\lambda_\alpha 2^{t/(\nu+1)} 2^{m(1-1/(\nu+1))}, \tag{7.10}$$

where $\lambda_\alpha = \min(\nu_\alpha, \lambda)$. ($\lambda = (5/4)^5$.)

As in [5, Theorem 2.1] one deduces under the hypotheses of the theorem the upper bound

$$|S(\chi, g, f, 2^m)| \le 2\lambda 2^{t/(d_p(\mathcal{C})+1)} 2^{m(1-1/(d_p(\mathcal{C})+1))}. \tag{7.11}$$

Proof of Theorem 7.1. The case $\nu = 1$ follows immediately from Theorem 6.1 and so we assume $\nu \ge 2$. The inequality is trivial if $m - t \le 3\nu + 3$, and so we assume further that $m - t \ge 3\nu + 4$. In this case, by (7.6) we have $m - \sigma \ge \tau + 4$. Thus we may apply (5.1) to the sum $S(G_\alpha, 2^{m-\sigma})$ and obtain from (7.4), (7.6) and (7.8),

$$\begin{aligned}|T_1| &= 2^{\sigma-2}|S(G_\alpha, 2^{m-\sigma})|\\ &\le 2^{\sigma-2}\min(d_p(H_\alpha), \lambda) 2^{\tau/(d_p(H_\alpha)+1)} 2^{(m-\sigma)(1-1/(d_p(H_\alpha)+1))}\\ &\le \lambda_\alpha 2^{\sigma-2} 2^{\tau/(\nu+1)} 2^{(m-\sigma)(1-1/(\nu+1))} \le \lambda_\alpha 2^{t/(\nu+1)} 2^{m(1-1/(\nu+1))},\end{aligned}$$

where $\lambda_\alpha = \min(\lambda, \nu_\alpha)$. The same bound holds for $|T_2|$, completing the proof. ∎

8. Proof of Corollary 1.1.

Let f, g be polynomials over $\mathbb{Z}$ of degrees d_1, d_2 respectively, p any prime, $m \ge 1$ and χ a multiplicative character (mod p^m). Put $d = d_1 + d_2$. Suppose that the sum $S(\chi, f, g, p^m)$ does not degenerate to one of smaller modulus, that is, either $d_p(f) \ge 1$, or χ is primitive and $d_p(g) \ge 1$. In particular, by Lemma 2.2 this implies that

$$p^t \le \max(d_1, d_2) \le d. \tag{8.1}$$

If $d = 1$ then $S(\chi, g, f, p^m) = 0$ and so we may assume that $d \ge 2$. If $m = 1$ the corollary follows from the upper bound of Weil (1.2) in the same manner that [5, Lemma 3.1] is proven. If $2 \le m \le t+1$ then using (8.1) we have the trivial upper bound

$$|S(\chi, g, f, p^m)| \le p^m \le 3p^{m(1-1/d)},$$

for in this case

$$p^t \le d \le 3^{d/2} \le 3^{dt/(t+1)} \le 3^{dt/m},$$

and so $p^{m/d} \le 3$. If $p = 2$ and $m = t+2$ then $p^{m/d} = 2^{(t+2)/d} \le (4d)^{1/d} \le 3$ and so the trivial bound suffices again. If p is odd and $m \ge t+2$ then by (1.14) and (8.1) we have

$$|S(\chi, g, f, p^m)| \le \lambda p^{t/d} p^{m(1-1/d)} \le \lambda d^{1/d} p^{m(1-1/d)} \le \lambda 3^{1/3} p^{m(1-1/d)}.$$

If $p = 2$ and $m \geq t + 3$ we can apply (7.11) in a similar manner to obtain the result of the corollary. ■

References

[1] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.

[2] J. H. H. Chalk, *On Hua's estimate for exponential sums*, Mathematika 34 (1987), 115–123.

[3] T. Cochrane and Z. Y. Zheng, *Pure and mixed exponential sums*, Acta Arith. 91 (1999), 249–278.

[4] —, —, *Exponential sums with rational function entries*, ibid. 95 (2000), 67–95.

[5] —, —, *On upper bounds of Chalk and Hua for exponential sums*, Proc. Amer. Math. Soc. 129 (2001), 2505–2516.

[6] 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.

[7] P. Ding, *An improvement to Chalk's estimation of exponential sums*, ibid. 59 (1991), 149–155.

[8] —, *On a conjecture of Chalk*, J. Number Theory 65 (1997), 116–129.

[9] D. Ismoilov, *Estimate of a character sum of polynomials*, Dokl. Akad. Nauk Tadzhik. SSR 29 (1986), 567–571 (in Russian).

[10] —, *Estimate of a character sum of rational functions*, ibid., 635–639 (in Russian).

[11] —, *Estimates for character sums of polynomials and rational functions*, in: Construction Methods and Algorithms in Number Theory, Abstracts of Reports, Minsk, 1989, 62 (in Russian).

[12] —, *On lower bounds of character sums of rational functions with respect to a composite modulus*, Vestnik Tadzhik. Gos. Univ. Mat. 5 (1990), 27–32 (in Russian).

[13] —, *Lower bounds on character sums of polynomials with respect to a composite modulus*, Dokl. Akad. Nauk Tadzhik. SSR 33 (1990), 501–505 (in Russian).

[14] —, *Estimates of complete character sums of polynomials*, Trudy Mat. Inst. Steklov. 200 (1991), 171–186 (in Russian); English transl.: Proc. Steklov Inst. Math. 200 (1993), 189–203.

[15] —, *A lower bound estimate for complete sums of characters of polynomials and rational functions*, Acta Math. Sinica (N.S.) 9 (1993), 90–99.

[16] —, *Estimates for complete trigonometric sums*, Number Theory and Analysis, Trudy Mat. Inst. Steklov. 207 (1994), 153–171 (in Russian); English transl.: Proc. Steklov Inst. Math. 207 (1995), 137–153.

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

[18] C. L. Liu, *Character sums of rational functions*, Sci. China Ser. A 38 (1995), 182–187.

[19] —, *Dirichlet character sums*, Acta Arith. 88 (1999), 299–309.

[20] —, *Dirichlet character sums of rational functions*, preprint, 2000.

[21] W. K. A. Loh, *Hua's Lemma*, Bull. Austral. Math. Soc. 50 (1994), 451–458.

[22] J. H. Loxton and R. C. Vaughan, *The estimation of complete exponential sums*, Canad. Math. Bull. 28 (1985), 442–454.

[23] J.-L. Mauclaire, *Sommes de Gauss modulo* p^α *I*, Proc. Japan Acad. Ser. A 59 (1983), 109–112.

[24] —, *Sommes de Gauss modulo* p^α *II*, ibid., 161–163.

[25] R. Odoni, *On Gauss sums* $(\operatorname{mod} p^n)$, $n \geq 2$, Bull. London Math. Soc. 5 (1973), 325–327.

[26] G. I. Perelmuter, *Estimate of a sum along an algebraic curve*, Mat. Zametki 5 (1969), 373–380 (in Russian).

[27] A. G. Postnikov, *On a character sum modulo a prime power of a prime*, Izv. Akad. Nauk SSSR Ser. Mat. 19 (1955), 11–16 (in Russian).

[28] H. Salié, *Über die Kloostermanschen Summen* $S(u,v;q)$, Math. Z. 34 (1931), 91–109.

[29] W. M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Math. 536, Springer, Berlin, 1976.

[30] S. A. Stepanov, *Arithmetic of Algebraic Curves*, Monographs in Contemporary Mathematics, Consultants Bureau, New York, 1994.

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

Received on 26.10.2000 (3905)