ACTA ARITHMETICA
108.1 (2003)

Sparse polynomial exponential sums

by

TODD COCHRANE, CHRISTOPHER PINNER and
JASON ROSENHOUSE (Manhattan, KS)

1. Introduction. In this paper we estimate the complete exponential sum

$$S(f,q)=\sum_{x=1}^{q} e_q(f(x)), \tag{1.1}$$

where $e_q(\cdot)$ is the additive character $e_q(\cdot)=e^{2\pi i\cdot/q}$, and f is a sparse integer polynomial,

$$f(x)=a_1x^{k_1}+\ldots+a_rx^{k_r} \tag{1.2}$$

with $0<k_1<\ldots<k_r$. We always assume that the content of f, $(a_1,\ldots,a_r)$, is relatively prime to the modulus q. Let $d=d(f)=k_r$ denote the degree of f and for any prime p let $d_p(f)$ denote the degree of f read modulo p. A fundamental problem is to determine whether there exists an absolute constant C such that for an arbitrary positive integer q,

$$|S(f,q)|\le Cq^{1-1/d}, \tag{1.3}$$

if f is not a constant function modulo p for each prime $p\,|\,q$. It is well known that the exponent $1-1/d$ is best possible. For the case of Gauss sums ($r=1$) Shparlinski [26], [27] showed that one may take $C=1+O(d^{-1/4+\varepsilon})$ and this was sharpened to $C=1+O(d^{-1+\varepsilon})$ in his subsequent work with Konyagin [14, Theorem 6.7].

The best upper bounds available for general f are

$$|S(f,q)|\le e^{d+O(d/\log d)}q^{1-1/d},$$

due to Stechkin [29], and

$$|S(f,q)|\le e^{1.74d}q^{1-1/d},$$

2000 *Mathematics Subject Classification*: 11L07, 11L03.
Key words and phrases: exponential sums.
The research of the second author was supported in part by the National Science Foundation under grant EPS-9874732 and matching support from the State of Kansas.

due to Qi and Ding [25]; see also Chen [2], [3], Hua [11]–[13], Lu [17]–[19], Nechaev [20], [21], Nechaev and Topunov [22], Qi and Ding [23], [24] and Zhang and Hong [31]. These authors noted that in order to make any further improvement one must first obtain a nontrivial upper bound on the prime modulus exponential sum $|S(f,p)|$ for $p<(d-1)^2$, the interval where Weil's [30] bound $|S(f,p)|\le (d-1)\sqrt{p}$ is worse than the trivial bound. In [5] we obtained a bound of this type in terms of the number of terms r of $f(x)$. Using this bound we establish here

Theorem 1.1. *For any positive integer r there exists a constant $C(r)$ such that for any polynomial f of type* (1.2) *and positive integer q relatively prime to the content of f*,

$$|S(f,q)|\le C(r)q^{1-1/d}.$$

Although our proof yields $C(r)\le e^{O(r^4)}$, no attempt was made to obtain the best possible value for $C(r)$.

For prime power moduli one can replace $C(r)$ with an absolute constant as shown by Stechkin [29] and Cochrane and Zheng [8], the latter result being

Lemma 1.1 [8, Theorem 1.1]. *Let f be a polynomial over $\mathbb{Z}$ of degree d and p a prime with $d_p(f)\ge 1$. Then for any $m\ge 1$*,

$$|S(f,p^m)|\le 4.41p^{m(1-1/d)}. \tag{1.4}$$

It is also well known (see [20], [3] or [8]) that for $p\ge (d-1)^{2d/(d-2)}$ and $m\ge 1$,

$$|S(f,p^m)|\le p^{m(1-1/d)}. \tag{1.5}$$

The significance of the constant one in (1.5) lies in the fact that bounds for exponential sums modulo prime powers lead to bounds for a general modulus $q=\prod_{i=1}^k p_i^{e_i}$ via the multiplicative formula

$$S(f,q)=\prod_{i=1}^{k} S(\lambda_i f,p_i^{e_i}), \tag{1.6}$$

where the λ_i are such that $\sum_{i=1}^k \lambda_i q/p_i^{e_i}=1$. Thus if (1.5) holds for all prime power divisors of q then it follows that $|S(f,q)|\le q^{1-1/d}$. It is desirable to extend the inequality in (1.5) to an interval of the type $p>Cd$ for some constant C.

In closing we note that for sums over reduced residue systems,

$$S^*(f,q)=\sum_{x=1,\,(x,q)=1}^{q} e_q(f(x)), \tag{1.7}$$

the exponent in the upper bound can be dramatically reduced. Shparlinski [28] showed that

$$|S^*(f,q)| \le C(d,\varepsilon)q^{1-1/r+\varepsilon},$$

for any sparse polynomial in r terms with content relatively prime to q. Loh [16] obtained a related upper bound but an error in his Lemma 3 leaves his results in doubt.

2. The method of recursion. A standard method for bounding exponential sums modulo prime powers is the method of recursion, also known as the method of critical points. For any polynomial f let $t = t_p(f) = \mathrm{ord}_p(f')$ be the largest power of p dividing all of the coefficients of f', $d_1 = d_p(p^{-t}f')$, and let $\mathcal{A} = \mathcal{A}(f,p)$ be the set of zeros of the congruence $p^{-t}f'(x) \equiv 0 \pmod p$. $\mathcal{A}$ is called the *set of critical points* associated with the sum $S(f,p^m)$, for any $m \ge 2$. Write

$$S(f,p^m) = \sum_{\alpha=0}^{p-1} S_\alpha(f,p^m)$$

with

$$S_\alpha(f,p^m) = \sum_{x\equiv\alpha \,(\mathrm{mod}\, p)} e_{p^m}(f(x)).$$

A fact of central importance is that if m is sufficiently large then $S_\alpha(f,p^m) = 0$ unless α is a critical point.

LEMMA 2.1 [6, Proposition 4.1]. *Suppose that p is an odd prime and $m \ge t+2$, or $p = 2$ and $m \ge t+3$, or $p = 2$, $t = 0$ and $m = 2$. Then if α is not a critical point, $S_\alpha(f,p^m) = 0$. Consequently,*

$$S(f,p^m) = \sum_{\alpha\in\mathcal{A}} S_\alpha(f,p^m).$$

For any $\alpha \in \mathcal{A}$ define

$$\sigma = \sigma_\alpha := \mathrm{ord}_p(f(px+\alpha) - f(\alpha)),$$
$$g_\alpha(x) := p^{-\sigma}(f(px+\alpha) - f(\alpha)). \tag{2.1}$$

LEMMA 2.2 [6, Proposition 4.1] (The recursion relationship). *Suppose that p is an odd prime and $m \ge t+2$, or $p = 2$ and $m \ge t+3$, or $p = 2$, $t = 0$ and $m = 2$. Then if $\alpha \in \mathcal{A}$,*

$$S_\alpha(f,p^m) = e_{p^m}(f(\alpha))p^{\sigma-1}S(g_\alpha,p^{m-\sigma}), \tag{2.2}$$

where

$$S(g_\alpha,p^{m-\sigma}) = \begin{cases} \sum_{x=1}^{p^{m-\sigma}} e_{p^{m-\sigma}}(g_\alpha(x)) & \text{if } m > \sigma, \\ p^{m-\sigma} & \text{if } m \le \sigma. \end{cases} \tag{2.3}$$

Under the hypotheses of the lemma we have

$$|S(f,p^m)| \le \sum_{\alpha\in\mathcal{A}} |S_\alpha(f,p^m)| = \sum_{\alpha\in\mathcal{A}} p^{\sigma_\alpha-1}|S(g_\alpha,p^{m-\sigma_\alpha})|. \tag{2.4}$$

In particular, since there are at most d_1 critical points we immediately have the upper bound

$$|S(f,p^m)| \le d_1 p^{m-1}. \tag{2.5}$$

In [8] we established the following bounds for $S_\alpha(f,p^m)$ and $S(f,p^m)$:

LEMMA 2.3 [8, Theorem 2.1]. *Let f be a polynomial over $\mathbb{Z}$ and p a prime with $d_p(f) \ge 1$. Suppose that p is odd and $m \ge t+2$, or $p=2$ and $m \ge t+3$. Set $\lambda = (5/4)^5 \approx 3.05$ and $d_1 = d_p(p^{-t}f')$. Then*

(i) *For any critical point α of multiplicity ν we have*

$$|S_\alpha(f,p^m)| \le \min\{\nu,\lambda\} p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}, \tag{2.6}$$

with equality if $\nu = 1$.

(ii) $|S(f,p^m)| \le \lambda p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}$.

Related results using the method of critical points were obtained by Chalk [1], Cochrane [4], Cochrane and Zheng [6], [7], Ding [9], [10], and Loh [15].

For any critical point α set

$$\tau := \mathrm{ord}_p(g'_\alpha(x)), \qquad g_1(x) := p^{-\tau} g'_\alpha(x). \tag{2.7}$$

The following relations are well known (see e.g. [6, Lemma 3.1]) and play a central role in the proof of the preceding lemma.

LEMMA 2.4.

$$\sigma \ge \begin{cases} t+2 & \text{if } p \text{ is odd or } \nu > 1, \\ t+1 & \text{if } p = 2 \text{ and } \nu = 1. \end{cases} \tag{2.8}$$

$$\sigma \le \nu + 1 + t - \tau. \tag{2.9}$$

$$d_p(g_\alpha) \le \begin{cases} \sigma - t + \mathrm{ord}_p(d_p(g_\alpha)) \le \nu + 1 + \mathrm{ord}_p(d_p(g_\alpha)), \\ \sigma \le \nu + 1 + t - \tau. \end{cases} \tag{2.10}$$

$$d_p(g_1) \le \sigma + \tau - t - 1 \le \nu. \tag{2.11}$$

$$p^\tau \mid d_p(g_\alpha). \tag{2.12}$$

An immediate consequence that we frequently make reference to is

LEMMA 2.5. *Suppose that α is a critical point of multiplicity ν with $\nu \ge 2$ and $p > \nu + 2$. Then $d_p(g_\alpha) \le \nu + 1$.*

Proof. Let $d_p = d_p(g_\alpha)$. Suppose that $\mathrm{ord}_p(d_p) \ge 1$. If $d_p = p$ then by (2.10) we have $p = d_p \le \nu + 2$ contradicting our assumption. Otherwise $d_p \ge 2p$ and we have $p \le d_p/2 \le d_p - \mathrm{ord}_p(d_p) \le \nu + 1$, again a contradiction. Thus $p \nmid d_p$ and we obtain (by (2.10)) $d_p \le \nu + 1$. ∎

3. Preliminary upper bounds. We begin with a couple of auxiliary lemmas.

LEMMA 3.1. *Define* $\lambda_i = i$ *for* $i = 1, 2, 3$ *and* $\lambda_i = \lambda$ *for* $i \geq 4$, *where* $\lambda = (5/4)^5 \approx 3.05$. *Then for* $1 \leq i \leq d$ *we have*

$$d\lambda_i \lambda^{(i-d)/(i+1)} \leq i\lambda.$$

Proof. For any fixed $i \geq 1$ the function $f_i(x) := (\lambda_i/i)x\lambda^{(i-x)/(i+1)}$ attains its maximum value at $x = (i+1)/\log(\lambda) < i+1$, and is decreasing for larger values of x. Thus for $d \geq i$, the maximum value of $f_i(d)$ occurs at $d = i$ or $d = i+1$. Now, $f_i(i) = \lambda_i \leq \lambda$ and $f_i(i+1) = \lambda_i(1+1/i)\lambda^{-1/(i+1)} \leq \lambda$, as can be seen by considering the different cases $i = 1, 2, 3$ and $i \geq 4$. ∎

LEMMA 3.2. *If* $p > cd_1$ *for some constant* c *then for* $1 \leq i \leq d_1 - 1$ *we have*

$$(4p/(cd_1))^{(i-d_1)/(i+1)} \leq i/d_1.$$

Proof. We first note that

$$(d_1/i)^{(i+1)/(d_1-i)} \leq 4 \quad \text{for } 1 \leq i \leq d_1 - 1.$$

This can be checked directly for $i = 1, 2, 3$. For $i \geq 4$ it follows from Lemma 3.1. Then $p > cd_1 \geq (c/4)d_1(d_1/i)^{(i+1)/(d_1-i)}$ and the result follows. ∎

LEMMA 3.3. *Let* p *be a prime and* f *be any integer polynomial with* $t = 0$ *and either* $d_1 = 0, 1$ *or* $p > d_1^{2+4/(d_1-1)}$ *where* $d_1 = d_p(p^{-t}f')$. *Then for* $m \geq 2$,

$$|S(f, p^m)| \leq p^{m(1-1/(d_1+1))}. \tag{3.1}$$

Proof. If $d_1 = 0$ then there are no critical points and the sum is zero. If $d_1 = 1$ then there is a single critical point of multiplicity one and the result follows from Lemma 2.3(i). Suppose that $d_1 \geq 2$. Let $\mathcal{A} = \mathcal{A}(f, p) \subset \mathbb{F}_p$ be the set of critical points. We prove by induction on m that, under the hypotheses of the theorem,

$$|S_\alpha| \leq p^{m(1-1/(\nu+1))} \tag{3.2}$$

for any critical point $\alpha \in \mathcal{A}$. We first note that (3.1) is an immediate consequence of (3.2). Indeed, if $p^m \leq (p/d_1)^{d_1+1}$ then using the trivial upper bound $|S_\alpha(f, p^m)| \leq p^{m-1}$ we have $|S(f, p^m)| \leq \sum_{\alpha \in \mathcal{A}} |S_\alpha(f, p^m)| \leq d_1 p^{m-1} \leq p^{m(1-1/(d_1+1))}$. Next, if there is a critical point α of multiplicity d_1 then it is the only critical point and we have $|S(f, p^m)| = |S_\alpha(f, p^m)| \leq p^{m(1-1/(d_1+1))}$.

Finally, suppose that $p^m > (p/d_1)^{d_1+1}$ and that every critical point is of multiplicity less than d_1. Letting n_i denote the number of critical points of multiplicity i we deduce from (3.2) that

$$(3.3)\qquad |S(f,p^m)| \le \sum_{\alpha\in\mathcal{A}} |S_\alpha(f,p^m)| \le \sum_{i=1}^{d_1-1} n_i p^{m(1-1/(i+1))} = p^{m(1-1/(d_1+1))}\Big(\sum_{i=1}^{d_1-1} n_i p^{m(i-d_1)/((i+1)(d_1+1))}\Big).$$

Then from $p^m > (p/d_1)^{d_1+1}$, $p > 4d_1$ and Lemma 3.2 with $c = 4$ we obtain

$$(3.4)\qquad |S(f,p^m)| \le p^{m(1-1/(d_1+1))}\Big(\sum_{i=1}^{d_1-1} n_i (p/d_1)^{(i-d_1)/(i+1)}\Big) \le \Big(\sum_{i=1}^{d_1-1} n_i i/d_1\Big) p^{m(1-1/(d_1+1))} \le p^{m(1-1/(d_1+1))}.$$

We now proceed to establish (3.2). If $\nu = 1$ then by Lemma 2.3 we have equality in (3.2). So we may assume that $\nu \ge 2$. When $m = 2$ the bound is trivial, $|S_\alpha| \le p \le p^{2(1-1/(\nu+1))}$. Suppose $m \ge 3$. If $\sigma \ge m$ then the result follows trivially,

$$|S_\alpha| \le p^{m-1} \le p^{m(1-1/(\nu+1))} p^{(\sigma-\nu-1)/(\nu+1)} \le p^{m(1-1/(\nu+1))},$$

the latter inequality following from (2.9). Suppose next that $\sigma = m-1$. Put $d_p = d_p(g_\alpha)$. Since $p > d_1^2 \ge \nu^2 \ge \nu + 2$ it follows from Lemma 2.5 that $d_p \le \nu + 1 \le d_1 + 1$. If $d_p \ge 3$ then $p \ge (d_p - 1)^{2+4/(d_p-2)}$, so by the Weil bound, $|S(g_\alpha, p)| \le (d_p - 1)\sqrt{p} \le p^{1-1/d_p} \le p^{1-1/(\nu+1)}$. If $d_p = 1$ or 2 the same bound is elementary. It follows from the recursion formula of Lemma 2.2 that

$$|S_\alpha| = p^{\sigma-1}|S(g_\alpha,p)| \le p^{m-1-1/(\nu+1)} = p^{(\sigma-\nu-1)/(\nu+1)} p^{m(1-1/(\nu+1))} \le p^{m(1-1/(\nu+1))}.$$

Suppose finally that $m \ge \sigma + 2$. We note that $\tau = 0$ since by (2.12), $p^\tau \le d_p(g_\alpha) \le \nu+1 \le d_1+1 < p$, and so we can apply the induction assumption to $S(g_\alpha, p^{m-\sigma})$. Putting $d_2 = d_p(g'_\alpha) \le \nu \le d_1$ and noting that either $d_2 = 0, 1$ or $p \ge d_2^{2+2/(d_2-1)}$ we obtain

$$|S_\alpha| = p^{\sigma-1}|S(g_\alpha, p^{m-\sigma})| \le p^{\sigma-1} p^{(m-\sigma)(1-1/(d_2+1))} \le p^{\sigma-1} p^{(m-\sigma)(1-1/(\nu+1))} \le p^{m(1-1/(\nu+1))}. \ \blacksquare$$

4. Multiplicity estimates. Next, we obtain an upper bound on the multiplicity of a nonzero zero of a sparse polynomial

$$f(x) = a_1 x^{k_1} + \ldots + a_r x^{k_r} \pmod p.$$

Let $a \not\equiv 0 \pmod p$ be a zero of multiplicity $\nu \pmod p$, that is,

$$(x-a)^\nu \parallel f(x) \pmod p.$$

For $1 \le i \le r$ let

$$S(i,\alpha) = \{k_j : k_j \equiv k_i \pmod{p^\alpha}\},$$

and set

$$\alpha_i = \max\{\alpha : |S(i,\alpha)| \ge 2\}, \tag{4.1}$$

$$r_i = |S(i,\alpha_i)|. \tag{4.2}$$

LEMMA 4.1. *The multiplicity ν of any nonzero zero of $f(x) \pmod p$ satisfies $\nu < \min_i r_i p^{\alpha_i}$. In particular, if p does not divide any $k_i - k_j$ with $i \ne j$ then $\nu < r$.*

Lemma 4.1 follows from the more precise

LEMMA 4.2. *Suppose that $k_1, \dots, k_t$ are the smallest distinct exponents modulo p so that*

$$f(x) = x^{k_1} f_1(x)^p + \dots + x^{k_t} f_t(x)^p \pmod p,$$

where

$$f_i(x) = \sum_{k_j = k_i + l_j p} a_j x^{l_j}.$$

Then if $f(x)$ has a nonzero zero a of multiplicity $\nu \pmod p$, we have

$$\nu = kp + u$$

where $u < t$ and $(x-a)^k$ is the highest power dividing all the $f_1, \dots, f_t$.

Proof. Suppose that $(x-a)^k \mid f_1, \dots, f_t$ with $(x-a)^{k+1} \nmid f_1$, and write $f_i(x) = (x-a)^k g_i(x) \pmod p$, $\nu = kp + u$, so that

$$(x-a)^u \parallel g(x) = x^{k_1} g_1(x)^p + \dots + x^{k_t} g_t(x)^p.$$

Writing $\nabla = x\frac{d}{dx}$ we must have $\nabla^i g(a) \equiv 0 \pmod p$ for $j = 0, \dots, u-1$. That is,

$$k_1^j a^{k_1} g_1(a)^p + \dots + k_t^j a^{k_t} g_t(a)^p \equiv 0 \pmod p$$

for $j = 0, \dots, u-1$. Since $|\det(k_i^j)_{i=1,\dots,t,\, j=0,\dots,t-1}| = \prod |k_i - k_j| \not\equiv 0 \pmod p$ and $a^{k_1} g_1(a)^p \not\equiv 0 \pmod p$ we must therefore have $u < t$. ∎

Proof of Lemma 4.1. Pick an arbitrary k_i, $i = 1, \dots, t$, and use the preceding lemma and induction on α_i: If $\alpha_i = 0$ then plainly $k = 0$ and $\nu = u < t \le r = r_i$. If $\alpha_i \ge 1$ then since $(x-a)^k \mid f_i(x)$ we have (by induction) $k < r_i p^{\alpha_i - 1}$ and $u < p$ giving

$$\nu = pk + u \le (r_i p^{\alpha_i - 1} - 1)p + (p-1) < r_i p^{\alpha_i}. \ ∎$$

In practice we apply the multiplicity estimate to the polynomial $p^{-t} f'(x)$ and so we let $r_1 = r_1(f,p)$ be the number of nonzero terms modulo p of the polynomial $p^{-t} f'(x)$. For critical points having multiplicity less than r_1 we have the following upper bound.

Lemma 4.3. *Let f be a sparse polynomial as in* (1.2) *and suppose that either $r_1 = 1, 2$ or $p > (r_1 - 1)^{2r_1/(r_1-2)}$. Then if $m \geq t + 2$ and α is a critical point of multiplicity $\nu < r_1$ we have*

$$(4.3) \qquad |S_\alpha| \leq p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}.$$

Proof. If $\nu = 1$ the result follows from Lemma 2.3, and so we may assume $\nu \geq 2$ and $r_1 \geq 3$. Let $d_p = d_p(g_\alpha)$. Since $p > \nu^{2+4/(\nu-1)}$, we get $d_p \leq \nu + 1$ by Lemma 2.5, and thus $p > (d_p - 1)^{2d_p/(d_p-2)}$. Also, since $p^\tau \leq d_p(g_\alpha) \leq \nu + 1 \leq r_1 + 1 < p$ we must have $\tau = 0$.

If $\sigma \geq m$ the result follows trivially,

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

Suppose next that $\sigma = m - 1$. Then applying the bound in (1.5) to $S(g_\alpha, p)$, we obtain

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

Finally, if $\sigma \leq m - 2$ then we can apply Lemma 3.3 to $S(g_\alpha, p^{m-\sigma})$, since $d_2 := d_p(g'_\alpha) \leq \nu < r_1$ and so $p \geq d_2^{2+4/(d_2-1)}$. We obtain

$$\begin{aligned} |S_\alpha| &\leq p^{\sigma-1} |S(g_\alpha, p^{m-\sigma})| \\ &\leq p^{\sigma-1} p^{(m-\sigma)(1-1/(d_2+1))} = p^{(\sigma-\nu-1)/(\nu+1)} p^{m(1-1/(\nu+1))}. \ \blacksquare \end{aligned}$$

5. Bounds for exponential sums with p small relative to d. First we consider sums modulo p. From the bound of Weil, one deduces (see [8, Lemma 3.1]) the upper bound

$$(5.1) \qquad |S(f, p)| \leq 1.75 p^{1-1/d}$$

for any polynomial f with $d_p(f) \geq 1$. Moreover the constant 1.75 may be replaced by 1 provided $p \gg d^2$. For our purposes here we need the constant 1 for $p \gg d$. We obtain this from the following result established in the authors' work [5, Corollary 1.1].

Lemma 5.1. *Let f be an integer polynomial of degree d as in* (1.2). *Then for any $\delta > 0$, if $p > (9/\delta^{1.06})d$ and $p > C_1(\delta)$, then*

$$(5.2) \qquad \Big| \sum_{x=1}^{p} e_p(f(x)) \Big| \leq p\left(1 - \frac{1}{rp^\delta}\right).$$

Lemma 5.2. *Let f be a polynomial as in* (1.2) *of degree $d = d_p(f) \geq 1$* $(\mathrm{mod}\, p)$ *and suppose that $p > C_2$ (an absolute constant), $p > 50d$ and $p > r^4$. Then*

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

Proof. The result is elementary for $d = 1, 2$ and so we assume $d > 2$. If $p > 16d^2$ then the result follows from the Weil bound $|S(f, p)| \leq (d - 1)\sqrt{p}$.

Suppose that $p \le 16d^2$. Applying Lemma 5.1 with $\delta = 1/5$ we deduce that if $p > 50d$ and $p > C_1(1/5)$ then $|S(f,p)| \le p(1 - 1/(rp^{1/5}))$. Since $p > r^4$ it follows that $|S(f,p)| \le p(1 - 1/p^{9/20})$, and since $p \le 16d^2$ the latter is $\le p^{1-1/d}$ for $p > 10^{60}$. ∎

LEMMA 5.3. *Let f be a sparse polynomial as in* (1.2) *with* $p \ge 50(d_1+1)$, $p > C_2$ (*the constant in Lemma* 5.2), $p > r^4$ *and* $m \ge t+2$. *Then for any critical point α of multiplicity ν we have*

$$|S_\alpha| \le p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}, \tag{5.3}$$

and

$$|S(f,p^m)| \le p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}. \tag{5.4}$$

Proof. We first observe that (5.4) is always an immediate consequence of (5.3). Indeed, if $p^{m-t} \le (p/d_1)^{d_1+1}$ then using the trivial upper bound $|S_\alpha(f,p^m)| \le p^{m-1}$ we have $|S(f,p^m)| \le \sum_{\alpha\in\mathcal{A}} |S_\alpha(f,p^m)| \le d_1 p^{m-1} \le p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}$. Next, if there is a critical point α of multiplicity d_1 then it is the only critical point and we have $|S(f,p^m)| = |S_\alpha(f,p^m)| \le p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}$.

Finally, suppose that $p^{m-t} > (p/d_1)^{d_1+1}$ and that every critical point is of multiplicity less than d_1. Letting n_i denote the number of critical points of multiplicity i we deduce from (5.3) that

$$\begin{aligned}|S(f,p^m)| &\le \sum_{i=1}^{d_1} n_i p^{t/(i+1)} p^{m(1-1/(i+1))}\\ &\le p^{t/(d_1+1)} p^{m(1-1/(d_1+1))} \sum_i n_i p^{(m-t)(i-d_1)/((i+1)(d_1+i))}\\ &\le p^{t/(d_1+1)} p^{m(1-1/(d_1+1))} \sum_i n_i (p/d_1)^{(i-d_1)/(i+1)}\\ &\le p^{t/(d_1+1)} p^{m(1-1/(d_1+1))},\end{aligned}$$

the last inequality following from Lemma 3.2 (with $c = 4$) and $\sum_i n_i i \le d_1$.

We now establish (5.3) by induction on m. The result is trivial if $m = 2$. Suppose that $m > 2$. If $\sigma \ge m$ then from (2.9),

$$|S_\alpha| \le p^{m-1} \le p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}.$$

If $\sigma = m-1$ and $\alpha \ne 0$ then since $p > d_1$ it follows from Lemma 4.1 that $\nu < r$. Also, since $p \ge 50d_1 \ge 50\nu$ we see by Lemma 2.5 that

$$d_p(g) \le \nu + 1 \le r < p^{1/4},$$

and so by (1.5), $|S(g_\alpha,p)| \le p^{1-1/d_p(g)} \le p^{1-1/(\nu+1)}$. It then follows from the recursion relation that

$$|S_\alpha| \le p^{\sigma-1} |S(g_\alpha,p)| \le p^{\sigma-1/(\nu+1)} \le p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}, \tag{5.5}$$

by (2.9). If $\alpha = 0$ then we have to argue differently since the multiplicity may be larger than r. In this case $g_\alpha(x) = f(px)$ is a sparse polynomial with the same number of terms as f. Since $p > 50(d_1+1) \ge 50(\nu+1) \ge 50d_p(g_\alpha)$ we can apply Lemma 5.2 to obtain $|S(g_\alpha, p)| \le p^{1-1/d_p(g_\alpha)}$, and the result follows as before.

Suppose now that $\sigma \le m-2$. We first note that by (2.12), $\tau = 0$ since $p > d_p(g_\alpha)$. Set $d_2 = d_p(g'_\alpha)$. If $\alpha \ne 0$ then by (2.11) and Lemma 4.1, $d_2 \le \nu < r < p^{1/4}$. Thus by Lemma 3.3,

$$|S(g_\alpha, p^{m-\sigma})| \le p^{(m-\sigma)(1-1/(d_2+1))}.$$

If $\alpha = 0$ then we can apply the induction assumption to the polynomial $g_\alpha = p^{-\sigma} f(px)$ and obtain the same bound. From the recursion relationship we then obtain

$$\begin{aligned}|S(f,p^m)| &\le p^{\sigma-1} p^{(m-\sigma)(1-1/(d_2+1))}\\ &\le p^{-1+\sigma/(\nu+1)} p^{m(1-1/(\nu+1))} \le p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}. \ \blacksquare\end{aligned}$$

Next we obtain a bound valid for even smaller values of p. Again, let d_1 and $r_1 = r_1(f,p)$ be the degree and number of nonzero terms of the polynomial $p^{-t} f'(x)$ read modulo p.

LEMMA 5.4. *Let f be a sparse polynomial in r terms and p a prime with $p > r^4$, $p > C_3$ and such that $p \nmid (k_j - k_i)$ for all $k_i < k_j \le d_1$. Then for $m \ge t+2$ and any critical point α of multiplicity ν we have*

(i) *If $\alpha \ne 0$ then* $|S_\alpha(f,p^m)| \le p^{t/(\nu+1)} p^{m(1-1/(\nu+1))}$.

(ii) *For $\alpha = 0$,* $|S_0(f,p^m)| \le p^{(2r+t)/(\nu+1)} p^{m(1-1/(\nu+1))}$.

(iii) $|S(f,p^m)| \le p^{(2r+t)/(d_1+1)} p^{m(1-1/(d_1+1))}$.

Proof. We take $C_3 = \max\{C_2, 200\}$ where C_2 is the constant in Lemma 5.3. The condition $p \nmid (k_i - k_j)$ implies (by Lemma 4.1) that $\nu < r_1$ for any nonzero critical point. So (i) is implied by Lemma 4.3. If $p \ge 50(d_1+1)$ then the lemma is implied by Lemma 5.3 and so we may assume $p < 50(d_1+1)$. In particular, it follows that $r \le d_1$ (if $r \ge 4$ then $r^4 < p < 50(d_1+1)$ implies $r < r \cdot r^3/50 < d_1 + 1$; if $r \le 3$ then $p > 200$ implies $d_1 > 3 \ge r$).

The proof of (ii) is by induction on m, but first we show that (i) and (ii) together imply (iii). If zero is the only critical point then (ii) immediately implies (iii) and so we assume henceforth that $r \ge 2$ and that $\nu(0) < d_1$.

If $m-t \le 2r$ then the upper bound in (iii) follows from the trivial bound $|S(f,p^m)| \le p^m$. Next write $m-t = 2r+1+j$ with $j \ge 0$ and set

$$\Delta = p^{(t+2r)/(d_1+1)} p^{m(1-1/(d_1+1))},$$

the desired bound. We have

$$|S(f,p^m)| \le |S_0(f,p^m)| + \sum_{\alpha \ne 0} |S_\alpha(f,p^m)|.$$

For the first term we have the trivial bound

$$|S_0(f,p^m)| \le p^{m-1} = p^{(j-d_1)/(d_1+1)}\Delta. \tag{5.6}$$

Now there are at most $p-1$ nonzero critical points, each of multiplicity $\le r_1 - 1 \le r-1$, and so by (i),

$$\sum_{\alpha\neq 0} |S_\alpha(f,p^m)| \le p\cdot p^{t/r}p^{m(1-1/r)} \tag{5.7}$$
$$= p^{(j(r-d_1-1)-rd_1-d_1-1)/((d_1+1)r)}\Delta = p^{(j-d_1)/(d_1+1)-(1+j)/r}\Delta.$$

Combining (5.6) and (5.7) we have, for $j \le d_1/2$,

$$|S(f,p^m)| \le p^{-d_1/(2(d_1+1))}(1+p^{-1/r})\Delta < 2p^{-1/4}\Delta < \Delta,$$

and for $d_1 > j > d_1/2$,

$$|S(f,p^m)| \le (p^{-d_1/(2r)}+1)p^{-1/(d_1+1)}\Delta \le (r^{-2d_1/r}+1)r^{-4/(d_1+1)}\Delta < \Delta.$$

If $j \ge d_1$ then by the bound in (ii) (replacing ν with $d_1 - 1$) we obtain

$$|S_0(f,p^m)| \le p^{(-j-1)/(d_1(d_1+1))}\Delta \le p^{-1/d_1}\Delta.$$

For the remaining critical points we use the upper bound of (5.7) replacing j with d_1. Thus

$$|S(f,p^m)| \le (p^{-1/d_1} + p^{(-d_1-1)/r})\Delta \le (r^{-4/d_1} + r^{-4(d_1+1)/r})\Delta < \Delta.$$

We return to the task of proving (ii) by induction on m. The bound follows trivially from $|S_0(f,p^m)| \le p^{m-1}$ if $m \le \nu+1+t+2r$, and so we assume $m \ge \nu+2+t+2r$. By (2.9) we have

$$m-\sigma \ge \nu+2+t+2r-(\nu+1+t-\tau) = 1+2r+\tau \ge \tau+2,$$

and by the recursion formula of Lemma 2.2, $|S_0(f,p^m)| = p^{\sigma-1}|S(g_0,p^{m-\sigma})|$, where $g_0(x) = p^{-\sigma}f(px)$. Since g_0 has the same degree monomials as f we can apply the induction assumption to g_0 and obtain,

$$|S_0(f,p^m)| \le p^{\sigma-1}p^{(\tau+2r)/(d_2+1)}p^{(m-\sigma)(1-1/(d_2+1))},$$

where $d_2 := d_p(p^{-\tau}g_0) \le d_1$. Now by (2.11), $d_2 \le \nu$ and so replacing d_2 by ν in the previous inequality and using the upper bound in (2.9) we deduce the inequality in (ii). ∎

6. Dealing with the primes that divide $k_i - k_j$ for some $i \neq j$.

If $p \mid (k_j - k_i)$ for some $k_i < k_j \le d_1$ then there may be nonzero critical points of multiplicity exceeding r and so we have to argue more carefully. Let $f(x)$ be a sparse polynomial as in (1.2) of degree d and set $d_1 = d_p(p^{-t}f'(x))$. For any pair (i,j) with $1 \le i < j \le r$ let p_{ij} be the maximal prime divisor of $k_j - k_i$ (taking $p_{ij} = 1$ in case $k_j - k_i = 1$) and put

$$\mathcal{P} = \{p_{ij} : 1 \le i < j \le r\}. \tag{6.1}$$

Assume now that $p > 4r$, $p \mid (k_j - k_i)$ for some $k_i < k_j \le d_1$ but that $p \notin \mathcal{P}$. Let

$$p_{ls} = \min\{p_{ij} : p \mid (k_j - k_i),\ k_i < k_j \le d_1\},$$

and define

$$M := rd_1/p_{ls}.$$

Then if $p^e \parallel (k_j - k_i)$ is the maximum power of p dividing any of the differences $k_j - k_i$ that actually occur in the critical point congruence for $S(f, p^m)$, it follows from Lemma 4.1 that the multiplicity ν of any nonzero critical point satisfies

$$\nu < rp^e \le r(k_j - k_i)/p_{ij} \le M. \tag{6.2}$$

Let $S^*(f, p^m)$ denote the sum over a reduced residue system (modulo p^m) as in (1.7). For $j \ge 0$ define μ_j, t_j by

$$p^{\mu_j} \parallel (a_1 p^{jk_1}, \ldots, a_r p^{jk_r}), \qquad p^{\mu_j + t_j} \parallel (a_1 k_1 p^{jk_1}, \ldots, a_r k_r p^{jk_r}). \tag{6.3}$$

Then we can write

$$S(f, p^m) = \sum_{j=0}^{m} S^*(f(p^j x), p^{m-j}) = \sum_{j=0}^{m} p^{\mu_j - j} S_j^*, \tag{6.4}$$

where for $0 \le j \le m$,

$$S_j^* = S^*(p^{-\mu_j} f(p^j x), p^{m-\mu_j}). \tag{6.5}$$

The critical point congruence associated with the sum S_j^* is just

$$g_j(x) := p^{-\mu_j - t_j}(a_1 k_1 p^{jk_1} x^{k_1 - 1} + \ldots + a_r k_r p^{jk_r} x^{k_r - 1}) \equiv 0 \pmod{p}.$$

Viewing $g_j(x)$ as a polynomial over $\mathbb{F}_p$ we observe that for any $j < m$ the largest degree term of $g_{j+1}(x)$ is at most the smallest degree term of $g_j(x)$. Indeed, if $p^{t_j + \mu_j} \parallel a_I k_I p^{jk_I}$ then $p^{t_j + \mu_j + k_I} \parallel a_I k_I p^{(j+1)k_I}$ and $p^{t_j + \mu_j + k_I + 1} \parallel a_l k_l p^{(j+1)k_l}$ for $l > I$. It follows that the degrees of the g_j are nonincreasing (with j) and that at most r of the $g_j(x)$ can have more than one nonzero term. The rest of the $g_j(x)$ are monomials and therefore the associated sums S_j^* are zero, provided $m - \mu_j \ge 2$. Thus there are at most r values of $j \le m$ for which $m - \mu_j \ge 2$ and S_j^* is nonzero. Moreover, for these nonzero sums the multiplicity of any nonzero critical point is bounded above by M.

Say $d_1 = k_I - 1$ for some I. Then since $p^t \parallel a_I k_I$ it is easily seen that for $0 \le j \le m$,

$$\mu_j + t_j \le t + j(d_1 + 1). \tag{6.6}$$

We split the sum in (6.4) into two parts according as $m - t_j - \mu_j \ge 8M$ or not. If this inequality holds then since S_j^* has at most p critical points, each of multiplicity $\le M$, it follows from Lemma 2.3 that

$$p^{\mu_j - j}|S_j^*| \le p^{\mu_j - j} 4pp^{t_j/M} p^{(m-\mu_j)(1-1/M)} = \frac{4p}{p^{(m-\mu_j-t_j)/(2M)}} \frac{p^{m-j}}{p^{(m-\mu_j-t_j)/(2M)}}.$$

Now $(m - \mu_j - t_j)/(2M) \ge 4$. Also, since $p > 2r$, $2M < d_1$ and so by (6.6),

$$\frac{m - \mu_j - t_j}{2M} \ge \frac{m - t - j(d_1+1)}{d_1+1} = \frac{m-t}{d_1+1} - j.$$

It follows that

$$p^{\mu_j - 1}|S_j^*| \le \frac{4}{p^3}\, p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}. \tag{6.7}$$

We consider next the set of j for which $m - t_j - \mu_j < 8M$ and let j_0 denote the least such j. Then

$$\sum_{j \ge j_0} p^{\mu_j - j}|S_j^*| \le p^{m - j_0} = p^{(m-t)/(d_1+1) - j_0} p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}.$$

Now

$$(m-t) - j_0(d_1+1) \le 8M + t_{j_0} + \mu_{j_0} - t - j_0(d_1+1) \le 8M = 8rd_1/p_{ls},$$

by (6.6). Thus

$$\sum_{j \ge j_0} p^{\mu_j - j}|S_j^*| \le p^{8r/p_{ls}} p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}. \tag{6.8}$$

From (6.7) and (6.8) we conclude that

$$\begin{aligned}|S(f,p^m)| &\le (4r/p^3 + p^{8r/p_{ls}}) p^{t/(d_1+1)} p^{m(1-1/(d_1+1))} \\ &\le p^{8r/p_{ls}}(1 + 1/p^2) p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}.\end{aligned}$$

This establishes

Lemma 6.1. *Suppose that $p \,|\, (k_j - k_i)$ for some $k_i < k_j \le d_1$, $p > 4r$ and $p \notin \mathcal{P}$. Then*

$$|S(f,p^m)| \le (1 + 1/p^2) p^{8r/p_{ls}} p^{t/(d_1+1)} p^{m(1-1/(d_1+1))}$$

for some $p_{ls} \in \mathcal{P}$ with $p \,|\, (k_l - k_s)$, $p < p_{ls}$.

7. Proof of Theorem 1.1. For any prime power p^m and polynomial f let

$$R(f,p^m) = \frac{|S(f,p^m)|}{p^{m(1-1/d)}}. \tag{7.1}$$

Let f be a sparse polynomial with r terms and let q be a positive integer such that $d_p(f) \ge 1$ for all prime divisors p of q. Write

$$\prod_{p^m \,\|\, q} R(f,p^m) = P_1 P_2 P_3 P_4 P_5 P_6$$

where the P_i are products over the prime power divisors of q satisfying the following constraints (counting prime powers only once if they happen to satisfy more than one constraint):

$$P_1 = \prod_{m=1} R(f,p^m), \tag{7.2}$$

$$P_2 = \prod_{1<m\le t+1} R(f,p^m), \tag{7.3}$$

$$P_3 = \prod_{\substack{p\le C_3 \text{ or} \\ p\le r^4 \text{ or } p\in\mathcal{P}}} R(f,p^m), \tag{7.4}$$

$$P_4 = \prod_{\substack{p>r^4 \\ p\mid(k_j-k_i) \text{ for some } k_i<k_j\le d_1,\, p\notin\mathcal{P}}} R(f,p^m), \tag{7.5}$$

$$P_5 = \prod_{\substack{m\ge t+2,\, 50d>p>r^4,\, p>C_3 \text{ and} \\ p\nmid(k_j-k_i) \text{ for all } k_i<k_j\le d_1}} R(f,p^m), \tag{7.6}$$

$$P_6 = \prod_{\substack{m\ge t+2,\, p>r^4,\, p>C_2 \text{ and} \\ p\ge 50d}} R(f,p^m), \tag{7.7}$$

where C_2, C_3 are the constants in Lemmas 5.3 and 5.4 respectively, and $\mathcal{P}$ is the set (6.1) of exceptional primes. By (1.6) the theorem follows if we show that each of the products P_i is bounded by a constant depending only on r.

By Lemma 5.2, the Weil bound (5.1) and the trivial bound $R(f,p) \le p^{1/d}$ we have

$$\begin{aligned} P_1 &\le \prod_{p<C_2} R(f,p) \prod_{p\le r^4} R(f,p) \prod_{p<50d} R(f,p) \\ &\le (1.75)^{C_2+r^4} \prod_{p<50d} p^{1/d} \ll (1.75)^{r^4}. \end{aligned}$$

For the next few products we need the following

Lemma 7.1. *Let f be a sparse polynomial with r terms of degree d. For any prime p let $t_p = \operatorname{ord}_p(f'(x))$. Then letting p run through the set of all primes for which $d_p(f) \ge 1$ we have*

$$\prod_{p,\, d_p(f)\ge 1} p^{t_p} \le d^r.$$

Proof. Let $f(x) = a_1x^{k_1} + \ldots + a_rx^{k_r}$ and p be a prime with $d_p(f) \ge 1$. Then for some i, $p \nmid a_i$, and so for this value of i, $p^{t_p} \mid k_i$. Thus the product over all such p^{t_p} is a divisor of $k_1 \ldots k_r$. ■

(We continue to write t for t_p.) For P_2 the condition $1 < m \le t+1$ implies that $t \ge 1$ and so $m \le 2t$. Thus we trivially have

$$P_2 \le \prod_p p^{m/d} \le \prod_p p^{2t/d} \le d^{2r/d} \le 2.1^r.$$

The number of primes in the product P_3 is less than $r^4/2 + r^2 + C_3 < r^4 + C_3$ and so by Lemma 1.1, $P_3 \le 5^{r^4+C_3}$. For P_4 we apply Lemma 6.1, to obtain

$$P_4 \le \prod_p \left(1 + \frac{1}{p^2}\right)\Big(\prod_p p^{t/d}\Big) \prod_{1\le i<j\le r} \prod_{p \le p_{i,j}} p^{8r/p_{ij}}$$
$$\ll d^{r/d} \prod_{1\le i<j\le r} C_5^{4r} \ll 1.5^r C_5^{2r^3}$$

for some absolute constant C_5. We may take $C_5 = \sup_x e^{\theta(x)/x}$, where $\theta(x) = \sum_{p\le x} \log p$.

For P_5, we apply Lemma 5.4(iii) to obtain,

$$P_5 \le \prod_{p<50d} p^{(2r+t)/d} \le \prod_p p^{t/d} \prod_{p<50d} p^{2r/d} \le d^{r/d} e^{2r\theta(50d)/d} \le 1.5^r C_5^{100r}.$$

Finally, we apply Lemma 5.3 to P_6 to obtain

$$P_6 \le \prod_p p^{t/d} \le d^{r/d} \le 1.5^r.$$

Thus the product $P_1P_2P_3P_4P_5P_6$ is bounded above by a constant depending only on r.

References

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

[2] J. R. Chen, *On the representation of natural numbers as a sum of terms of the form* $x(x+1)\dots(x+k-1)/k!$, Acta Math. Sinica 8 (1958), 253–257.

[3] —, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711–719.

[4] T. Cochrane, *Exponential sums modulo prime powers*, Acta Arith. 101 (2002), 131–149.

[5] T. Cochrane, C. Pinner and J. Rosenhouse, *Bounds on exponential sums and the polynomial Waring's problem mod p*, preprint.

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

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

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

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

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

[11] L. K. Hua, *On exponential sums*, J. Chinese Math. Soc. 20 (1940), 301–312.

[12] L. K. Hua, *On exponential sums*, Sci. Record (Peking) (N.S.) 1 (1957), 1–4.
[13] —, *Additive Primzahltheorie*, Teubner, Leipzig, 1959, 2–7.
[14] S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and Their Applications*, Cambridge Univ. Press, Cambridge, 1999.
[15] W. K. A. Loh, *On Hua's lemma*, Bull. Austral. Math. Soc. 50 (1994), 451–458.
[16] —, *Exponential sums on reduced residue systems*, Canad. Math. Bull. 41 (1998), 187–195.
[17] M. Lu, *A note on the estimation of a complete rational trigonometric sum*, Acta Math. Sinica 27 (1984), 817–823 (in Chinese).
[18] —, *Estimate of a complete trigonometric sum*, Sci. Sinica Ser. A 28 (1985), 561–578.
[19] —, *A note on complete trigonometric sums for prime powers*, Sichuan Daxue Xuebao 26 (1989), 156–159.
[20] V. I. Nečaev [V. I. Nechaev], *An estimate of the complete rational trigonometric sum*, Mat. Zametki 17 (1975), 839–849 (in Russian); English transl.: Math. Notes 17 (1975), 504–511.
[21] —, *On the least upper bound on the modulus of complete trigonometric sums of degrees three and four*, in: Investigations in Number Theory, Saratov. Gos. Univ., Saratov, 1988, 71–76 (in Russian).
[22] V. I. Nečaev [V. I. Nechaev] and V. L. Topunov, *Estimation of the modulus of complete rational trigonometric sums of degree three and four*, Trudy Mat. Inst. Steklov. 158 (1981), 125–129 (in Russian); English transl. in: Analytic Number Theory, Mathematical Analysis and Their Applications, Proc. Steklov Inst. Math. 158 (1983), 135–140.
[23] M. Qi and P. Ding, *Estimate of complete trigonometric sums*, Kexue Tongbao 29 (1984), 1567–1569.
[24] —, —, *On an estimate of complete trigonometric sums*, Chinese Ann. Math. Ser. B 6 (1985), 109–120.
[25] —, —, *Further estimates of complete trigonometric sums*, J. Tsinghua Univ. Sci. Technol. 29 (1989), no. 6, 74–85.
[26] I. E. Shparlinski, *On bounds of Gaussian sums*, Mat. Zametki 50 (1991), 122–130 (in Russian).
[27] —, *On Gaussian sums for finite fields and elliptic curves*, in: Algebraic Coding (First French-Soviet Workshop, Paris, 1991), Lecture Notes in Comput. Sci. 573, Springer, 1992, 5–15.
[28] —, *On exponential sums with sparse polynomials and rational functions*, J. Number Theory 60 (1996), 233–244.
[29] S. B. Stečkin [S. B. Stechkin], *Estimate of a complete rational trigonometric sum*, Trudy Mat. Inst. Stoklov. 143 (1977), 188–220 (in Russian); English transl.: Proc. Steklov. Inst. Math. 143 (1980), 201–220.
[30] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.
[31] M. Zhang and Y. Hong, *On the maximum modulus of complete trigonometric sums*, Acta Math. Sinica (N.S.) 3 (1987), 341–350.

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

Received on 30.4.2002 (4276)