

EXPLICIT BOUNDS ON MONOMIAL AND BINOMIAL EXPONENTIAL SUMS

TODD COCHRANE AND CHRISTOPHER PINNER

ABSTRACT. Let p be a prime and $e_p(\cdot) = e^{2\pi i \cdot / p}$. First, we make explicit the monomial sum bounds of Heath-Brown and Konyagin:

$$\left| \sum_{x=1}^{p-1} e_p(ax^d) \right| \leq \min\{\lambda d^{5/8} p^{5/8}, \lambda d^{3/8} p^{3/4}\},$$

where $\lambda = 2/\sqrt[4]{3} = 1.51967\dots$. Second, letting $d = (k, l, p-1)$, we obtain the explicit binomial sum bound

$$\left| \sum_{x=1}^{p-1} e_p(ax^k + bx^l) \right| \leq (k-l, p-1) + 2.292 d^{13/46} p^{89/92},$$

for any nonconstant binomial $ax^k + bx^l$ on \mathbb{Z}_p , by sharpening the estimate for the number of solutions of the system $x_1^k + x_2^k = x_3^k + x_4^k$, $x_1^l + x_2^l = x_3^l + x_4^l$. Finally, we apply the latter estimate to establish the Goresky-Klapper conjecture on the decimation of ℓ -sequences for $p > 4.92 \cdot 10^{34}$.

1. INTRODUCTION

For prime p and polynomial $f(x)$ over \mathbb{Z} , let $S(f)$ denote the exponential sum,

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

where $e_p(\cdot) = e^{2\pi i \cdot / p}$ is the additive character on \mathbb{Z}_p . The need for precise numeric estimates for such sums has become apparent in many areas of mathematics. For instance, to quantify the distribution of k -th powers $(\bmod p)$ one needs estimates for the monomial sum $S(x^k)$ and the binomial sum $S(x^k + bx)$. Such estimates were used by Bourgain, Paulhus and the authors [7], to resolve the Goresky-Klapper conjecture on the decimation of l -sequences for all sufficiently large primes, a problem of interest to computer scientists; see Section 7. In that paper we were able to establish the validity of the conjecture for $p > 2.26 \cdot 10^{55}$. A computer has verified the conjecture for $p < 2 \cdot 10^6$. In order to close this gap it is useful to have more precise estimates for a binomial sum. In this paper we obtain numeric estimates for $S(f)$ in the cases where f is a monomial or binomial. In particular the bounds obtained allow us to establish the Goresky-Klapper conjecture for $p > 4.92 \cdot 10^{34}$.

First we make explicit the monomial exponential sum bounds of Heath-Brown and Konyagin [14].

Theorem 1.1. *For any prime p , multiplicative subgroup A of \mathbb{Z}_p^* and integer a with $p \nmid a$, we have, with $\lambda = 2/\sqrt[4]{3} = 1.51967\dots$,*

$$\left| \sum_{x \in A} e_p(ax) \right| \leq \begin{cases} p^{1/2}, & |A| > \frac{1}{3}p^{2/3} \\ \lambda |A|^{3/8} p^{1/4}, & p^{1/2} < |A| \leq \frac{1}{3}p^{2/3} \\ \lambda |A|^{5/8} p^{1/8}, & 3 p^{1/3} < |A| \leq p^{1/2}. \end{cases}$$

Equivalently, letting $A \subset \mathbb{Z}_p^*$ be the subgroup of d -th powers we have

Theorem 1.2. *Let p be a prime and d a positive integer with $d|(p-1)$. Then for any integer a with $p \nmid a$,*

$$\left| \sum_{x=1}^{p-1} e_p(ax^d) \right| \leq \begin{cases} (d-1)p^{1/2} + 1, & d < 3p^{1/3}, \\ \lambda d^{5/8} p^{5/8}, & 3p^{1/3} \leq d < p^{1/2}, \\ \lambda d^{3/8} p^{3/4}, & p^{1/2} \leq d < \frac{1}{3}p^{2/3}, \end{cases}$$

with $\lambda = \frac{2}{\sqrt[3]{3}} = 1.51967\dots$.

Each of the bounds in Theorems 1.1 and 1.2 is valid for arbitrary d . We have indicated to the right the interval where the bound is optimal. The first bound in each of these theorems is just the classical bound for a Gauss sum. For $|A| < 3p^{1/3}$, or equivalently $d > \frac{1}{3}p^{2/3}$ all of these bounds are trivial. Konyagin [15] has obtained nontrivial bounds for $|A| > p^{\frac{1}{4}+\epsilon}$ that can be made explicit, but he (and we) have not computed the constants. Bourgain and Garaev [4] also have the bound $|\sum_{x \in A} e_p(ax)| \ll |A|^{0.999981\dots}$ for any A with $|A| > p^{1/4}$, but the implied constant has not been computed. Bourgain and Konyagin [6], and Bourgain, Glibichuck and Konyagin [5] obtained estimates valid for $|A| > p^\epsilon$. More recently Bourgain [3] has proved that

$$\left| \sum_{x \in A} e_p(ax) \right| < p^{-\exp(-C \frac{\log p}{\log |A|})} |A|$$

for some absolute (undetermined) constant $C > 1$. For example, to save a factor $e^{-\sqrt{\log p}}$ on the trivial bound one needs only $\log |A| > 2C \log p / \log \log p$.

Next, we turn to binomial sums. Let a, b, k, l be integers and $f(x) = ax^k + bx^l$. We shall only insist that f be nonconstant on \mathbb{Z}_p . Thus, it is allowed to collapse to a nonconstant monomial. Set

$$d = (k, l, p-1).$$

In [8, Corollary 1.1] the authors established the upper bound

$$\left| \sum_{x=1}^{p-1} e_p(ax^k + bx^l) \right| \ll (k-l, p-1) + d^{3/13} p^{51/52},$$

for any nonconstant binomial $f(x)$ on \mathbb{Z}_p , a bound that is nontrivial for $d \ll p^{1/12}$. Here we establish a stronger (and explicit) bound, that remains nontrivial for $d \ll p^{3/26}$.

Theorem 1.3. *For any nonconstant binomial $f(x)$ on \mathbb{Z}_p we have*

$$\left| \sum_{x=1}^{p-1} e_p(ax^k + bx^l) \right| \leq (k-l, p-1) + 2.292 d^{13/46} p^{89/92}.$$

The first term can be removed if $-b\bar{a}$ is not a $(k-l)$ -th power in \mathbb{Z}_p .

The term $d^* := (k-l, p-1)$ cannot be removed from the right-hand side when $-b\bar{a}$ is a d^* -th power. Indeed, in this case we see that $S(f) \sim d^*$ if $d^* \gg \min\{d^{1/2}p^{3/4}, d^{5/13}p^{10/13}\}$ by estimate (29) and the bounds in Theorem 1.2. In Theorem 4.1 we give a slightly stronger upper bound, nontrivial for $d < p^{1/3}$ but requiring $(k, p-1)$ or $(l, p-1)$ to be sufficiently large. By the work of Bourgain [2],

it is known that if $d < p^{1-\epsilon}$ and $d^* < p^{1-\epsilon}$, then $|S(f)| \leq p^{1-\delta}$ for some $\delta = \delta(\epsilon)$; see [11].

Crucial for our binomial bounds will be estimates for $M(k, l)$, the number of solutions in $(\mathbb{Z}_p^*)^4$ of the system of simultaneous equations

$$\begin{aligned} x_1^k + x_2^k &= x_3^k + x_4^k \\ x_1^l + x_2^l &= x_3^l + x_4^l. \end{aligned}$$

For example when the exponents $1 \leq l < k$ have $(kl, p-1) = 1$ and $(k \mp l, p-1) \leq 1.68(p-1)^{16/23}$ we obtain the bound (see Theorem 7.1)

$$M(k, \pm l) \leq 27.57p^{66/23}.$$

The special case $l = 1$ of this will be used in Corollary 7.1 when verifying the Goresky-Klapper conjecture, 27.57 replacing the 13658 in Theorem 3 of our earlier paper [7]. Good bounds for $M(k, l)$ translate immediately into good bounds for the corresponding binomial exponential sum via

$$\left| \sum_{x=1}^{p-1} e_p(ax^k + bx^{\pm l}) \right| \leq M(k, \pm l)^{1/4} p^{1/4}.$$

We should remark that the various inequalities above in fact hold for the more general mixed exponential sum $\sum_{x=1}^{p-1} \chi(x) e_p(f(x))$, where χ is a multiplicative character mod p and f is a monomial or binomial.

2. PROOFS OF THEOREMS 1.1 AND 1.2

Define

$$N(A) = |\{(x_1, x_2, y_1, y_2) \in A^4 : x_1 + x_2 = y_1 + y_2\}|,$$

and for any $a \in \mathbb{F}_p$ let

$$N(A, a) = |\{(x_1, x_2) \in A^2 : x_1 + x_2 = a\}|.$$

In order to pass from the estimate of $N(A)$ to the estimate of the monomial exponential sum, we use

Lemma 2.1. [14] *For any subgroup A of \mathbb{Z}_p^* ,*

$$\left| \sum_{x \in A} e_p(ax) \right| \leq \begin{cases} N(A)^{\frac{1}{4}} |A|^{-\frac{1}{4}} p^{\frac{1}{4}}, \\ N(A)^{\frac{1}{4}} p^{\frac{1}{8}}. \end{cases}$$

If $|A| \geq p^{2/3}$ then Theorem 1.1 follows from the classical estimate for a Gauss sum, $|\sum_{x \in A} e_p(ax)| \leq \sqrt{p}$. For $|A| < p^{2/3}$ it is an immediate consequence of Lemma 2.1 and

Theorem 2.1. *For any multiplicative subgroup A of \mathbb{Z}_p with $|A| < p^{2/3}$ we have $N(A) \leq \frac{16}{3}|A|^{5/2}$.*

The classical estimate of Hua, Vandiver and Weil for the number of solutions of the homogeneous equation $x_1^d + x_2^d = x_3^d + x_4^d$ can be stated in the manner $|N(A) - \frac{|A|^4}{p}| < p|A|$. Thus for $|A| \geq p^{2/3}$ one has $|N(A)| < \frac{|A|^4}{p} + |A|^{5/2}$. One also sees that the hypothesis $|A| < p^{2/3}$ in the theorem cannot be relaxed. To obtain the constant 16/3 in the theorem, we make use of the following lemma of Mattarei [17], for counting the number of solutions of the Fermat equation $x^d + y^d = z^d$ over

a finite field. It is a refinement of a result of Garcia and Voloch [12]. A similar upper bound is also given in [16] with an undetermined constant.

Lemma 2.2. *For any nonzero $a \in \mathbb{Z}_p$ and multiplicative subgroup A of \mathbb{Z}_p with $|A| < (1/4)^{1/4}(p-1)^{3/4}$, we have $N(A, a) \leq 3 \cdot 2^{-2/3}|A|^{2/3}$.*

The result of [17] has an extra hypothesis that $d \geq 4$, where $d = (p-1)/|A|$, but one can check that the lemma holds trivially for $d < 4$. Indeed, for $d = 3$, $N(A, a) \leq |A| \leq 3 \cdot 2^{-2/3}|A|^{2/3}$ provided that $|A| \leq 6$. If $|A| \geq 7$ then since $p = 3|A| + 1 \geq 22$ we have $|A| = (p-1)/3 \geq (1/4)^{1/4}(p-1)^{3/4}$, contrary to assumption. A similar argument applies when $d = 1$ or 2 . In [12] the upper bound $4|A|^{2/3}$ is obtained for $|A| < (p-1)/((p-1)^{1/4} + 1)$.

Let A be a multiplicative subgroup of \mathbb{Z}_p , with $t = |A|$. We start by writing $A + A$ as a disjoint union of cosets of A ,

$$A + A = Ax_1 \cup Ax_2 \cdots \cup Ax_n \cup \{0\},$$

where $\{0\}$ is omitted if $-1 \notin A$.

For any coset Ax_j let

$$N_j = |\{x \in A : x + 1 \in Ax_j\}| = |\{(x, y) \in A \times A : x + y = x_j\}|.$$

We assume the sets Ax_i have been ordered so that

$$N_1 \geq N_2 \geq N_3 \geq \cdots \geq N_n.$$

Now for any $x \in A$, $x \neq -1$, $x + 1 \in Ax_j$ for some j and so

$$(1) \quad \sum_{j=1}^n N_j = t - \delta,$$

where

$$\delta = \begin{cases} 1, & \text{if } -1 \in A, \\ 0, & \text{if } -1 \notin A, \end{cases}$$

and

$$(2) \quad N(A) = \delta t^2 + t \sum_{j=1}^n N_j^2.$$

The next lemma is extracted from the proof of [16, Lemma 3.2].

Lemma 2.3. *Let a, b, d, s be positive integers such that $s \leq n$, $sad + \frac{1}{2}sd(d-1) < ab^2$, $ab \leq t$, $tb < p$, where $t = |A|$. Then*

$$\sum_{j=1}^s N_j \leq \frac{a-1+2t(b-1)}{d}.$$

Proof. The lower case a, b, d in the lemma correspond to the upper case A, B, D in [16]. In equation (3.11) of [16] one actually has $sad + \frac{1}{2}sd(d-1) < ab^2$ by summing over k in the preceding line of their proof. \square

Apply the lemma with

$$b = [(4st)^{1/3}] + 1, \quad a = [t/b], \quad d = 2a.$$

Then

$$sad + \frac{1}{2}sd(d-1) < 4a^2s = 4a(as) \leq \frac{4t}{b}(as) \leq ab^2,$$

and so if $tb \leq p$ then we deduce

$$(3) \quad \sum_{j=1}^s N_j \leq \frac{1}{2} - \frac{1}{2a} + \frac{t(b-1)}{a} \leq \frac{1}{2} + \frac{t(b-1)}{\frac{t}{b} - 1} = \frac{1}{2} + b^2 \frac{1 - \frac{1}{b}}{1 - \frac{1}{t}}.$$

If we assume further that $b^2 < t$ we get from (3),

$$(4) \quad \sum_{j=1}^s N_j \leq \frac{1}{2} + b^2.$$

If $b^2 \geq t$ then the same bound holds trivially by (1). Since the left-hand side is an integer the $\frac{1}{2}$ can be dropped, thus establishing

Lemma 2.4. *For any positive integer $s \leq n$ such that $bt < p$,*

$$\sum_{j=1}^s N_j \leq ((4ts)^{1/3} + 1)^2.$$

Sections 5 and 8 will require us to asymptotically evaluate sums of the form $\sum_{j \leq s} j^{-c}$. Hence for $0 < c < 1$ we define

$$(5) \quad \gamma_c(s) = \frac{c}{1-c} + c \int_1^s \{x\} x^{-1-c} dx.$$

In §5 we will need estimates for the quantity

$$(6) \quad \kappa_0(s) = -\frac{2^{14/3}}{9} \gamma_{2/3}(s) + \left(2^{5/3} + \frac{16}{9}\right) \gamma_{1/3}(s),$$

and in §8

$$(7) \quad \kappa_1(s) = \frac{8}{3} \gamma_{2/5}(s) - \gamma_{4/5}(s).$$

Lemma 2.5. *For $0 < c < 1$ and s in \mathbb{N}*

$$(8) \quad \sum_{j \leq s} j^{-c} = \frac{s^{1-c}}{1-c} - \gamma_c(s).$$

The functions $\kappa_0(s)$ and $\kappa_1(s)$ are increasing for s in \mathbb{N} with

$$(9) \quad \kappa_0(s) < -2.083,$$

and

$$(10) \quad \kappa_1(s) < -1.4$$

for all s in \mathbb{N} , with

$$(11) \quad \kappa_1(1) = -\frac{20}{9}.$$

Proof. Partial summation gives (8). Claims (9) and (10) follow from

$$\begin{aligned} \kappa_0(s) &= \kappa_0(\infty) - \frac{2^{5/3}}{27} \int_s^\infty \frac{\{x\}}{x^{5/3}} \left((9 + 2^{7/3})x^{1/3} - 16 \right) dx, \\ \kappa_1(s) &= \kappa_1(\infty) - \frac{4}{5} \int_s^\infty \frac{\{x\}}{x^{9/5}} \left(\frac{4}{3}x^{2/5} - 1 \right) dx, \end{aligned}$$

(checking numerically that $\kappa_0(1) < \kappa_0(2)$) and numerical computation $\kappa_0(\infty) < -2.083$ and $\kappa_1(\infty) < -1.4$.

□

3. PROOF OF THEOREM 2.1

Suppose $t < p^{2/3}$. Since $N(A) \leq t^3 \leq \frac{16}{3}t^{5/2}$ for $t \leq 28$ we may assume that $t \geq 29$ and $p \geq 157$. Hence $t < p^{2/3} < 0.7(p-1)^{3/4}$, and by (2) and (1) and Lemma 2.2 we have

$$N(A) \leq \delta t^2 + tN_1 \sum_{j=1}^n N_j = \delta t^2 + tN_1(t - \delta) \leq t^2 + 3 \cdot 2^{-2/3} t^{5/3} (t - 1) < \frac{16}{3} t^{5/2}$$

for $t \leq 485$. Hence we assume that $t \geq 486$ and, setting

$$J = \left\lceil \sqrt{t}/4 \right\rceil,$$

that $J \geq 5$. We define

$$m_j = \frac{2^{7/3}}{3} t^{2/3} j^{-1/3}, \quad w_j = N_j - m_j, \quad C(s) = \sum_{j \leq s} w_j.$$

From Lemma 2.2

$$C(s) = \sum_{j \leq s} N_j - \sum_{j \leq s} m_j \leq t^{2/3} \left(3 \cdot 2^{-2/3} s - \frac{2^{7/3}}{3} \sum_{j \leq s} j^{-1/3} \right),$$

giving

$$(12) \quad C(1) \leq 0.210t^{2/3}, \quad C(2) \leq 0.767t^{2/3}, \quad C(3) \leq 1.492t^{2/3}.$$

For $s \leq J - 1 \leq \frac{1}{4}t^{1/2} - 1$ we have

$$b^2 \leq \left(4^{1/3} t^{1/3} \left(\frac{1}{4} t^{1/2} - 1 \right)^{1/3} + 1 \right)^2 < t,$$

$bt < t^{3/2} < p$, and Lemma 2.4 gives $\sum_{j \leq s} N_j \leq ([2^{2/3} t^{1/3} s^{1/3}] + 1)^2$. Hence, using the notation (5) and Lemma 2.5, for $s \leq J - 1$

$$\begin{aligned} C(s) &\leq \left([2^{2/3} t^{1/3} s^{1/3}] + 1 \right)^2 - \frac{2^{7/3}}{3} t^{2/3} \sum_{j \leq s} j^{-1/3} \\ &\leq (2^{2/3} t^{1/3} s^{1/3} + 1)^2 - \frac{2^{7/3}}{3} \left(\frac{3}{2} s^{2/3} - \gamma_{1/3}(s) \right) t^{2/3} \\ (13) \quad &= \frac{2^{7/3}}{3} \gamma_{1/3}(s) t^{2/3} + 2^{5/3} t^{1/3} s^{1/3} + 1 \leq \frac{2^{7/3}}{3} \gamma_{1/3}(J-1) t^{2/3} + 2t^{1/2}, \end{aligned}$$

and by Lemma 2.4

$$(14) \quad N_s \leq s^{-1} \sum_{i=1}^s N_i \leq \frac{([2^{2/3} t^{1/3} s^{1/3}] + 1)^2}{s}.$$

Using (1) and (2) we write

$$\begin{aligned}
N(A)t^{-1} &= \sum_{j=1}^n N_j^2 + \delta t \\
&\leq \sum_{j<J} N_j^2 + N_J \sum_{j \geq J} N_j + \delta t \\
&= \sum_{j<J} N_j(N_j - N_J) + N_J(t - \delta) + \delta t \\
&\leq \sum_{j<J} m_j(N_j - N_J) + \sum_{j<J} w_j(N_j - N_J) + N_J(t - 1) + t \\
&= \sum_{j<J} m_j^2 + \sum_{j<J} w_j(N_j - N_J) + \sum_{j<J} m_j w_j + N_J \left(t - 1 - \sum_{j<J} m_j \right) + t \\
&= M_1 + E_1 + E_2 + E_3 + t,
\end{aligned}$$

where

$$\begin{aligned}
M_1 &= \sum_{j<J} m_j^2 = \frac{2^{14/3}}{9} t^{4/3} \sum_{j<J} j^{-2/3} \\
&= \frac{2^{14/3}}{9} t^{4/3} \left(3(J-1)^{1/3} - \gamma_{2/3}(J-1) \right) \\
&= \frac{16}{3} t^{3/2} - \frac{2^{14/3}}{9} \gamma_{2/3}(J-1) t^{4/3} - \frac{2^{14/3}}{3} t^{4/3} \left(\left(\frac{\sqrt{t}}{4} \right)^{1/3} - (J-1)^{1/3} \right)
\end{aligned}$$

and

$$\begin{aligned}
E_3 &= N_J \left(t - 1 - \sum_{j<J} m_j \right) \\
&= N_J \left(t - 1 - \frac{2^{7/3}}{3} t^{2/3} \left(\frac{3}{2} (J-1)^{2/3} - \gamma_{1/3}(J-1) \right) \right) \\
&= N_J \left(\frac{2^{7/3}}{3} \gamma_{1/3}(J-1) t^{2/3} + 2^{4/3} t^{2/3} \left(\left(\frac{\sqrt{t}}{4} \right)^{2/3} - (J-1)^{2/3} \right) - 1 \right).
\end{aligned}$$

Using partial summation (eg Hardy & Wright Theorem 421), (13) and $N_1 \leq 3 \cdot 2^{-2/3} t^{2/3}$,

$$\begin{aligned}
E_1 &= \sum_{j<J} w_j(N_j - N_J) = C(J-1)(N_{J-1} - N_J) + \sum_{1 \leq j \leq J-2} C(j)(N_j - N_{j+1}) \\
&\leq \left(\frac{2^{7/3}}{3} \gamma_{1/3}(J-1) t^{2/3} + 2t^{1/2} \right) \sum_{1 \leq j \leq J-1} (N_j - N_{j+1}) \\
&= \left(\frac{2^{7/3}}{3} \gamma_{1/3}(J-1) t^{2/3} + 2t^{1/2} \right) (N_1 - N_J) \\
&\leq 2^{5/3} \gamma_{1/3}(J-1) t^{4/3} + 3 \cdot 2^{1/3} t^{7/6} - N_J \left(\frac{2^{7/3}}{3} \gamma_{1/3}(J-1) t^{2/3} + 2t^{1/2} \right).
\end{aligned}$$

Similarly, using the bounds (12) on $C(j)$ for $j \leq 3$ and (13) for $j \geq 4$,

$$\begin{aligned}
E_2 &= \sum_{j < J} m_j w_j = \frac{2^{7/3}}{3} t^{2/3} \sum_{j < J} w_j j^{-1/3} \\
&= \frac{2^{7/3}}{3} t^{2/3} \left(C(J-1)(J-1)^{-1/3} + \sum_{1 \leq j \leq J-2} C(j) \left(j^{-1/3} - (j+1)^{-1/3} \right) \right) \\
&\leq \frac{2^{7/3}}{3} t^{4/3} \left(0.210(1 - 2^{-1/3}) + 0.767(2^{-1/3} - 3^{-1/3}) + 1.492(3^{-1/3} - 4^{-1/3}) \right) \\
&\quad + \frac{2^{7/3}}{3} t^{2/3} \left(\frac{2^{7/3}}{3} \gamma_{1/3}(J-1)t^{2/3} + 2t^{1/2} \right) \left((J-1)^{-1/3} + \sum_{4 \leq j \leq J-2} \left(j^{-1/3} - (j+1)^{-1/3} \right) \right) \\
&\leq \left(\frac{16}{9} \gamma_{1/3}(J-1) + 0.361 \right) t^{4/3} + \frac{2^{8/3}}{3} t^{7/6}.
\end{aligned}$$

Hence

$$N(A)t^{-1} \leq \frac{16}{3} t^{3/2} + t^{4/3} (E_4 + E_5)$$

where, with $\kappa_0(J-1)$ as defined in (6),

$$E_4 = \kappa_0(J-1) + 0.361 + 5.897t^{-1/6} + t^{-1/3},$$

and

$$E_5 = N_J \left(2^{4/3} \left(\left(\frac{\sqrt{t}}{4} \right)^{2/3} - (J-1)^{2/3} \right) t^{-2/3} - 2t^{-5/6} - t^{-4/3} \right) - \frac{2^{14/3}}{3} \left(\left(\frac{\sqrt{t}}{4} \right)^{1/3} - (J-1)^{1/3} \right).$$

Also, from (14),

$$N_J \leq N_{J-1} \leq \frac{([2^{2/3}(J-1)^{1/3}t^{1/3}] + 1)^2}{(J-1)}.$$

For $t < 2704$ one checks numerically that $E_4 + E_5 < -0.4743$, whence $N(A)t^{-1} \leq \frac{16}{3} t^{3/2}$.

For $t \geq 2704$ we have $J \geq 13$. The bounds

$$N_J \leq \frac{(2^{2/3}(J-1)^{1/3}t^{1/3} + 1)^2}{(J-1)} \leq \frac{(2^{2/3} + 12^{-1/3}2704^{-1/3})^2}{(J-1)^{1/3}} t^{2/3} \leq \frac{2.621t^{2/3}}{(J-1)^{1/3}},$$

$$(15) \quad \left(\frac{\sqrt{t}}{4} \right)^{1/3} - (J-1)^{1/3} \leq \frac{2}{3} (J-1)^{-2/3},$$

and, using (15),

$$\begin{aligned}
\left(\frac{\sqrt{t}}{4} \right)^{2/3} - (J-1)^{2/3} &= \left((J-1)^{1/3} + \left(\frac{\sqrt{t}}{4} \right)^{1/3} \right) \left(\left(\frac{\sqrt{t}}{4} \right)^{1/3} - (J-1)^{1/3} \right) \\
&\leq \left(2(J-1)^{1/3} + \frac{2}{3}(J-1)^{-2/3} \right) \left(\left(\frac{\sqrt{t}}{4} \right)^{1/3} - (J-1)^{1/3} \right) \\
&\leq 2.056 \left(\left(\frac{\sqrt{t}}{4} \right)^{1/3} - (J-1)^{1/3} \right) (J-1)^{1/3},
\end{aligned}$$

give

$$\begin{aligned}
E_5 &\leq \left(2.621 \cdot 2^{4/3} \cdot 2.056 - \frac{2^{14/3}}{3}\right) \left(\left(\frac{\sqrt{t}}{4}\right)^{1/3} - (J-1)^{1/3}\right) - 2.621 \cdot 2t^{-1/6}(J-1)^{-1/3} \\
&\leq 3.409(J-1)^{-2/3} - 5.242t^{-1/6}(J-1)^{-1/3} = \left(3.409\left(\frac{\sqrt{t}}{J-1}\right)^{2/3} - 5.242\left(\frac{\sqrt{t}}{J-1}\right)^{1/3}\right)t^{-1/3} \\
&\leq \left(3.409\left(4 + \frac{8}{J-1}\right)^{2/3} - 5.242\left(4 + \frac{8}{J-1}\right)^{1/3}\right)t^{-1/3} \\
&\leq \left(3.409\left(\frac{14}{3}\right)^{2/3} - 5.242\left(\frac{14}{3}\right)^{1/3}\right)t^{-1/3} < 0.760t^{-1/3}.
\end{aligned}$$

From Lemma 2.5 we have $\kappa_0(J-1) < -2.083$. Hence for $t \geq 2704$ we have $E_4 + E_5 \leq -1.722 + 5.897t^{-1/6} + 1.760t^{-1/3} < 0$, and $N(A)t^{-1} < \frac{16}{3}t^{3/2}$.

4. ANOTHER BINOMIAL SUM BOUND

The following theorem is needed in the proof of Theorem 1.3, but it has independent interest. It yields a nontrivial bound on any binomial exponential sum with $d \ll p^{1/3}$ and either $(k, p-1) > d$ or $(l, p-1) > d$, where $d = (k, l, p-1)$.

Theorem 4.1. *For any nonconstant binomial $f(x) = ax^k + bx^l$, and constant λ as in Theorem 1.2, we have the bound*

$$|S(f)| \leq p \left(\frac{d}{(k, p-1)}\right)^{1/2} + \min\{\lambda^{8/11} d^{15/88} p^{21/22}, \lambda^{2/3} d^{1/8} p^{23/24}\}.$$

The proof uses averaging methods similar to what is found in Akulnichev [1], Yu [20] and the author's work [10], together with the bounds for a monomial sum given in Theorem 1.2. For any integer k , set

$$(16) \quad \Phi(k) = \max_{a \neq 0} \left| \sum_{x=1}^{p-1} e_p(ax^k) \right|.$$

Lemma 4.1. *For any binomial $f(x) = ax^k + bx^l$, we have $|S(f)| \leq \Phi\left(\frac{d(p-1)}{(l, p-1)}\right)$. In particular, with λ as in Theorem 1.2,*

$$(17) \quad |S(f)| \leq \frac{p^{3/2}d}{(l, p-1)}, \quad (l, p-1) > \frac{1}{3}dp^{2/3},$$

$$(18) \quad |S(f)| \leq \frac{\lambda p^{5/4}d^{5/8}}{(l, p-1)^{5/8}}, \quad \sqrt{p}d < (l, p-1) < \frac{1}{3}dp^{2/3},$$

$$(19) \quad |S(f)| \leq \frac{\lambda p^{9/8}d^{3/8}}{(l, p-1)^{3/8}}, \quad (l, p-1) < d\sqrt{p}.$$

The inequality in (18) is a generalization of Yu [20, Theorem 2]. His theorem required $l|p-1$ and $d = 1$. From this he deduced the uniform bound $|S(f)| \ll p^{23/24}$ under the same constraints.

Proof. Set $m = \frac{p-1}{(l, p-1)}$. Then

$$(p-1)S(f) = \sum_{y=1}^{p-1} \sum_{x=1}^{p-1} e_p(f(xy^m)) = \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} e_p(ax^k y^{km} + bx^l)$$

and so,

$$|S(f)| \leq \frac{1}{p-1} \sum_{x=1}^{p-1} \left| \sum_{y=1}^{p-1} e_p(ax^k y^{km}) \right|.$$

The first result follows from the observation that $(km, p-1) = \frac{p-1}{(l, p-1)}d$. The remaining inequalities are an immediate consequence of Theorem 1.2. \square

In [10, Lemma 3.1] the authors proved

$$|S(f)| \leq p \left(\frac{d}{(k, p-1)} \right)^{1/2} + \sqrt{p} \Phi((l, p-1))^{1/2}.$$

We deduce from Theorem 1.2,

Lemma 4.2. *For any nonconstant binomial $f(x) = ax^k + bx^l$ on \mathbb{Z}_p ,*

(20)

$$|S(f)| \leq p \left(\frac{d}{(k, p-1)} \right)^{1/2} + p^{3/4} (l, p-1)^{1/2}, \quad (l, p-1) < 3p^{1/3},$$

(21)

$$|S(f)| \leq p \left(\frac{d}{(k, p-1)} \right)^{1/2} + \lambda^{1/2} p^{13/16} (l, p-1)^{5/16}, \quad 3p^{1/3} \leq (l, p-1) < p^{1/2},$$

(22)

$$|S(f)| \leq p \left(\frac{d}{(k, p-1)} \right)^{1/2} + \lambda^{1/2} p^{7/8} (l, p-1)^{3/16}, \quad p^{1/2} \leq (l, p-1) < \frac{1}{3}p^{2/3},$$

with λ as in Theorem 1.2.

Proof of Theorem 4.1. We treat a number of separate cases which may be of independent interest. The theorem itself just needs the argument presented in cases (iv) and (v).

(i). If $(l, p-1) > \frac{1}{3}dp^{2/3}$ then by (17), $|S(f)| < 3p^{5/6}$.

(ii). If $d\sqrt{p} < (l, p-1) \leq \frac{1}{3}dp^{2/3}$ then by (18), $|S(f)| < \lambda p^{15/16}$.

(iii). If $(l, p-1) < 3p^{1/3}$ then by (20), $|S(f)| < A + p^{3/4}(3p^{1/3})^{1/2} < A + \sqrt{3}p^{11/12}$, where A is the first term in the theorem.

(iv). Suppose next that $3p^{1/3} \leq (l, p-1) \leq \sqrt{p}$. If $(l, p-1) \geq \lambda^{8/11}p^{5/11}d^{6/11}$ we use (19) to get $|S(f)| \leq \lambda^{8/11}d^{15/88}p^{21/22}$. If $(l, p-1) \leq \lambda^{8/11}p^{5/11}d^{6/11}$ then we use (21) to get the same bound with A added.

(v). Suppose that $\sqrt{p} \leq (l, p-1) \leq \frac{1}{3}p^{2/3}$. If $(l, p-1) > \lambda^{8/9}d^{2/3}p^{4/9}$ then use (19) to get $|S(f)| \leq \lambda^{2/3}d^{1/8}p^{23/24}$. If $(l, p-1) \leq \lambda^{8/9}d^{2/3}p^{4/9}$, then we use (22) to get the same with A added. \square

5. LEMMAS FOR THEOREM 1.3

For any integers k, l let $M(k, l)$ denote the number of solutions in $(\mathbb{Z}_p^*)^4$ of the system

$$\begin{aligned} x_1^k + x_2^k &= x_3^k + x_4^k \\ x_1^l + x_2^l &= x_3^l + x_4^l, \end{aligned}$$

and put $M_+(k, l) = M(k, l)$ for $1 \leq l < k < p - 1$, $M_-(k, l) = M(k, -l)$ for $1 \leq l < k$, $k + l < p - 1$. Let

$$(23) \quad S_+(k, l) = \sum_{x=1}^{p-1} e_p(ax^k + bx^l), \quad p \nmid ab, \quad 1 \leq l < k < p - 1,$$

and

$$(24) \quad S_-(k, l) = \sum_{x=1}^{p-1} e_p(ax^k + bx^{-l}), \quad p \nmid ab, \quad 1 \leq l \leq k, \quad (k + l) < p - 1.$$

In [8] we established the Mordell type bound

$$(25) \quad |S_{\pm}(k, l)| \leq p^{1/4} M_{\pm}(k, l)^{1/4},$$

and the elementary bounds ([8, Lemma 3.2])

$$(26) \quad \begin{aligned} M_+(k, l) &\leq kl(p-1)^2, \quad \text{for } 1 \leq l < k < p - 1, \\ M_-(k, l) &\leq 3kl(p-1)^2, \quad \text{for } 1 \leq l \leq k, \quad l + k < p - 1, \end{aligned}$$

from which we immediately deduce

Lemma 5.1. *For any k, l ,*

$$|S_+(k, l)| \leq (kl)^{1/4} p^{3/4}, \quad |S_-(k, l)| \leq (3kl)^{1/4} p^{3/4}.$$

Set

$$\begin{aligned} d &= (k, l, p-1), \quad d_1 = (k, l), \quad d^* = d_{\pm}^* = (k \mp l, p-1) \\ l_+ &= l, \quad l_- = 2l, \quad \delta_+ = \frac{(k-l)}{d_1}, \quad \delta_- = \frac{(k+l)}{d_1}. \end{aligned}$$

In [7, Lemma 3] we proved that if $k < \frac{1}{32}(p-1)^{\frac{3}{2}} d_1^{\frac{1}{6}} l_{\pm}^{\frac{1}{6}}$, then

$$M_{\pm}(k, l) \leq d^2(p-1)^2 + 2k^2 l_{\pm}(p-1) + (p-1)^2 \mu$$

where

$$\mu = \max\{768 \cdot 5^{2/3} kl_{\pm} \delta_{\pm}^{-\frac{1}{3}} d/d_1, 557 \delta_{\pm} d\}.$$

In the next section we prove a version with substantially improved constants.

Theorem 5.1. *If*

$$(27) \quad (k+l)^5 \delta_{\pm}^2 < 2.1 (kl_{\pm}/d_1)(p-1)^4$$

then

$$M_{\pm}(k, l) \leq d^2(p-1)^2 + 2k^2 l_{\pm}(p-1) + (p-1)^2 \mu$$

with

$$\mu = \begin{cases} 27 \left(\frac{7}{50}\right)^{1/6} \frac{(kl_{\pm}/d_1)}{\delta_{\pm}^{1/3}} d, & \text{if } (kl_{\pm}/d_1) \geq \frac{3}{2} \left(\frac{7}{50}\right)^{1/3} \delta_{\pm}^{4/3}, \\ \frac{7^{1/2}}{50^{3/10}} \left(\frac{81}{4}\right) \delta_{\pm} d, & \text{if } (kl_{\pm}/d_1) \leq \frac{3}{2} \left(\frac{7}{50}\right)^{1/3} \delta_{\pm}^{4/3}. \end{cases}$$

Note that condition (27) certainly holds if $k \leq \frac{1}{2}(1.05)^{\frac{1}{6}}(p-1)^{\frac{2}{3}}d_1^{\frac{1}{6}}l_{\pm}^{\frac{1}{6}}$. From Theorem 5.1 we readily obtain an effective form of Theorem 1.1 and Lemma 1.1 in [7].

Corollary 5.1. *If*

$$(28) \quad k < \frac{1}{2}(p-1)^{2/3}d^{1/3},$$

then

$$M_{\pm}(k, l) \leq 19.74 \max \left\{ 1, l_{\pm} \Delta_{\pm}^{-1/3} \right\} k(p-1)^2$$

and

$$S_{\pm}(k, l) \leq 2.11 \max \left\{ 1, l_{\pm} \Delta_{\pm}^{-1/3} \right\}^{1/4} k^{1/4} p^{3/4},$$

where $\Delta_{\pm} = (k \mp l)/d$.

Proof. The bound for $S_{\pm}(k, l)$ follows at once from the bound on $M_{\pm}(k, l)$ by (25), so it suffices to prove the latter. We may assume that $(k \mp l) > (19.74/1.5)^3 d$, else the bound is trivial by (26). By (28) we certainly have $(p-1)^{2/3}d^{1/3} > 2k > (k \mp l) > (19.74/1.5)^3 d$, so $(p-1) > (19.74/1.5)^{9/2} d$. Hence

$$\frac{d^2(p-1)^2}{kl_{\pm} \Delta_{\pm}^{-1/3} (p-1)^2} = \frac{d^{5/3}(k \mp l)^{1/3}}{kl_{\pm}} \leq \frac{d^{5/3}}{(k \mp l)^{2/3} l} \leq \left(\frac{1.5}{19.74} \right)^2 \frac{d}{l} \leq 0.006,$$

and

$$\begin{aligned} \frac{2k^2 l_{\pm} (p-1)}{kl_{\pm} \Delta_{\pm}^{-1/3} (p-1)^2} &= \frac{2k(k \mp l)^{1/3}}{d^{1/3}(p-1)} \leq \frac{2^{4/3} k^{4/3}}{d^{1/3}(p-1)} \\ &\leq \frac{2^{4/3} (\frac{1}{2}(p-1)^{2/3} d^{1/3})^{4/3}}{d^{1/3}(p-1)} = \frac{d^{1/9}}{(p-1)^{1/9}} \leq \left(\frac{1.5}{19.74} \right)^{1/2} < 0.276. \end{aligned}$$

If $(kl_{\pm}/d_1) \leq \frac{3}{2} \left(\frac{7}{50} \right)^{1/3} \delta_{\pm}^{4/3}$ then

$$\begin{aligned} \frac{l}{k} &\leq \frac{3}{2} \left(\frac{7}{50} \right)^{1/3} \frac{d_1}{k^2} \frac{l}{l_{\pm}} \left(\frac{k \mp l}{d_1} \right)^{4/3} \leq \frac{3}{2} \left(\frac{7}{50} \right)^{1/3} \frac{d_1}{k^2} 2^{1/3} \left(\frac{k}{d_1} \right)^{4/3} \\ &\leq \frac{3}{2^{2/3}} \left(\frac{7}{50} \right)^{1/3} \frac{1}{d^{1/3} k^{2/3}} \leq \frac{3}{2^{2/3}} \left(\frac{7}{50} \right)^{1/3} \frac{1}{d^{1/3} (\frac{1}{2}(19.74/1.5)^3 d)^{2/3}} < \frac{0.009}{d}, \end{aligned}$$

and

$$\frac{\delta_{\pm} d (p-1)^2}{k(p-1)^2} = \frac{(k \pm l)}{k} \frac{d}{d_1} \leq 1 + \frac{l}{k} < 1.009.$$

Hence from Theorem 5.1

$$\begin{aligned} M_{\pm}(k, l) &\leq (0.006 + 0.276) kl_{\pm} \Delta_{\pm}^{-1/3} (p-1)^2 + \max \left\{ 19.456 kl_{\pm} \Delta_{\pm}^{-1/3} (p-1)^2, 16.569 \cdot 1.009 k(p-1)^2 \right\} \\ &\leq 19.74 \max \left\{ kl_{\pm} \Delta_{\pm}^{-1/3} (p-1)^2, k(p-1)^2 \right\}. \end{aligned}$$

□

Finally, we need the following

Lemma 5.2. *With λ as in Theorem 1.1,*

$$|S_{\pm}(k, l)| \leq d^* + \lambda(d/d^*)^{5/8} p^{5/4}.$$

Moreover, if $-\bar{b}a$ is not a d^* power, then the term d^* may be removed.

Proof. We use the technique of Akulinichev [1] to average over the d^* -th roots of unity.

$$\begin{aligned} (p-1)S_{\pm}(k, l) &= \sum_{y=1}^{p-1} \sum_{x=1}^{p-1} e_p \left(a(xy^{\frac{p-1}{d^*}})^k + b(xy^{\frac{p-1}{d^*}})^{\pm l} \right) \\ &= \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} e_p \left((ax^k + bx^{\pm l})y^{\frac{l(p-1)}{d^*}} \right). \end{aligned}$$

If $ax^k + bx^{\pm l} \neq 0$ then the bound of Theorem 1.2 gives

$$\begin{aligned} \left| \sum_{y=1}^{p-1} e_p \left((ax^k + bx^{\pm l})y^{\frac{l(p-1)}{d^*}} \right) \right| &\leq \Phi \left(\frac{l(p-1)}{d^*} \right) = \Phi \left(\frac{d(p-1)}{d^*} \right) \\ &\leq \lambda (d/d^*)^{5/8} (p-1)^{5/8} p^{5/8}. \end{aligned}$$

If $-b\bar{a}$ is not a d^* -th power, then this bound hold for all nonzero x and so, $|S_{\pm}(k, l)| \leq \lambda (d/d^*)^{5/8} p^{5/4}$.

If $-b\bar{a}$ is a d^* -th power in \mathbb{Z}_p^* then we also have the d^* values of x with $ax^k + bx^{\pm l} = 0$, each contributing $p-1$ to the sum, and we obtain

$$(29) \quad |S_{\pm}(k, l) - d^*| \leq \frac{p-1-d^*}{p-1} \Phi \left(\frac{d(p-1)}{d^*} \right) < \lambda (d/d^*)^{5/8} p^{5/4}.$$

□

6. PROOF OF THEOREM 5.1

We follow the proof of Corollary 3.1 of [8]. For $\mathbf{u} = (u_1, u_2) \in \mathbb{Z}_p^{*2}$ define

$$C_{\pm}(\mathbf{u}) = \#\{x \in \mathbb{Z}_p^* : x^k - 1 = u_1 y^k, x^{\pm l} - 1 = u_2 y^{\pm l} \text{ for some } y \in \mathbb{Z}_p^*\}.$$

From (2.1) of [8] we have

$$(30) \quad M_{\pm}(k, l) \leq d^2(p-1)^2 + 2k^2 l_{\pm}(p-1) + d(p-1) \sum_{i=1}^N C_{\pm}^2(\mathbf{u}_i),$$

where $\mathbf{u}_1, \dots, \mathbf{u}_N$ represent the N distinct non-empty sets of x being counted as \mathbf{u} varies, ordered so that

$$(31) \quad C_{\pm}(\mathbf{u}_1) \geq C_{\pm}(\mathbf{u}_2) \geq \dots \geq C_{\pm}(\mathbf{u}_N) > 0.$$

Observe the trivial bounds (see (2.2) and §3 of [8])

$$(32) \quad \sum_{i=1}^N C_{\pm}(\mathbf{u}_i) \leq (p-1),$$

and

$$(33) \quad C_{\pm}(\mathbf{u}_i) \leq \min \left\{ \frac{(p-1)}{i}, (kl_{\pm}/d_1) \right\}.$$

We begin with a more precise version of Lemma 3.1 of [8]. Define

$$(34) \quad T = [T_1], \quad T_1 = \frac{5}{7} \left(\frac{2}{3} \right)^{7/2} \frac{(kl_{\pm}/d_1)^{3/2}}{\delta_{\pm}^3} (p-1).$$

Lemma 6.1. *For*

$$(35) \quad (k+l)^5 \delta_{\pm}^2 < 2.1 (kl_{\pm}/d_1)(p-1)^4 s$$

and $s \leq T$

$$\sum_{i \leq s} C_{\pm}(\mathbf{u}_i) \leq (2.1)^{1/10} \sqrt{15} \frac{(p-1)^{2/5} (kl_{\pm}/d_1)^{3/5}}{\delta_{\pm}^{1/5}} s^{3/5}.$$

Proof. We follow the proof of Lemma 3.1 of [8] but with an adjusted selection of parameters

$$(36) \quad C = D = [C_1], \quad C_1 = \left(\frac{9}{14}\right)^{1/5} \left(\frac{8}{9}\right)^{1/5} \left(\frac{5}{6}\right)^{1/5} \frac{(p-1)^{1/5} \delta_{\pm}^{2/5}}{(kl_{\pm}/d_1)^{1/5} s^{1/5}},$$

$$(37) \quad B = [B_1], \quad B_1 = \left(\frac{14}{9}\right)^{2/5} \left(\frac{9}{8}\right)^{2/5} \left(\frac{6}{5}\right)^{2/5} \frac{(kl_{\pm}/d_1)^{2/5} \delta_{\pm}^{1/5} s^{2/5}}{(p-1)^{2/5}},$$

$$(38) \quad A = [A_1], \quad A_1 = \frac{7}{3} \left(\frac{9}{14}\right)^{3/5} \left(\frac{8}{9}\right)^{3/5} \left(\frac{6}{5}\right)^{2/5} \frac{(p-1)^{3/5} \delta_{\pm}^{1/5} s^{2/5}}{(kl_{\pm}/d_1)^{3/5}}.$$

We leave the fractions unsimplified to show the dependence on (46). Analogous to restrictions (3.4) to (3.9) of [8] we require our choice to satisfy

$$(39) \quad A, B, C \geq 1,$$

$$(40) \quad C(k+l) \leq (p-1),$$

$$(41) \quad BC^2 \leq \delta_{\pm},$$

$$(42) \quad A\delta_{\pm} \leq (p-1),$$

$$(43) \quad D \left(C^2 + CD + \frac{1}{3} D^2 \right) s \leq ABC^2.$$

Since we have $(C+r)^2$ equations and

$$\sum_{r=0}^{D-1} (C+r)^2 = C^2 D + 2C \frac{1}{2} (D-1)D + \frac{1}{6} (D-1)D(2D-1) < D \left(C^2 + CD + \frac{1}{3} D^2 \right)$$

we may replace (3.9) by (43). Restriction (3.8) was not required for the construction (only simplification of the final algebra). The slightly weaker restriction (40) can replace (3.5).

From (32) and (33) we have the trivial bounds

$$(44) \quad \sum_{i=1}^s C_{\pm}(\mathbf{u}_i) \leq (kl_{\pm}/d_1)s,$$

and, applying Cauchy-Schwartz,

$$(45) \quad \sum_{i=1}^s C_{\pm}(\mathbf{u}_i) \leq (kl_{\pm}/d_1)^{1/2} \sum_{i=1}^s C_{\pm}(\mathbf{u}_i)^{1/2} \leq (kl_{\pm}/d_1)^{1/2} (p-1)^{1/2} s^{1/2}.$$

So from (32) we may certainly assume that

$$\frac{(p-1)^{3/5} \delta_{\pm}^{1/5}}{(kl_{\pm}/d_1)^{3/5}} > (2.1)^{1/10} \sqrt{15} s^{3/5} \Rightarrow A_1 > \sqrt{56}s > 7.48s,$$

from (44) that

$$\frac{(kl_{\pm}/d_1)^{2/5}\delta_{\pm}^{1/5}s^{2/5}}{(p-1)^{2/5}} > (2.1)^{1/10}\sqrt{15} \Rightarrow B_1 > 3\left(\frac{7}{2}\right)^{1/2} > 5.61,$$

and from (45) that

$$\frac{(p-1)^{1/5}\delta_{\pm}^{2/5}}{(kl_{\pm}/d_1)^{1/5}s^{1/5}} > (2.1)^{1/5}15 \Rightarrow C_1 > 15.$$

So $A \geq 8$, $B \geq 5$, $C \geq 15$ and (39) holds; moreover

$$(46) \quad C \geq \frac{15}{16}C_1, \quad B \geq \frac{5}{6}B_1, \quad A \leq \frac{9}{8}A_1.$$

Restriction (35) ensures (40):

$$C(k+l) \leq C_1(k+l) = (k+l) \left(\frac{10}{21}\right)^{1/5} \frac{\delta_{\pm}^{2/5}(p-1)^{1/5}}{(kl_{\pm}/d_1)^{1/5}s^{1/5}} \leq (p-1).$$

Since $BC^2 \leq B_1C_1^2 = \delta_{\pm}$ we plainly have (41).

For (42) observe that

$$A\delta_{\pm} \leq \frac{9}{8}A_1\delta_{\pm} = \frac{7}{3} \left(\frac{9}{14}\right)^{3/5} \left(\frac{9}{8}\right)^{2/5} \left(\frac{6}{5}\right)^{2/5} \frac{(p-1)^{3/5}\delta_{\pm}^{6/5}s^{2/5}}{(kl_{\pm}/d_1)^{3/5}} \leq (p-1),$$

as long as $s \leq T_1$.

Since $C = D$ restriction (43) amounts to $\frac{7}{3}Cs \leq AB$ and we have

$$\frac{7}{3} \frac{C}{B} s < \frac{7}{3} \frac{C_1}{(5B_1/6)} s = A_1 \leq A.$$

Hence as in Lemma 3.1 of [8] we can deduce that

$$\begin{aligned} \sum_{i=1}^s C_{\pm}(\mathbf{u}_i) &\leq \frac{A(kl_{\pm}/d_1) + (B-1)(p-1) + Ck + Cl}{D} \\ &\leq \frac{A(kl_{\pm}/d_1) + B(p-1)}{C} \\ &\leq \frac{\frac{9}{8}A_1(kl_{\pm}/d_1) + B_1(p-1)}{\frac{15}{16}C_1} \\ &= \frac{\left(\frac{9}{14}\right)^{3/5} \left(\frac{9}{8}\right)^{2/5} \left(\frac{6}{5}\right)^{2/5} \left(\frac{7}{3} + \frac{14}{9}\right) (p-1)^{2/5} (kl_{\pm}/d_1)^{3/5} s^{3/5}}{\frac{15}{16} \left(\frac{9}{14}\right)^{1/5} \left(\frac{8}{9}\right)^{1/5} \left(\frac{5}{6}\right)^{1/5} \delta_{\pm}^{1/5}} \\ &= 2.1^{3/5} \left(\frac{8}{3}\right) \frac{(p-1)^{2/5} (kl_{\pm}/d_1)^{3/5} s^{3/5}}{\delta_{\pm}^{1/5}}. \end{aligned}$$

Note that $2.1^{3/5} \left(\frac{8}{3}\right) = 4.1619\dots < 4.1712\dots = (2.1)^{1/10}\sqrt{15}$. □

Theorem 5.1 will follow at once from (30) and the following lemma:

Lemma 6.2. *For*

$$(47) \quad (k+l)^5\delta_{\pm}^2 < 2.1(kl_{\pm}/d_1)(p-1)^4$$

we have

$$\sum_{i \leq N} C_{\pm}(\mathbf{u}_i)^2 \leq \begin{cases} 27 \left(\frac{7}{50}\right)^{1/6} \frac{(kl_{\pm}/d_1)}{\delta_{\pm}^{1/3}} (p-1), & \text{if } (kl_{\pm}/d_1) \geq \frac{3}{2} \left(\frac{7}{50}\right)^{1/3} \delta_{\pm}^{4/3}, \\ \frac{\sqrt{7}}{50^{3/10}} \left(\frac{81}{4}\right) \delta_{\pm} (p-1), & \text{if } (kl_{\pm}/d_1) \leq \frac{3}{2} \left(\frac{7}{50}\right)^{1/3} \delta_{\pm}^{4/3}. \end{cases}$$

Proof. Setting

$$\mathcal{B} = (2.1)^{1/10} \sqrt{15} \frac{(p-1)^{2/5} (kl_{\pm}/d_1)^{3/5}}{\delta_{\pm}^{1/5}}$$

Lemma 6.1 implies that for any $1 \leq s \leq T$

$$(48) \quad \sum_{i \leq s} C_{\pm}(\mathbf{u}_i) \leq \mathcal{B} s^{3/5}.$$

So, putting

$$C_{\pm}(\mathbf{u}_i) = \frac{3}{5} \mathcal{B} i^{-2/5} + w_i, \quad W(s) = \sum_{i \leq s} w_i,$$

for $s \leq T$ we have, by (48) and Lemma 2.5,

$$(49) \quad W(s) = \sum_{i \leq s} C_{\pm}(\mathbf{u}_i) - \frac{3}{5} \mathcal{B} \sum_{i \leq s} i^{-2/5} \leq \mathcal{B} s^{3/5} - \frac{3}{5} \mathcal{B} \sum_{i \leq s} i^{-2/5} = \frac{3}{5} \gamma_{2/5}(s) \mathcal{B}.$$

Thus for any $J \geq 2$ with $J-1 \leq T$ we have

$$\begin{aligned} \sum_{i=1}^N C_{\pm}(\mathbf{u}_i)^2 &\leq \sum_{i < J} C_{\pm}(\mathbf{u}_i)^2 + C_{\pm}(\mathbf{u}_J) \sum_{i \geq J} C_{\pm}(\mathbf{u}_i) \\ &\leq \sum_{i < J} C_{\pm}(\mathbf{u}_i) (C_{\pm}(\mathbf{u}_i) - C_{\pm}(\mathbf{u}_J)) + C_{\pm}(\mathbf{u}_J)(p-1) \\ &= \sum_{i < J} \frac{3}{5} \mathcal{B} i^{-2/5} (C_{\pm}(\mathbf{u}_i) - C_{\pm}(\mathbf{u}_J)) + \sum_{i < J} w_i (C_{\pm}(\mathbf{u}_i) - C_{\pm}(\mathbf{u}_J)) + C_{\pm}(\mathbf{u}_J)(p-1) \\ &= M_1 + E_1 + E_2 + E_3, \end{aligned}$$

where

$$M_1 = \sum_{i < J} \frac{9}{25} \mathcal{B}^2 i^{-4/5} = \frac{9}{25} \mathcal{B}^2 \left(5(J-1)^{1/5} - \gamma_{4/5}(J-1) \right),$$

$$E_1 = \frac{3}{5} \mathcal{B} \sum_{i < J} w_i i^{-2/5},$$

$$E_2 = \sum_{i < J} w_i (C_{\pm}(\mathbf{u}_i) - C_{\pm}(\mathbf{u}_J)),$$

$$E_3 = C_{\pm}(\mathbf{u}_J) \left(p-1 - \sum_{i < J} \frac{3}{5} \mathcal{B} i^{-2/5} \right) = C_{\pm}(\mathbf{u}_J) \left(p-1 - \mathcal{B}(J-1)^{3/5} + \frac{3}{5} \mathcal{B} \gamma_{2/5}(J-1) \right).$$

By (49) we have

$$E_1 = \frac{3}{5} \mathcal{B} \left(\frac{W(J-1)}{(J-1)^{2/5}} + \sum_{1 \leq j \leq J-2} W(j) \left(\frac{1}{j^{2/5}} - \frac{1}{(j+1)^{2/5}} \right) \right) \leq \frac{9}{25} \mathcal{B}^2 \gamma_{2/5}(J-1).$$

By (49) and (31)

$$\begin{aligned} E_2 &= W(J-1)(C_{\pm}(\mathbf{u}_{J-1}) - C_{\pm}(\mathbf{u}_J)) + \sum_{1 \leq j \leq J-2} W(j)(C_{\pm}(\mathbf{u}_j) - C_{\pm}(\mathbf{u}_{j+1})) \\ &\leq \frac{3}{5} \mathcal{B} \gamma_{2/5}(J-1)(C_{\pm}(\mathbf{u}_1) - C_{\pm}(\mathbf{u}_J)). \end{aligned}$$

Observing from (48) that $C_{\pm}(\mathbf{u}_1) \leq \mathcal{B}$ we then get

$$E_2 \leq \frac{3}{5} \mathcal{B}^2 \gamma_{2/5}(J-1) - \frac{3}{5} \mathcal{B} \gamma_{2/5}(J-1) C_{\pm}(\mathbf{u}_J).$$

Hence, with $\kappa_1(J-1)$ as defined in (7),

$$\sum_{i=1}^N C_{\pm}(\mathbf{u}_i)^2 \leq \frac{9}{25} \mathcal{B}^2 \left(5(J-1)^{1/5} + \kappa_1(J-1) \right) + C_{\pm}(\mathbf{u}_J) \left(p-1 - \mathcal{B}(J-1)^{3/5} \right),$$

From Lemma 2.5 we have $\kappa_1(J-1) < -1.4$ for any $J \geq 2$, so for any $2 \leq J \leq T+1$

$$(50) \quad \sum_{i=1}^N C_{\pm}(\mathbf{u}_i)^2 \leq \frac{9}{5} \mathcal{B}^2 (J-1)^{1/5} - 0.504 \mathcal{B}^2 + C_{\pm}(\mathbf{u}_J) \left(p-1 - \mathcal{B}(J-1)^{3/5} \right),$$

where the 0.504 can be replaced by 0.8 when $J=2$ using $\kappa_1(1) = -20/9$. We note from (33) the trivial bounds

$$(51) \quad \sum_{i=1}^N C_{\pm}(\mathbf{u}_i)^2 \leq (p-1) \sum_{i=1}^N C_{\pm}(\mathbf{u}_i) \leq (p-1)^2,$$

and

$$(52) \quad \sum_{i=1}^N C_{\pm}(\mathbf{u}_i)^2 \leq (kl_{\pm}/d_1) \sum_{i=1}^N C_{\pm}(\mathbf{u}_i) \leq (kl_{\pm}/d_1)(p-1).$$

We consider two cases.

Case 1: Suppose first that $(kl_{\pm}/d_1) \geq \frac{3}{2} \left(\frac{7}{50} \right)^{1/3} \delta_{\pm}^{4/3}$. Equivalently

$$\left(\frac{p-1}{\mathcal{B}} \right)^{5/3} = \frac{1}{15} \left(\frac{50}{7} \right)^{1/6} \frac{\delta_{\pm}^{1/3}}{(kl_{\pm}/d_1)} (p-1) \leq \left(\frac{5}{7} \right) \left(\frac{2}{3} \right)^{7/2} \frac{(kl_{\pm}/d_1)^{3/2}}{\delta_{\pm}^3} (p-1) = T_1.$$

In this situation we take

$$J = \left\lceil \left(\frac{p-1}{\mathcal{B}} \right)^{5/3} \right\rceil.$$

If $J=1$ then $\frac{(kl_{\pm}/d_1)}{\delta_{\pm}^{1/3}} \geq \frac{1}{15} \left(\frac{50}{7} \right)^{1/6} (p-1)$ and the bound claimed is at least $\frac{9}{5}(p-1)^2$ and trivial. Hence we may assume that $2 \leq J \leq T+1$. By (48) we have $C_{\pm}(\mathbf{u}_J) \leq C_{\pm}(\mathbf{u}_{J-1}) \leq \mathcal{B}/(J-1)^{2/5}$ and, using that $x^{3/5} - ([x]-1)^{3/5} \leq \frac{3}{5}([x]-1)^{-2/5}$,

$$\begin{aligned} C_{\pm}(\mathbf{u}_J)((p-1) - \mathcal{B}(J-1)^{3/5}) &\leq \frac{\mathcal{B}^2}{(J-1)^{2/5}} \left(\left(\left(\frac{p-1}{\mathcal{B}} \right)^{5/3} \right)^{3/5} - (J-1)^{3/5} \right) \\ &\leq \frac{3}{5} \frac{\mathcal{B}^2}{(J-1)^{4/5}} \leq \begin{cases} 0.6\mathcal{B}^2 & \text{if } J=2, \\ 0.345\mathcal{B}^2 & \text{if } J \geq 3. \end{cases} \end{aligned}$$

Hence from (50)

$$\begin{aligned} \sum_{i=1}^N C_{\pm}(\mathbf{u}_i)^2 &\leq \frac{9}{5} \mathcal{B}^2 (J-1)^{1/5} \\ &\leq \frac{9}{5} \mathcal{B}^2 \left(\frac{p-1}{\mathcal{B}} \right)^{1/3} \\ &= 27 \left(\frac{7}{50} \right)^{1/6} \frac{(kl_{\pm}/d_1)}{\delta_{\pm}^{1/3}} (p-1). \end{aligned}$$

Case 2: Suppose now that $(kl_{\pm}/d_1) < \frac{3}{2} \left(\frac{7}{50} \right)^{1/6} \delta_{\pm}^{4/3}$ (that is $\left(\frac{p-1}{\mathcal{B}} \right)^{5/3} > T_1$).

From (52) we can assume that $(kl_{\pm}/d_1) > 16.568\delta_{\pm}$ and from (47) that $(kl/d_1)^{1/4}(p-1) > \left(\frac{10}{21} \right)^{1/4} (k+l)^{5/4} \delta_{\pm}^{1/2}$. So

$$\begin{aligned} T_1 &> 0.1728 \frac{(kl_{\pm}/d_1)^{3/2}}{\delta_{\pm}^3} (p-1) \geq 0.1728 (16.568)^{5/4} \frac{(kl_{\pm}/d_1)^{1/4}}{\delta_{\pm}^{7/4}} (p-1) \\ &\geq 0.1728 (16.568)^{5/4} \frac{(kl_{\pm}/d_1)^{1/4}}{((k+l)/d_1)^{5/4} \delta_{\pm}^{1/2}} (p-1) \\ &\geq 0.1728 (16.568)^{5/4} \left(\frac{10}{21} \right)^{1/4} d_1^{5/4} > 4.79d_1^{5/4}, \end{aligned}$$

and $T \geq 4$ and $T \geq \frac{4}{5}T_1$.

We take

$$J = T + 1,$$

where $T^{3/5} \leq T_1^{3/5} < (p-1)/\mathcal{B}$. Hence, with $C_{\pm}(\mathbf{u}_T) \leq \mathcal{B}/T^{2/5}$ from (48), (50) gives

$$\begin{aligned} \sum_{i=1}^N C_{\pm}(\mathbf{u}_i)^2 &< \frac{9}{5} \mathcal{B}^2 T^{1/5} - 0.504\mathcal{B}^2 + \frac{\mathcal{B}}{T^{2/5}} (p-1 - \mathcal{B}T^{3/5}) \\ &= \frac{9}{5} \frac{\mathcal{B}}{T^{2/5}} (p-1) - 0.504\mathcal{B}^2 - \frac{4}{5} \frac{\mathcal{B}}{T^{2/5}} (p-1 - \mathcal{B}T^{3/5}) \\ &< \frac{9}{5} \frac{\mathcal{B}}{T^{2/5}} (p-1) \\ &< \frac{9}{5} \frac{\mathcal{B}}{\left(\frac{4}{5}T_1 \right)^{2/5}} (p-1) = \frac{\sqrt{7}}{50^{3/10}} \left(\frac{81}{4} \right) \delta_{\pm} (p-1). \end{aligned}$$

□

7. DECIMATIONS AND A BOUND ON $M_{\pm}(k, l)$

Of independent interest and as a byproduct of the proof of Theorem 1.3 we also prove the following bound on $M_{\pm}(k, l)$:

Theorem 7.1. *Let $c = 0.59349$. If*

$$(53) \quad d^* = (k \mp l, p-1) < c^{-1} \left(\frac{p-1}{d} \right)^{16/23},$$

$$(54) \quad (k, p-1) < c^{-1} \left(\frac{p-1}{d} \right)^{16/23},$$

and

$$(55) \quad (l, p-1) < c \left(\frac{p-1}{d} \right)^{7/23},$$

then

$$M_{\pm}(k, l) \leq 27.57 d^{26/23} (p-1)^{66/23}.$$

The theorem has a direct application to a conjecture of Goresky and Klapper [13] on the decimation of ℓ -sequences.

Let $\mathbb{E} = \{2, 4, 6, \dots, p-1\}$ be the set of (non-zero) even residues in \mathbb{Z}_p and $\mathbb{O} = \{1, 3, 5, \dots, p-2\}$ the set of odd residues. If $(k, p-1) = 1$ and $p \nmid A$ then the mapping $x \rightarrow Ax^k$ is a permutation of \mathbb{Z}_p . Our interest is in determining when it is a permutation of \mathbb{E} . The conjecture is essentially equivalent to the following.

GK-conjecture: For $p > 13$, if the mapping $x \rightarrow Ax^k$ is a nontrivial permutation of \mathbb{Z}_p then there exists an $x \in \mathbb{E}$ such that $Ax^k \in \mathbb{O}$.

In [7] Bourgain, Paulhus and the authors established the conjecture for $p > 2.26 \cdot 10^{55}$. Here we obtain,

Corollary 7.1. *The GK-conjecture holds for $p > 4.92 \times 10^{34}$.*

Proof. By [7] Theorem 1 we know that the GK-conjecture holds as long as $M = M_+(k, 1) < 0.000823p^3$. If $d^* \leq 1.62p^{16/23}$ then ($d = 1$ and $(k, p-1) = 1$) by Theorem 7.1 we have $M \leq 27.57(p-1)^{66/23}$ and the conjecture holds for p larger than

$$\left(\frac{27.57}{0.000823} \right)^{23/3} \leq 4.92 \times 10^{34}.$$

If $p > 2.1 \times 10^7$ and $d^* > 1.62p^{16/23}$ then $d^* > 10\sqrt{p}$ and the result follows from Theorem 4b of [7]. \square

8. PROOF OF THEOREMS 1.3 AND 7.1

For Theorem 1.3 we need to show that

$$|S_{\pm}(k, l)| \leq d^* + 27.57^{1/4} d^{13/46} p^{89/92}$$

and for Theorem 7.1 that (subject to restrictions (53), (54), (55))

$$M_{\pm}(k, l) \leq 27.57 d^{26/23} (p-1)^{66/23}.$$

Observing the trivial bounds $|S_{\pm}(k, l)| \leq p$, and $M_{\pm}(k, l) \leq d(p-1)^3$ we may certainly assume that

$$(56) \quad p > 27.57^{23/3} d^{26/3}$$

for Theorem 1.3 and

$$(57) \quad p-1 > 27.57^{23/3} d$$

for Theorem 7.1.

Make a change of variables $x \rightarrow x^m$ with m chosen so that

$$(58) \quad mk \equiv \alpha \pmod{p-1}, \quad \pm ml \equiv \beta \pmod{p-1},$$

(plus sign for $S_+(k, l)$ or $M_+(k, l)$ and minus for $S_-(k, l)$ or $M_-(k, l)$) with

$$(59) \quad 0 \leq \alpha \leq \frac{1}{c} d^{7/23} (p-1)^{16/23}, \quad |\beta| \leq cd^{16/23} (p-1)^{7/23}, \quad c = 0.59349,$$

$(\alpha, \beta) \neq (0, 0)$. Such a pair (α, β) exists since the set of all (α, β) satisfying (58) is a lattice of volume $d(p-1)$ (or one can apply Dirichlet's box principle.) Set

$$\lambda = (\alpha, \beta, p-1), \quad \lambda_1 = (\alpha, \beta).$$

and

$$\beta' = \begin{cases} |\beta| & \text{if } \beta > 0, \\ 2|\beta| & \text{if } \beta < 0, \end{cases} \quad \frac{(\alpha - \beta)}{\lambda_1} = \begin{cases} \delta_+ & \text{if } \beta > 0, \\ \delta_- & \text{if } \beta < 0. \end{cases}$$

Suppose first that $\alpha, \beta \neq 0, \alpha \neq \beta$. We will establish that for the pair (α, β) we have

$$(60) \quad M(\alpha, \beta) \leq 27.57 d^{26/23} p^{66/23}.$$

From Lemma 1 of [7] we know that

$$M_{\pm}(k, l) \leq M(\alpha, \beta)$$

and Theorem 7.1 is clear.

Suppose that $(m, p-1) = \nu$ and write $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^m = \{w_1, \dots, w_{\nu}\}$ so that

$$(61) \quad S_{\pm}(k, l) = \frac{1}{\nu} \sum_{i=1}^{\nu} S_i(\alpha, \beta), \quad S_i(\alpha, \beta) = \sum_{x=1}^{p-1} e_p(aw_i^k x^{\alpha} + bw_i^{\pm l} x^{\beta}).$$

Since $\alpha, \beta \neq 0, \alpha \neq \beta$ the inner sum $S_i(\alpha, \beta)$ in (61) is a genuine binomial sum. Thus by (25) and (60)

$$|S_i(\alpha, \beta)| \leq 27.57^{1/4} d^{\frac{26}{23} \frac{1}{4}} p^{\frac{66}{23} \frac{1}{4}} p^{\frac{1}{4}} \leq 27.57^{1/4} d^{13/46} p^{89/92},$$

and $|S_{\pm}(k, l)| \leq 27.57^{1/4} d^{13/46} p^{89/92}$, proving Theorem 1.3.

We consider separately the three cases:

Case 1: $\alpha \leq 10000|\beta|$,

Case 2: $\alpha > 10000|\beta|$ and $(\alpha + |\beta|)^5 \delta_{\pm}^2 \geq 2.1 (\alpha\beta'/\lambda_1)(p-1)^4$,

Case 3: $\alpha > 10000|\beta|$ and $(\alpha + |\beta|)^5 \delta_{\pm}^2 \leq 2.1 (\alpha\beta'/\lambda_1)(p-1)^4$,

Case 1: From (26), (59) and (57) or (56)

$$\begin{aligned} M(\alpha, \beta) &\leq 3\alpha|\beta|(p-1)^2 \leq 30000|\beta|^2(p-1)^2 \leq 30000c^2 d^{32/23} (p-1)^{60/23} \\ &= \frac{30000c^2}{\left(\frac{p-1}{d}\right)^{6/23}} d^{26/23} (p-1)^{66/23} < \frac{30000c^2}{27.57^2} d^{26/23} (p-1)^{66/23} < 13.91 d^{26/23} (p-1)^{66/23}. \end{aligned}$$

In Cases 2 to 4 we have $\alpha > 10000|\beta|$ and

$$0.9999 \frac{\alpha}{\lambda_1} \leq \delta_+ \leq \frac{\alpha}{\lambda_1}, \quad \frac{\alpha}{\lambda_1} \leq \delta_- \leq 1.0001 \frac{\alpha}{\lambda_1}.$$

Case 2: In this case we have

$$\beta' \leq \frac{1}{2.1} \frac{(\alpha + |\beta|)^5 \lambda_1}{\alpha(p-1)^4} \delta_{\pm}^2 \leq \frac{1.0001^7}{2.1} \frac{\alpha^6}{(p-1)^4 \lambda_1},$$

and, using that $d \mid \lambda_1$,

$$\begin{aligned} M(\alpha, \beta) &\leq \frac{3}{2} \alpha \beta' (p-1)^2 \leq \frac{3}{2} \cdot \frac{1.0001^7}{2.1} \frac{\alpha^7}{d(p-1)^2} \\ &\leq \frac{3}{2} \cdot \frac{1.0001^7}{2.1 c^7} d^{26/23} (p-1)^{66/23} < 27.561 d^{26/23} (p-1)^{66/23}. \end{aligned}$$

Case 3: Here we can apply Theorem 5.1 to obtain

$$M(\alpha, \beta) \leq \lambda^2 (p-1)^2 + 2\alpha^2 \beta' (p-1) + (p-1)^2 \mu,$$

where

$$\mu \leq \max \left\{ 19.456 \frac{(\alpha \beta' / \lambda_1)}{\delta_{\pm}^{1/3}} \lambda, 16.569 \delta_{\pm} \lambda \right\}.$$

Since

$$\frac{\beta'}{\delta_{\pm}^{1/3}} \leq \frac{2|\beta|}{(\alpha/\lambda_1)^{1/3}},$$

and $\lambda \leq \lambda_1 \leq |\beta|$, we have

$$\begin{aligned} 19.456 \frac{(\alpha \beta' / \lambda_1)}{\delta_{\pm}^{1/3}} \lambda &\leq 19.456 \cdot 2\alpha^{2/3} |\beta| \frac{\lambda}{\lambda_1^{2/3}} \leq 19.456 \cdot 2\alpha^{2/3} |\beta|^{4/3} \\ &\leq 19.456 \cdot 2c^{2/3} d^{26/23} (p-1)^{20/23} < 27.4806 d^{26/23} (p-1)^{20/23}, \end{aligned}$$

while using (57)

$$\begin{aligned} 16.569 \delta_{\pm} \lambda &< 16.569 \cdot 1.0001 \alpha \leq 16.569 \cdot 1.0001 c^{-1} d^{7/23} (p-1)^{16/23} = 16.569 \cdot 1.0001 c^{-1} \frac{d^{3/23} (p-1)^{20/23}}{\left(\frac{p-1}{d}\right)^{4/23}} \\ &\leq 16.569 \cdot 1.0001 c^{-1} 27.57^{-4/3} d^{3/23} (p-1)^{20/23} < 0.34 d^{3/23} (p-1)^{20/23}. \end{aligned}$$

So $(p-1)^2 \mu \leq 27.4806 d^{26/23} (p-1)^{66/23}$.

From the lower bound (57)

$$\begin{aligned} \lambda^2 (p-1)^2 &\leq |\beta|^2 (p-1)^2 \leq c^2 d^{32/23} (p-1)^{60/23} = \frac{c^2}{\left(\frac{p-1}{d}\right)^{6/23}} d^{26/23} (p-1)^{66/23} \\ &\leq \frac{c^2}{27.57^2} d^{26/23} (p-1)^{66/23} < 0.00047 d^{26/23} (p-1)^{66/23}, \end{aligned}$$

and

$$\begin{aligned} 2\alpha^2 \beta' (p-1) &\leq 4\alpha^2 |\beta| (p-1) \leq \frac{4}{c} d^{30/23} (p-1)^{62/23} = \frac{4}{c \left(\frac{p-1}{d}\right)^{4/23}} d^{26/23} (p-1)^{66/23} \\ &< \frac{4}{c (27.57)^{4/3}} d^{26/23} (p-1)^{66/23} < 0.08093 d^{26/23} (p-1)^{66/23}. \end{aligned}$$

Hence

$$M(\alpha, \beta) < (27.4806 + 0.00047 + 0.08093) d^{26/23} (p-1)^{66/23} < 27.562 d^{26/23} (p-1)^{66/23}.$$

It remains to consider $\alpha = \beta$ or $\alpha = 0$ or $\beta = 0$.

If $\alpha = \beta$ then $mk \equiv \pm ml \pmod{p-1}$. So $\frac{(p-1)}{d^*} \mid m$ and $\frac{(p-1)}{d^*} \mid \beta$. In particular $\frac{(p-1)}{d^*} \leq |\beta| \leq cd^{16/23} (p-1)^{7/23}$ and $d^* \geq c^{-1} \left(\frac{p-1}{d}\right)^{16/23}$. This is ruled out in Theorem 7.1 by (53).

For Theorem 1.3 we use Lemma 5.2, with $d < (27.57)^{-23/26} p^{3/26}$ from (56), to get

$$\begin{aligned}
|S_{\pm}(k, l)| &\leq d^* + 1.52 \left(\frac{d}{d^*} \right)^{5/8} p^{5/4} \\
&\leq d^* + 1.52 c^{5/8} (1 - p^{-1})^{-10/23} d^{195/184} p^{75/92} \\
&< d^* + 1.1 d^{13/46} d^{143/184} p^{75/92} \\
&\leq d^* + 1.1 d^{13/46} \left(\frac{p^{3/26}}{27.57^{23/26}} \right)^{143/184} p^{75/92} \\
&= d^* + \frac{1.1}{(27.57)^{11/16}} d^{13/46} p^{333/368} \\
&< d^* + 0.12 d^{13/46} p^{89/92-1/16}.
\end{aligned}$$

If $\alpha = 0$ then $(p-1) | mk$. Hence $\frac{(p-1)}{(p-1, k)} | m$ and $\frac{(p-1)}{(p-1, k)} \leq |\beta| \leq cd^{16/23} (p-1)^{7/23}$, and so $(p-1, k) \geq c^{-1} \left(\frac{p-1}{d} \right)^{16/23}$. This is ruled out in Theorem 7.1 by (54). For Theorem 1.3 we have by the Weil bound for exponential sums,

$$\begin{aligned}
|S_{\pm}(k, l)| &\leq |\beta| \sqrt{p} \leq cd^{16/23} p^{37/46} = cd^{13/46} (d/p^{3/26})^{19/46} p^{1019/1196} \\
&\leq \frac{c}{27.57^{19/52}} d^{13/46} p^{1019/1196} < 0.18 d^{13/46} p^{89/92-3/26}.
\end{aligned}$$

Similarly if $\beta = 0$ then $(p-1) | ml$. So $\frac{(p-1)}{(p-1, l)} | m$ and $\frac{(p-1)}{(p-1, l)} | \alpha$, and so $\frac{(p-1)}{(p-1, l)} \leq \alpha \leq c^{-1} d^{7/23} (p-1)^{16/23}$. Hence $(p-1, l) \geq c \left(\frac{p-1}{d} \right)^{7/23}$; again ruled out in Theorem 7.1 by (55). For Theorem 1.3 we have, from Theorem 4.1 with $\lambda = 1.51967\dots$,

$$\begin{aligned}
|S_{\pm}(k, l)| &\leq p \left(\frac{d}{(l, p-1)} \right)^{1/2} + 1.36 d^{15/88} p^{21/22} \\
&\leq \frac{1}{c^{1/2} (1-1/p)^{7/46}} d^{15/23} p^{39/46} + 1.36 d^{15/88} p^{21/22} \leq 1.30 d^{15/23} p^{39/46} + 1.36 d^{15/88} p^{21/22} \\
&= d^{13/46} p^{89/92} \left(1.30 \frac{(d/p^{3/26})^{17/46}}{p^{1/13}} + \frac{1.36}{p^{13/1012}} \right) \\
&\leq d^{13/46} p^{89/92} \left(1.30 \frac{(27.57)^{-17/52}}{(27.57)^{23/39}} + \frac{1.36}{(27.57)^{13/132}} \right) < 1.02 d^{13/46} p^{89/92}.
\end{aligned}$$

REFERENCES

- [1] N. M. Akulnitscev, *Bounds for rational trigonometric sums of a special type*, (Russian) Dokl. Akad. Nauk SSSR 161 (1965), 743-745.
- [2] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc. 18, no. 2 (2005), 477-499.
- [3] J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, Geom. funct. anal. 18 (2009), 1477-1502.
- [4] J. Bourgain and M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields.*, Math. Proc. Cambridge Philos. Soc. 146 (2009), no. 1, 1-21.
- [5] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) 73 (2006), no. 2, 380-398.
- [6] J. Bourgain and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C. R. Math. Acad. Sci. Paris 337 (2003), no. 2, 75-80.

- [7] J. Bourgain, T. Cochrane, J. Paulhus and C. Pinner, *Decimations of L -sequences and permutations of even residues mod p* , SIAM J. of Discrete Math. 23 (2009), no. 2, 842-857.
- [8] T. Cochrane and C. Pinner, *Stepanov's method applied to binomial exponential sums*, Quart. J. Math. 54 (2003), 243-255.
- [9] ———, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. 133 (2005), no. 2, 313-320.
- [10] ———, *Bounds on fewnomial exponential sums over \mathbb{Z}_p^** , preprint (2009).
- [11] ———, *Exponential sums over subgroups of \mathbb{Z}_p^** , preprint (2009).
- [12] A. Garcia and J.F. Voloch, *Fermat curves over finite fields*, J. Number Theory 30 (1988), 345-356.
- [13] M. Goresky, A. Klapper, *Arithmetic cross-correlations of FCSR sequences*, IEEE Trans. Inform. Theory, 43 (1997), 1342-1346.
- [14] D.R. Heath-Brown and S.V. Konyagin, *New bounds for Gauss sums derived from k th powers, and for Heilbronn's exponential sum*, Q. J. Math. 51 (2000), no. 2, 221-235.
- [15] S.V. Konyagin, *Estimates for trigonometric sums over subgroups and for Gauss sums*. (Russian) IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part III (Russian) (Tula, 2001), 86-114, Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002.
- [16] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.
- [17] S. Mattarei, *On a bound of Garcia and Voloch for the number of points of a Fermat Curve over a prime field*, Finite Fields and Applications 13, no. 4, (2007), 773-777.
- [18] O. Moreno and F.N. Castro, *On the calculation and estimation of Waring number for finite fields*, Séminaires et Congrès 11 (2005), 29-40.
- [19] A. Weil, *Number of solutions of equations in finite fields*, Bull. AMS 55 (1949), 497-508.
- [20] Hong Bing Yu, *Estimates for complete exponential sums of special types*, Math. Proc. Cambridge Philos. Soc. 131 (2001), no. 2, 321-326.

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`