

ON UPPER BOUNDS OF CHALK AND HUA FOR EXPONENTIAL SUMS

TODD COCHRANE AND ZHIYONG ZHENG

(Communicated by Dennis A. Hejhal)

ABSTRACT. Let f be a polynomial of degree d with integer coefficients, p any prime, m any positive integer and $S(f, p^m)$ the exponential sum $S(f, p^m) = \sum_{x=1}^{p^m} e_p^m(f(x))$. We establish that if f is nonconstant when read (mod p), then $|S(f, p^m)| \leq 4.41p^{m(1-\frac{1}{d})}$. Let $t = \text{ord}_p(f')$, let α be a zero of the congruence $p^{-t}f'(x) \equiv 0 \pmod{p}$ of multiplicity ν and let $S_\alpha(f, p^m)$ be the sum $S(f, p^m)$ with x restricted to values congruent to $\alpha \pmod{p^m}$. We obtain $|S_\alpha(f, p^m)| \leq \min\{\nu, 3.06\}p^{\frac{t}{\nu+1}}p^{m(1-\frac{1}{\nu+1})}$ for p odd, $m \geq t+2$ and $d_p(f) \geq 1$. If, in addition, $p \geq (d-1)^{(2d)/(d-2)}$, then we obtain the sharp upper bound $|S_\alpha(f, p^m)| \leq p^{m(1-\frac{1}{\nu+1})}$.

1. INTRODUCTION

In many applications in number theory one is faced with the estimation of exponential sums of the type

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

with q a positive integer, $f(x) \in \mathbb{Z}[x]$ and $e_q(f(x)) = e^{2\pi i f(x)/q}$. These sums enjoy the multiplicative property

$$(1.1) \quad S(f, q) = \prod_{i=1}^k S(\lambda_i f, p_i^{m_i}),$$

where $q = \prod_{i=1}^k p_i^{m_i}$ and $\sum_{i=1}^k \lambda_i q / p_i^{m_i} = 1$, reducing their estimation to the case of prime power moduli.

Let p^m be a prime power with $m \geq 1$, let f be a polynomial over \mathbb{Z} of degree d and let $d_p(f)$ denote the degree of f read (mod p). When $m = 1$ it was established by Mordell [29] that for any f and p with $d_p(f) \geq 1$, one has

$$(1.2) \quad |S(f, p)| \leq \sqrt{d} p^{1-\frac{1}{d}}.$$

Received by the editors June 3, 1999.

1991 *Mathematics Subject Classification*. Primary 11L07, 11L03.

Key words and phrases. Exponential sums.

The research of the second author was supported by the National Science Fund of The People's Republic of China for Distinguished Young Scholars.

Mordell actually stated his result in a somewhat more complicated manner but the constant \sqrt{d} may be easily deduced from the inequality

$$|S(f, p)|^{2d} \leq \frac{(d, p-1)}{p(p-1)} d! p^{2d}$$

(Vaughan [45] (p. 92)) and the fact that $2d(d!) \leq d^d$ for $d \geq 4$. Weil [46] established the much stronger upper bound

$$|S(f, p)| \leq (d-1)\sqrt{p},$$

for any f with $d_p(f) \geq 1$, from which it is easy to replace the constant \sqrt{d} in (1.2) with an absolute constant. In Lemma 3.1 we obtain in such a manner the upper bound

$$(1.3) \quad |S(f, p)| \leq 1.75 p^{1-\frac{1}{d}}$$

for any f and p with $d_p(f) \geq 1$. The constant 1.75 in (1.3) cannot be replaced with 1 (for example $S(X^2 - X, 2) = \sqrt{2} p^{1-\frac{1}{d}}$), but it can be replaced with a constant depending on d that tends to 1 as d goes to infinity; see (3.3).

For $m \geq 2$ Hua [12], [13], [14] showed that if $d_p(f) \geq 1$, then

$$(1.4) \quad |S(f, p^m)| \leq d^3 p^{m(1-\frac{1}{d})}.$$

It is well known that the exponent $m(1 - \frac{1}{d})$ in (1.4) is best possible, as a uniform upper bound on $S(f, p^m)$. For instance, if $p \nmid a$ and $d|m$, then $S(aX^d, p^m) = p^{m(1-\frac{1}{d})}$ as noted by Hardy and Littlewood [10]; see also [6] (Example 9.1) for a more general example. Chen [4], Chalk [2], Ding [8], [9], Loh [22], Lu [26], [27], Nečaev [31], [32], Stečkin [43] and the authors of this paper [6], [7] made further improvements in the constant on the right-hand side of (1.4). In [27] Lu established the constant $d - 1$. Nečaev [31] and Chen [4] obtained the sharp upper bound

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

under the assumption that $p \geq (d-1)^{\frac{2d}{d-2}}$. (This interval for p coincides with the interval where Weil's upper bound implies $|S(f, p)| \leq p^{1-\frac{1}{d}}$.) The constant 1 in (1.5) is highly desirable for the estimation of $S(f, q)$ for arbitrary q in view of the multiplication formula (1.1).

Stečkin [43] proved that the constant d^3 in (1.4) can be replaced by an absolute constant, but he did not indicate how large it must be. In this paper we obtain a very small value for this absolute constant.

Theorem 1.1. *Let f be any polynomial over \mathbb{Z} and p any prime with $d_p(f) \geq 1$. Then for any $m \geq 1$,*

$$(1.6) \quad |S(f, p^m)| \leq 4.41 p^{m(1-\frac{1}{d})}.$$

The theorem is deduced from a local type upper bound on exponential sums given in Theorem 2.1. For polynomials of degree 2, it was already known to Gauss that the best possible constant in (1.6) is $\sqrt{2}$. Nečaev and Topunov [33] determined the best possible constant in (1.6) for polynomials of degree 3 and 4, 1.986 and 2.263 (rounded to three places) respectively; see also Nečaev [31] and [32].

Question 1. What is the best possible constant in (1.6) for a polynomial of arbitrary degree? Can one replace 4.41 with $1 + \epsilon_d$ with $\epsilon_d \rightarrow 0$ as $d \rightarrow \infty$?

Question 2. Is there an absolute constant C such that for an arbitrary positive integer q ,

$$(1.7) \quad |S(f, q)| \leq C q^{1-\frac{1}{d}},$$

if f is not a constant function (mod p) for each prime $p|q$? The following example, pointed out to us by Igor Shparlinski, shows that it is not enough to merely insist that f be a nonconstant polynomial (mod p) ($d_p(f) \geq 1$) for each prime $p|q$. Let $q = d!$. Then

$$\sum_{x=1}^q e_q\{x(x+1)\dots(x+d-1)\} = q \geq \frac{1}{3}d q^{1-\frac{1}{d}}.$$

Currently, the best upper bounds known for a general modulus are

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

due to Stečkin [43], and

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

due to Qi and Ding [36]; see also Chen [3], [4], Lu [25], [26], Nečaev [31], Qi and Ding [34], [35] and Zhang and Hong [47]. These authors have noted that in order to make any further improvement one must first obtain a nontrivial upper bound for $|S(f, p)|$ for $p < (d-1)^2$, the interval where Weil’s bound is worse than the trivial bound. There appears to be little progress in this direction for a general polynomial but progress has been made for the case of sparse polynomials. Indeed, the most significant nontrivial bound known for small p was already given by Mordell [29], in the same work where he established (1.2). Let $f = \sum_{i=1}^n a_i X^{d_i}$, with $p \nmid a_i$ and $d_i \geq 1$ for all i . Then

$$(1.8) \quad |S(f, p)| \leq (d_1 d_2 \dots d_n (p-1, d_1, d_2, \dots, d_n))^{\frac{1}{2n}} p^{1-\frac{1}{2n}}.$$

This is actually a slightly refined version of Mordell’s result as given by Shparlinski [40], p. 88. Thus, for instance,

$$(1.9) \quad |S(aX^d + bX, p)| \leq d^{1/4} p^{3/4}.$$

For the case of monomials, several nontrivial upper bounds are available. Heath-Brown and Konyagin [11], sharpening earlier bounds of Konyagin and Shparlinski [19], Mullen and Shparlinski [30] and Shparlinski [41], established the following: for $p \nmid a$,

$$(1.10) \quad |S(aX^d, p)| \ll \begin{cases} d^{5/8} p^{5/8}, \\ d^{3/8} p^{3/4}. \end{cases}$$

These bounds are sharper than Weil and nontrivial on the interval $d^{\frac{3}{2}} \ll p \ll d^3$. Konyagin [18] recently informed us that he can sharpen (1.10) to obtain nontrivial bounds for $p > d^{\frac{4}{3}+\epsilon}$. Konyagin [17] and Konyagin and Shparlinski [20] give upper bounds of a much weaker type that are nontrivial for much smaller values of p relative to d . Shparlinski [39] utilized an upper bound of the type (1.10) to establish an affirmative answer to the second question above for the case of monomials. See also Akulinichev [1], Chen and Pan [5], Karatsuba [16], Lachaud [21], Loxton and Vaughan [24] and Montgomery, Vaughan and Wooley [28] for further discussion of this problem.

2. LOCAL UPPER BOUNDS ON EXPONENTIAL SUMS

More precise upper bounds on exponential sums can be given using information about the zeros f' . Two such approaches are available, one considering the factorization of f' over \mathbb{C} and the other considering the factorization of $f' \pmod{p}$. We take up the latter approach here, and talk briefly about the former approach in the closing paragraph of this section.

For any polynomial f with integer coefficients and prime p let $\text{ord}_p(f)$ denote the largest power of p dividing all of the coefficients of f . Thus in $\mathbb{Z}[X]$ we have $p^{\text{ord}_p(f)} \parallel f$. Set $t = t(f) = \text{ord}_p(f')$ and let $\mathcal{A} = \mathcal{A}(f, p)$ be the set of zeros of the congruence

$$(2.1) \quad p^{-t} f'(x) \equiv 0 \pmod{p}.$$

We call \mathcal{A} the set of critical points associated with the sum $S(f, p^m)$. For any $\alpha \in \mathcal{A}$ let $\nu = \nu_\alpha$ denote its multiplicity as a zero of (2.1). Write

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

where for any integer α ,

$$(2.2) \quad S_\alpha = S_\alpha(f, p^m) := \sum_{\substack{x=1 \\ x \equiv \alpha \pmod{p}}}^{p^m} e_{p^m}(f(x)).$$

Refining earlier work by Chalk [2] and Ding [8] we established in [6], Theorem 2.1, the following: If p is odd and $m \geq t + 2$, or $p = 2$ and $m \geq t + 3$, then

- (i) If $\alpha \notin \mathcal{A}$, then $S_\alpha(f, p^m) = 0$.
- (ii) If α is a critical point of multiplicity ν , then

$$(2.3) \quad |S_\alpha(f, p^m)| \leq \nu p^{\frac{t}{\nu+1}} p^{m(1-\frac{1}{\nu+1})},$$

with equality if $\nu = 1$.

- (iii) If M is the maximum multiplicity of the set of critical points, then

$$(2.4) \quad |S(f, p^m)| \leq \left(\sum_{\alpha \in \mathcal{A}} \nu_\alpha \right) p^{\frac{t}{M+1}} p^{m(1-\frac{1}{M+1})}.$$

The inequality in (2.4), first conjectured by Chalk in [2], was also obtained independently by Loh [22] and Ding [9]. In this paper we refine this result and prove

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 $\lambda = (\frac{5}{4})^5 = 3.0517\dots$ and $d_1 = d_p(p^{-t} f')$. Then*

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

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

with equality if $\nu = 1$.

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

Under the hypotheses of the theorem we immediately deduce the inequality

$$(2.5) \quad |S(f, p^m)| \leq 3.06 \left(\sum_{\alpha \in \mathcal{A}} 1 \right) p^{\frac{t}{M+1}} p^{m(1-\frac{1}{M+1})}.$$

We also offer the following local version of the result of Chen and Nečaev given in (1.5).

Theorem 2.2. *Let f be a polynomial over \mathbb{Z} of degree d , let p be an odd prime with $p \geq (d - 1)^{2d/(d-2)}$ and $d_p(f) \geq 1$, and let $m \geq 2$. Then*

- (i) *For any critical point α of multiplicity ν we have $|S_\alpha(f, p^m)| \leq p^{m(1-\frac{1}{\nu+1})}$.*
- (ii) $|S(f, p^m)| \leq p^{m(1-\frac{1}{d+1})} \leq p^{m(1-\frac{1}{d})}$.

The same result would hold for $p > 4d$, if we only knew that for such p , $|S(f, p)| \leq p^{1-\frac{1}{d}}$ for any f with $d_p(f) \geq 1$. The upper bound in (i) is sharp. In fact if $\nu = 1$, then we always have equality in (i). Also for $f = X^d$ there is a single critical point $\alpha = 0$ of multiplicity $\nu = d - 1$ and we have for $d|m$, $S_\alpha(f, p^m) = p^{m(1-\frac{1}{d+1})}$.

Another approach for bounding exponential sums was taken up in the work of Smith [42], Loxton and Smith [23] and Loxton and Vaughan [24], with the latter obtaining the bound

$$(2.6) \quad |S(f, p^m)| \leq (d - 1)p^{\frac{\delta+\tau}{e+1}} p^{m(1-\frac{1}{e+1})},$$

where e is the maximum multiplicity of any of the complex zeros of f' , $\tau = 0$ if $d < p$, $\tau = 1$ if $d \geq p$, and $\delta = \text{ord}_p(\mathcal{D}(f'))$, where $\mathcal{D}(f')$ is the different of f' . The results of the former two papers were weaker, but their method may still be of interest because of the connection made between the estimation of $S(f, p^m)$ and the estimation of the number of solutions $N(F, p^m)$ of a polynomial congruence

$$F(x) \equiv 0 \pmod{p^m}.$$

For instance, when m is even Smith [42] proved

$$(2.7) \quad |S(f, p^m)| \leq N(f', p^{m/2})p^{m/2},$$

and then applied the following upper bound of Sándor [37]: For any polynomial F over \mathbb{Z} with content coprime to p and having nonzero discriminant D ,

$$N(F, p^m) \leq \deg(F)p^{l/2},$$

for $m > l$, where $p^l \parallel D$. Huxley [15] and Loxton and Smith [23] extended Sándor's bound to arbitrary $m \geq 1$. Stečkin [43] proceeded in the opposite direction using upper bounds on $S(f, p^m)$ to obtain upper bounds for $N(F, p^m)$. Further improvements on $N(F, p^m)$ were made by Stewart [44] and Stewart and Schmidt [38]. In particular Stewart [44] showed that if $D \neq 0$, then

$$N(F, p^m) \leq 2p^{\lfloor l/2 \rfloor} + \deg(F) - 2.$$

Inserting this upper bound into (2.7) may, for some f , lead to a sharpening of the constant in (2.6), in the case that $e = 1$ and $d \gg p^{1/4}$. A direct application of the bound on $N(F, p^m)$ in Stewart and Schmidt [38] doesn't appear to lead to any improvement on (2.6). It may be possible, however, to state a new (and more precise) upper bound on $S(f, p^m)$ in terms of information given by the p -adic solution tree of f' , following the ideas of Stewart and Schmidt [38].

3. LEMMAS

The proofs of Theorems 2.1 and 2.2 require several lemmas. We start with a weaker version of Weil's upper bound that, for our purposes, is more useful.

Lemma 3.1. *Let f be a polynomial over \mathbb{Z} of degree d . Then for any prime p with $d_p(f) \geq 1$ we have*

$$(3.1) \quad |S(f, p)| \leq 1.75 p^{1-\frac{1}{d}}.$$

Proof. First we note that the classical upper bound of Weil,

$$(3.2) \quad |S(f, p)| \leq (d - 1)\sqrt{p},$$

holds for any f and p with $d_p(f) \geq 1$ except for the case where $d = 2$ and $p = 2$. In the latter case the upper bound in (3.1) is trivial. Suppose now that $(d, p) \neq (2, 2)$. We claim that in this case we have the stronger upper bound

$$(3.3) \quad |S(f, p)| \leq (d - 1)^{2/d} p^{1-\frac{1}{d}},$$

whenever $d_p(f) \geq 1$. To see this, suppose first that $p \leq (d - 1)^2$. Then we have the trivial upper bound $|S(f, p)| \leq p \leq (d - 1)^{2/d} p^{1-\frac{1}{d}}$. If $p \geq (d - 1)^2$, then we deduce the upper bound in (3.3) from the upper bound of Weil. \square

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

$$(3.4) \quad \sigma := \text{ord}_p(f(pY + \alpha) - f(\alpha)), \quad g_\alpha(Y) := p^{-\sigma}(f(pY + \alpha) - f(\alpha)).$$

The following recursion relationship is well known and can be found for example in [6], Proposition 4.1.

Lemma 3.2 (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*

- (i) *If $\alpha \notin \mathcal{A}$, then $S_\alpha = 0$.*
- (ii) *If $\alpha \in \mathcal{A}$ and $0 \leq \alpha < p$, then*

$$(3.5) \quad S_\alpha(f, p^m) = e_{p^m}(f(\alpha))p^{\sigma-1}S(g_\alpha, p^{m-\sigma}),$$

where

$$(3.6) \quad S(g_\alpha, p^{m-\sigma}) = \begin{cases} \sum_{s=1}^{p^{m-\sigma}} e_{p^{m-\sigma}}(g_\alpha(s)) & \text{if } m > \sigma, \\ p^{m-\sigma} & \text{if } m \leq \sigma. \end{cases}$$

Set

$$(3.7) \quad \tau := \text{ord}_p(g'_\alpha(Y)), \quad g_1(Y) := p^{-\tau}g'_\alpha(Y).$$

In [6], Lemma 3.1, we established the following relations.

Lemma 3.3. *We have*

- (i)
$$\sigma \geq \begin{cases} t + 2 & \text{if } p \text{ is odd or } \nu > 1, \\ t + 1 & \text{if } p = 2 \text{ and } \nu = 1. \end{cases}$$
- (ii)
$$\sigma \leq \nu + 1 + t - \tau.$$
- (iii)
$$d_p(g) \leq \begin{cases} \sigma - t + \text{ord}_p(d_p(g)) \leq \nu + 1 + \text{ord}_p(d_p(g)), \\ \sigma \leq \nu + 1 + t - \tau. \end{cases}$$
- (iv)
$$d_p(g_1) \leq \sigma + \tau - t - 1 \leq \nu.$$
- (v)
$$p^\tau | d_p(g).$$

Lemma 3.4. *Define $\lambda_i = i$ for $i = 1, 2, 3$ and $\lambda_i = \lambda$ for $i \geq 4$, where λ is the value given in Theorem 2.1. 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 $x = (i + 1)/\lambda < i + 1$, 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 $i \geq 4$. □

4. PROOF OF THEOREM 2.1

The proof is by induction on m . We start by noting that the inequality in part (ii) of the theorem,

$$(4.1) \quad |S(f, p^m)| \leq \lambda p^{\frac{t}{d_1+1}} p^{m(1-\frac{1}{d_1+1})},$$

where $d_1 = d_p(p^{-t}f')$, can always be deduced from part (i) as follows: If $p^{m-t} \leq \lambda^{d_1+1}$, then the upper bound in (4.1) is trivial, that is, $p^m \leq \lambda p^{\frac{t}{d_1+1}} p^{m(1-\frac{1}{d_1+1})}$. Suppose now that $p^{m-t} > \lambda^{d_1+1}$. Since $S_\alpha = 0$ for $\alpha \notin \mathcal{A}$, we have

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

where, for each i , n_i denotes the number of critical points of multiplicity i . Rewriting the expression, using the bound $p^{m-t} > \lambda^{d_1+1}$, and then applying Lemma 3.4 in turn we obtain

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

We proceed now to the proof of part (i) of the theorem. Suppose first that p is odd and that $m \geq t + 2$. If $\nu \leq 3$, then part (i) follows from (2.3). Thus we may assume $\nu \geq 4$. In this case the inequality in part (i) is just

$$(4.2) \quad |S_\alpha(f, p^m)| \leq \lambda p^{\frac{t}{\nu+1}} p^{m(1-\frac{1}{\nu+1})}.$$

When $m = 2$, then since $\sigma \geq 2$ we obtain from (3.5) that $|S_\alpha(f, p^2)| = p \leq p^{2(1-\frac{1}{\nu+1})}$, which is stronger than (4.2). Suppose now that $m \geq 3$ and that the result is true for all smaller values of m . We consider four cases: $\sigma \geq m$, $\sigma = m - 1$, $m - 1 - \tau \leq \sigma \leq m - 2$ and $\sigma \leq m - 2 - \tau$.

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

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

with the last inequality following from Lemma 3.3 (ii).

Case ii. Suppose next that $\sigma = m - 1$. We start by noting that by the inequality $\sigma \leq \nu + t + 1 - \tau$ of Lemma 3.3 (ii) we have trivially

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

unless $\tau = 0$ and $p > 2^{\nu+1}$, and so we may assume that $p > 2^{\nu+1}$. Let $d_p = d_p(g_\alpha)$. We note that, since f is nonconstant, $d_p(g_\alpha) \geq 1$. By Lemma 3.3 (iii) we have

$$(4.3) \quad d_p \leq \nu + 1 + \text{ord}_p(d_p).$$

Suppose that $\text{ord}_p(d_p) \geq 1$. If $d_p = p$, then by (4.3) $p \leq \nu + 2$, contradicting our assumptions that $p > 2^{\nu+1}$ and $\nu \geq 2$. Otherwise $d_p \geq 2p$ and thus since $\text{ord}_p(d_p) \leq d_p/2$ we have by (4.3) that

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

again contradicting our assumptions.

Thus we must have $\text{ord}_p(d_p) = 0$ and so by (4.3), $d_p \leq \nu + 1$. It follows from (3.5) and the upper bound of Lemma 3.1 that

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

By Lemma 3.3 (ii) we then obtain (4.2).

Case iii. Suppose that $m - 1 - \tau \leq \sigma \leq m - 2$. In particular, we must have $\tau \geq 1$. Then we have the trivial estimate

$$(4.4) \quad \begin{aligned} |S_\alpha| &\leq p^{m-1} = p^{\frac{m-\nu-1}{\nu+1}} p^{m(1-\frac{1}{\nu+1})} \\ &\leq p^{\frac{1}{\nu+1}} p^{\frac{\sigma+\tau-\nu-1}{\nu+1}} p^{m(1-\frac{1}{\nu+1})} \leq p^{\frac{1}{\nu+1}} p^{\frac{t}{\nu+1}} p^{m(1-\frac{1}{\nu+1})}, \end{aligned}$$

with the latter inequality following from Lemma 3.3 (ii). Now, by Lemma 3.3 (v) $p^\tau |d_p(g_\alpha)|$. Since $\tau \geq 1$ and $d_p(g_\alpha) \geq 1$, it follows from Lemma 3.3 (iii) that

$$p - 1 \leq p^\tau - \tau \leq d_p(g_\alpha) - \text{ord}_p(d_p(g_\alpha)) \leq \nu + 1.$$

Thus for $\nu \geq 2$ we have $p^{\frac{1}{\nu+1}} \leq (\nu + 2)^{1/\nu+1} \leq 4^{1/3} \leq 2$, and so (4.2) follows from (4.4).

Case iv. Suppose finally that $\sigma \leq m - 2 - \tau$. In this case we can apply the induction assumption to the sum $S(g_\alpha, p^{m-\sigma})$ and obtain from (3.5) and (4.1) that

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

where $d_2 = d_p(p^{-\tau} g'_\alpha)$. Now from Lemma 3.3 (iv) we have $d_2 \leq \nu$ and thus since $m - \sigma - \tau > 0$ we obtain

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

and thus (4.2) follows from Lemma 3.3 (ii). This completes the proof of the theorem for the case of odd p .

Suppose now that $p = 2$ and that $m \geq t + 3$. Again, by (2.3) we may assume that $\nu \geq 4$. The inequality in (4.2) is trivial if $m \leq 2\nu + 2 + t$ and so we may assume that $m \geq 2\nu + 3 + t$. By the inequality $\sigma \leq \nu + t + 1 - \tau$ of Lemma 3.3 (ii) it follows that $m - \sigma \geq \tau + 3$. Thus we can apply the recursion relationship of

Lemma 3.2 and obtain from the induction assumption that

$$|S_\alpha| = 2^{\sigma-1} |S(g_\alpha, 2^{m-\sigma})| \leq \lambda 2^{\sigma-1} 2^{\frac{\tau}{\nu+1}} 2^{(m-\sigma)(1-\frac{1}{\nu+1})} \leq \lambda 2^{\frac{t}{\nu+1}} 2^{m(1-\frac{1}{\nu+1})},$$

completing the proof.

5. PROOF OF THEOREM 2.2

The proof of Theorem 2.2 follows the same line of argument as the proof of Theorem 2.1. We need only add the following lemma.

Lemma 5.1. *Let f be a polynomial of degree d , let p be a prime with $p \geq 4(d-1)$ and $d_p(f) \geq 1$, and let $m \geq 2$. If for each critical point α associated with the sum $S(f, p^m)$ we have $|S_\alpha(f, p^m)| \leq p^{m(1-\frac{1}{\nu+1})}$, then*

$$(5.1) \quad |S(f, p^m)| \leq p^{m(1-\frac{1}{d_1+1})} \leq p^{m(1-\frac{1}{d})}.$$

Proof. 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 $|S(f, p^m)| = |S_\alpha(f, p^m)| \leq p^{m(1-\frac{1}{d_1+1})}$, by assumption. Finally, suppose that $p^m > (p/d_1)^{d_1+1}$ and that every critical point is of multiplicity less than d_1 . We 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 $i = 1, 2, 3$ and for $i \geq 4$ it follows from Lemma 3.4. It follows that

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

and thus

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

Letting n_i denote the number of critical points of multiplicity i , we obtain

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

□

The proof of Theorem 2.2 proceeds by induction. Suppose that p is odd with $p \geq (d-1)^{2d/(d-1)}$, that $m \geq 2$ and that f is a polynomial over \mathbb{Z} with $d_p(f) \geq 1$. If $d = 1$ or $d = 2$ the result is well known. Suppose now that $d \geq 3$. Then, in particular, $t = 0$ and $p \geq 4(d-1)$. We shall prove by induction on m that for any critical point α of multiplicity ν ,

$$(5.2) \quad |S_\alpha(f, p^m)| \leq p^{m(1-\frac{1}{\nu+1})}.$$

The cases $m = 2$ and $\sigma \geq m$ are identical as before. Suppose next that $\sigma = m - 1$. By Weil and our assumption on p , $|S(g_\alpha, p)| \leq p^{1-\frac{1}{d_p}}$, and thus since $d_p \leq \nu + 1$ we obtain

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

Since $\tau = 0$ the third case never occurs. Finally suppose that $\sigma \leq m - 2$. In this case we apply the induction assumption to $|S(g_\alpha, p^{m-\sigma})|$. Let $d_2 = d_p(g'_\alpha)$. By Lemma 5.1 it follows that

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

as before.

6. PROOF OF THEOREM 1.1

Let f be a polynomial over \mathbb{Z} and p any prime with $d_p(f) \geq 1$. If $d = 1$, then $S(f, p^m) = 0$ and so we may assume $d \geq 2$. If $m = 1$, then the theorem is just a weaker version of Lemma 3.1. If $2 \leq m \leq t + 1$, then using the fact that $p^t \leq d_p(f) \leq d$ we have the trivial upper bound

$$|S(f, p^m)| \leq p^m \leq 3p^{m(1-\frac{1}{d})},$$

for in this case

$$p^t \leq d \leq 3^{d/2} \leq 3^{d\frac{t}{t+1}} \leq 3^{\frac{dt}{m}},$$

and so $p^{m/d} \leq 3$. If $p = 2$ and $m = t + 2$, then $p^{m/d} = 2^{\frac{t+2}{d}} \leq (4d)^{1/d} \leq 3$ and so the trivial bound suffices again. If p is odd and $m \geq t + 2$ or $p = 2$ and $m \geq 3$, then by Theorem 2.1 (ii) and the fact that $p^t \leq d$ we have

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

REFERENCES

1. N.M. Akulinichev, *Estimates for rational trigonometric sums of a special type*, Doklady Acad. Sci. USSR 161 (1965), 743-745. English transl. in Doklady 161, no. 4 (1965), 480-482.
2. J.H.H. Chalk, *On Hua's estimate for exponential sums*, Mathematika 34 (1987), 115-123. MR **89d**:11067
3. 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.
4. ———, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711-719. MR **58**:542
5. J.R. Chen and C. Pan, *Analytic number theory in China I*, in Number Theory and Its Applications in China, Contemp. Math. 77, Amer. Math. Soc. (1988), 1-17. MR **90c**:11060
6. T. Cochrane and Z. Zheng, *Pure and mixed exponential sums*, Acta Arithmetica 91, no. 3 (1999), 249-278. MR **2000k**:11093
7. ———, *Exponential sums with rational function entries*, Acta Arithmetica 95, no. 1 (2000), 67-95. CMP 2001:02
8. P. Ding, *An improvement to Chalk's estimation of exponential sums*, Acta Arith. 59 no. 2 (1991), 149-155. MR **93a**:11069
9. ———, *On a conjecture of Chalk*, J. Number Theory 65 no. 2 (1997), 116-129. MR **98f**:11086

10. G.H. Hardy and J.E. Littlewood, *Some problems of "Partitio Numerorum"; I: A new solution of Waring's problem*, Nachrichten von der K. Gesellschaft der Wissenschaften zu Göttingen Math.-phys. Klasse, (1920), 33-54.
11. D.R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from k th powers, and for Heilbronn's exponential sum*, Quart. J. Math. 51 (2000), 221-235. CMP 2000:14
12. L.K. Hua, *On exponential sums*, J. Chinese Math. Soc. 20 (1940), 301-312. MR **2**:347h
13. ———, *On exponential sums*, Sci. Record (Peking) (N.S.) 1 (1957), 1-4. MR **20**:22
14. ———, *Additiv Primzahltheorie*, Teubner, Leipzig (1959), 2-7.
15. M.N. Huxley, *A note on polynomial congruences*, Recent Progress in Analytic Number Theory, Vol. 1 (H. Halberstam and C. Hooley, eds.), Academic Press, London, 1981, 193-196. MR **83e**:10005
16. A.A. Karatsuba, *On bounds of complete trigonometrical sums*, Matem. Zametki 1 no. 2 (1967), 199-208. English transl. in Math. Notes. Acad. Sci. USSR 1 (1967), 133-139.
17. S.V. Konyagin, *Estimates for Gaussian sums and Waring's problem modulo a prime*, Trudy Mat. Inst. Steklov 198 (1992), 111-124; translation in Proc. Steklov Inst. Math. 1994, 105-107. MR **96e**:11122
18. ———, *Exponential sums over multiplicative groups of residues*, preprint, (2000).
19. 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.
20. ———, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999. MR **2000h**:11089
21. G. Lachaud, *Bounds for exponential sums with invariant phase function*, preprint.
22. W.K.A. Loh, *Hua's Lemma*, Bull. Austral. Math. Soc. 50, no. 3 (1994), 451-458. MR **95i**:11091
23. J.H. Loxton and R.A. Smith, *On Hua's estimate for exponential sums*, J. London Math. Soc. (2), 26 (1982), 15-20. MR **84c**:10033
24. J.H. Loxton and R.C. Vaughan, *The estimation of complete exponential sums*, Canad. Math. Bull. 28 no. 4 (1985), 442-454. MR **87c**:11075
25. M. Lu, *A note on the estimate of a complete rational trigonometric sum*, Acta Math. Sin. 27 (1984), 817-823. MR **87a**:11075
26. ———, *The estimate of complete trigonometric sums*, Sci. Sin. 28, no. 6, (1985), 561-578. MR **87h**:11078
27. ———, *A note on complete trigonometric sums for prime powers*, Sichuan Daxue Xuebao 26 (1989), 156-159. MR **91g**:11090
28. H.L. Montgomery, R.C. Vaughan and T.D. Wooley, *Some remarks on Gauss sums associated with k th powers*, Math. Proc. Cambridge Philos. Soc. 118, no. 1, (1995), 21-33. MR **96e**:11110
29. L.J. Mordell, *On a sum analogous to a Gauss's sum*, Quart. J. Math., 3 (1932), 161-167.
30. G.L. Mullen and I.E. Shparlinski, *Open problems and conjectures in finite fields*, in Finite Fields and Applications (Glasgow, 1995), London Math. Soc. Lecture Note Series, No. 233, S. Cohen and H. Niederreiter, eds., Cambridge University Press, Cambridge, 1996, 243-268. MR **97m**:11145
31. V.I. Nečaev, *An estimate of a complete rational trigonometric sum*, Mat. Zametki 17 (1975), 839-849; English translation in Math. Notes 17 (1975). MR **53**:5501
32. ———, *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. MR **91f**:11059
33. 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. MR **83i**:10048
34. M. Qi and P. Ding, *Estimate of complete trigonometric sums*, Kexue Tongbao 29 (1984), 1567-1569. MR **87b**:11082a
35. ———, *On estimate of complete trigonometric sums*, China Ann. Math. B6 (1985), 110-120. MR **87b**:11082b
36. ———, *Further estimate of complete trigonometric sums*, J. Tsinghua Univ. 29, no. 6, (1989), 74-85. MR **91m**:11061

37. G. Sándor, *Über die Anzahl der Lösungen einer Kongruenz*, Acta Math. 87 (1952), 13-17. MR **13**:913d
38. W.M. Schmidt and C.L. Stewart, *Congruences, trees and p -adic integers*, Trans. Amer. Math. Soc. 349, no. 2, (1997), 605-639. MR **97e**:11045
39. I.E. Shparlinski, *On bounds of Gaussian sums*, Matem. Zametki, 50 (1991), 122-130 (in Russian).
40. ———, *Computational and Algorithmic Problems in Finite Fields*, Kluwer Academic Pub., Boston, (1992). MR **94j**:11122
41. ———, *On Gaussian sums for finite fields and elliptic curves*, Proc. 1-st French-Soviet Workshop on Algebraic Coding, Paris, 1991, Lect. Notes in Computer Sci., 537 (1992), 5-15. MR **95c**:11146
42. R.A. Smith, *Estimates for exponential sums*, Proc. Amer. Math. Soc. 79, no. 3, (1980), 365-368. MR **81k**:10059
43. 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. MR **58**:543
44. C.L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc. 4, no. 4, (1991), 793-835. MR **92j**:11032
45. R.C. Vaughan, *The Hardy-Littlewood method*, Cambridge Univ. Press, New York, (1981). MR **84b**:10002
46. A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204-207. MR **10**:234e
47. M. Zhang and Y. Hong, *On the maximum modulus of complete trigonometric sums*, Acta Math. Sinica, New Series 3, no. 4 (1987), 341-350. MR **89d**:11068

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KANSAS 66506
E-mail address: cochrane@math.ksu.edu

DEPARTMENT OF MATHEMATICS, TSINGHUA UNIVERSITY, BEIJING, PEOPLE'S REPUBLIC OF CHINA
E-mail address: zzheng@math.tsinghua.edu.cn