A FURTHER REFINEMENT OF MORDELL'S BOUND ON EXPONENTIAL SUMS

TODD COCHRANE, JEREMY COFFELT, AND CHRISTOPHER PINNER

1. Introduction

For a prime p, integer Laurent polynomial

$$f(x) = a_1 x^{k_1} + \cdots + a_r x^{k_r}, \quad p \nmid a_i, \quad k_i \in \mathbb{Z}, \tag{1.1}$$

where the k_i are distinct and nonzero mod $(p-1)$, and multiplicative character χ 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 $\mathbb{Z}_p$. For such sums the classical Weil bound [5] (see [1] or [4] for Laurent f) yields,

$$|S(\chi, f)| \leq d p^{\frac{1}{2}}, \tag{1.2}$$

where d is the degree of f for a polynomial (degree of the numerator when f has both positive and negative exponents), nontrivial only if $d < \sqrt{p}$. Mordell [3] gave a different type of bound which depended rather on the product of all the exponents k_i. In [2] we obtained the following improvement in Mordell's bound

$$|S(\chi, f)| \leq 4^{\frac{1}{r}} (\ell_1 \ell_2 \cdots \ell_r)^{\frac{1}{r^2}} p^{1 - \frac{1}{2r}}, \tag{1.3}$$

where

$$\ell_i = \begin{cases} k_i, & \text{if } k_i > 0, \\ r|k_i|, & \text{if } k_i < 0, \end{cases} \tag{1.4}$$

non-trivial as long as $(l_1 \cdots l_r) \leq \frac{1}{4^r} p^{\frac{1}{2}r}$. We show here that some of the larger l_i can in fact be omitted from the product (at the cost of a worse dependence on p) once $r \geq 3$:

Theorem 1.1. *For any f and χ as above and positive integer m with $\frac{1}{2}r < m \leq r$,*

$$|S(\chi, f)| \leq 4^{\frac{1}{m}} (\ell_1 \cdots \ell_m)^{\frac{1}{m^2}} p^{1 - \frac{1}{m^2}(m - \frac{1}{2}r)},$$

Date: September 6, 2009.

1991 *Mathematics Subject Classification.* 11L07;11L03.

Key words and phrases. exponential sums.

where

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

The theorem thus implies a nontrivial bound on $|S(\chi,f)|$ as long as $(\ell_1\ell_2\cdots\ell_m) < 4^{-m}p^{m-r/2}$ for some $\frac{1}{2}r < m \le r$. Inequality (1.3) is just the case $m = r$. One can in fact save an extra factor of $((k_1,...,k_r,p-1)/(k_1,...,k_m))^{\frac{1}{m^2}}$ on the stated bound, as we explain in Section 3 below. Theorem 1.1 is particularly useful when more than half of the exponents are small; in particular (for fixed r) if at least $R = \lfloor \frac{1}{2}r \rfloor + 1$ of the k_i are bounded, $l_i \le B$ say, then one obtains a uniform bound

$$|S(\chi,f)| \le (4B)^{\frac{1}{R}} p^{1-\delta}$$

with $\delta = 1/R^2$ or $1/2R^2$ as r is even or odd, irrespective of the size of the remaining l_i. Notice one cannot expect a bound of order $p^{1-\delta}$ with some $\delta > 0$ if only $\lfloor \frac{1}{2}r \rfloor$ of the k_i are bounded as can be seen by the sums $|S(\chi,f)| = \frac{1}{2}p + O(r\sqrt{p})$ when

$$f = \varepsilon a_0 x^{\frac{1}{2}(p-1)} + \sum_{i=1}^{\lfloor \frac{1}{2}r \rfloor} a_i(x^i - x^{i+\frac{1}{2}(p-1)}), \quad \chi(x) = \chi_0(x) \text{ or } \left(\frac{x}{p}\right), \tag{1.5}$$

with $\varepsilon = 0$ or 1 as r is even or odd.

For monomials and binomials we gain nothing new, but for trinomials

$$f = ax^{k_1} + bx^{k_2} + cx^{k_3},$$

we obtain the $m = 2$ Theorem 1.1 bound

$$|S(\chi,f)| \le (k_1k_2)^{\frac{1}{4}} p^{\frac{7}{8}}, \tag{1.6}$$

avoiding entirely the need to involve the largest exponent, in contrast to the Weil bound and our previous Mordell type bound ($m = 3$):

$$|S(\chi,f)| \le \max\{k_1,k_2,k_3\}p^{\frac{1}{2}}, \quad |S(\chi,f)| \le \sqrt[9]{\frac{80}{9}}(k_1k_2k_3)^{\frac{1}{9}} p^{\frac{5}{6}}.$$

The proof of the theorem is very similar to that of (1.3) and involves bounding the number of solutions $(x_1,...,x_m,y_1,...,y_m)$ in $\mathbb{Z}_p^{*2m}$ to the system of simultaneous equations

$$x_1^{k_i} + \cdots + x_m^{k_i} \equiv y_1^{k_i} + \cdots + y_m^{k_i} \bmod p \tag{1.7}$$

for $i = 1,...,r$. We denote the number of such solutions by M_m. For $m \le r$ we can merely use the first m equations (discarding the remaining $r-m$) and appeal to the bound of Mordell [3] or Lemma 3.1 in [2] to obtain:

$$M_m \le 4^m(l_1\cdots l_m)(p-1)^m. \tag{1.8}$$

The theorem is then immediate from (1.8) by taking $v = w = m$ in the following Lemma relating $S(\chi,f)$ to M_m:

Lemma 1.1. *For any f and χ as above, and positive integers v, w,*

$$|S(\chi, f)| \leq (p-1)^{1-\frac{1}{v}-\frac{1}{w}} p^{\frac{r}{2vw}} (M_v M_w)^{\frac{1}{2vw}}.$$

2. Slight improvements in the bound for M_m

Although it seems wasteful to simply discard the remaining $(r-m)$ equations in (1.7) there are certainly cases where these equations are redundant. For instance, if the first m exponents take the form $k_i = il$, $i = 1, ..., m$ with $l | k_i$ for the remaining k_i then the x_i^l are merely a permutation of the y_i^l whatever those remaining exponents. Moreover when $m = 2$ our [2] bound for the first two equations

$$M_2 \leq \begin{cases} k_1 k_2 (p-1)^2 & \text{if } k_1 k_2 > 0, \\ 3|k_1 k_2|(p-1)^2 & \text{if } k_1 k_2 < 0, \end{cases}$$

can be asymptotically sharp; for example for exponents $k_1 = l, k_2 = 2l$, with $l | k_i$, $i = 3, ..., r$ and $l | (p-1)$ or $k_1 = l, k_2 = -l$ or $3l$ and $l | k_i$, $i = 3, ..., r$ with the k_i / l odd and $2l | (p-1)$, it is not hard to see that

$$M_2 = 2l^2 (p-1)^2 - l^3 (p-1)$$
$$M_2 = 3l^2 (p-1)^2 - 3l^3 (p-1),$$

respectively. In certain cases though we can utilize the remaining equations for a slight saving:

Lemma 2.1. *If $r \geq 2$ and*

$$L_{ij} = \begin{cases} k_i k_j & \textit{if } k_i k_j > 0, \\ 3|k_i k_j| & \textit{if } k_i k_j < 0, \end{cases}$$

then for $m = 2$ we have

$$M_2 \leq (k_1, k_2, ..., k_r, p-1) \min_{1 \leq i < j \leq r} \frac{L_{ij}}{(k_i, k_j)} (p-1)^2.$$

Thus for example in the trinomial case (1.6) can be slightly refined to

$$|S(\chi, f)| \leq \left(\frac{(k_1, k_2, k_3, p-1)}{(k_1, k_2)} \right)^{\frac{1}{4}} (k_1 k_2)^{\frac{1}{4}} p^{\frac{7}{8}},$$

of use if k_1 and k_2 share a common factor not shared with k_3. More generally a slight modification of the proof of Lemma 3.1 in [2] allows a similar saving of a factor $(k_1, k_2, \ldots, k_r, p-1)/(k_1, k_2, \ldots, k_m)$ on the previous bound (1.8):

Lemma 2.2. *If $r \geq 3$, then for any $3 \leq m \leq r$ and choice of m exponents $k_1, ..., k_m$,*

$$M_m \leq \frac{4e}{m^2} \binom{2m}{m} \frac{(k_1, k_2, \ldots, k_r, p-1)}{(k_1, k_2, \ldots, k_m)} (l_1 \cdots l_m)(p-1)^m.$$

3. Proof of Lemma 1.1

For $\vec{u}=(u_1,...,u_r)\in\mathbb{Z}_p^r$ and positive integer m, we define

$$N_m(\vec{u})=\#\Big\{(x_1,...,x_m)\in\mathbb{Z}_p^{*m}\ :\ \sum_{i=1}^m x_i^{k_j}=u_j,\ \ j=1,...,r\Big\},$$

and observe that

$$\sum_{\vec{u}\in\mathbb{Z}_p^r} N_m(\vec{u})=(p-1)^m,\qquad \sum_{\vec{u}\in\mathbb{Z}_p^r} N_m^2(\vec{u})=M_m. \tag{3.1}$$

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

(3.2)
$$\begin{aligned}
&\sum_{\vec{u}\in\mathbb{Z}_p^r}\left|\sum_{x=1}^{p-1}\chi(x)e_p(a_1u_1x^{k_1}+\cdots+a_ru_rx^{k_r})\right|^{2m}\\
&=\sum_{\substack{x_1,...,x_m,\\ y_1,..,y_m\in\mathbb{Z}_p^*}}\chi(x_1\cdots x_m y_1^{-1}\cdots y_m^{-1})\sum_{\vec{u}\in\mathbb{Z}_p^r} e_p\left(\sum_{j=1}^r a_ju_j(x_1^{k_j}+\cdots+x_m^{k_j}-y_1^{k_j}\cdots-y_m^{k_j})\right)\\
&=p^r{\sum}^*\chi(x_1\cdots x_m y_1^{-1}\cdots y_m^{-1})\le p^rM_m,
\end{aligned}$$

where $\sum^*$ denotes a sum over the $x_1,...,x_m,y_1,...,y_m$ in $\mathbb{Z}_p^*$ satisfying $\sum_{j=1}^m x_j^{k_i}\equiv\sum_{j=1}^m y_j^{k_i} \pmod p$ for $1\le i\le r$.

Writing $S=S(\chi,f)$, we have

$$\begin{aligned}
(p-1)S^w&=\sum_{m=1}^{p-1}\left(\sum_{x=1}^{p-1}\chi(mx)e_p(a_1(mx)^{k_1}+\cdots+a_r(mx)^{k_r})\right)^w\\
&=\sum_{m=1}^{p-1}\chi^w(m)\sum_{x_1,...,x_w\in\mathbb{Z}_p^*}\chi(x_1\cdots x_w)e_p\left(\sum_{j=1}^r a_jm^{k_j}(x_1^{k_j}+\cdots+x_w^{k_j})\right)\\
&=\sum_{x_1,...,x_w\in\mathbb{Z}_p^*}\chi(x_1\cdots x_w)\sum_{m=1}^{p-1}\chi^w(m)e_p\left(\sum_{j=1}^r a_jm^{k_j}(x_1^{k_j}+\cdots+x_w^{k_j})\right),
\end{aligned}$$

and so

$$(p-1)|S|^w\le\sum_{\vec{u}\in\mathbb{Z}_p^r}N_w(\vec{u})\left|\sum_{m=1}^{p-1}\chi^w(m)e_p\left(\sum_{j=1}^r a_ju_jm^{k_j}\right)\right|. \tag{3.3}$$

Applying Hölder's inequality twice, the second time splitting

$$N_w(\vec{u})^{\frac{2v}{2v-1}}=N_w(\vec{u})^{\frac{2v-2}{2v-1}}N_w(\vec{u})^{\frac{2}{2v-1}}, \tag{3.4}$$

and using (3.1) and (3.2) gives

$$(p-1)\,|S|^w \le \left(\sum_{\vec{u}} N_w(\vec{u})^{\frac{2v}{2v-1}}\right)^{\frac{2v-1}{2v}} \left(\sum_{\vec{u}} \left|\sum_{m=1}^{p-1} \chi^w(m) e_p(a_1u_1m^{k_1}+\cdots+a_ru_rm^{k_r})\right|^{2v}\right)^{\frac{1}{2v}}$$

$$\le \left(\left(\sum_{\vec{u}} N_w(\vec{u})\right)^{\frac{2v-2}{2v-1}} \left(\sum_{\vec{u}} N_w^2(\vec{u})\right)^{\frac{1}{2v-1}}\right)^{\frac{2v-1}{2v}} (M_v p^r)^{\frac{1}{2v}}$$

$$= ((p-1)^w)^{\frac{v-1}{v}} (M_w)^{\frac{1}{2v}} (M_v p^r)^{\frac{1}{2v}} = (p-1)^{w(1-\frac{1}{v})} p^{\frac{r}{2v}} (M_v M_w)^{\frac{1}{2v}}. \tag{3.5}$$

Hence

$$|S| < (p-1)^{1-\frac{1}{v}-\frac{1}{w}} p^{\frac{r}{2vw}} (M_v M_w)^{\frac{1}{2vw}}. \ \square$$

4. Proof of Lemma 2.1

Write $M_2 = \sum_{\vec{u}\in\mathbb{Z}_p^r} C(\vec{u})^2$ where

$$\begin{aligned} C(u_1,u_2,\ldots,u_r) &= \#\{(x,y)\in\mathbb{Z}_p^{*2} :\ x^{k_i}-y^{k_i}=u_i \text{ for } i=1,2,\ldots,r\} \\ &= d\#\{x\in\mathbb{Z}_p^* :\ \exists\, y\in\mathbb{Z}_p^* \text{ satisfying } x^{k_i}-y^{k_i}=u_i \text{ for } i=1,2,\ldots,r\}, \end{aligned}$$

and $d=(k_1,k_2,\ldots,k_r,p-1)$ (since for each x with a solution y_0 there will be d solutions y satisfying $y^{(k_1,k_2,\ldots,k_r)}=y_0^{(k_1,k_2,\ldots,k_r)}$). Note the trivial bound $C(\vec{u})\le d(p-1)$.

If $0<k_1<k_2$ and $(u_1,u_2)\ne(0,0)$ then any x in the latter set must be a root of the non-zero polynomial

$$f=(x^{k_1}-u_1)^{k_2/(k_1,k_2)}-(x^{k_2}-u_2)^{k_1/(k_1,k_2)}$$

which has degree at most $k_1(k_2/(k_1,k_2)-1)$, and so

$$C(\vec{u}) \le \frac{dk_1k_2}{(k_1,k_2)} - dk_1.$$

On the other hand, if $k_1<0<k_2$ and $(u_1,u_2)\ne(0,0)$ then x will be a root of the non-zero polynomial

$$f=(x^{k_2}-u_2)^{|k_1|/(k_1,k_2)}(1-u_1x^{|k_1|})^{k_2/(k_1,k_2)} - x^{|k_1|k_2/(k_1,k_2)}$$

of degree at most $2|k_1|k_2/(k_1,k_2)$, and so

$$C(\vec{u}) \le 2\frac{d}{(k_1,k_2)}|k_1|k_2.$$

Now for $(u_1, u_2) = (0, 0)$, we will evaluate the sum $\sum_{(u_1,u_2)=(0,0)} C(\vec{u})$. Since $x^{k_1} = y^{k_1}$ and $x^{k_2} = y^{k_2}$ imply $x^{(k_1,k_2)} = y^{(k_1,k_2)}$, we have

$$\begin{aligned}\sum_{(u_1,u_2)=(0,0)} C(\vec{u}) &= \sum_{(u_1,u_2)=(0,0)} \#\left\{(x,y) \in \mathbb{Z}_p^{*2} :\ x^{(k_1,k_2)} = y^{(k_1,k_2)},\ x^{k_l} - y^{k_l} = u_l \text{ for } l \neq 1,2\right\} \\ &= \#\left\{(x,y) \in \mathbb{Z}_p^{*2} :\ x^{(k_1,k_2)} = y^{(k_1,k_2)}\right\} \\ &= (k_1, k_2, p-1)(p-1)\end{aligned}$$

Finally, since $\sum_{\vec{u}\in\mathbb{Z}_p^r} C(\vec{u}) = (p-1)^2$, we have for $0 < k_1 < k_2$,

$$\begin{aligned}M_2 &= \sum_{(u_1,u_2)\neq(0,0)} C(\vec{u})^2 + \sum_{(u_1,u_2)=(0,0)} C(\vec{u})^2 \\ &\leq \left(\frac{dk_1k_2}{(k_1,k_2)} - dk_1\right) \sum_{(u_1,u_2)\neq(0,0)} C(\vec{u}) + d(p-1) \sum_{(u_1,u_2)=(0,0)} C(\vec{u}) \\ &= \left(\frac{dk_1k_2}{(k_1,k_2)} - d\big(k_1 - (k_1,k_2,p-1)\big)\right)(p-1)^2 - (k_1,k_2,p-1)\left(\frac{dk_1k_2}{(k_1,k_2)} - dk_1\right)(p-1) \\ &< d\frac{k_1k_2}{(k_1,k_2)}(p-1)^2,\end{aligned}$$

and for $k_1 < 0 < k_2$,

$$\begin{aligned}M_2 &= \sum_{(u_1,u_2)\neq(0,0)} C(\vec{u})^2 + \sum_{(u_1,u_2)=(0,0)} C(\vec{u})^2 \\ &\leq 2\frac{d}{(k_1,k_2)}|k_1|k_2 \sum_{(u_1,u_2)\neq(0,0)} C(\vec{u}) + d(p-1) \sum_{(u_1,u_2)=(0,0)} C(\vec{u}) \\ &= \left(2\frac{d}{(k_1,k_2)}|k_1|k_2 + d(k_1,k_2,p-1)\right)(p-1)^2 - 2\frac{d}{(k_1,k_2)}(k_1,k_2,p-1)|k_1|k_2(p-1) \\ &< 3\frac{d}{(k_1,k_2)}|k_1|k_2(p-1)^2.\end{aligned}$$

Since the proof holds when the k_i's are interchanged, we have the desired result. □

5. Proof of Lemma 2.2

The proof is almost identical to that of Lemma 3.1 in [2]. Simply ignore the $(r-m)$ remaining equations for all of the proof except for the instance where Wooley's result [6] was applied to bound the number of solutions to

$$u_1^{k_j} + u_2^{k_j} + \cdots + u_t^{k_j} = \alpha_j \text{ for } j = 1, \ldots, t,$$

for some $1 \leq t \leq m$ with $D_t(\vec{u}) \neq 0$. Instead of bounding the number of solutions to the above system, bound instead the number of solutions to

$$X_1^{k_j/d} + X_2^{k_j/d} + \cdots + X_t^{k_j/d} = \alpha_j \text{ for } j = 1, \ldots, t$$

where $d = (k_1, k_2, \ldots, k_m)$ and $X_i = u_i^d$. By the previously mentioned result of Wooley, we know that the number of solutions to the second system is no more than $(k_1/d)(k_2/d)\cdots(k_t/d)$. However, for a given value of X_i there are at most $(d, p-1)$ values for u_i such that $u_i^d = X_i$. After fixing values for all but one of the u_i, say u_1, the values $u_1^{k_1}, \ldots, u_1^{k_r}$ are all determined, so that the number of choices for u_1 is at most $(k_1, k_2, \ldots, k_r, p-1)$. This gives no more than

$$(k_1, k_2, \ldots, k_r, p-1)(d, p-1)^{t-1}(k_1/d)(k_2/d)\cdots(k_t/d) \le \frac{(k_1, k_2, \ldots, k_r, p-1)}{d} k_1 k_2 \cdots k_t$$

solutions, improving on the previous bound of $k_1 k_2 \cdots k_t$ (given by the direct application of Wooley's result on only the first t equations) by the desired factor. $\square$

References

[1] F. N. Castro & C. J. Moreno, *Mixed exponential sums over finite fields*, Proc. Amer. Math. Soc. 128, no. 9 (2000), 2529-2537.

[2] T. Cochrane & C. Pinner, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. to appear.

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

[4] G. I. Perel'muter, *Estimate of a sum along an algebraic curve*, Mat. Zametki 5 (1969), 373-380.

[5] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204-207.

[6] T. Wooley, *A note on simultaneous congruences*, J. Number Theory 58 (1996), no. 2, 288-297.

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: `jcoffelt@math.ksu.edu`

Department of Mathematics, Kansas State University, Manhattan, KS 66506

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