

SPARSE POLYNOMIAL EXPONENTIAL SUMS

TODD COCHRANE, CHRISTOPHER PINNER, AND JASON ROSENHOUSE

1. INTRODUCTION

In this paper we estimate the complete exponential sum

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

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

$$(1.2) \quad f(x) = a_1 x^{k_1} + \cdots + a_r x^{k_r}$$

with $0 < k_1 < k_2 < \cdots < k_r$. We assume always that the content of f , (a_1, a_2, \dots, 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 ,

$$(1.3) \quad |S(f, q)| \leq C q^{1-\frac{1}{d}},$$

Date: November 18, 2002.

1991 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.

if f is not a constant function modulo p for each prime $p|q$. It is well known that the exponent $1 - \frac{1}{d}$ is best possible. For the case of Gauss sums ($r = 1$) Shparlinski [29], [30] showed that one may take $C = 1 + O(d^{-1/4+\epsilon})$ and this was sharpened to $C = 1 + O(d^{-1+\epsilon})$ in his subsequent work with Konyagin [15, Theorem 6.7].

The best upper bounds available for general f are

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

due to Stečkin [33], and

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

due to Qi and Ding [27]; see also Chen [2], [3], Lu [19], [20], [21], Nečaev [22], [23], Qi and Ding [25], [26] and Zhang and Hong [35]. 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 bound [34] $|S(f, p)| \leq (d - 1)\sqrt{p}$ 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 ,*

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

Although our proof yields $C(r) \leq e^{O(r^4)}$, 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 Stečkin [33] 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 $d_p(f) \geq 1$. Then for any $m \geq 1$,*

$$(1.4) \quad |S(f, p^m)| \leq 4.41 p^{m(1-\frac{1}{d})}.$$

It is also well known (see [22], [3] or [8]) that for $p \geq (d-1)^{2d/(d-2)}$ and $m \geq 1$,

$$(1.5) \quad |S(f, p^m)| \leq p^{m(1-\frac{1}{d})}.$$

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

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

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

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

the exponent in the upper bound can be dramatically reduced. Shparlinski [31] showed that

$$|S^*(f, q)| \leq C(d, \epsilon) q^{1-\frac{1}{r}+\epsilon},$$

for any sparse polynomial in r terms with content relatively prime to q . Loh [17] 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 $t = t_p(f) = \text{ord}_p(f')$ 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 $m \geq 2$. Write

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

with

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

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 $m \geq t + 2$, or $p = 2$ and $m \geq t + 3$, 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

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

Lemma 2.2. [6, Proposition 4.1] *The Recursion Relationship. Suppose that p is an odd prime and $m \geq t + 2$, or $p = 2$ and $m \geq t + 3$, or $p = 2$, $t = 0$ and $m = 2$. Then if $\alpha \in \mathcal{A}$*

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

where

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

Under the hypotheses of the lemma we have

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

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

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

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 $d_p(f) \geq 1$. Suppose that p is odd and $m \geq t+2$ or $p = 2$ and $m \geq t+3$.*

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*

$$(2.6) \quad |S_\alpha(f, p^m)| \leq \min\{\nu, \lambda\} p^{\frac{t}{\nu+1}} p^{m(1-\frac{1}{\nu+1})},$$

with equality if $\nu = 1$.

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

For any critical point α set

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

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

Lemma 2.4.

$$(2.8) \quad \sigma \geq \begin{cases} t+2 & \text{if } p \text{ is odd or } \nu > 1 \\ t+1 & \text{if } p = 2 \text{ and } \nu = 1. \end{cases}$$

$$(2.9) \quad \sigma \leq \nu + 1 + t - \tau.$$

$$(2.10) \quad d_p(g_\alpha) \leq \begin{cases} \sigma - t + \text{ord}_p(d_p(g_\alpha)) \leq \nu + 1 + \text{ord}_p(d_p(g_\alpha)) \\ \sigma \leq \nu + 1 + t - \tau. \end{cases}$$

$$(2.11) \quad d_p(g_1) \leq \sigma + \tau - t - 1 \leq \nu.$$

$$(2.12) \quad p^\tau | d_p(g_\alpha).$$

An immediate consequence that we frequently make reference to is

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

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

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*

$$d\lambda_i \lambda^{\frac{i-d}{i+1}} \leq i\lambda.$$

Proof. For any fixed $i \geq 1$ the function $f_i(x) := \frac{\lambda_i}{i} x \lambda^{\frac{i-x}{i+1}}$ 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 $f_i(i+1) = \lambda_i(1 + \frac{1}{i})\lambda^{\frac{-1}{i+1}} \leq \lambda$, as can be seen by considering the different cases $i = 1, 2, 3$ and $i \geq 4$. \square

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

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

Proof. We first note that

$$\left(\frac{d_1}{i}\right)^{\frac{i+1}{d_1-i}} \leq 4, \quad \text{for } 1 \leq i \leq d_1 - 1.$$

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

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 $m \geq 2$*

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

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

$$(3.2) \quad |S_\alpha| \leq p^{m(1-\frac{1}{d_1+1})},$$

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 $|S(f, p^m)| \leq \sum_{\alpha \in \mathcal{A}} |S_\alpha(f, p^m)| \leq d_1 p^{m-1} \leq p^{m(1-\frac{1}{d_1+1})}$. Next, if there is a critical point α of multiplicity d_1 then it is the only critical point and we have $|S(f, p^m)| = |S_\alpha(f, p^m)| \leq p^{m(1-\frac{1}{d_1+1})}$.

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 obtain from (3.2)

$$(3.3) \quad |S(f, p^m)| \leq \sum_{\alpha \in \mathcal{A}} |S_\alpha(f, p^m)| \leq \sum_{i=1}^{d_1-1} n_i p^{m(1-\frac{1}{i+1})} \\ = p^{m(1-\frac{1}{d_1+1})} \left(\sum_{i=1}^{d_1-1} n_i p^{\frac{m(i-d_1)}{(i+1)(d_1+1)}} \right).$$

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

$$(3.4) \quad |S(f, p^m)| \leq p^{m(1-\frac{1}{d_1+1})} \left(\sum_{i=1}^{d_1-1} n_i (p/d_1)^{\frac{i-d_1}{i+1}} \right) \\ \leq \left(\sum_{i=1}^{d_1-1} n_i i/d_1 \right) p^{m(1-\frac{1}{d_1+1})} \leq p^{m(1-\frac{1}{d_1+1})}.$$

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

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

the latter inequality following from (2.9). Suppose next that $\sigma = m - 1$.

Put $d_p = d_p(g_\alpha)$. Since $p > d_1^2 \geq \nu^2 \geq \nu + 2$ it follows from Lemma 2.5 that

$d_p \leq \nu + 1 \leq d_1 + 1$. If $d_p \geq 3$ then $p \geq (d_p - 1)^{2+4/(d_p-2)}$, so by the Weil bound, $|S(g_\alpha, p)| \leq (d_p - 1)\sqrt{p} \leq p^{1-\frac{1}{d_p}} \leq p^{1-\frac{1}{\nu+1}}$. If $d_p = 1$ or 2 the same bound is elementary. It follows from the recursion formula of Lemma 2.2 that

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

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

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

□

4. MULTIPLICITY ESTIMATES

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

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

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 $1 \leq i \leq r$ let

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

and set

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

$$(4.2) \quad r_i = |S(i, \alpha_i)|.$$

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 $i \neq j$ 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 mod 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 ν mod 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 $(x-a)^k | f_1, \dots, f_t$ 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

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

Writing $\nabla = x \frac{d}{dx}$ we must have $\nabla^j g(a) \equiv 0 \pmod p$ 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 $|\det(k_i^j)_{\substack{i=1, \dots, t \\ j=0, \dots, u-1}}| = \prod |k_i - k_j| \not\equiv 0 \pmod p$ and $a^{k_1} g_1(a)^p \not\equiv 0 \pmod p$ we must therefore have $u < t$. \square

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 $\nu = u < t \leq r = r_i$. If $\alpha_i \geq 1$ then since $(x-a)^k | f_i(x)$ we have (by induction) $k < r_i p^{\alpha_i - 1}$ and $u < p$ giving

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

\square

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 mod 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 that $p > (r_1 - 1)^{2r_1/(r_1-2)}$. Then if $m \geq t + 2$ and α is a critical point of multiplicity $\nu < r_1$ we have*

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

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 $p > \nu^{2+4/(\nu-1)}$, $d_p \leq \nu + 1$ 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,

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

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

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

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

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

□

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

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

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 constant 1 for $p \gg d$. We obtain this from the following result established in the author's 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 $p > \left(\frac{9}{\delta^{1.06}}\right) d$ and $p > C_1(\delta)$, then*

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

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

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

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 $p \leq 16d^2$. Applying Lemma 5.1 with $\delta = \frac{1}{5}$ we obtain that if $p > 50d$ and $p > C_1(\frac{1}{5})$ then $|S(f, p)| \leq p(1 - 1/rp^{1/5})$. Since, $p > r^4$

it follows that $|S(f, p)| \leq p(1 - 1/p^{9/20})$, and since $p \leq 16d^2$ the latter is $\leq p^{1-\frac{1}{d}}$ for $p > 10^{60}$. \square

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

$$(5.3) \quad |S_\alpha| \leq p^{\frac{t}{\nu+1}} p^{m(1-\frac{1}{\nu+1})},$$

and

$$(5.4) \quad |S(f, p^m)| \leq p^{\frac{t}{d_1+1}} p^{m(1-\frac{1}{d_1+1})}.$$

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

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 obtain from (5.3)

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

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

We now establish (5.3) by induction on m . The result is trivial if $m = 2$.

Suppose that $m > 2$. If $\sigma \geq m$ then from (2.9),

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

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

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

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

$$(5.5) \quad |S_\alpha| \leq p^{\sigma-1} |S(g_\alpha, p)| \leq p^{\sigma-\frac{1}{\nu+1}} \leq p^{\frac{t}{\nu+1}} p^{m(1-\frac{1}{\nu+1})},$$

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 $p > 50(d_1 + 1) \geq 50(\nu + 1) \geq 50d_p(g_\alpha)$ we can apply Lemma 5.2 to obtain $|S(g_\alpha, p)| \leq p^{1-\frac{1}{d_p(g_\alpha)}}$, and the result follows as before.

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

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

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

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

□

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 mod 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 $k_i < k_j \leq d_1$. Then for $m \geq t + 2$ and any critical point α of multiplicity ν we have*

- (i) *If $\alpha \neq 0$ then $|S_\alpha(f, p^m)| \leq p^{\frac{t}{\nu+1}} p^{m(1-\frac{1}{\nu+1})}$.*
- (ii) *For $\alpha = 0$, $|S_0(f, p^m)| \leq p^{\frac{2r+t}{\nu+1}} p^{m(1-\frac{1}{\nu+1})}$.*
- (iii) *$|S(f, p^m)| \leq p^{\frac{2r+t}{d_1+1}} p^{m(1-\frac{1}{d_1+1})}$.*

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 $p \geq 50(d_1 + 1)$ then the lemma is implied by Lemma 5.3 and so we may assume $p < 50(d_1 + 1)$. In particular, it follows that $r \leq d_1$ (if $r \geq 4$ then $r^4 < p < 50(d_1 + 1)$ implies $r < r \cdot \frac{r^3}{50} < d_1 + 1$; if $r \leq 3$ then $p > 200$ implies $d_1 > 3 \geq r$).

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 $r \geq 2$ and that $\nu(0) < d_1$.

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

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

the desired bound. We have

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

For the first term we have the trivial bound

$$(5.6) \quad |S_0(f, p^m)| \leq p^{m-1} = p^{\frac{j-d_1}{d_1+1}} \Delta.$$

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

$$(5.7) \quad \begin{aligned} \sum_{\alpha \neq 0} |S_\alpha(f, p^m)| &\leq p \cdot p^{t/r} p^{m(1-\frac{1}{r})} = p^{\frac{j(r-d_1-1)-rd_1-d_1-1}{(d_1+1)r}} \Delta \\ &= p^{\frac{j-d_1}{d_1+1} - \frac{1+j}{r}} \Delta. \end{aligned}$$

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

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

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

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

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

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

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

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

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

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

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,

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

where $d_2 := d_p(p^{-\tau} g_0) \leq d_1$. Now by (2.11) $d_2 \leq \nu$ 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 $p|(k_j - k_i)$ for some $k_i < k_j \leq d_1$ 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 $1 \leq i < j \leq r$ 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

$$(6.1) \quad \mathcal{P} = \{p_{ij} : 1 \leq i < j \leq r\}.$$

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

Let

$$p_{\ell_s} = \min\{p_{ij} : p|(k_j - k_i), \quad k_i < k_j \leq d_1\},$$

and define

$$M := rd_1/p_{\ell_s}.$$

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

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

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

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

Then we can write

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

where for $0 \leq j \leq m$

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

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

$$g_j(x) := p^{-\mu_j - t_j} (a_1 k_1 p^{j k_1} x^{k_1 - 1} + \dots + a_r k_r p^{j k_r} x^{k_r - 1}) \equiv 0 \pmod{p},$$

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 $p^{t_j + \mu_j} \parallel a_I k_I p^{j k_I}$ then $p^{t_j + \mu_j + k_I} \parallel a_I k_I p^{(j+1)k_I}$ and $p^{t_j + \mu_j + k_I + 1} \parallel a_\ell k_\ell p^{(j+1)k_\ell}$ for $\ell > I$. 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 $m - \mu_j \geq 2$. Thus there are at most r values of $j \leq m$ for which $m - \mu_j \geq 2$ 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 $0 \leq j \leq m$

$$(6.6) \quad \mu_j + t_j \leq t + j(d_1 + 1).$$

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

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

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

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

It follows that

$$(6.7) \quad p^{\mu_j - 1} |S_j^*| \leq \frac{4}{p^3} p^{\frac{t}{d_1 + 1}} p^{m(1 - \frac{1}{d_1 + 1})}.$$

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

$$\sum_{j \geq j_o} p^{\mu_j - j} |S_j^*| \leq p^{m - j_o} = p^{\frac{m - t}{d_1 + 1} - j_o} p^{\frac{t}{d_1 + 1}} p^{m(1 - \frac{1}{d_1 + 1})}$$

Now

$$(m - t) - j_o(d_1 + 1) \leq 8M + t_{j_o} + \mu_{j_o} - t - j_o(d_1 + 1) \leq 8M = 8rd_1/p_{\ell_s},$$

by (6.6). Thus

$$(6.8) \quad \sum_{j \geq j_o} p^{\mu_j - j} |S_j^*| \leq p^{\frac{8r}{p_{\ell_s}}} p^{\frac{t}{d_1 + 1}} p^{m(1 - \frac{1}{d_1 + 1})}.$$

From (6.7) and (6.8) we conclude that

$$|S(f, p^m)| \leq \left(\frac{4r}{p^3} + p^{\frac{8r}{p_{\ell_s}}} \right) p^{\frac{t}{d_1 + 1}} p^{m(1 - \frac{1}{d_1 + 1})} \leq p^{\frac{8r}{p_{\ell_s}}} \left(1 + \frac{1}{p^2} \right) p^{\frac{t}{d_1 + 1}} p^{m(1 - \frac{1}{d_1 + 1})}.$$

This establishes

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

$$|S(f, p^m)| \leq \left(1 + \frac{1}{p^2}\right) p^{\frac{8r}{p_{\ell s}}} p^{\frac{t}{d_1+1}} p^{m(1-\frac{1}{d_1+1})},$$

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

7. PROOF OF THEOREM 1.1

For any prime power p^m and polynomial f let

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

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

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

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):

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

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

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

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

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

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

where C_2, C_3 are the constants in Lemmas 5.3 and 5.4 respectively, and \mathcal{P} is the set of exceptional primes (6.1). 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 $R(f, p) \leq p^{1/d}$ we have

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

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 $t_p = \text{ord}_p(f'(x))$. Then letting p run through the set of all*

primes for which $d_p(f) \geq 1$ we have

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

Proof. Let $f(x) = a_1x^{k_1} + \dots + a_rx^{k_r}$ and p be a prime with $d_p(f) \geq 1$. Then for some i , $p \nmid a_i$, and so for this value of i , $p^{t_p} | k_i$. Thus the product over all such p^{t_p} is a divisor of $k_1k_2 \dots k_r$. \square

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

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

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 $P_3 \leq 5^{r^4+C_3}$. For P_4 we apply Lemma 6.1 to obtain

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

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

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

$$\begin{aligned} P_5 &\leq \prod_{p < 50d} p^{\frac{2r+t}{d}} \leq \prod_p p^{t/d} \prod_{p < 50d} p^{2r/d} \\ &\leq d^{r/d} e^{2r\theta(50d)/d} \leq 1.5^r C_5^{100r}. \end{aligned}$$

Finally, we apply Lemma 5.3 to P_6 to obtain

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

Thus the product $P_1 P_2 P_3 P_4 P_5 P_6$ 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. Sin. 8 (1958), 253-257.
- [3] ——— *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711-719.
- [4] T. Cochrane, *Mixed exponential sums modulo prime powers*, preprint.
- [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. Zheng, *Pure and mixed exponential sums*, Acta Arithmetica 91, no. 3, (1999), 249-278.
- [7] T. Cochrane and Z. Zheng, *Exponential sums with rational function entries*, to appear in Acta Arithmetica.
- [8] T. Cochrane and Z. Zheng, *On upper bounds of Chalk and Hua for exponential sums*, preprint.
- [9] P. Ding, *An improvement to Chalk's estimation of exponential sums*, Acta Arith. 59 no. 2 (1991), 149-155.
- [10] ——— *On a conjecture of Chalk*, J. Number Theory 65 no. 2 (1997), 116-129.
- [11] L.K. Hua, *On exponential sums*, J. Chinese Math. Soc. 20 (1940), 301-312.
- [12] ——— *On exponential sums*, Sci. Record (Peking) (N.S.) 1 (1957), 1-4.
- [13] ——— *Additiv Primzahltheorie*, Teubner, Leipzig (1959), 2-7.
- [14] S.V. Konyagin and I.E. Shparlinski, *On the distribution of residues of finitely generated multiplicative groups and their applications*, Macquarie Mathematics Reports, Macquarie University, 1995.
- [15] ——— *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.
- [16] W.K.A. Loh, *Hua's Lemma*, Bull. Australian Math. Soc. (3) 50 (1994), 451-458.
- [17] ——— *Exponential sums on reduced residue systems*, Canad. Math. Bull. Vol. 41 (2) (1997), 187-195.
- [18] J.H. Loxton and R.C. Vaughan, *The estimation of complete exponential sums*, Canad. Math. Bull. 28 no. 4 (1985), 442-454.
- [19] M. Lu, *A note on the estimate of a complete rational trigonometric sum*, Acta Math. Sin. 27 (1984), 817-823.
- [20] ——— *The estimate of complete trigonometric sums*, Sci. Sin. 28, no. 6, (1985), 561-578.

- [21] ——— *A note on complete trigonometric sums for prime powers*, Sichuan Daxue Xuebao 26 (1989), 156-159.
- [22] V.I. Nečaev, *An estimate of a complete rational trigonometric sum*, Mat. Zametki 17 (1975), 839-849; English translation in Math. Notes 17 (1975).
- [23] ——— *On the least upper bound on the modulus of complete trigonometric sums of degrees three and four*, Investigations in number theory (Russian), Saratov. Gos. Univ., Saratov, (1988), 71-76.
- [24] V.I. Nečaev 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; English translation in Proceedings of the Steklov Institute of Mathematics 1983, no. 4, Analytic number theory, mathematical analysis and their applications, Amer. Math. Soc., 135-140.
- [25] M. Qi and P. Ding, *Estimate of complete trigonometric sums*, Kexue Tongbao 29 (1984), 1567-1569.
- [26] ——— *On Estimates of complete trigonometric sums*, China Ann. Math. B6 (1985), 110-120.
- [27] ——— *Further estimates of complete trigonometric sums*, J. Tsinghua Univ. 29, no. 6, (1989), 74-85.
- [28] W.M. Schmidt, *Equations over finite fields*, L.N.M. **536**, Springer-Verlag, Berlin, (1976).
- [29] I.E. Shparlinski, *On bounds of Gaussian sums*, Matem. Zametki, 50 (1991), 122-130 (in Russian).
- [30] ——— *On Gaussian sums for finite fields and elliptic curves*, Proc. 1st French-Soviet Workshop on Algebraic Coding, Paris, 1991, Lect. Notes in Computer Sci., 537 (1992), 5-15.
- [31] ——— *On exponential sums with sparse polynomials and rational functions*, J. Number Theory 60 (1996), 233-244.
- [32] S.A. Stepanov, *Arithmetic of Algebraic Curves*, English translation, Monographs in Contemporary Mathematics, Consultants Bureau, New York, (1994).
- [33] S.B. Stečkin, *Estimate of a complete rational trigonometric sum*, Proc. Steklov Inst. 143 (1977), 188-220, English translation, A.M.S. Issue 1 (1980), 201-220.
- [34] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204-207.
- [35] M. Zhang and Y. Hong, *On the maximum modulus of complete trigonometric sums*, Acta Math. Sinica, New Series 3, no. 4 (1987), 341-350.

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506

E-mail address: `cochrane@math.ksu.edu`

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506

E-mail address: `pinner@math.ksu.edu`

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506

E-mail address: `jasonr@math.ksu.edu`