Bounds on fewnomial exponential sums over Z*p.*

Todd Cochrane and Christopher Pinner

How to cite this manuscript

If you make reference to this version of the manuscript, use the following information:

Cochrane, T., & Pinner, C. (2010). Bounds on fewnomial exponential sums over Z*p.* Retrieved from http://krex.ksu.edu

Published Version Information

Citation: Cochrane, T., & Pinner, C. (2010). Bounds on fewnomial exponential sums over Z*p.* Mathematical Proceedings of the Cambridge Philosophical Society, 149(2), 217-227.

Digital Object Identifier (DOI): doi:10.1017/S0305004110000319

Publisher's Link: http://journals.cambridge.org/action/displayBackIssues?jid=PSP

Math. Proc. Camb. Phil. Soc. (2010), **149**, 217 © *Cambridge Philosophical Society* 2010
doi:10.1017/S0305004110000319
First published online 22 June 2010

Bounds on fewnomial exponential sums over $\mathbb{Z}_p$

BY TODD COCHRANE AND CHRISTOPHER PINNER
Department of Mathematics, Kansas State University, Manhattan, KS 66506, *U.S.A.*
e-mail: cochrane@math.ksu.edu, pinner@math.ksu.edu

(*Received* 15 *January* 2010; *revised* 27 *April* 2010)

Abstract

We obtain a number of new bounds for exponential sums of the type $S(\chi, f) = \sum_{x=1}^{p-1} \chi(x)e_p(f(x))$, with p a prime, $f(x) = \sum_{i=1}^{r} a_i x^{k_i}$, $a_i, k_i \in \mathbb{Z}$, $1 \leqslant i \leqslant r$ and χ a multiplicative character $\pmod p$. The bounds refine earlier Mordell-type estimates and are particularly effective for polynomials in which a certain number of the k_i have a large gcd with $p-1$. For instance, if $f(x) = \sum_{i=1}^{m} a_i x^{k_i} + g(x^d)$ with $d|(p-1)$ then $|S(\chi, f)| \leqslant p\,(k_1 \cdots k_m)^{\frac{1}{m^2}}/d^{\frac{1}{2m}}$. If $f(x) = ax^k + h(x^d)$ with $d|(p-1)$ and $(k, p-1) = 1$ then $|S(\chi, f)| \leqslant p/\sqrt{d}$, and if $f(x) = ax^k + bx^{-k} + h(x^d)$ with $d|(p-1)$ and $(k, p-1) = 1$ then $|S(\chi, f)| \leqslant p/\sqrt{d} + \sqrt{2}p^{3/4}$.

1. *Introduction*

For a prime p, Laurent polynomial

$$f(x) = a_1 x^{k_1} + \cdots + a_r x^{k_r}, \tag{1·1}$$

with $a_i, k_i \in \mathbb{Z}$, $1 \leqslant i \leqslant r$, and multiplicative character $\chi \mod p$ we consider the mixed exponential sum

$$S(\chi, f) := \sum_{x=1}^{p-1} \chi(x)e_p(f(x)),$$

where $e_p(\cdot)$ is the additive character $e_p(\cdot) = e^{2\pi i \cdot/p}$ on the finite field $\mathbb{Z}_p$. (Unless specified, the k_i need not be distinct, or nonzero.) We shall say that f is in 'standard form' when $p \nmid a_1 \cdots a_r$ and the k_i are distinct mod $p-1$. For such sums the classical Weil bound [**10**] (see [**3**] or [**9**] for Laurent f) yields,

$$|S(\chi, f)| \leqslant \max\{|k_i|, |k_i - k_j|\}p^{\frac{1}{2}}, \tag{1·2}$$

nontrivial only if $\max\{|k_i|, |k_i - k_j|\} < \sqrt{p}$. Mordell [**8**] gave a different type of bound which depended rather on the product of all the exponents k_i. In [**4**] we obtained the following improvement in Mordell's bound:

$$|S(\chi, f)| \leqslant 4^{\frac{1}{r}}(\ell_1' \ell_2' \cdots \ell_r')^{\frac{1}{r^2}} p^{1-\frac{1}{2r}}, \tag{1·3}$$

for any nonconstant f in standard form, where

$$\ell_i' = \begin{cases} k_i, & \text{if } k_i > 0, \\ r|k_i|, & \text{if } k_i < 0. \end{cases} \tag{1·4}$$

In [**5**] we showed that some of the larger ℓ_i' can in fact be omitted from the product (at the cost of a worse dependence on p), obtaining for any m with $r/2 < m \leqslant r$,

$$|S(\chi, f)| \leqslant 4^{\frac{1}{m}} (\ell_1 \cdots \ell_m)^{\frac{1}{m^2}} p^{1-\frac{1}{m^2}\left(m-\frac{1}{2}r\right)}, \tag{1·5}$$

provided $k_1, \ldots, k_m$ are distinct and nonzero $\pmod{p-1}$ and $p \nmid a_1 \cdots a_m$, where

$$\ell_i = \begin{cases} k_i, & \text{if } k_i > 0, \\ m|k_i|, & \text{if } k_i < 0. \end{cases} \tag{1·6}$$

A different type of bound was obtained by Akuliničev [**1**], showing for binomials that

$$|S(\chi, ax^{k_1} + bx^{k_2})| \leqslant \frac{p}{\sqrt{k_1}} + \sqrt{(k_2, p-1) - 1}\, p^{\frac{3}{4}}, \tag{1·7}$$

when $k_1 | (p-1)$ and $(k_1, k_2) = 1$, and for trinomials that

$$|S(\chi, ax^{k_1} + bx^{k_2} + cx^{k_3})| \leqslant \sqrt{2} p\, k_2^{-\frac{1}{4}}, \tag{1·8}$$

if $(k_3, p-1) = 1$ and $k_1, k_2 | (p-1)$ with $(k_1, k_2) = 1$ and $k_2 < k_1$. The condition $k_2 < k_1$ is certainly needed in view of the example

$$|S(\chi, ax^{(p-1)/2} + bx^{(p+1)/2} - bx)| = \frac{1}{2} p + O(\sqrt{p}),$$

when χ is the principal character or the Legendre symbol. For trinomial polynomials the authors showed in [**4**] and [**5**] the Mordell [**8**] type bounds

$$|S(\chi, ax^{k_1} + bx^{k_2} + cx^{k_3})| \leqslant \left(\frac{80}{9}\right)^{\frac{1}{9}} (k_1 k_2 k_3)^{\frac{1}{9}} p^{\frac{5}{6}}, \tag{1·9}$$

and

$$|S(\chi, ax^{k_1} + bx^{k_2} + cx^{k_3})| \leqslant \left(\frac{(k_1, k_2, k_3, p-1)}{(k_2, k_3)}\right)^{1/4} (k_2 k_3)^{\frac{1}{4}} p^{\frac{7}{8}}, \tag{1·10}$$

while in [**6**] they obtained

$$|S(\chi, ax^{k_1} + bx^{k_2} + cx^{k_3})| \leqslant 3^{\frac{1}{4}} (k_1, k_2, k_3, p-1)^{\frac{1}{2}} p^{\frac{7}{8}} + \sqrt{5} (k_1 k_2 k_3)^{\frac{1}{4}} p^{\frac{5}{8}}. \tag{1·11}$$

In general, if all but one of the exponents (or all but a few small degree exponents) have a large common factor with $(p-1)$ then repeatedly applying Akuliničev's averaging method gives the following bound:

THEOREM 1·1. *Suppose that f is of the form*

$$f(x) = g(x) + g_2(x^{k_2}) + \cdots + g_r(x^{k_r})$$

with $r \geqslant 2$, where $g, g_2, \ldots, g_r$ are Laurent polynomials over $\mathbb{Z}$, and g (written in standard form) contains a monomial $a_1 x^{k_1}$, $k_1 \neq 0$, with $p \nmid a_1$.

Then for any multiplicative character $\chi \pmod{p}$,

$$|S(\chi, f)| \leqslant p \sum_{i=0}^{r-2} \left(\frac{(k_{r-i}, k_1, p-1)}{(k_{r-i}, p-1)}\right)^{\frac{1}{2^{i+1}}} + D^{\frac{1}{2^{r-1}}} p^{1-\frac{1}{2^r}}, \tag{1·12}$$

where

$$D = \begin{cases} \deg g - 1, & \textit{if } g(x) \textit{ is a polynomial,} \\ (k_1, p-1) - 1, & \textit{if } g(x) = a_1 x^{k_1} \textit{ is a monomial,} \end{cases}$$

and D is the maximum difference of the exponents when g contains exponents of both signs.

Replacing x by x^{-1} we can of course assume that g contains at least one positive exponent. The same bound also holds for the complete untwisted sum $\sum_{x=0}^{p-1} e_p(f(x))$ when f is a polynomial (no extra $+1$ is needed to account for the $x=0$ term). The second term in (1·12) arises from using the Weil bound for exponential sums involving Laurent polynomials with the same set of exponents as g. The more general version given in (3·3) can be used when there are better bounds for such sums. Notice that when g is a monomial $a_1x^{k_1}$ with $(k_1, p-1)=1$ this second term vanishes. The bound of Akuliničev (1·7) is implied by the case $r=2$ and (1·8) essentially from $r=3$ (using the unsimplified form (3·3) to obtain the same constant). The theorem follows from the reduction formula given in Lemma 3·1.

We observe here that combining the approach we used in [**5**] with features of the Akuliničev approach can lead to a variety of new fewnomial bounds appropriate when t of the exponents, $k_{r-t+1}, \ldots, k_r$ say, share a large common factor with $(p-1)$:

THEOREM 1·2. *For positive integers m, r, t with $1 \leqslant t < r$ and $(r-t)/2 < m \leqslant (r-t)$, any Laurent polynomial $f(x)$ as in* (1·1) *with $k_1, \ldots, k_{r-t}$ distinct and nonzero* $\pmod{p-1}$, *$p \nmid a_1 \cdots a_{r-t}$, and any multiplicative character χ* $\pmod{p}$,

$$|S(\chi, f)| \leqslant c_m(\ell_1 \cdots \ell_m)^{\frac{1}{m^2}} p^{1+\frac{1}{2m^2}(r-t-m)} (k_{r-t+1}, \ldots, k_r, p-1)^{-\frac{1}{2m}} \mu_{m,t},$$

where

$$\mu_{m,t} = \left(\frac{(k_1, \ldots, k_r, p-1)(k_1, \ldots, k_{r-t}, p-1)(k_1, \ldots, k_m, p-1)^{m-1}(k_1, \ldots, k_m, k_{r-t+1}, \ldots, k_r, p-1)^{m-1}}{(k_1, \ldots, k_m)^{2m}} \right)^{\frac{1}{2m^2}},$$

the l_i are as defined in (1·6), *and $c_1 = 1$, $c_2 = (3/2)^{\frac{1}{4}}$, $c_m = (m+1)^{\frac{1}{m^2}}$ for $m \geqslant 3$. If $k_1, \ldots, k_m$ are all positive then we can take $c_m = 1$ for any m.*

In particular, this bound is non-trivial if $(k_{r-t+1}, \ldots, k_r, p-1) \geqslant 4^{2/3}(\ell_1 \cdots \ell_m)^{\frac{2}{m}} p^{(r-t-m)/m}$ and improves upon (1·5) if $(k_{r-t+1}, \ldots, k_r, p-1) \geqslant p^{1-\frac{t}{m}}$. The factor $\mu_{m,t}$ is at most one, and yields a bonus savings in certain situations. The bound comes from counting the number of solutions $T_{m,t}$ in $\mathbb{Z}_p^{*\,2m}$ to the system

$$x_1^{k_i} + \cdots + x_m^{k_i} \equiv y_1^{k_i} + \cdots + y_m^{k_i} \pmod{p}, \qquad 1 \leqslant i \leqslant r-t, \tag{1·13}$$

and $T_{m,t}^*$ the number of those solutions with $x_j^{k_i} = y_j^{k_i} = 1$, $i = r-t+1, \ldots, r$, $j = 1, \ldots, m$. The theorem follows at once from the estimates for $T_{m,t}$, $T_{m,t}^*$ given in Lemma 2·1,

$$\begin{aligned} T_{m,t} &\leqslant C_m \frac{(k_1, \ldots, k_{r-t}, p-1)(k_1, \ldots, k_m, p-1)^{m-1}}{(k_1, \ldots, k_m)^m} (\ell_1 \ldots \ell_m)\,(p-1)^m, \\ T_{m,t}^* &\leqslant C_m \frac{(k_1, \ldots, k_r, p-1)(k_1, \ldots, k_m, k_{r-t+1}, \ldots, k_r, p-1)^{m-1}}{(k_1, \ldots, k_m)^m} \\ &\quad \times (\ell_1 \ldots \ell_m)(k_{r-t+1}, \ldots, k_r, p-1)^m, \end{aligned}$$

and the following, (setting $v = w = m$), with $c_m = C_m^{\frac{1}{m^2}}$.

LEMMA 1·1. *For any positive integers r, t, v, w with $1 \leqslant t < r$ and Laurent polynomial $f(x)$ as in* (1·1) *with $k_1, \ldots, k_{r-t}$ distinct and nonzero* $\pmod{p-1}$, $p \nmid a_1 \cdots a_{r-t}$, *and multiplicative character $\chi \pmod{p}$,*

$$|S(\chi, f)| \leqslant (p-1)^{1-\frac{1}{v}} p^{\frac{r-t}{2vw}} (T^*_{v,t} T_{w,t})^{\frac{1}{2vw}} (k_{r-t+1}, \ldots, k_r, p-1)^{-\frac{1}{w}}.$$

The case $m = 1$ of Theorem 1·2 may be stated as follows: For $r \geqslant 2$ and any $f(x)$ as in (1·1) with k_1 nonzero $\pmod{p-1}$ and $p \nmid a_1$,

$$|S(\chi, f)| \leqslant p \left(\frac{(k_1, p-1)(k_1, \ldots, k_r, p-1)}{(k_2, \ldots, k_r, p-1)} \right)^{1/2}, \tag{1·14}$$

a bound also discovered by Yu [**12**, theorem 1] for the case of binomials. The case $r - t = m$ gives for any m with $1 \leqslant m \leqslant r-1$, and any $f(x)$ as in (1·1) with $k_1, \ldots, k_m$ distinct and nonzero $\pmod{p-1}$, $p \nmid a_1 \cdots a_m$,

$$|S(\chi, f)| \leqslant c_m p \frac{(\ell_1 \cdots \ell_m)^{\frac{1}{m^2}}}{(k_{m+1}, \ldots, k_r, p-1)^{\frac{1}{2m}}} \left(\frac{(k_1, \ldots, k_r, p-1)(k_1, \ldots, k_m, p-1)}{(k_1, \ldots, k_m)^2} \right)^{\frac{1}{2m}}. \tag{1·15}$$

In particular for any $f(x)$ in standard form of the type $f(x) = a_1 x^{k_1} + \cdots + a_m x^{k_m} + h(x^d)$ with $d | (p-1)$, $k_i > 0$, $1 \leqslant i \leqslant m$ and $h(x)$ any Laurent polynomial,

$$|S(\chi, f)| \leqslant p\, (k_1 \cdots k_m)^{\frac{1}{m^2}} / d^{\frac{1}{2m}}. \tag{1·16}$$

For monomials we gain nothing new from Theorem 1·2 while for binomials we just have the bound in (1·14). For trinomials we can take $m = 2$, $t = 1$ to gain the new bound,

$$|S(\chi, f)| \leqslant \left(\frac{3}{2}\right)^{1/4} \left(\frac{(k_1, k_2, k_3, p-1)(k_1, k_2, p-1)}{(k_1, k_2)^2} \right)^{\frac{1}{4}} (\ell_1 \ell_2)^{\frac{1}{4}} (k_3, p-1)^{-\frac{1}{4}} p. \tag{1·17}$$

Example 1·1. Let $f(x) = ax^k + h(x^d)$ where $d | (p-1)$, k is nonzero $\pmod{p-1}$, $p \nmid a$, and $h(x)$ is any Laurent polynomial. Then by (1·14),

$$|S(\chi, f)| \leqslant p \sqrt{\frac{(k, p-1)(k, d)}{d}} \leqslant \frac{p(k, p-1)}{\sqrt{d}},$$

while from Theorem 1·1 (using $r = 2$, $g(x) = ax^k$),

$$|S(\chi, f)| \leqslant p \frac{\sqrt{(k, d)}}{\sqrt{d}} + \sqrt{(k, p-1) - 1}\; p^{\frac{3}{4}}.$$

Example 1·2. Let $f(x) = ax^k + bx^{-k} + h(x^d)$, where $d | (p-1)$, $k > 0$ is nonzero $\pmod{p-1}$, $p \nmid ab$, and $h(x)$ is any Laurent polynomial. Then, by (1·15) with $m = 2$ we have

$$|S(\chi, f)| \leqslant 3^{\frac{1}{4}} \frac{(k, p-1)^{1/4} (k, d)^{1/4} p}{d^{1/4}},$$

while from Theorem 1·1 (using $r = 2$, $g(x) = ax^k + bx^{-k}$),

$$|S(\chi, f)| \leqslant p \frac{\sqrt{(k, d)}}{\sqrt{d}} + \sqrt{2(k, p-1)}\, p^{\frac{3}{4}}.$$

Example 1·3. Let $f(x)=ax^k+bx^{-k}+cx^{\ell}+h(x^d)$ with $d|(p-1)$, k, $-k$, ℓ distinct and nonzero $\pmod{p-1}$, $k>0$, $p\nmid abc$, and $h(x)$ is any Laurent polynomial. Then using Theorem 1·2 with $m=2$, $t=r-3$, we have

$$|S(\chi,f)|\leqslant 3^{\frac{1}{4}}\frac{[(k,d)(k,p-1)(k,l,d)(k,l,p-1)]^{1/8}p^{9/8}}{d^{1/4}}\leqslant 3^{\frac{1}{4}}\frac{(k,p-1)^{1/2}p^{9/8}}{d^{1/4}}.$$

while from Theorem 1·1 (using $r=2$, $g(x)=ax^k+bx^{-k}+cx^l$),

$$|S(\chi,f)|\leqslant p\frac{\sqrt{(k,d)}}{\sqrt{d}}+\sqrt{\max\{2k,k+|l|\}}p^{\frac{3}{4}}.$$

Another class of polynomials for which nontrivial estimates are available was introduced by Bourgain [**2**]:

THEOREM 1·3. [**2**, theorem 7]. *For $r\in\mathbb{Z}_+$, $\epsilon>0$, there is a $\delta=\delta(r,\epsilon)$ such that if $\{k_1,\ldots,k_r\}$ are distinct positive integers with $k_1<p^{\frac{1}{2}-\epsilon}$, $(k_i-k_1,p-1)<p^{1-\epsilon}$, $2\leqslant i\leqslant r$, and $f(x)=g(x)+a_2x^{k_2}+\cdots+a_rx^{k_r}\in\mathbb{Z}[x]$ with $g(x)$ a polynomial of degree $d<p^{\frac{1}{2}-\epsilon}$ involving (when written in standard form) a monomial $a_1x^{k_1}$, $p\nmid a_1$, then $|\sum_{x=1}^{p}e_p(f(x)|<p^{1-\delta}$.*

In this direction we offer the following corollary of Theorem 1·1

COROLLARY 1·1. *Let $\epsilon>0$, $r\geqslant 2$ and $\{k_1,\ldots,k_r\}$ be integers such that $1\leqslant k_1<p^{\frac{1}{2}-\epsilon}$ and*

$$(k_1,k_i,p-1)<(k_i,p-1)p^{-\epsilon},\quad 2\leqslant i\leqslant r.$$

Suppose that f is of the form

$$f(x)=g(x)+g_2(x^{k_2})+\cdots+g_r(x^{k_r})$$

where $g,g_2,\ldots,g_2$ are Laurent polynomials over $\mathbb{Z}$ and $g(x)$ (written in standard form) contains a monomial $a_1x^{k_1}$, $p\nmid a_1$, and has degree (maximum difference of exponents if g has negative exponents)

$$d<p^{\frac{1}{2}-\epsilon}.$$

Then

$$|S(\chi,f)|\leqslant 3\ p^{1-\frac{\epsilon}{2^{r-1}}}.$$

2. *Proofs of Lemma 1·1 and Lemma 1·2*

Let r,t,v,w be positive integers with $1\leqslant t<r$ and k_i,a_i be integers with $p\nmid a_1\cdots a_{r-t}$. The proof of Lemma 1·1 is similar to that of [**5**, lemma 1·1] except we average only over those y from the set

$$Y=\left\{y\in\mathbb{Z}_p^*\ :\ y^{k_i}=1,\ i=r-t+1,\ldots,r\right\},\quad |Y|=(k_{r-t+1},\ldots,k_r,p-1).$$

For $\vec{u}=(u_1,\ldots,u_{r-t})\in\mathbb{Z}_p^{r-t}$ and positive integer w, put

$$N_w(\vec{u})=\#\left\{(x_1,\ldots,x_w)\in{\mathbb{Z}_p^*}^{w}\ :\ \sum_{i=1}^{w}x_i^{k_j}=u_j,\quad j=1,\ldots,r-t\right\},$$

so that

$$\sum_{\vec{u}\in\mathbb{Z}_p^{r-t}} N_w(\vec{u}) = (p-1)^w, \qquad \sum_{\vec{u}\in\mathbb{Z}_p^{r-t}} N_w^2(\vec{u}) = T_{w,t}. \tag{2·1}$$

For any multiplicative character χ and positive integer v, the simple observation that $\sum_{u\in\mathbb{Z}_p} e_p(au) = p$ if $a \equiv 0 \pmod{p}$ and zero otherwise, gives

$$\begin{aligned}
&\sum_{\vec{u}\in\mathbb{Z}_p^{r-t}} \left| \sum_{y\in Y} \chi(y) e_p(a_1 u_1 y^{k_1} + \cdots + a_{r-t} u_{r-t} y^{k_{r-t}}) \right|^{2v} \\
&= \sum_{\substack{x_1,\ldots,x_v,\\ y_1,\ldots,y_v\in Y}} \chi\big(x_1\cdots x_v y_1^{-1}\cdots y_v^{-1}\big) \sum_{\vec{u}\in\mathbb{Z}_p^{r-t}} e_p\left(\sum_{j=1}^{r-t} a_j u_j \big(x_1^{k_j} + \cdots + x_v^{k_j} - y_1^{k_j} - \cdots - y_v^{k_j}\big)\right) \\
&= p^{r-t} {\sum}^{*} \chi\big(x_1\cdots x_v y_1^{-1}\cdots y_v^{-1}\big) \leqslant p^{r-t} T_{v,t}^{*},
\end{aligned} \tag{2·2}$$

where $\sum^*$ denotes a sum over the $x_1,\ldots,x_v,y_1,\ldots,y_v$ in Y satisfying $\sum_{j=1}^{v} x_j^{k_i} \equiv \sum_{j=1}^{v} y_j^{k_i} \pmod{p}$ for $1 \leqslant i \leqslant r-t$.

Writing $S = S(\chi, f)$, we have for any positive integer w,

$$\begin{aligned}
|Y|S^w &= \sum_{y\in Y}\left(\sum_{x=1}^{p-1} \chi(yx) e_p\big(a_1(yx)^{k_1} + \cdots + a_r(yx)^{k_r}\big)\right)^w \\
&= \sum_{y\in Y} \chi^w(y) \sum_{x_1,\ldots,x_w\in\mathbb{Z}_p^*} \chi(x_1\cdots x_w) e_p\left(\sum_{j=1}^{r} a_j y^{k_j}\big(x_1^{k_j} + \cdots + x_w^{k_j}\big)\right) \\
&= \sum_{x_1,\ldots,x_w\in\mathbb{Z}_p^*} \chi(x_1\cdots x_w) e_p\left(\sum_{j=r-t+1}^{r} a_j\big(x_1^{k_j} + \cdots + x_w^{k_j}\big)\right) \\
&\quad \cdot \sum_{y\in Y} \chi^w(y) e_p\left(\sum_{j=1}^{r-t} a_j y^{k_j}\big(x_1^{k_j} + \cdots + x_w^{k_j}\big)\right),
\end{aligned}$$

and so

$$|Y||S|^w \leqslant \sum_{\vec{u}\in\mathbb{Z}_p^{r-t}} N_w(\vec{u}) \left| \sum_{y\in Y} \chi^w(y) e_p\left(\sum_{j=1}^{r-t} a_j u_j y^{k_j}\right)\right|. \tag{2·3}$$

Applying Hölder's inequality twice, the second time splitting

$$N_w(\vec{u})^{\frac{2v}{2v-1}} = N_w(\vec{u})^{\frac{2v-2}{2v-1}} N_w(\vec{u})^{\frac{2}{2v-1}}, \tag{2·4}$$

and using (2·1) and (2·2) gives

$$|Y|\,|S|^w \leqslant \left(\sum_{\vec{u}} N_w(\vec{u})^{\frac{2v}{2v-1}}\right)^{\frac{2v-1}{2v}} \left(\sum_{\vec{u}} \left|\sum_{y\in Y} \chi^w(y) e_p(a_1u_1y^{k_1}+\cdots+a_{r-t}u_{r-t}y^{k_{r-t}})\right|^{2v}\right)^{\frac{1}{2v}}$$

$$\leqslant \left(\left(\sum_{\vec{u}} N_w(\vec{u})\right)^{\frac{2v-2}{2v-1}} \left(\sum_{\vec{u}} N_w^2(\vec{u})\right)^{\frac{1}{2v-1}}\right)^{\frac{2v-1}{2v}} (T^*_{v,t}p^{r-t})^{\frac{1}{2v}}$$

$$= ((p-1)^w)^{\frac{v-1}{v}} (T_{w,t})^{\frac{1}{2v}} (T^*_{v,t}p^{r-t})^{\frac{1}{2v}} = (p-1)^{w\left(1-\frac{1}{v}\right)} p^{\frac{r-t}{2v}} (T^*_{v,t}T_{w,t})^{\frac{1}{2v}}.$$

Hence, as claimed,

$$|S| < (p-1)^{1-\frac{1}{v}} p^{\frac{r-t}{2vw}} (T^*_{v,t}T_{w,t})^{\frac{1}{2vw}} |Y|^{-\frac{1}{w}}.$$

LEMMA 2·1. *Let $m \in \mathbb{N}$, $k_1, \ldots, k_r \in \mathbb{Z}$ such that $k_1, \ldots, k_m$ are distinct and nonzero* (mod $p-1$). *Then we have the following estimates for $T_{m,t}$ and $T^*_{m,t}$.*

(i) $m = 1$: *for $r \geqslant 2$, $1 \leqslant t \leqslant r-1$,*

$$T_{1,t} = (k_1, \ldots, k_{r-t}, p-1)(p-1), \qquad T^*_{1,t} = (k_1, \ldots, k_r, p-1)(k_{r-t+1}, \ldots, k_r, p-1).$$

(ii) $m \geqslant 2$: *for $r \geqslant 3$, $t \geqslant 1$ and $2 \leqslant m \leqslant r-t$,*

$$T_{m,t} \leqslant C_m \frac{(k_1, k_2, \ldots, k_{r-t}, p-1)(k_1, \ldots, k_m, p-1)^{m-1}}{(k_1, \ldots, k_m)^m} (\ell_1 \cdots \ell_m)(p-1)^m,$$

$$T^*_{m,t} \leqslant C_m \frac{(k_1, k_2, \ldots, k_r, p-1)(k_1, \ldots, k_m, k_{r-t+1}, \ldots, k_r, p-1)^{m-1}}{(k_1, \ldots, k_m)^m}$$
$$\times (\ell_1 \cdots \ell_m)(k_{r-t+1}, \ldots, k_r, p-1)^m,$$

where $C_m = 1$ if $k_1, \ldots, k_m$ are all positive, $C_m = 1/m^m$ if $k_1, \ldots, k_m$ are all negative, and $C_2 = 3/2$ and $C_m = m+1$, $m \geqslant 3$, if $k_1, \ldots, k_m$ have mixed signs.

The Lemma refines estimates of [**5**, lemma 2·1 and 2·2].

Proof. The $m = 1$ bounds are immediate. For $m \geqslant 2$ we set

$$d^* = (k_1, \ldots, k_m), \quad d = (k_1, \ldots, k_m, p-1), \quad d_1 = (k_1, \ldots, k_{r-t}, p-1)$$

and observe that

$$T_{m,t} = \#\left\{(x_1, \ldots, x_m, y_1, \ldots, y_m) \in \mathbb{Z}_p^{*2m} : \sum_{i=1}^m x_i^{k_j} = \sum_{i=1}^m y_i^{k_j},\ j = 1, \ldots, r-t\right\}$$

$$= \#\left\{(z, x_1, \ldots, x_m, y_1, \ldots, y_m) \in \mathbb{Z}_p^{*2m+1} : z^{k_j/d} + \sum_{i=2}^m x_i^{k_j} = \sum_{i=1}^m y_i^{k_j},\ j = 1, \ldots, m,\right.$$
$$\left. x_1^d = z,\ \ x_1^{k_j} = \sum_{i=1}^m y_i^{k_j} - \sum_{i=2}^m x_i^{k_j}, j = m+1, \ldots, r-t\right\}$$

$$\leqslant d_1 \#\left\{(z, x_2, \ldots, x_m, y_1, \ldots, y_m) \in \mathbb{Z}_p^{*2m} : z^{k_j/d} + \sum_{i=2}^m x_i^{k_j} = \sum_{i=1}^m y_i^{k_j},\right.$$
$$\left. j = 1, \ldots, m,\ z \text{ is a } d\text{th power}\right\} = \frac{d_1}{d} N$$

where

$$N = \#\left\{(x_1,\ldots,x_m,y_1,\ldots,y_m) \in \mathbb{Z}_p^{*2m} \;:\; \sum_{i=1}^{m} x_i^{k_j} = \sum_{i=1}^{m} y_i^{k_j},\; j=1,\ldots,m\right\}.$$

Further

$$\begin{aligned} N &= d^{2m}\#\left\{(u_1,\ldots,u_m,v_1,\ldots,v_m) \in \mathbb{Z}_p^{*2m} \;:\; \sum_{i=1}^{m} u_i^{k_j/d^*} = \sum_{i=1}^{m} v_i^{k_j/d^*},\right.\\ &\qquad\qquad \left. j=1,\ldots,m,\; u_i, v_i \text{ are } d^*\text{th powers}\right\}\\ &= d^{2m}\#\left\{(u_1,\ldots,u_m,v_1,\ldots,v_m) \in \mathbb{Z}_p^{*2m} \;:\; \sum_{i=1}^{m} u_i^{k_j/d^*} = \sum_{i=1}^{m} v_i^{k_j/d^*},\right.\\ &\qquad\qquad \left. j=1,\ldots,m,\; u_i, v_i \text{ are } d\text{th powers}\right\}\\ &= \#\left\{(x_1,\ldots,x_m,y_1,\ldots,y_m) \in \mathbb{Z}_p^{*2m} \;:\; \sum_{i=1}^{m} x_i^{k_j d/d^*} = \sum_{i=1}^{m} y_i^{k_j d/d^*},\; j=1,\ldots,m\right\}. \end{aligned}$$

Applying Wooley's [**11**, theorem 1·2] for $m \geqslant 3$ and [**4**, lemma 3·2] for $m = 2$, we have

$$N \leqslant C_m \left(\frac{\ell_1 d}{d^*} \cdots \frac{\ell_m d}{d^*}\right)(p-1)^m,$$

with the stated values of C_m and

$$T_{m,t} \leqslant C_m \frac{d_1}{d^*}\left(\frac{d}{d^*}\right)^{m-1} (\ell_1 \cdots \ell_m)\,(p-1)^m.$$

Observing that $((p-1)/(k_{r-t+1},\ldots,k_r,p-1))^{2m} T^*_{m,t}$ equals $T_{m,t}$ with exponents $(p-1)k_i/(k_{r-t+1},\ldots,k_r,p-1)$, $i=1,\ldots,r-t$, after making the substitution $x_i = X_i^{(p-1)/(k_{r-t+1},\ldots,k_r,p-1)}$, then gives the bound for $T^*_{m,t}$.

3. *Proof of Theorem* 1·1

For any integers $k_1,\ldots,k_r$ we define

$$B(k_1,\ldots,k_r) = \max\left|\sum_{x=1}^{p-1} e_p(f(x))\right|,$$

where the max is taken over all Laurent polynomials over $\mathbb{Z}$ of the form

$$f = a_1 x^{k_1} + \cdots + a_r x^{k_r}, \quad p \nmid a_1.$$

When none of the k_i are negative we similarly define

$$B^*(k_1,\ldots,k_r) = \max\left|\sum_{x=0}^{p-1} e_p(f(x))\right|,$$

the max taken over the same set of Laurent polynomials as before.

LEMMA 3·1. (a) *For $r \geqslant 2$, if $d \mid k_{t+1}, \ldots, k_r$ for some $1 \leqslant t < r$, and $p \nmid a_1$ then*

$$\left|S(\chi, a_1x^{k_1} + \cdots + a_rx^{k_r})\right| \leqslant p\left(\frac{(k_1, d, p-1)}{(d, p-1)} + \frac{B(k_1, \ldots, k_t)}{p}\right)^{\frac{1}{2}}. \tag{3·1}$$

(b) *If the $k_1, \ldots, k_t$ are all non-negative then $B(k_1, \ldots, k_t)$ may be replaced by $B^*(k_1, \ldots, k_t)$ in* (3·1). *In this case we also have the same bound for pure exponential sums with the $x = 0$ term included*:

$$\left|\sum_{x=0}^{p-1} e_p(f(x))\right| \leqslant p\left(\frac{(k_1, d, p-1)}{(d, p-1)} + \frac{B^*(k_1, \ldots, k_t)}{p}\right)^{\frac{1}{2}}. \tag{3·2}$$

For

$$f(x) = g(x) + g_2(x^{k_2}) + \cdots + g_r(x^{k_r})$$

where g has distinct exponents $k_1, t_1, \ldots, t_s$ say, repeated application of the Lemma gives

$$\begin{aligned}|S(\chi, f)| &\leqslant p\sqrt{\frac{(k_1, k_r, p-1)}{(k_r, p-1)} + \sqrt{\cdots + \sqrt{\frac{(k_1, k_2, p-1)}{(k_2, p-1)} + \frac{B(k_1, t_1, \ldots, t_s)}{p}}}} \\ &\leqslant p\sum_{i=0}^{r-2}\left(\frac{(k_1, k_{r-i}, p-1)}{(k_{r-i}, p-1)}\right)^{\frac{1}{2^{i+1}}} + B(k_1, t_1, \ldots, t_s)^{\frac{1}{2^{r-1}}} p^{1-\frac{1}{2^{r-1}}},\end{aligned} \tag{3·3}$$

where $B(k_1, t_1, \ldots, t_s)$ may be replaced by $B^*(k_1, t_1, \ldots, t_s)$ if g is a polynomial. The Weil bound $B^*(k_1, t_1, \ldots, t_s) \leqslant D\sqrt{p}$ when g is a polynomial, and $B(k_1, t_1, \ldots, t_s) \leqslant D\sqrt{p}$ when g contains exponents of both signs, completes the proof of Theorem 1·1.

Proof of Lemma 3·1. Suppose that $f(x) = a_1x^{k_1} + \cdots + a_rx^{k_r}$ is a Laurent polynomial over $\mathbb{Z}$ with $p \nmid a_1$ and $d \mid k_{t+1}, \ldots, k_r$ and define

$$Y = \left\{y \in \mathbb{Z}_p^* \ :\ y^d = 1\right\}.$$

Then, with χ a multiplicative character,

$$\begin{aligned}(d, p-1)\sum_{x=1}^{p-1} \chi(x)e_p(f(x)) &= \sum_{y\in Y}\sum_{x=1}^{p-1} \chi(xy)e_p(f(xy)) \\ &= \sum_{x=1}^{p-1} \chi(x)e_p\big(a_{t+1}x^{k_{t+1}} + \cdots + a_rx^{k_r}\big)\sum_{y\in Y} \chi(y)e_p\big(a_1y^{k_1}x^{k_1} + \cdots + a_ty^{k_t}x^{k_t}\big).\end{aligned}$$

Applying the Cauchy–Schwarz inequality,

$$\begin{aligned}\left|\sum_{x=1}^{p-1} \chi(x)e_p(f(x))\right| &\leqslant \frac{1}{(d, p-1)}\sum_{x=1}^{p-1}\left|\sum_{y\in Y} \chi(y)e_p\left(a_1y^{k_1}x^{k_1} + \cdots + a_ty^{k_t}x^{k_t}\right)\right| \\ &\leqslant \frac{1}{(d, p-1)}p^{\frac{1}{2}}\left(\sum_{x=1}^{p-1}\left|\sum_{y\in Y} \chi(y)e_p\left(a_1y^{k_1}x^{k_1} + \cdots + a_ty^{k_t}x^{k_t}\right)\right|^2\right)^{\frac{1}{2}}\end{aligned}$$

$$= \frac{p^{\frac{1}{2}}}{(d,p-1)} \left(\sum_{y_1,y_2 \in Y} \chi\left(y_1 y_2^{-1}\right) \sum_{x=1}^{p-1} e_p\left(a_1\left(y_1^{k_1}-y_2^{k_1}\right)x^{k_1}+\cdots+a_t\left(y_1^{k_t}-y_2^{k_t}\right)x^{k_t}\right)\right)^{\frac{1}{2}}$$

$$\leqslant \frac{p^{\frac{1}{2}}}{(d,p-1)} \left(\sum_{y_1,y_2\in Y, y_1^{k_1}=y_2^{k_1}} p + \sum_{y_1,y_2\in Y, y_1^{k_1}\neq y_2^{k_1}} B(k_1,\ldots,k_t)\right)^{\frac{1}{2}}$$

$$\leqslant \frac{p^{\frac{1}{2}}}{(d,p-1)} \left((d,p-1)(k_1,d,p-1)p + (d,p-1)^2 B(k_1,\ldots,k_t)\right)^{\frac{1}{2}},$$

and the claimed result follows. In these last inequalities we can plainly add an extra $x = 0$ term on the right to obtain B^* in place of B when the $k_1,\ldots,k_t$ are all non-negative. When f is a polynomial, starting with $\sum_{x=0}^{p-1} e_p(f(x))$ we obtain (3·2) in the same way.

4. *Proof of Corollary* 1·1

Suppose that f is of the form

$$f(x) = g(x) + g_2(x^{k_2}) + \cdots + g_r(x^{k_r}),$$

with $g(x)$ containing a monomial $a_1x^{k_1}$, satisfying the hypotheses of Corollary 1·1. Then $(k_1,k_i,p-1)/(k_i,p-1) \leqslant p^{-\epsilon}$, $2 \leqslant i \leqslant r$, and the value D in Theorem 1·1 satisfies $D < p^{\frac{1}{2}-\epsilon}$. We get from Theorem 1·1,

$$|S(\chi,f)| \leqslant p\sum_{i=0}^{r-2} p^{-\epsilon/2^{i+1}} + \left(p^{\frac{1}{2}-\epsilon}\right)^{\frac{1}{2^{r-1}}} p^{1-\frac{1}{2^r}} = p\sum_{i=1}^{r-1} p^{-\epsilon/2^i} + p^{1-\frac{\epsilon}{2^{r-1}}} < 3p^{1-\frac{\epsilon}{2^{r-1}}}.$$

To obtain the constant 3 in the last inequality observe that trivially $|S(\chi,f)| \leqslant p < 2p^{1-\frac{\epsilon}{2^{r-1}}}$ if $p^\epsilon < 2^{2^{r-1}}$ so we may assume $p^\epsilon \geqslant 2^{2^{r-1}}$. Set $\rho = p^{-\epsilon/2^{r-1}}$ so that $\rho \leqslant 1/2$. Then

$$\sum_{i=1}^{r-1} p^{-\epsilon/2^i} < \rho + \rho^2 + \rho^4 + \rho^8 + \cdots < 2\rho.$$

REFERENCES

[1] N. M. AKULINIČEV. Estimates for rational trigonometric sums of a special type. *Dokl. Acad. Sci. USSR* **161** (1965), 743–745. English trans in Doklady 161, no. 4 (1965), 480–482.

[2] J. BOURGAIN. Some arithmetical applications of the sum-product theorems in finite fields. *Geometric aspects of functional analysis*. 99–116, Lecture Notes in Math. 1910 (Springer, 2007).

[3] F. N. CASTRO and C. J. MORENO. Mixed exponential sums over finite fields. *Proc. Amer. Math. Soc.* **128**, no. 9 (2000), 2529–2537.

[4] T. COCHRANE and C. PINNER. An improved Mordell type bound for exponential sums. *Proc. Amer. Math. Soc.* **133** (2005), no. 2, 313–320.

[5] T. COCHRANE, J. COFFELT and C. PINNER. A further refinement of Mordell's bound on exponential sums. *Acta Arith.* **116** (2005), no. 1, 35–41.

[6] T. COCHRANE, J. COFFELT and C. PINNER. A system of simultaneous congruences arising from trinomial exponential sums. *J. Théor. Nombres Bordeaux* **18** (2006), no. 1, 59–72.

[7] H. D. KLOOSTERMAN. On the Representation of Numbers in the Form $ax^2+by^2+cz^2+dt^2$. *Acta Math.* **49** (1926), 407–464.

[**8**] L. J. MORDELL. On a sum analagous to a Gauss's sum. *Quart. J. Math.* **3** (1932), 161–167.

[**9**] G. I. PEREL'MUTER. Estimate of a sum along an algebraic curve. *Mat. Zametki* **5** (1969), 373–380.

[**10**] A. WEIL. On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204–207.

[**11**] T. D. WOOLEY. A note on simultaneous congruences, II: Mordell revised. *J. Aust. Math. Soc.* **88** (2010), 261–275.

[**12**] H. B. YU. Estimates for complete exponential sums of special types. *Math. Proc. Cam. Phil. Soc.* **131** (2001), no. 2, 321–326.