A NOTE ON SIMULTANEOUS CONGRUENCES, II: MORDELL REVISED

TREVOR D. WOOLEY*

Abstract. When p is a prime number, and $k_1,\ldots,k_t$ are natural numbers with $1\leqslant k_1<k_2<\cdots<k_t<p$, we show that the simultaneous congruences $\sum_1^t x_i^{k_j}\equiv \sum_1^t y_i^{k_j}\pmod{p}$ $(1\leqslant j\leqslant t)$, possess at most $k_1\ldots k_tp^t$ solutions with $1\leqslant x_i,y_i\leqslant p$ $(1\leqslant i\leqslant t)$. Analogous conclusions are provided when one or more of the exponents k_i are negative.

1. Introduction

In a paper devoted to generalisations of Gauss sums published in 1932, Mordell [11] obtained upper bounds for exponential sums over finite fields through estimates for their mean values. Although eclipsed by Weil's resolution of the Riemann Hypothesis for curves over finite fields (see [13]), Mordell's approach motivates Vinogradov's use [12] of mean values in estimating Weyl sums and their generalisations, and as such leaves an indelible mark on the literature. Weil's estimates are worse than trivial when the degree of the exponential sum is large compared to the associated prime modulus, and in recent years much effort has been expended on deriving estimates that remain nontrivial for larger degrees (see [1], [2], [4], [5], [6], [7], [10], and [16]). The bulk of this work revisits Mordell's original approach, and is based on an estimate for the number of solutions of certain polynomial congruences equivalent to a mean value estimate (see [11], equation (16)). Mordell's proof of this estimate involves notions of independent parameters and unstated elements of elimination theory that are vestiges of a bygone era prior to the development of modern algebraic geometry. As such, the mathematical reader of today will likely demand some renovation of this proof going beyond a lick of paint to a certain amount of structural reinforcement. Our object in this note is to address the latter concerns, at the same time providing an estimate sharper than that due to Mordell that is, in many respects, best possible. Improved estimates for certain associated exponential sums are immediate corollaries of our sharper bounds.

Before announcing our conclusions, we must introduce some notation. When q is a power of a prime number p, we denote by $\mathbb{F}_q$ the finite field having q elements. Let t be a natural number, and suppose that $k_1,\ldots,k_t$ are positive integers. We write $N_t(q;\mathbf{k})$ for the number of solutions of the system of

2010 *Mathematics Subject Classification.* 11D79, 11L15.

Key words and phrases. Congruences in many variables, exponential sums.

*The author is supported by a Royal Society Wolfson Research Merit Award.

equations

$$x_1^{k_j}+\dots+x_t^{k_j}=x_{t+1}^{k_j}+\dots+x_{2t}^{k_j}\quad (1\leqslant j\leqslant t),\tag{1.1}$$

with $\mathbf{x}\in\mathbb{F}_q^{2t}$. In view of the relation $a^q=a$, valid for each element a of $\mathbb{F}_q$, it is apparent that there is no loss of generality in supposing that

$$1\leqslant k_1<k_2<\dots<k_t<q.\tag{1.2}$$

Furthermore, since the characteristic of $\mathbb{F}_q$ is p, for each natural number l one has

$$(x_1^l+x_2^l+\dots+x_t^l)^p=x_1^{lp}+x_2^{lp}+\dots+x_t^{lp}.$$

Thus we see that there is in addition no loss of generality in restricting attention to systems (1.1) for which $p\nmid k_j$ $(1\leqslant j\leqslant t)$.

Theorem 1.1. *Suppose that $k_1,\dots,k_t$ are integers with $p\nmid k_j$ $(1\leqslant j\leqslant t)$, and satisfying the condition* (1.2)*. Then one has*

$$N_t(q;\mathbf{k})\leqslant k_1k_2\dots k_tq^t.\tag{1.3}$$

In the situation in which q is a prime number, the estimate (16) of Mordell [11] supplies the bound

$$N_t(q;\mathbf{k})\leqslant\frac{(2t)!}{(t!)^2}k_1k_2\dots k_tq^t.$$

Under the same circumstances, Cochrane and Pinner (see Lemma 3.1 of [6]) provide an estimate analogous to this upper bound of Mordell, save that the right hand side is multiplied by a factor $4/t^2$. Their proof avoids Mordell's result, instead applying a version of Bézout's theorem for non-singular solutions of polynomial congruences due to the author [15], and as such provides a robust proof of Mordell's estimate. The conclusion of Theorem 1.1 is superior to both the estimates of Mordell and of Cochrane and Pinner. Moreover, as is apparent from the discussion of Example 3.1 of [6], when k is a fixed natural number with $k|(q-1)$, and $k_i=ik$ $(1\leqslant i\leqslant t)$, one has the lower bound

$$N_t(q;\mathbf{k})\geqslant k_1k_2\dots k_t(q^t+O_t(q^{t-1})),$$

and thus the inequality (1.3) is asymptotically sharp. In some sense, therefore, the conclusion of Theorem 1.1 is best possible. We should note in this context that in the special case in which $t=2$ and q is a prime number, the conclusion of Theorem 1.1 is derived in Lemma 7 of [14], and is also recorded rather later in Lemma 3.2 of [6].

Consider next the situation analogous to that described in the preamble to Theorem 1.1 in which the exponents $k_1,\dots,k_t$ are now non-zero integers, but potentially not all of the same sign. In this situation, we define $M_t(q;\mathbf{k})$ to be the number of solutions of the system of equations (1.1) with $\mathbf{x}\in(\mathbb{F}_q^\times)^{2t}$. Here, we may suppose without loss that

$$-q<k_1<k_2<\dots<k_t<q,\tag{1.4}$$

that $p\nmid k_j$ $(1\leqslant j\leqslant t)$, and further that

$$(q-1)\nmid(k_i-k_j)\qquad(1\leqslant i<j\leqslant t).\tag{1.5}$$

Finally, it is convenient to put

$$l_i = \begin{cases} k_i, & \text{when } k_i > 0, \\ t|k_i|, & \text{when } k_i < 0, \end{cases}$$

and

$$m_i = \begin{cases} k_i, & \text{when } k_i > 0, \\ (2t-1)|k_i|, & \text{when } k_i < 0. \end{cases}$$

Theorem 1.2. *Suppose that $k_1, \dots, k_t$ are integers with $p \nmid k_j$ $(1 \leqslant j \leqslant t)$, and satisfying the conditions* (1.4) *and* (1.5)*. Then one has the estimates*

$$M_t(q;\mathbf{k}) \leqslant m_1 m_2 \dots m_t (q-1)^t,$$
$$M_t(q;\mathbf{k}) \leqslant 2^{2t} |k_1 k_2 \dots k_t| (q-1)^t,$$
$$M_t(q;\mathbf{k}) \leqslant (t+1) l_1 l_2 \dots l_t (q-1)^t.$$

By way of comparison, when q is a prime number, the estimate (16) of Mordell [11] essentially provides the bound

$$M_t(q;\mathbf{k}) \leqslant \frac{(2t)!}{(t!)^2} l_1 \dots l_t (q-1)^t. \tag{1.6}$$

One may verify that the third estimate of Theorem 1.2 is superior to (1.6) for every natural number t exceeding 1. Moreover, the second estimate of Theorem 1.2 will be superior to the third whenever $t > 2$, and the number of the exponents k_i that are negative is more than about $(2\log 2)t/\log t$. We should also remark that Lemma 3.2 of Cochrane and Pinner [6] establishes an estimate matching the first provided by Theorem 1.2 in those special cases wherein $t = 2$ and q is prime.

We finish by recording some consequences of Theorems 1.1 and 1.2 for exponential sums. Let χ be a Dirichlet character modulo p, and write $e_p(z)$ for $e^{2\pi i z/p}$. Then, when $\mathbf{a} \in (\mathbb{F}_p^\times)^t$, we define the Laurent polynomial $f(x) = a_1 x^{k_1} + \dots + a_t x^{k_t}$, and also the mixed exponential sum

$$S(\chi, f) = \sum_{x \in \mathbb{F}_p^\times} \chi(x) e_p(f(x)).$$

Corollary 1.3. *When $k_1, \dots k_t$ are non-zero integers with $p \nmid k_j$ $(1 \leqslant j \leqslant t)$, and satisfying $1 \leqslant k_1 < k_2 < \dots < k_t < p$, one has*

$$|S(\chi, f)| \leqslant (k_1 \dots k_t)^{1/t^2} p^{1-1/(2t)}. \tag{1.7}$$

Meanwhile, when instead $-p < k_1 < k_2 < \dots < k_t < p$ and $p \nmid (k_i - k_j)$ for $1 \leqslant i < j \leqslant t$, then one has the estimates

$$|S(\chi, f)| \leqslant (m_1 m_2 \dots m_t)^{1/t^2} p^{1-1/(2t)},$$
$$|S(\chi, f)| \leqslant 2^{2/t} |k_1 \dots k_t|^{1/t^2} p^{1-1/(2t)}, \tag{1.8}$$
$$|S(\chi, f)| \leqslant (t+1)^{1/t^2} (l_1 \dots l_t)^{1/t^2} p^{1-1/(2t)}. \tag{1.9}$$

For comparison, Theorem 1.1 of Cochrane and Pinner [6] provides the bound

$$|S(\chi, f)| \leqslant 2^{2/t}(l_1 \dots l_t)^{1/t^2} p^{1-1/(2t)}. \tag{1.10}$$

This is weaker than the estimate (1.9) in all cases, since $t + 1 < 4^t$ for every natural number t. It is also weaker than (1.8) whenever there is a change of sign amongst the k_i. Finally, in circumstances wherein the k_i are all of the same sign, the estimate (1.7) yields bounds superior to those of (1.10) by a factor $2^{2/t}$. See [4] and [5] for refinements in special cases that may prove superior to the estimates of Corollary 1.3.

Although the conclusion of Theorem 1.1 is, in some sense, best possible, it is not apparent what the truth may be for the analogous situation examined in Theorem 1.2, in which the exponents are of mixed sign. Let w be a natural number, put $t = 2w$, and write

$$\mathbf{a} = (-w, 1 - w, \dots, -2, -1, 1, 2, \dots, w - 1, w).$$

Then by considering solutions $\mathbf{x}$ of (1.1) in which $(x_1^k, \dots, x_{2w}^k)$ is a permutation of $(x_{2w+1}^k, \dots, x_{4w}^k)$, one finds that when q is large and $k|(q - 1)$, one has

$$M_{2w}(q; k\mathbf{a}) \geqslant (2w)!k^{2w}(q - 1)^{2w} + O_{k,w}(q^{2w-1}).$$

Consequently, the bound

$$M_t(q; \mathbf{k}) \leqslant C_t|k_1 \dots k_t|(q - 1)^t$$

cannot hold in general when $C_t < \binom{t}{[t/2]}$.

The author is grateful to the referee for useful comments.

2. Counting solutions of equations in finite fields

In this section we bound $N_t(q; \mathbf{k})$ and $M_t(q; \mathbf{k})$ by making use of rough data available from modern versions of Bézout's theorem, in combination with crude but robust estimates for the number of $\mathbb{F}_q$-rational points on algebraic varieties made available only relatively recently. We begin with a direct consequence of Bézout's theorem. In this context, we write $\deg(W)$ for the degree of a variety W, and $\overline{\mathbb{F}}_q$ for the algebraic closure of $\mathbb{F}_q$.

Lemma 2.1. *Suppose that $f_i(\mathbf{x}) \in \overline{\mathbb{F}}_q[x_1, \dots, x_s]$ is a polynomial of degree d_i for $1 \leqslant i \leqslant t$. Let $V_1, \dots, V_h \subset \mathbb{A}^s$ be the components of the complete intersection defined by the system of equations $f_i(\mathbf{x}) = 0$ $(1 \leqslant i \leqslant t)$. Then*

$$\sum_{i=1}^{h} \deg(V_i) \leqslant d_1 d_2 \dots d_t.$$

Proof. Let Y be a variety in $\mathbb{P}^n$, and let H be a hypersurface not containing Y. Also, let $Z_1, \dots, Z_m$ be the irreducible components of $Y \cap H$, and let $i(Y, H; Z_j)$ denote the intersection multiplicity of the varieties Y and H along Z_j. Then according to Theorem 7.7 of Chapter 1 of Harsthorne [8], one has

$$\sum_{j=1}^{m} i(Y, H; Z_j) \deg Z_j = (\deg Y)(\deg H).$$

But $i(Y,H;Z_j)\geqslant 1$ for each j, and so it follows by induction that for the complete intersection defined by the t polynomials in question, one has

$$\sum_{i=1}^h \deg(V_i)\leqslant \prod_{i=1}^t \deg(f_i)=d_1d_2\dots d_t.$$

□

Next we provide an upper bound for the number of $\mathbb{F}_q$-rational points on a variety of given degree and dimension.

Lemma 2.2. *Let $V\subset \mathbb{A}^s$ be an $\mathbb{F}_q$-variety of dimension $r\geqslant 0$ and degree δ. Then one has*

$$\mathrm{card}(V\cap \mathbb{F}_q^s)\leqslant \delta q^r,$$

and also

$$\mathrm{card}(V\cap (\mathbb{F}_q^\times)^s)\leqslant \delta (q-1)^r.$$

Proof. The first estimate is supplied by Lemma 2.1 of Cafure and Matera [3]. The second estimate may be established using an immediate modification of the argument of the proof of the latter lemma. For when $1\leqslant i\leqslant s$, we may take $W_i\subset \mathbb{A}^s$ to be the $\mathbb{F}_q$-hypersurface defined by $x_i^{q-1}-1$. Then we have $V\cap (\mathbb{F}_q^\times)^s=V\cap W_1\cap\dots\cap W_s$, and so from the argument underlying the proof of Proposition 2.3 of [9], we obtain the inequality

$$\mathrm{card}(V\cap (\mathbb{F}_q^\times)^s)\leqslant \deg(V\cap W_1\cap\dots\cap W_s)\leqslant \delta(q-1)^r.$$

This completes the proof of the lemma. □

By combining Lemmata 2.1 and 2.2, we obtain an estimate for the number of $\mathbb{F}_q$-rational points on a complete intersection.

Lemma 2.3. *Suppose that $f_i(\mathbf{x})\in \overline{\mathbb{F}}_q[x_1,\dots,x_s]$ is a polynomial of degree d_i for $1\leqslant i\leqslant t$. Let $V_1,\dots,V_n$ be the components in $\overline{\mathbb{F}}_q^s$ of the complete intersection V defined by the system of equations $f_i(\mathbf{x})=0$ $(1\leqslant i\leqslant t)$, and denote by U_r the union of the components $V_1,\dots,V_n$ having dimension not exceeding r. Then*

$$\mathrm{card}(U_r\cap \mathbb{F}_q^s)\leqslant d_1d_2\dots d_tq^r.$$

In the analogous situation wherein we consider the complete intersection in $(\overline{\mathbb{F}}_q^\times)^s$, one has instead

$$\mathrm{card}(U_r\cap (\mathbb{F}_q^\times)^s)\leqslant d_1d_2\dots d_t(q-1)^r.$$

Proof. Suppose that $V_{i_1},\dots,V_{i_l}$ are the components of V having dimension not exceeding r. Then U_r is the union of $V_{i_1},\dots,V_{i_l}$, so by first applying Lemma 2.2, and then Lemma 2.1, we obtain

$$\mathrm{card}(U_r\cap \mathbb{F}_q^s)\leqslant \sum_{j=1}^l \deg(V_{i_j})q^r\leqslant q^r\sum_{i=1}^n \deg(V_i)\leqslant d_1d_2\dots d_tq^r.$$

The second conclusion of the lemma follows in like manner. □

In order to discuss the singular locus of the complete intersection (1.1), we require a lemma concerning the rank of matrices of Vandermonde type. Suppose that $k_1,\dots,k_t$ are distinct integers, and that s is a natural number with $s\geqslant t$. When $i_1,\dots,i_t$ are natural numbers with $1\leqslant i_1<i_2<\dots<i_t\leqslant s$, we define the determinant

$$\Delta_{\mathbf{i}}(\mathbf{x};\mathbf{k})=\det(x_{i_l}^{k_j-1})_{1\leqslant j,l\leqslant t}.$$

Also, when $k_i>0$ $(1\leqslant i\leqslant t)$, we define $\mathfrak{X}_s(\mathbf{k})$ to be the set of points $\mathbf{x}\in\overline{\mathbb{F}}_q^s$ satisfying the system of equations

$$\Delta_{\mathbf{i}}(\mathbf{x};\mathbf{k})=0\quad(1\leqslant i_1<i_2<\dots<i_t\leqslant s).\tag{2.1}$$

Likewise, without condition on $\mathbf{k}$, we define $\mathfrak{Y}_s(\mathbf{k})$ to be the set of points $\mathbf{x}\in(\overline{\mathbb{F}}_q^\times)^s$ satisfying the system of equations (2.1).

Lemma 2.4. *(i) Suppose that $k_1,\dots,k_t$ are integers with $1\leqslant k_1<\dots<k_t<q$, and that $s\geqslant t$. Then the components of the complete intersection $\mathfrak{X}_s(\mathbf{k})$ have dimension at most $t-1$;*

(ii) Suppose that $k_1,\dots,k_t$ are integers with $-q<k_1<\dots<k_t<q$, and further that $(q-1)|(k_i-k_j)$ for no indices i and j with $1\leqslant i<j\leqslant t$. Then for $s\geqslant t$, the components of the complete intersection $\mathfrak{Y}_s(\mathbf{k})$ have dimension at most $t-1$.

Proof. The proof of part (ii) of the lemma may be applied, mutatis mutandis, to establish part (i); all that is required is to include 0 as a possible value of each coordinate. We therefore consider only part (ii), and assume the hypotheses ambient in that part of the lemma.

Consider the subset $\mathfrak{Y}_s(\mathbf{k})\subset(\overline{\mathbb{F}}_q^\times)^s$ defined by the vanishing of all the $(t\times t)$-determinants (2.1). The elements $\mathbf{x}$ of $\mathfrak{Y}_s(\mathbf{k})$ may be classified according to the dimension of the linear space spanned by the column vectors $(x_i^{k_j-1})_{1\leqslant j\leqslant t}$ for $1\leqslant i\leqslant s$. This space must have affine dimension at most $t-1$ for every element $\mathbf{x}$ of $\mathfrak{Y}_s(\mathbf{k})$, for if the dimension were larger, then one could find a non-vanishing $(t\times t)$-determinant $\Delta_{\mathbf{i}}(\mathbf{x};\mathbf{k})$, contradicting the definition of $\mathfrak{Y}_s(\mathbf{k})$.

Let m be an integer with $1\leqslant m\leqslant t-1$, consider indices i_l $(1\leqslant l\leqslant m)$ with

$$1\leqslant i_1<i_2<\dots<i_m\leqslant s,\tag{2.2}$$

and suppose that the column vectors $(x_{i_l}^{k_j-1})_{1\leqslant j\leqslant t}$ are linearly independent for $1\leqslant l\leqslant m$. Write $\mathfrak{T}_m(\mathbf{i})$ for the set of points $\mathbf{x}\in\mathfrak{Y}_s(\mathbf{k})$ satisfying the property that for $1\leqslant i\leqslant s$, all of the column vectors $(x_i^{k_j-1})_{1\leqslant j\leqslant t}$ belong to the linear space spanned by vectors of the above type, and let $\mathfrak{Y}_s^{(m)}(\mathbf{k})$ denote the union of the sets $\mathfrak{T}_m(\mathbf{i})$ over all choices of $\mathbf{i}$ satisfying (2.2). Then one finds that $\mathfrak{Y}_s(\mathbf{k})$ is the union of $\mathfrak{Y}_s^{(1)}(\mathbf{k}),\mathfrak{Y}_s^{(2)}(\mathbf{k}),\dots,\mathfrak{Y}_s^{(t-1)}(\mathbf{k})$. Moreover, for $1\leqslant m\leqslant t-1$, the set $\mathfrak{T}_m(\mathbf{i})$ is determined by the non-vanishing of at least one $(m\times m)$-determinant involving the variables $x_{i_1},\dots,x_{i_m}$, together with the vanishing of all $((m+1)\times(m+1))$-determinants obtained by adjoining another variable

x_i with $i \notin \{i_1, \dots, i_m\}$. The determinants in question here are of submatrices of the matrix

$$(x_i^{k_j-1})_{\substack{1\leqslant j\leqslant t \\ 1\leqslant i\leqslant s}}.$$

It follows that each x_i with $i \notin \{i_1, \dots, i_m\}$ satisfies a non-trivial polynomial equation determined by $x_{i_1}, \dots, x_{i_m}$. We therefore deduce that the components of $\mathfrak{Y}_s^{(m)}(\mathbf{k})$ have affine dimension at most m, whence the components of $\mathfrak{Y}_s(\mathbf{k})$ have affine dimension at most $t-1$. This completes the proof of the lemma. □

We are now equipped to establish the principal conclusions of this note.

The proof of Theorem 1.1. Suppose that $k_1, \dots, k_t$ are natural numbers with $1 \leqslant k_1 < k_2 < \dots < k_t$. Recall from the discussion in the preamble to the statement of Theorem 1.1 that we may suppose, without loss of generality, that $k_t < q$ and $p \nmid k_i$ $(1 \leqslant i \leqslant t)$. Consider the complete intersection $\mathcal{Z}$ defined by the simultaneous equations (1.1) with $\mathbf{x} \in \overline{\mathbb{F}}_q^{2t}$. Note that $\mathcal{Z}$ is defined by a system of t polynomial equations, of respective degrees $k_1, \dots, k_t$, in $2t$ variables. Let $\mathcal{Z}_1, \dots, \mathcal{Z}_d$ be the distinct components of $\mathcal{Z}$. We claim that the affine dimension of each component $\mathcal{Z}_i$ is at most t. If such were not the case for the component $\mathcal{Z}_i$, then the intersection (1.1) must be improper, and $\mathcal{Z}_i$ must belong to the singular locus of $\mathcal{Z}$. The latter is contained within the set of points $\mathbf{x} \in \overline{\mathbb{F}}_q^{2t}$ satisfying the simultaneous equations

$$\det(k_j x_{i_l}^{k_j-1})_{1\leqslant j,l\leqslant t} = 0,$$

with $1 \leqslant i_1 < i_2 < \dots < i_t \leqslant 2t$. Since $p \nmid k_j$ $(1 \leqslant j \leqslant t)$, it follows that this singular locus is contained in the set $\mathfrak{X}_{2t}(\mathbf{k})$ defined in the preamble to Lemma 2.4. It therefore follows from Lemma 2.4(i) that the component $\mathcal{Z}_i$ in question must have dimension at most $t-1$, contradicting our earlier hypothesis.

We have shown that the components $\mathcal{Z}_1, \dots, \mathcal{Z}_d$ of $\mathcal{Z}$ each have dimension at most t, and so we may infer from Lemma 2.3 that

$$N_t(q; \mathbf{k}) = \operatorname{card}(\mathcal{Z} \cap \mathbb{F}_q^{2t}) \leqslant k_1 k_2 \dots k_t q^t.$$

This completes the proof of Theorem 1.1. □

The proof of Theorem 1.2. Suppose now that $k_1, \dots, k_t$ are non-zero integers with $-q < k_1 < k_2 < \dots < k_t < q$ for which $(q-1) \nmid (k_i - k_j)$ for $1 \leqslant i < j \leqslant t$. There is again no loss of generality in supposing that $p \nmid k_i$ $(1 \leqslant i \leqslant t)$. We suppose that $k_i < 0$ for $1 \leqslant i \leqslant u$ and $k_i > 0$ for $u+1 \leqslant i \leqslant t$. Here, there is no loss of generality in supposing that $u \geqslant 1$ and $t > u$, for otherwise the conclusion of Theorem 1.1 delivers the desired estimate, if necessary by replacing x_i by x_i^{-1} for $1 \leqslant i \leqslant 2t$. It is convenient for the purpose of concision to introduce the notational device of writing

$$\check{x}_i = \prod_{\substack{1\leqslant l\leqslant 2t \\ l\neq i}} x_l \quad (1 \leqslant i \leqslant 2t).$$

In addition, we write κ_j for $-k_j$. Then by clearing denominators, it is apparent that $M_t(q;\mathbf{k})$ counts the number of solutions of the system

$$\sum_{i=1}^{t} \breve{x}_i^{\kappa_j} = \sum_{i=t+1}^{2t} \breve{x}_i^{\kappa_j} \quad (1 \leqslant j \leqslant u), \tag{2.3}$$

$$\sum_{i=1}^{t} x_i^{k_j} = \sum_{i=t+1}^{2t} x_i^{k_j} \quad (u+1 \leqslant j \leqslant t), \tag{2.4}$$

with $\mathbf{x} \in (\mathbb{F}_q^\times)^{2t}$. Notice here that, in view of the definition of $\breve{x}_i$, the degree of the jth equation in (2.3) is $(2t-1)|k_j| = m_j$.

The system (2.3), (2.4) is defined by a system of t polynomial equations, of respective degrees $m_1, \dots, m_t$, in $2t$ variables. Let $\mathcal{Z}$ be the complete intersection defined by the system (2.3), (2.4) with $\mathbf{x} \in (\overline{\mathbb{F}}_q^\times)^{2t}$, and let $\mathcal{Z}_1, \dots, \mathcal{Z}_d$ be the distinct components of $\mathcal{Z}$. We claim that the affine dimension of each component $\mathcal{Z}_i$ is at most t. If such were not the case for the component $\mathcal{Z}_i$, then the intersection defined by (2.3), (2.4) must be improper, and $\mathcal{Z}_i$ must belong to the singular locus of $\mathcal{Z}$. Notice that for $1 \leqslant j \leqslant u$, one has

$$\frac{\partial}{\partial y_i}\left(\sum_{l=1}^{t} \breve{y}_l^{\kappa_j} - \sum_{l=t+1}^{2t} \breve{y}_l^{\kappa_j}\right) = \kappa_j y_i^{-1}\left(\sum_{l=1}^{t} \breve{y}_l^{\kappa_j} - \sum_{l=t+1}^{2t} \breve{y}_l^{\kappa_j} - \omega \breve{y}_i^{\kappa_j}\right),$$

where ω is 1 for $1 \leqslant i \leqslant t$, and -1 for $t+1 \leqslant i \leqslant 2t$. Thus, when $\mathbf{x}$ satisfies (2.3), (2.4), we find that

$$\left[\frac{\partial}{\partial y_i}\left(\sum_{l=1}^{t} \breve{y}_l^{\kappa_j} - \sum_{l=t+1}^{2t} \breve{y}_l^{\kappa_j}\right)\right]_{\mathbf{y}=\mathbf{x}} = -\omega\kappa_j x_i^{-1}\breve{x}_i^{\kappa_j} = -\omega\kappa_j x_i^{k_j-1}(x_1x_2\dots x_{2t})^{\kappa_j}.$$

Consequently, by considering the Jacobian determinants arising from the system (2.3), (2.4), and noting that $x_1x_2\dots x_{2t} \neq 0$, we find that the singular locus of $\mathcal{Z}$ is contained within the set of points $\mathbf{x} \in (\overline{\mathbb{F}}_q^\times)^{2t}$ satisfying the simultaneous equations

$$k_1k_2\dots k_t \det(x_{i_l}^{k_j-1})_{1\leqslant l,j\leqslant t} = 0, \tag{2.5}$$

with $1 \leqslant i_1 < i_2 < \dots < i_t \leqslant 2t$. According to Lemma 2.4(ii), the set of points $\mathbf{x} \in (\overline{\mathbb{F}}_q^\times)^{2t}$ satisfying (2.5) has dimension at most $t-1$, contradicting our earlier hypothesis.

We have shown as before that the components $\mathcal{Z}_1, \dots, \mathcal{Z}_d$ of $\mathcal{Z}$ each have dimension at most t, and so we may infer from Lemma 2.3 that

$$M_t(q;\mathbf{k}) = \mathrm{card}(\mathcal{Z} \cap (\mathbb{F}_q^\times)^{2t}) \leqslant m_1m_2\dots m_t(q-1)^t.$$

This completes the proof of the first estimate of Theorem 1.2.

We next seek to establish the third estimate of Theorem 1.2. On this occasion, we introduce the notational device of writing

$$\hat{x}_i = \prod_{\substack{0\leqslant l\leqslant t\\ l\neq i}} x_l \quad (1 \leqslant i \leqslant t),$$

and

$$\hat{x}_i = \prod_{\substack{t+1\leqslant l\leqslant 2t+1\\ l\neq i}} x_l \quad (t+1\leqslant i\leqslant 2t).$$

We again write κ_j for $-k_j$. Finally, we define $L_t(q;\mathbf{k})$ to be the number of solutions of the system of equations

$$\prod_{i=0}^{t} x_i = \prod_{i=t+1}^{2t+1} x_i, \tag{2.6}$$

$$\sum_{i=1}^{t} \hat{x}_i^{\kappa_j} = \sum_{i=t+1}^{2t} \hat{x}_i^{\kappa_j} \quad (1\leqslant j\leqslant u), \tag{2.7}$$

$$\sum_{i=1}^{t} x_i^{k_j} = \sum_{i=t+1}^{2t} x_i^{k_j} \quad (u+1\leqslant j\leqslant t), \tag{2.8}$$

with $\mathbf{x}\in(\mathbb{F}_q^\times)^{2t+2}$. Notice here that in view of the definition of $\hat{x}_i$, the degree of the jth equation in (2.7) is $t|k_j| = l_j$.

Given a solution $\mathbf{x}$ of the system (1.1) counted by $M_t(q;\mathbf{k})$, one has both $x_1\dots x_t\neq 0$ and $x_{t+1}\dots x_{2t}\neq 0$. Then given $x_0\in\mathbb{F}_q^\times$, there is a unique element x_{2t+1} in $\mathbb{F}_q^\times$ for which the equation (2.6) holds. Given such a $(2t+2)$-tuple $\mathbf{x}$, we may multiply the equations of (1.1) with $1\leqslant j\leqslant u$ by the non-zero factor $(x_0x_1\dots x_t)^{\kappa_j}$ on the left hand side, and by $(x_{t+1}\dots x_{2t}x_{2t+1})^{\kappa_j}$ on the right hand side. In view of the relation (2.6), this is the same non-zero factor, and so we obtain the equivalent equations (2.7). In this way we find not only that the system (2.6)-(2.8) is satisfied, but further that

$$L_t(q;\mathbf{k}) = (q-1)M_t(q;\mathbf{k}). \tag{2.9}$$

Recall the definition of the integers l_i $(1\leqslant i\leqslant t)$ given in the preamble to the statement of Theorem 1.2. Then keeping in mind the definition of $\hat{x}_i$, we find that the system (2.6)-(2.8) is defined by a system of $t+1$ polynomial equations, of respective degrees $t+1$ and $l_1,\dots,l_t$, in $2t+2$ variables. Let $\mathcal{Z}$ be the complete intersection defined by the system (2.6)-(2.8) with $\mathbf{x}\in(\overline{\mathbb{F}}_q^\times)^{2t+2}$, and let $\mathcal{Z}_1,\dots,\mathcal{Z}_d$ be the distinct components of $\mathcal{Z}$. We claim that the affine dimension of each component $\mathcal{Z}_i$ is at most $t+1$. If such were not the case for the component $\mathcal{Z}_i$, then the intersection defined by (2.6)-(2.8) must be improper, and $\mathcal{Z}_i$ must belong to the singular locus of $\mathcal{Z}$. Notice that when $\mathbf{x}$ satisfies (2.6), one has

$$\left[\frac{\partial}{\partial y_i}\left(\prod_{l=0}^{t} y_l - \prod_{l=t+1}^{2t+1} y_l\right)\right]_{\mathbf{y}=\mathbf{x}} = \omega x_i^{-1}\prod_{l=0}^{t} x_l,$$

where ω is 1 for $0\leqslant i\leqslant t$, and -1 for $t+1\leqslant i\leqslant 2t+1$. Next, when $1\leqslant j\leqslant u$ and $\mathbf{x}$ satisfies (2.6)-(2.8), write

$$\lambda_j(\mathbf{x}) = \sum_{l=1}^{t} \hat{x}_l^{\kappa_j} = \sum_{l=t+1}^{2t} \hat{x}_l^{\kappa_j}.$$

Then, when $1 \leqslant i \leqslant t$, one has

$$\left[\frac{\partial}{\partial y_i}\left(\sum_{l=1}^{t}\hat{y}_l^{\kappa_j}-\sum_{l=t+1}^{2t}\hat{y}_l^{\kappa_j}\right)\right]_{\mathbf{y}=\mathbf{x}}=\left[\kappa_j y_i^{-1}\left(\sum_{l=1}^{t}\hat{y}_l^{\kappa_j}-\hat{y}_i^{\kappa_j}\right)\right]_{\mathbf{y}=\mathbf{x}}$$
$$=\kappa_j x_i^{-1}\lambda_j(\mathbf{x})-\kappa_j x_i^{k_j-1}(x_0x_1\dots x_t)^{\kappa_j}.$$

Likewise, when $t+1 \leqslant i \leqslant 2t$, one finds that

$$\left[\frac{\partial}{\partial y_i}\left(\sum_{l=1}^{t}\hat{y}_l^{\kappa_j}-\sum_{l=t+1}^{2t}\hat{y}_l^{\kappa_j}\right)\right]_{\mathbf{y}=\mathbf{x}}=-\kappa_j x_i^{-1}\lambda_j(\mathbf{x})+\kappa_j x_i^{k_j-1}(x_0x_1\dots x_t)^{\kappa_j}.$$

In addition,

$$\left[\frac{\partial}{\partial y_0}\left(\sum_{l=1}^{t}\hat{y}_l^{\kappa_j}-\sum_{l=t+1}^{2t}\hat{y}_l^{\kappa_j}\right)\right]_{\mathbf{y}=\mathbf{x}}=\kappa_j x_0^{-1}\lambda_j(\mathbf{x}).$$

We extend the definition of $\lambda_j(\mathbf{x})$ by setting $\lambda_j(\mathbf{x})=0$ for $u+1<j\leqslant 2t$. Then, when $1\leqslant i_1<i_2<\dots<i_t\leqslant 2t$, we define the determinant $\Xi(\mathbf{i})=\Xi_{\mathbf{k}}(\mathbf{x};\mathbf{i})$ by

$$\Xi(\mathbf{i})=\det\begin{pmatrix}x_0^{-1} & \mathbf{u}^T\\ \mathbf{v} & A\end{pmatrix},$$

where $\mathbf{u}$ and $\mathbf{v}$ are the column vectors

$$\mathbf{u}=(x_{i_l}^{-1})_{1\leqslant l\leqslant t},\quad \mathbf{v}=(x_0^{-1}\lambda_j(\mathbf{x}))_{1\leqslant j\leqslant t},$$

and

$$A=\left(-x_{i_l}^{k_j-1}(x_0x_1\dots x_t)^{\kappa_j}+x_{i_l}^{-1}\lambda_j(\mathbf{x})\right)_{1\leqslant l,j\leqslant t}.$$

Given a singular point $\mathbf{x}\in(\overline{\mathbb{F}}_q^\times)^{2t+2}$ on $\mathscr{Z}$, the determinant $\Xi_{\mathbf{k}}(\mathbf{x};\mathbf{i})$ must vanish for $1\leqslant i_1<i_2<\dots<i_t\leqslant 2t$. In order to see this, one has only to note that $x_0x_1\dots x_t=x_{t+1}\dots x_{2t}x_{2t+1}\neq 0$, and to observe that the Jacobian determinant, corresponding to the partial derivatives indexed by $x_0,x_{i_1},\dots,x_{i_t}$, vanishes if and only if $\Xi(\mathbf{i})=0$. For $1\leqslant l\leqslant t$, we may subtract the first column multiplied by $x_0x_{i_l}^{-1}$ from the $(l+1)$th column. In this way we find that

$$\Xi(\mathbf{i})=\det\begin{pmatrix}x_0^{-1} & O\\ \mathbf{v} & B\end{pmatrix},$$

where

$$B=\left(-x_{i_l}^{k_j-1}(x_0x_1\dots x_t)^{\kappa_j}\right)_{1\leqslant l,j\leqslant t}.$$

But then $\Xi(\mathbf{i})=x_0^{-1}\det(B)$, and hence $\Xi(\mathbf{i})$ vanishes if and only if

$$\det(x_{i_l}^{k_j-1})_{1\leqslant l,j\leqslant t}=0.$$

From the above discussion, we find that if $\mathscr{Z}_i$ has dimension exceeding $t+1$, then the set of points $(x_1,x_2,\dots,x_{2t})\in(\overline{\mathbb{F}}_q^\times)^{2t}$, for which $(x_0,x_1,\dots,x_{2t+1})$ lies on $\mathscr{Z}_i$, must be contained in $\mathfrak{Y}_{2t}(\mathbf{k})$. From Lemma 2.4(ii), this set has dimension at most $t-1$. But the equation (2.6) ensures that x_0 is uniquely determined from x_{2t+1} together with a given choice of $(x_1,x_2,\dots,x_{2t})$, and so

$\mathcal{Z}_i$ can have dimension at most $(t-1)+1=t$. This contradicts our earlier hypothesis that $\dim(\mathcal{Z}_i) > t+1$.

We have shown on this occasion that the components $\mathcal{Z}_1, \dots, \mathcal{Z}_d$ each have dimension at most $t+1$, so by Lemma 2.3 we deduce that

$$L_t(q;\mathbf{k}) = \mathrm{card}(\mathcal{Z} \cap (\mathbb{F}_q^\times)^{2t+2}) \leqslant (t+1)l_1 l_2 \dots l_t (q-1)^{t+1}.$$

Consequently, the relation (2.9) delivers the estimate

$$M_t(q;\mathbf{k}) \leqslant (t+1)l_1 l_2 \dots l_t (q-1)^t,$$

and this confirms the third estimate of Theorem 1.2.

An alternative approach is required to establish the second estimate of Theorem 1.2. Given a solution $\mathbf{x} \in (\mathbb{F}_q^\times)^{2t}$ of the system (1.1), there is a unique element $\mathbf{y} \in (\mathbb{F}_q^\times)^{2t}$ for which $x_i y_i = 1$ $(1 \leqslant i \leqslant 2t)$. Consequently, if we define $K_t(q;\mathbf{k})$ to be the number of solutions of the system of equations

$$\sum_{i=1}^t (y_i^{\kappa_j} - y_{t+i}^{\kappa_j}) = 0 \quad (1 \leqslant j \leqslant u), \tag{2.10}$$

$$\sum_{i=1}^t (x_i^{k_j} - x_{t+i}^{k_j}) = 0 \quad (u+1 \leqslant j \leqslant t), \tag{2.11}$$

$$x_l y_l = 1 \quad (1 \leqslant l \leqslant 2t), \tag{2.12}$$

with $\mathbf{x}, \mathbf{y} \in (\mathbb{F}_q^\times)^{2t}$, then one finds that

$$K_t(q;\mathbf{k}) = M_t(q;\mathbf{k}). \tag{2.13}$$

Let $\mathcal{Z}$ be the complete intersection defined by the system (2.10)-(2.12) with $\mathbf{x}, \mathbf{y} \in (\mathbb{F}_q^\times)^{2t}$. Let $\mathcal{Z}_1, \dots, \mathcal{Z}_d$ be the distinct components of $\mathcal{Z}$. We claim that the affine dimension of each component $\mathcal{Z}_i$ is at most t. If such were not the case, then the intersection defined by (2.10)-(2.12) must be improper, and $\mathcal{Z}_i$ must belong to the singular locus of $\mathcal{Z}$. The Jacobian determinants corresponding to the system (2.10)-(2.12) are not particularly simple to describe, and so we must introduce some additional notation. The system (2.10)-(2.12) possesses $3t$ equations and $4t$ variables. Let $h_1, \dots, h_t$ be integers with $1 \leqslant h_1 < h_2 < \dots < h_t \leqslant 2t$, and write $\mathcal{H} = \{h_1, \dots, h_t\}$ and define $\mathcal{I} = \mathcal{I}(\mathcal{H})$ by $\mathcal{I} = \{1, \dots, 2t\} \setminus \mathcal{H}$. Then $\mathcal{I}$ is a set of integers $i_1, \dots, i_t$ with $1 \leqslant i_1 < \dots < i_t \leqslant 2t$. For each set $\mathcal{H}$ of the above type, we define the Jacobian determinant $\Upsilon(\mathcal{H}) = \Upsilon_{\mathbf{k}}(\mathbf{x};\mathcal{H})$ by

$$\Upsilon(\mathcal{H}) = \det \begin{pmatrix} A & O & B \\ O & C & O \\ O & O & F \\ D & E & O \end{pmatrix},$$

where A, B, C are the diagonal matrices

$$A = \mathrm{diag}(y_h)_{h \in \mathcal{H}}, \quad B = \mathrm{diag}(x_h)_{h \in \mathcal{H}}, \quad C = \mathrm{diag}(y_i)_{i \in \mathcal{I}(\mathcal{H})},$$

and D, E, F are the generalised Vandermonde matrices

$$D=(k_jx_{h_l}^{k_j-1})_{\substack{1\leqslant l\leqslant t\\ u+1\leqslant j\leqslant t}},\quad E=(k_jx_{i_l}^{k_j-1})_{\substack{1\leqslant l\leqslant t\\ u+1\leqslant j\leqslant t}},\quad F=(\kappa_jy_{h_l}^{\kappa_j-1})_{\substack{1\leqslant l\leqslant t\\ 1\leqslant j\leqslant u}}.$$

That $\Upsilon(\mathcal{H})$ is indeed a Jacobian determinant may be seen by rearranging the equations comprising (2.10)-(2.12) to correspond to the rows of $\Upsilon(\mathcal{H})$, so that the first t equations become $x_hy_h=1$ $(h\in\mathcal{H})$, the next t become $x_iy_i=1$ $(i\in\mathcal{I}(\mathcal{H}))$, and the final t become the t equations of (2.10) and (2.11). Likewise, we rearrange the partial derivatives so that the first t columns of $\Upsilon(\mathcal{H})$ correspond to the partial derivatives $\partial/\partial x_h$ $(h\in\mathcal{H})$, the second t correspond to the partial derivatives $\partial/\partial x_i$ $(i\in\mathcal{I}(\mathcal{H}))$, and the third t correspond to the partial derivatives $\partial/\partial y_h$ $(h\in\mathcal{H})$. It follows, in particular, that if $\mathcal{Z}_i$ has dimension exceeding t, then its points satisfy the system of equations $x_iy_i=1$ $(1\leqslant i\leqslant 2t)$, and

$$\Upsilon(\mathcal{H})=0\quad (\mathcal{H}=\{h_1,\dots,h_t\}\subset\{1,2,\dots,2t\}).$$

One has

$$\det(\Upsilon(\mathcal{H}))=\det(C)\det\begin{pmatrix}A&B\\O&F\\D&O\end{pmatrix}.$$

For $1\leqslant l\leqslant t$, we may subtract $x_{h_l}y_{h_l}^{-1}$ times the lth column of the last determinant from the $(t+l)$th column, without affecting its value. In this way, we find that

$$\det(\Upsilon(\mathcal{H}))=\det(C)\det\begin{pmatrix}A&O\\O&F\\D&G\end{pmatrix},$$

where

$$G=(k_jx_{h_l}^{k_j}y_{h_l}^{-1})_{\substack{1\leqslant l\leqslant t\\ u+1\leqslant j\leqslant t}}.$$

Making use of the relations $x_iy_i=1$ $(1\leqslant i\leqslant 2t)$, we find that

$$\begin{aligned}\det(\Upsilon(\mathcal{H}))&=\pm\det(A)\det(C)\det(k_jx_{h_l}^{k_j}y_{h_l}^{-1})_{1\leqslant l,j\leqslant t}\\&=\pm k_1\dots k_t\Bigl(\prod_{h\in\mathcal{H}}x_h\Bigr)\Bigl(\prod_{i\in\mathcal{I}(\mathcal{H})}y_i\Bigr)\det\left(x_{h_l}^{k_j-1}\right)_{1\leqslant l,j\leqslant t}.\end{aligned}$$

From the above discussion, we find that if $\mathcal{Z}_i$ has dimension exceeding t, then the set of points $\mathbf{x}\in(\overline{\mathbb{F}}_q^\times)^{2t}$, for which $(\mathbf{x},\mathbf{y})$ lies on $\mathcal{Z}_i$, must be contained in $\mathfrak{Y}_{2t}(\mathbf{k})$. But Lemma 2.4(ii) shows that the latter has dimension at most $t-1$. Since for $(\mathbf{x},\mathbf{y})\in\mathcal{Z}_i$ one has $x_iy_i=1$ $(1\leqslant i\leqslant 2t)$, each coordinate y_i is uniquely determined from x_i, whence $\mathcal{Z}_i$ itself can have dimension at most $t-1$, contradicting our early hypothesis.

The components $\mathcal{Z}_1,\dots,\mathcal{Z}_d$ of $\mathcal{Z}$ therefore each have dimension at most t, whence by Lemma 2.3 we obtain the estimate

$$K_t(q;\mathbf{k})=\text{card}(\mathcal{Z}\cap(\mathbb{F}_q^\times)^{4t})\leqslant 2^{2t}\kappa_1\dots\kappa_uk_{u+1}\dots k_t(q-1)^t.$$

In view of (2.13), the second estimate for $M_t(q;\mathbf{k})$ asserted by Theorem 1.2 follows on recalling that $\kappa_i = -k_i$. This completes our account of the proof of Theorem 1.2. □

The conclusions of Corollary 1.3 follow at once from Theorems 1.1 and 1.2 by means of the argument of Theorem 1.2 of Cochrane and Pinner [6]. Under the hypotheses of Corollary 1.3, the estimate of Cochrane and Pinner shows that

$$|S(\chi, f)| < (p-1)^{1-2/t} p^{1/(2t)} M^{1/t^2},$$

where $M = N_t(p;\mathbf{k})$ when $k_i > 0$ $(1 \leqslant i \leqslant t)$, and otherwise $M = M_t(p;\mathbf{k})$. In the first instance, Theorem 1.1 delivers the bound

$$|S(\chi, f)| < p^{1-3/(2t)} (k_1 k_2 \dots k_t p^t)^{1/t^2} = (k_1 \dots k_t)^{1/t^2} p^{1-1/(2t)}.$$

If the exponents k_i are not all positive, then one obtains in like manner the remaining estimates of Corollary 1.3 as immediate corollaries of Theorem 1.2.

References

[1] N. M. Akulinchev, *Bounds for rational trigonometric sums of a special type*, Dokl. Akad. Nauk SSSR **161** (1965), 743–745.

[2] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc. **18** (2005), 477–499.

[3] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. **12** (2006), 155-185.

[4] T. Cochrane, J. Coffelt and C. Pinner, *A further refinement of Mordell's bound on exponential sums*, Acta Arith. **116** (2005), 35–41.

[5] T. Cochrane, J. Coffelt and C. Pinner, *A system of simultaneous congruences arising from trinomial exponential sums*, J. Théor. Nombres Bordeaux **18** (2006), 59–72.

[6] T. Cochrane and C. Pinner, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. **133** (2005), 313–320.

[7] T. Cochrane, C. Pinner and J. Rosenhouse, *Bounds on exponential sums and the polynomial Waring problem mod p*, J. London Math. Soc. (2) **67** (2003), 319–336.

[8] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, Berlin, 1977.

[9] J. Heintz and C.-P. Schnorr, *Testing polynomials which are easy to compute*, Logic and Algorithmic (Zurich, 1980), pp. 237–254, Monograph. Enseign. Math., **30**, Univ. Genève, Geneva, 1982.

[10] A. A. Karatsuba, *Estimates of complete trigonometric sums*, Mat. Zametki **1** (1967), 199–208.

[11] L. J. Mordell, *On a sum analogous to Gauss's sum*, Quart. J. Math. Oxford **3** (1932), 161–167.

[12] I. M. Vinogradov, *New estimates for Weyl sums*, Dokl. Akad. Nauk SSSR **8** (1935), 195–198.

[13] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. USA **34** (1948), 204–207.

[14] T. D. Wooley, *On simultaneous additive equations, III*, Mathematika **37** (1990), 85–96.

[15] T. D. Wooley, *A note on simultaneous congruences*, J. Number Theory **58** (1996), 288–297.

[16] H. B. Yu, *Estimates for complete exponential sums of special types*, Math. Proc. Cambridge Philos. Soc. **131** (2001), 321–326.

TDW: School of Mathematics, University of Bristol, University Walk, Clifton, Bristol BS8 1TW, United Kingdom

E-mail address: matdw@bristol.ac.uk