AN IMPROVED MORDELL TYPE BOUND FOR EXPONENTIAL SUMS

TODD COCHRANE AND CHRISTOPHER PINNER

ABSTRACT. For a sparse polynomial \( f(x) = \sum_{i=1}^{r} a_i x^{k_i} \in \mathbb{Z}[x] \), with \( p \nmid a_i \) and \( 1 \leq k_1 < \cdots < k_r < p - 1 \), we show that
\[
\left| \sum_{x=1}^{p-1} e^{2\pi i f(x)/p} \right| \leq 2^{\frac{r}{2} (k_1 \cdots k_r)^{1/2}} p^{1 - \frac{1}{r}},
\]
thus improving upon a bound of Mordell. Analogous results are obtained for Laurent polynomials and for mixed exponential sums.

1. Introduction

For a prime \( p \), integer Laurent polynomial
\[
f(x) = a_1 x^{k_1} + \cdots + a_r x^{k_r}, \quad p \nmid a_i, \quad k_i \in \mathbb{Z},
\]
where the \( k_i \) are distinct and nonzero mod \( (p - 1) \), 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 \( \mathbb{Z}_p \). For \( \chi = \chi_0 \), the principal character, the sum is just a pure exponential sum \( S(\chi_0,f) = \sum_{x=1}^{p-1} e_p(f(x)) \). Of course \( S(\chi,f) = 0 \) unless \( \chi^{(p-1)/d} = \chi_0 \) where \( d = (k_1, \ldots, k_r, p-1) \), as is easily seen from the change of variables \( x \to xu \) if there is a \( u \) with \( u^d = 1 \) and \( \chi(u) \neq 1 \). The classical Weil bound [12] (see [2] or [10] for Laurent \( f \)),
\[
|S(\chi,f)| \leq d(f) \cdot p^{\frac{1}{2}},
\]
where, (assuming for the moment that \( k_2 < \cdots < k_r \)),
\[
d(f) = \begin{cases} 
    k_r, & \text{if all } k_i \text{ are positive}, \\
    |k_1|, & \text{if all } k_i \text{ are negative}, \\
    (k_r - k_1), & \text{otherwise},
\end{cases}
\]
is nontrivial only if \( d(f) < \sqrt{p} \). The task of improving the Weil bound when \( d(f) \) is large remains an open problem. Nontrivial bounds of this kind have only been obtained for monomials, binomials and certain sparse polynomials of the type (1.1). Perhaps the most significant result of this type is a bound of Mordell [9] that predates the work of Weil:
\[
|S(\chi,f)| \leq \left( \binom{2r}{r} \right)^{1/2} (1 - \frac{1}{p})^{\frac{1}{2r}} (p-1,k_1,\ldots,k_r)^{1/2} (\ell_1 \ell_2 \cdots \ell_r)^{1/2} p^{1 - \frac{1}{r}},
\]

\[\text{Date: September 6, 2009.}\]
\[1991 \text{ Mathematics Subject Classification.} \ 11L07;11L03.\]
\[\text{Key words and phrases.} \ \text{exponential sums.}\]
where

\[ \ell_i = \begin{cases} k_i, & \text{if } k_i > 0, \\ p|k_i|, & \text{if } k_i < 0. \end{cases} \]

Although Mordell only considered pure exponential sums his method easily extends to the case of mixed sums. Davenport [5] obtained some refinements of Mordell’s work but his results were superseded by Weil; see also Shparlinski [11, p.88]. For further discussion of the case of monomials see [6] and [8], and for binomials [7], [1], [3] and [14].

We show here how a simple application of Hölder’s inequality (of the type employed by Heath-Brown and Konyagin in [6]) can substantially improve the bound of Mordell:

**Theorem 1.1.** For any \( f \) and \( \chi \) as above,

\[ |S(\chi, f)| \leq 2^{\frac{r}{2}} (\ell_1 \cdots \ell_r)^{\frac{r}{2}} p^{1 - \frac{1}{r}}. \]

The theorem implies a nontrivial bound on \( |S(\chi, f)| \) for \( \ell_1 \ell_2 \cdots \ell_r < 4^{-\frac{1}{r}} p^{r/2} \). The following example shows that in general the exponent \( 1/r^2 \) on the product \( (\ell_1 \cdots \ell_r) \) cannot be improved. In this example, \( (\ell_1 \ell_2 \cdots \ell_r)^{1/2} \sim p^{1/2r} 2^{-\frac{1}{r}} (r/2)!^{\frac{1}{r}} \) as \( p \to \infty \), while \( |S(\chi, f)| \sim p^{r/2} \).

**Example 1.1.** If \( r \) is even, \( p > r/2 \) and \( f(x) = \sum_{i=1}^{r/2} (x^{2^{i-1}} - x^i) \), then

\[ \sum_{x=1}^{p-1} e_p(f(x)) = \frac{p-1}{2} + \sum_{(\frac{2}{p})=-1} e_p \left(-2(x + x^2 + \cdots + x^{r/2})\right), \]

and so by Weil’s bound

\[ |S(\chi, f) - \frac{p-1}{2}| \leq \frac{r}{2} \sqrt{p}. \]

Weaker types of bounds on \( |S(\chi_0, f)| \), nontrivial even when all the \( k_i \) are on the order of \( p \) in size, were obtained by the authors in [4].

A key ingredient in the proof of both Mordell’s theorem and our own is the estimation of

\[ M = \# \{ (x_1, \ldots, x_r, y_1, \ldots, y_r) \in \mathbb{Z}_p^{2r} : \sum_{i=1}^{r} x_i^{k_i} = \sum_{i=1}^{r} y_i^{k_j}, \quad j = 1, \ldots, r \}. \]

Mordell deduced (1.3) from the bounds

\[ |S(\chi, f)| \leq \left(1 - \frac{A}{p}\right)^{-1/2r} (p-1, k_1, \ldots, k_r)^{1/2r} p^{1/2} M^{1/2r}, \]

and

\[ M \leq (2^r)^{r}\ell_1 \ell_2 \cdots \ell_r p^r. \]

Here, we prove

**Theorem 1.2.** For any \( f \) and \( \chi \) as above,

\[ |S(\chi, f)| < (p-1)^{\frac{1}{2}} p^{\frac{1}{2r}} M^{\frac{1}{2r}}. \]

Using the bound of Mordell (1.5) and \( (2^r)^{r} < 2^{2r} \) one immediately obtains Theorem 1.1. In Lemma 3.1, we obtain a slight refinement of (1.5) using a version of Bezout’s Theorem proved by Wooley [13]. We also state a sharp upper bound on \( M \) for the case \( r = 2 \) in Lemma 3.2.

For \( r = 1 \) and \( k_1 = k \), plainly \( M = (k, p-1)(p-1) \), and we recover from Theorem 1.2 the Weil bound for twisted Gauss sums,

\[ \left| \sum_{x=1}^{p-1} \chi(x) e_p(ax^k) \right| \leq (k, p-1) \sqrt{p}. \]
For any multiplicative character which is nontrivial and improves on Weil (1.2) when \((pl)^{1/4} < k < p/l\), and observe that
\[
\sum_{x < \sqrt{N}} x^{k_1} \leq 2, \quad 1 \leq i < k.
\]
Applying Hölder’s inequality twice, the second time splitting the sum over the \(r\) variables, we obtain from Theorem 1.2 and Lemma 3.2,

\[
\left| \sum_{x=1}^{p-1} \chi(x)e_p(\alpha x^k + bx^l) \right| \leq (kl)^{1/4} p^{3/4},
\]

which is nontrivial and improves on Weil (1.2) when \((pl)^{1/4} < k < p/l\), and

\[
\left| \sum_{x=1}^{p-1} \chi(x)e_p(\alpha x^k + bx^{-l}) \right| \leq (3kl)^{1/4} p^{3/4}.
\]

2. Proof of Theorem 1.2

For \(\bar{u} = (u_1, \ldots, u_r) \in \mathbb{Z}_p^r\), we define

\[
N(\bar{u}) = \# \left\{ (x_1, \ldots, x_r) \in \mathbb{Z}_p^r : \sum_{i=1}^{r} x_i^{k_j} = u_j, \quad j = 1, \ldots, r \right\},
\]

and observe that

\[
(2.1) \quad \sum_{\bar{a} \in \mathbb{Z}_p^r} N(\bar{u}) = (p-1)^r, \quad \sum_{\bar{a} \in \mathbb{Z}_p^r} N^2(\bar{u}) = M.
\]

For any multiplicative character \(\chi\),

\[
(2.2) \quad \sum_{\bar{a} \in \mathbb{Z}_p^r} \left| \sum_{m=1}^{p-1} \chi'(m)e_p(a_1u_1m^{k_1} + \cdots + a_ru_rm^{k_r}) \right|^{2r}
\]

\[
= \sum_{y_1, \ldots, y_r \in \mathbb{Z}_p^r} \chi'(x_1 \ldots x_r) \left| \sum_{\bar{a} \in \mathbb{Z}_p^r} e_p \left( \sum_{j=1}^{r} a_ju_j(x_1^{k_j} + \cdots + x_r^{k_j} - y_1^{k_j} \cdots - y_r^{k_j}) \right) \right|
\]

\[
= p^r \sum_{y_1, \ldots, y_r \in \mathbb{Z}_p^r} \chi'(x_1 \ldots x_r) \left| \sum_{\bar{a} \in \mathbb{Z}_p^r} e_p \left( \sum_{j=1}^{r} a_ju_jx_j^{k_j} \right) \right|
\]

where \(\sum_{\bar{x}}\) denotes a sum over the \(x_1, \ldots, x_r, y_1, \ldots, y_r\) in \(\mathbb{Z}_p^r\) satisfying \(\sum_{j=1}^{r} x_j^{k_j} = \sum_{j=1}^{r} y_j^{k_j}\) for \(1 \leq i \leq r\).

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

\[
(p-1)S^r = \sum_{m=1}^{p-1} \left( \sum_{x=1}^{p-1} e_p(a_1x^{k_1} + \cdots + a_rx^{k_r}) \right)^r
\]

\[
= \sum_{m=1}^{p-1} e_p(\sum_{x=1}^{p-1} \chi(x) e_p(a_1x^{k_1} + \cdots + a_rx^{k_r}))
\]

\[
= \sum_{x_1, \ldots, x_r \in \mathbb{Z}_p^r} \chi(x_1 \ldots x_r) \sum_{m=1}^{p-1} e_p(\sum_{j=1}^{r} a_jm^{k_j}(x_1^{k_j} + \cdots + x_r^{k_j}))
\]

\[
= \sum_{x_1, \ldots, x_r \in \mathbb{Z}_p^r} \chi(x_1 \ldots x_r) \sum_{m=1}^{p-1} e_p(\sum_{j=1}^{r} a_jm^{k_j} x_j^{k_j} + \cdots + x_r^{k_j}),
\]

and so

\[
(2.3) \quad (p-1)|S|^r \leq \sum_{\bar{a} \in \mathbb{Z}_p^r} N(\bar{u}) \left| \sum_{m=1}^{p-1} \chi'(m)e_p(\sum_{j=1}^{r} a_ju_jm^{k_j}) \right|.
\]

Applying Hölder’s inequality twice, the second time splitting the terms, we have

\[
N(\bar{u}) \frac{2r}{p} = N(\bar{u}) \frac{2r-2}{r} N(\bar{u}) \frac{2}{r},
\]

For \(r = 2, 1 \leq l < k\), we obtain from Theorem 1.2 and Lemma 3.2,
and using (2.1) and (2.2) gives
\[
(p - 1) |S|^r \leq \left( \sum_u N(u) \left( \frac{2r}{2r-1} \right) \right)^{2r-1} \left( \sum_u \left( \sum_{m=1}^{p-1} \chi^r (m)e_p (a_1 u_1 m^k + \cdots + a_r u_r m^{kr}) \right)^2 \right)^{\frac{1}{2r}}
\]
\[
\leq \left( \sum_u N(u) \left( \frac{2r}{2r-1} \right) \right)^{2r-2} \left( \sum_u N^2(u) \right)^{\frac{1}{2r-1}} \left( \sum_{m=1}^{p-1} \chi^r (m) \left( \sum_{u=1}^{p-1} \chi^r (m) \right) \right)^{\frac{2r-1}{2r}} (M^p)^{\frac{1}{2r}}
\]
\[
= ((p - 1)^r \left( \frac{2r}{2r-1} \right) (M^p)^{\frac{1}{2r}}) \leq (p - 1)^{r-1} p^{\frac{1}{2r}} M^\frac{1}{2r}
\]
Hence
\[
|S| < (p - 1)^{1-\frac{1}{2r}} p^{\frac{1}{2r}} M^\frac{1}{2r}.
\]

3. Estimation of $M$

We establish here the following refinement of Mordell’s upper bound (1.5).

**Lemma 3.1.** For any integers $k_i, 1 \leq i \leq r$, distinct and nonzero mod $(p - 1)$,
\[
M \leq \frac{4e}{\pi^2} \left( \frac{2r}{r} \right) (\ell_1 \cdots \ell_r) (p - 1)^r,
\]
where the $e = 2.718\ldots$ can be dropped if all the exponents are positive.

The factor of $e$ can also be removed when $r = 3$ while for $r = 2$ we have the sharper Lemma 3.2. If all $k_i$ are positive, it is reasonable to conjecture
\[
M \leq k_1 k_2 \cdots k_r p^r,
\]
which would be best possible in view of the following example.

**Example 3.1.** Let $k|p - 1$ be a fixed positive integer and suppose that $k_i = k \cdot i$, $1 \leq i \leq r$ and $p > r$. Then for any choice of $y_1, y_2, \ldots, y_r$, it follows from the Newton-Girard identities (see, e.g., Mordell [9]), that for any solution $x_1, x_2, \ldots, x_r$, satisfying the defining system for $M$, the $r$-tuple $(x_1^k, x_2^k, \ldots, x_r^k)$ is just a permutation of the $r$-tuple $(y_1^k, y_2^k, \ldots, y_r^k)$. Conversely, any such $x_1, \ldots, x_r$ is trivially a solution. Hence we obtain
\[
M \sim k_1 k_2 \cdots k_r p^r, \quad \text{as } p \to \infty.
\]

For the case $r = 2$ we obtain this best possible estimate.

**Lemma 3.2.** If $r = 2$ then we have
\[
M \leq \begin{cases} 
  k_1 k_2 (p - 1)^2, & \text{if } 1 \leq k_1 < k_2, \\
  3|k_1| k_2 (p - 1)^2, & \text{if } k_1 < 0 < k_2.
\end{cases}
\]

For a positive integer $l|\frac{1}{2}(p - 1)$ and exponents $k_1 = l, k_2 = 2l$ or $k_1 = -l, k_2 = l$ it is readily verified that $M = 2l^2 (p - 1)^2 - l^3 (p - 1)$ and $M = 3l^2 (p - 1)^2 - 3l^3 (p - 1)$ respectively, so the constants in both these bounds are sharp. If $r > 2$ and some of the $k_i$ are negative then it is unclear to the authors what the best possible upper bound should be, although the example $k_1, k_2 = -l, l$ just noted shows that one can not get $M < \ell_1 \cdots \ell_r p^r$ in general.

**Proof of Lemma 3.1.** Order the $k_i$ in terms of increasing $\ell_i$,
\[
(3.1) \quad \ell_1 \leq \ell_2 \leq \cdots \leq \ell_r.
\]
Let $S$ denote the set of solutions to be counted
\[
S = \{(x, y) : x = (x_1, \ldots, x_r), y = (y_1, \ldots, y_r) \in \mathbb{Z}_p^r, \sum_{j=1}^{r} x_j^{k_j} = \sum_{j=1}^{r} y_j^{k_j}, i = 1, \ldots, r\}.
\]
For $d \leq r$ write 
\[ D_d(u_1, \ldots, u_d) = \det \left( u_i^{k_j} \right)_{1 \leq i, j \leq d}. \]
A result of Wooley [13] shows that for any set of $\alpha_1, \ldots, \alpha_d \in \mathbb{Z}_p$,
\[ \# \left\{ \vec{u} = (u_1, \ldots, u_d) \in \mathbb{Z}_p^d : D_d(\vec{u}) \neq 0, \sum_{j=1}^d u_j^{k_j} = \alpha_i, \ i = 1, \ldots, d \right\} \leq \ell_1 \cdots \ell_d, \]
(since we are solving the simultaneous polynomial congruences $F_i(u_1, \ldots, u_d) = 0, i = 1, \ldots, d$, with the degree $k_i$ polynomial $F_i = \sum_{j=1}^d u_j^{k_j} - \alpha_i$ when $k_i > 0$ and the degree $(at most) d|k_i|$ polynomial $F_i = u_1^{k_1} \cdots u_d^{k_d}(\alpha_i - \sum_{j=1}^d u_j^{k_j})$ when $k_i < 0$; it is readily checked that the non-vanishing of det $\left( \frac{\partial F_i}{\partial u_j} \right)$ amounts to $D_d(u_1, \ldots, u_d) \neq 0$).

For a vector $\vec{u} = (u_1, \ldots, u_d) \in \mathbb{Z}_p^d$ define \[ \kappa(\vec{u}) = \max \{ l : D_l(v_1, \ldots, v_l) \neq 0 \text{ for some } \{ v_1, \ldots, v_l \} \subseteq \{ u_1, \ldots, u_d \} \}, \]
and for $l \leq d$
\[ N_{d,l} = \# \{ (\vec{x}, \vec{y}) \in S : \kappa(\vec{x}) = d, \kappa(\vec{y}) = l \}, \]
Hence, interchanging $\vec{x}$ and $\vec{y}$ as necessary, 
\[ (3.2) \quad M = \sum_{l \leq d \leq r} M_{d,l} = \sum_{l \leq d \leq r} M_{d,d} + 2 \sum_{l < d \leq r} M_{d,l}. \]

For a particular solution $x_1, \ldots, x_r, y_1, \ldots, y_r$ with $\kappa(\vec{x}) = d, \kappa(\vec{y}) = l$, we have subsets $\{ u_1, \ldots, u_d \} \subseteq \{ x_1, \ldots, x_r \}$ and $\{ v_1, \ldots, v_d \} \subseteq \{ y_1, \ldots, y_r \}$ with $D_d(u_1, \ldots, u_d) \neq 0, D_l(v_1, \ldots, v_l) \neq 0$. Clearly there are $\binom{d}{l}^2$ possibilities for $\{ u_1, \ldots, u_d \}$, and $\{ v_1, \ldots, v_d \}$, though each $\vec{x}$ will be associated with at least $(r - d + 1)$ different subsets $\{ u_1, \ldots, u_d \}$ (since given one collection $\{ u_1, \ldots, u_d \}$ with $D_d(u_1, \ldots, u_d) \neq 0$ we can add one of the $(r - d)$ omitted $x_j$ in place of an appropriate $u_i$). Likewise for the $\{ v_1, \ldots, v_d \}$ if $l = d$. If $l < d$ we have at least $(r - l) + \binom{d-l}{d-1} = \binom{r-d}{d-l}$ different $\{ v_1, \ldots, v_d \}$ associated to a given $\vec{y}$ (since given one collection $v_1, \ldots, v_l$ with $D_l(v_1, \ldots, v_l) \neq 0$ we have $\binom{d-l}{d-1}$ ways to simply add an additional $(d - l)$ from the $(r - l)$ remaining $y_j$ and $\binom{r-l}{d-l}$ ways of adding $(d - l + 1)$ positions from the remaining $y_j$, and dropping one of the $v_1, \ldots, v_l$). Observe that
\[ \binom{r-l}{d-l} = \begin{cases} \frac{(r - d + 1)}{(d - l + 1)}, & \text{if } d = r, \\ 2(r - d + 1), & \text{if } l < d \leq r - 2, \text{ or } d = r - 1 \text{ and } l < r - 2, \\ \frac{2}{2}(r - d + 1), & \text{if } d = r - 1 \text{ and } l = r - 2. \end{cases} \]

Bound the number of values for $v_1, \ldots, v_d$ by $N_{d,l}$ and the number of $\{ x_1, \ldots, x_r \} \setminus \{ u_1, \ldots, u_d \}$ by $(p - 1)^r - d$. When $d < r$, once the values of $\{ v_1, \ldots, v_d \}$ have been chosen, containing some subset $\{ v_1, \ldots, v_l \}$ with $D_l(v_1, \ldots, v_l) \neq 0$, the remaining $y_j$ satisfy
\[ (3.3) \quad 0 = D_{l+1}(y_1, \ldots, y_l) = y_i^{k_i+1} D_l(v_1, \ldots, v_l) + \sum_{j=1}^l \lambda_j (v_1, \ldots, v_l) y_i^{k_j}, \]
for some polynomials $\lambda_j$.

If $k_1, k_2, \ldots, k_{l+1}$ are all of the same sign then the degree of the resulting polynomial in $y_i$, and so number of possible $y_i$, is bounded by $(|k_{l+1}| + |k_l|) < \ell_{l+1}$. Otherwise, let $k_j$ denote the largest magnitude exponent with $J \leq l$, opposite in sign to $k_{l+1}$. If $k_{l+1} > 0$, so that $k_j < 0$, then $k_{l+1} = \ell_{l+1}$ and $r|k_j| = \ell_j \leq \ell_{l+1}$, by (3.1). It follows that the degree of the resulting polynomial in (3.4) will be at most $(k_{l+1} + |k_j|) \leq (1 + 1/r) \ell_{l+1}$. If $k_{l+1} < 0$, then $k_{l+1} = \frac{1}{r} \ell_{l+1}$ and $k_j = \ell_j \leq \ell_{l+1}$. Thus the degree is at most $(|k_{l+1}| + k_j) \leq (1 + 1/r) \ell_{l+1}$. Hence the number of possibilities for $\{ y_1, \ldots, y_r \} \setminus \{ v_1, \ldots, v_d \}$ is certainly bounded by
(1 + \frac{1}{d})^{-d} < e^{\ell_1 \cdots \ell_r}. Writing (\frac{r}{d})^2(r - d + 1)^{-2} = \binom{r+1}{d}(r+1)^{-2} and using (3.3) we have

\[ M_{d,l} \leq e \binom{r+1}{d} \binom{r-1}{(p-1)r} \times \begin{cases} 1, & \text{if } l = d \text{ or } d = r, \\ \frac{1}{2}, & \text{if } l < d \leq l - 2, \text{ or } d = r - 1 \text{ and } l < r - 2, \\ \frac{3}{4}, & \text{if } d = r - 1 \text{ and } l = r - 2. \end{cases} \]

It follows from (3.2) that

\[ M \leq e^{(p-1)^r \ell_1 \cdots \ell_r} \binom{r+1}{d}(r+1)^{-2} \]

where the factor of e may be omitted if all the \( k_i \) are positive, and

\[ M_1 \leq \sum_{d=1}^{r} \binom{r+1}{d} \binom{r-1}{(p-1)r} \binom{r-1}{(p-1)r} + \binom{r+1}{d} \binom{r-1}{(p-1)r} + \frac{1}{4} \binom{r+1}{d} \binom{r-1}{(p-1)r} \]

the second term coming from the extra contribution when \( d = r \) and \( l < r \) and the third term the extra contribution when \( d = r - 1 \), \( l = r - 2 \). Now,

\[ M_1 \leq \binom{2r+2}{r+1} - 2 + (r+1)^2 + \frac{1}{12} r^2 + \frac{1}{12} r^2 < \frac{1}{12} (r+1)^2, \]

and so the lemma follows. The saving of the factor of e when \( r = 3 \) can be seen by a more careful analysis of the above proof. \( \square \)

Proof of Lemma 3.2. For \( r = 2 \) write \( M = \sum_{d} C(\vec{u})^{2} \) where

\[ C(u_1, u_2) = \#\{(x, y) \in \mathbb{Z}_p^{2x} : x^{k_1} - y^{k_1} = u_1, x^{k_2} - y^{k_2} = u_2\} \]

\[ = d\#\{x \in \mathbb{Z}_p^* : x^{k_1} - y^{k_1} = u_1, x^{k_2} - y^{k_2} = u_2 \text{ for some } y \in \mathbb{Z}_p^*\} \]

where \( d = (k_1, k_2, p-1) \) (since for each \( x \) with a solution there will be \( d \) solutions \( y \) satisfying \( y^{(k_1, k_2)} = (x^{k_1} - u_1)^x(x^{k_2} - u_2)^y \) where \( (k_1, k_2) = k_1 s + k_2 t \).

Clearly if \( 0 < k_1 < k_2 \) are both positive then \( x \) will be a zero of the polynomial

\[ f = (x^{k_1} - u_1)^{k_2/d} - (x^{k_2} - u_2)^{k_1/d} \]

and for \( \vec{u} \neq 0 \) this will be a non-zero polynomial (if \( u_1 \neq 0 \) then \( f \) contains a term \( x^{k_1} \) and if \( u_1 = 0 \) and \( u_2 \neq 0 \) a constant term) of degree (and so number of solutions) at most \( (k_2/d - 1)k_1 \).

If \( k_1 < 0 < k_2 \) then \( x \) will be a root of the non-zero polynomial

\[ f = (x^{k_2} - u_2)^{k_1/d} (1 - x^{k_1} u_1)^{k_2/d} - x^{k_1} k_2/d \]

of degree at most \( 2k_1k_2/d \) when \( \vec{u} \neq 0 \).

For \( u_1 = u_2 = 0 \) the number of solutions \( C(\vec{0}) \) to \( x^{k_1} = y^{k_1}, x^{k_2} = y^{k_2} \) (and hence \( x = y \)) is \((p-1)^2\). Hence, since \( \sum_{d} C(\vec{u}) = (p-1)^2 \), we have when \( k_1 \) is positive,

\[ M \leq k_1(k_2 - d) \sum_{\vec{u} \neq \vec{0}} C(\vec{u}) + d^2(p-1)^2 \]

\[ = (k_1k_2 - d(k_1 - d))(p-1)^2 - dk_1(k_2 - d)(p-1) \leq k_1k_2(p-1)^2 \]

and when \( k_1 \) is negative,

\[ M \leq 2k_1 |k_2| \sum_{\vec{u} \neq \vec{0}} C(\vec{u}) + d^2(p-1)^2 \]

\[ = (2k_1 |k_2| + d^2)(p-1)^2 - 2d |k_1| k_2(p-1) < 3 |k_1| k_2(p-1)^2. \]

\( \square \)
References


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