EXACT EVALUATION OF SECOND MOMENTS ASSOCIATED WITH SOME FAMILIES OF CURVES OVER A FINITE FIELD

RAVI DONEPUDI, JUNXIAN LI, AND ALEXANDRU ZAHARESCU

Abstract. Let $\mathbb{F}_q$ be the finite field with q elements. Given an N-tuple $Q \in \mathbb{F}_q^N$, we associate with it an affine plane curve $\mathscr{C}_Q$ over $\mathbb{F}_q$. We consider the distribution of the quantity $q - \#\mathscr{C}_{q,Q}$ where $\#\mathscr{C}_{q,Q}$ denotes the number of $\mathbb{F}_q$-points of the affine curve $\mathscr{C}_Q$, for families of curves parameterized by Q. Exact formulae for first and second moments are obtained in several cases when Q varies over a subset of $\mathbb{F}_q^N$. Families of Fermat type curves, Hasse-Davenport curves and Artin-Schreier curves are also considered and results are obtained when Q varies along a straight line.

1. Introduction

Given an elliptic curve E over the finite field $\mathbb{F}_q$ with q elements, the number of points of E over $\mathbb{F}_q$ can be expressed as $q + 1 - T_E$, where T_E is the trace of the Frobenius of E. A classical result of Hasse [7] states that

$$|T_E| \leq 2\sqrt{q}.$$

Questions on the distribution of the number of points have been studied by a number of authors. In particular, for a fixed $\mathbb{F}_q$, one can consider the trace distribution of a family of elliptic curves. Let $E_{q,a,b}$ denote the elliptic curve with Weierstrass form $y^2 = x^3 + ax + b$, and let $T_{E_{q,a,b}}$ denote the trace of Frobenius of $E_{q,a,b}$. In [2], Birch gave asymptotic formulae for the average of even moments $\sum_{a,b\in\mathbb{F}_q} T^{2R}_{E_{q,a,b}}$ by using the Selberg trace formula. More recently, in [8], He and Mc Laughlin obtained exact formulae for $\sum_{a\in\mathbb{F}_p} T^2_{E_{p,a,b}}$ when the field is taken to be the prime field $\mathbb{F}_p$. For a smooth algebraic curve $\mathscr{C}$ over $\mathbb{F}_q$ of genus g, a well known theorem of Weil [11] states that

$$|q + 1 - \#\mathscr{C}_q| \leq 2g\sqrt{q}, \tag{1}$$

where $\#\mathscr{C}_q$ denotes the number of $\mathbb{F}_q$-points of the projective curve. As with the case of elliptic curves where $g = 1$, the distribution of the quantity $T_{\mathscr{C}_q} := q + 1 - \#\mathscr{C}_q$ has also attracted attention. In the present paper, we establish exact formulae for the first and second moments of analogous quantities to $T_{\mathscr{C}_q}$ over some general families of plane curves over a finite field $\mathbb{F}_q$.

For fixed non-negative integers $a_i, b_i, i \in \{1, 2, \ldots, N\}$ and an N-tuple

$$Q = (c_1, c_2, \ldots, c_N) \in \mathbb{F}_q^N,$$

2010 *Mathematics Subject Classification.* Primary: 11T23, Secondary: 11T99.

Key words and phrases. Families of Polynomials, Curves over finite fields, Exponential sums, Exact Formulae .

we associate with it a plane curve $\mathscr{C}_Q$ whose affine model is given by

$$\mathscr{C}_Q : \sum_{i=1}^{N} c_i x^{a_i} y^{b_i} = 0. \tag{2}$$

We set $T_Q = q - \#\mathscr{C}_Q$, where $\#\mathscr{C}_Q$ denotes the number of $\mathbb{F}_q$-points, which are the $\mathbb{F}_q$-solutions (x, y) to the defining equation (2) of $\mathscr{C}_Q$. We will use points or solutions instead of $\mathbb{F}_q$-points or $\mathbb{F}_q$-solutions for short later on. Note that if we homogenize equation (2), then the points at infinity are determined by the highest degree homogeneous equation in x and y. For elliptic curves in Weierstrass form, there is only one point at infinity, and our definition of T_Q matches the usual definition of T_Q as $q + 1 - \#P\mathscr{C}$, where $\#P\mathscr{C}$ is the number of point on the projective curve associated to $\mathscr{C}$. In either case, T_Q measures the difference between the number of points on the curve and the expected value. Given a subset $S \subseteq \mathbb{F}_q^N$, we are interested in the distribution of T_Q as Q ranges over S. In particular, we consider the variance of T_Q for $Q \in S$,

$$\mathbb{V}[T_Q] := \frac{1}{|S|} \sum_{Q \in S} (T_Q - M_1^S)^2 = M_2^S - (M_1^S)^2, \tag{3}$$

where M_1^S is the average of T_Q over all $Q \in S$ given by

$$M_1^S := \frac{1}{|S|} \sum_{Q \in S} T_Q, \tag{4}$$

and M_2^S is the second moment of T_Q over all $Q \in S$ defined as

$$M_2^S := \frac{1}{|S|} \sum_{Q \in S} T_Q^2. \tag{5}$$

Under some restrictions on the set S, we establish exact formulae for M_1^S and M_2^S. First we introduce some notation. For an index set $I \subseteq \{1, 2, \ldots, N\}$ and an N-tuple $\mathbf{v} = (v_j) \in \mathbb{F}_q^N$, let $S_I(\mathbf{v})$ be the set of N-tuples whose coordinate with indices outside I are given by the corresponding coordinates of $\mathbf{v}$. More precisely, we are defining

$$S_I(\mathbf{v}) = \{(c_1, c_2, \ldots, c_N) | c_j = v_j \text{ for } j \notin I \text{ and } c_i \in \mathbb{F}_q \text{ for } i \in I\}, \tag{6}$$

and letting

$$I_0 = \{i \in I |\ a_i = 0,\ b_i = 0,\ \}, \tag{7}$$

$$I_0^c = \{i \notin I |\ a_i = 0,\ b_i = 0, \}, \tag{8}$$

$$n_x^I = \#\{(a_i, b_i) |\ a_i \neq 0,\ b_i = 0,\ i \in I\}, \tag{9}$$

$$n_y^I = \#\{(a_i, b_i) |\ a_i = 0,\ b_i \neq 0,\ i \in I\}, \tag{10}$$

$$n_x^{I^c} = \#\{(a_i, b_i) |\ a_i \neq 0\ b_i = 0,\ i \notin I\}, \tag{11}$$

$$n_y^{I^c} = \#\{(a_i, b_i) |\ a_i = 0,\ b_i \neq 0,\ i \notin I\}, \tag{12}$$

where I^c denotes the complement set of I in $\{1, 2, \ldots, N\}$. For example, if $q = 17$, $N = 5$, let $(a_1, \ldots, a_5) = (2, 3, 0, 5, 0)$, $(b_1, \ldots, b_5) = (1, 0, 0, 3, 4)$, $I = \{2, 3\}$ and

$\mathbf{v} = (0, 1, 2, 3, 4)$, then

$$S_I(\mathbf{v}) = \{(0, c_2, c_3, 3, 4) | c_2, c_3 \in \mathbb{F}_{17}\},$$
$$I_0 = \{3\}, I_0^c = \{1, 2, 4, 5\}, n_x^I = 1, n_y^I = 0, n_x^{I^c} = 0, n_y^{I^c} = 1.$$

Intuitively, I_0 gives the indices of constant polynomials in the set $\{x^{a_i}y^{b_i}, i \in I\}$, n_x^I gives the number of monomials in x from the set $\{x^{a_i}y^{b_i}, i \in I\}$ and n_y^I gives the number of monomials in y from the set $\{x^{a_i}y^{b_i}, i \in I\}$.

Consider the $\mathbb{F}_q$-vector space spanned by $\{x^{a_i}y^{b_i} | i \in \{1, 2, \ldots, N\}\}$ for some non-negative integers $a_i, b_i, i \in \{1, 2, \ldots, N\}$. For any $I \subseteq \{1, 2, \ldots, N\}$ and $\mathbf{v} \in \mathbb{F}_q^N$, we are interested in finding the second moment of T_Q, where $Q \in S_I(\mathbf{v}) \subset \mathbb{F}_q^N$.

Theorem 1.1 *Given fixed exponents $a_i, b_i \in \mathbb{Z}_{\geq 0}$ for $i = 1, \ldots, N$, consider a subset $I \subseteq \{1, 2, \ldots, N\}$. Let I^c denote the complement of I in $\{1, 2, \ldots, N\}$ and $n_x^I, n_y^I, n_x^{I^c}, n_y^{I^c}$ be defined as above. Then, for any $\mathbf{v} = (v_j) \in \mathbb{F}_q^N$ and all $Q \in S_I(\mathbf{v})$,*

$$M_1^{S_I(\mathbf{v})} = \frac{1}{q^{|I|}} \sum_{Q \in S_I(\mathbf{v})} T_Q = \begin{cases} -\kappa\nu(b) & \text{if } I_0 = \emptyset \\ 0 & \text{if } I_0 \neq \emptyset \end{cases}, \tag{13}$$

where

$$b = \sum_{i \in I_0^c} v_i, \tag{14}$$

$$\nu(b) = \begin{cases} q - 1 & \text{if } b = 0, \\ -1 & \text{if } b \neq 0, \end{cases} \tag{15}$$

$$\text{and } \kappa = \begin{cases} \frac{2q-1}{q} & \text{if } n_x^I = 0,\ n_y^I = 0,\ n_x^{I^c} = 0,\ n_y^{I^c} = 0, \\ 1 & \text{if } n_x^I > 0,\ n_y^I = 0,\ n_y^{I^c} = 0, \\ 1 & \text{if } n_x^I = 0,\ n_y^I > 0,\ n_x^{I^c} = 0, \\ \frac{1}{q} & \text{if } n_x^I > 0,\ n_y^I > 0. \end{cases} \tag{16}$$

Before stating our next result, we discuss the notion of injectivity of an index set. For a given set $I \subseteq \{1, 2, 3, .., N\}$ and distinct $i, j, k \in I$, let

$$M_{ijk} = \det \begin{bmatrix} a_i - a_j & b_i - b_j \\ a_i - a_k & b_i - b_k \end{bmatrix}.$$

We call I injective if the following condition hold,

$$\gcd\{\gcd(M_{ijk}, q - 1) |\ M_{ijk} \neq 0,\ i, j, k \in I, i, j, k \text{ distinct}\} = 1.$$

We also introduce the following notation, which will be used to obtain exact number of solutions for families of curves. Let

$$d_x^I := \gcd\{\gcd(a_t - a_r, q-1) |\ t, r \in I,\ b_t = b_r = 0\}, \tag{17}$$
$$d_y^I := \gcd\{\gcd(b_l - b_s, q-1) |\ l, s \in I, a_l = a_s = 0\}, \tag{18}$$
$$m_x^I := \gcd\{\gcd(a_t, q-1) |\ t \in I,\ b_t = 0\}, \tag{19}$$
$$m_y^I := \gcd\{\gcd(b_l, q-1) |\ l \in I,\ a_l = 0\}. \tag{20}$$

As an example that illustrates this notation, let $q = 2^4$, $N = 5$ and suppose that $(a_1, \dots, a_5) = (2, 3, 0, 5, 0)$ and $(b_1, \dots, b_5) = (1, 0, 0, 3, 5)$. Then, $I_1 = \{1, 2, 3, 4\}$ is injective, but $I_2 = \{1, 2, 5\}$ is not. Also, $m_x^{I_1} = 1$, $d_x^{I_1} = 3$, $d_y^{I_2} = 5$ and $m_y^{I_2} = 5$.

Theorem 1.2 *Given fixed exponents $a_i, b_i \in \mathbb{Z}_{\geq 0}$ for $i = 1, \dots, N$, suppose that a subset $I \subseteq \{1, 2, 3, .., N\}$ is injective and that $n_x^{I^c} = 0$, $n_y^{I^c} = 0$. Then, for any given $\mathbf{v} = (v_j) \in \mathbb{F}_q^N$ and all $Q \in S_I(\mathbf{v})$,*

$$M_2^{S_I(\mathbf{v})} = \frac{1}{q^{|I|}} \sum_{Q \in S_I(\mathbf{v})} T_Q^2 = \begin{cases} \left(1 - \frac{1}{q}\right)^2 \left(q - 1 + \frac{\nu(b)\kappa'}{q-1} + \frac{z(b) q \kappa''}{q-1}\right) & \text{if } I_0 = \emptyset, \\ \left(1 - \frac{1}{q}\right)^2 (q - 1 + \kappa'') & \text{if } I_0 \neq \emptyset, \end{cases}$$

where b and $\nu(b)$ are defined as above, and κ', κ'' and $z(b)$ are defined as follows:

$$z(b) = \begin{cases} 0 & \text{if } b = 0, \\ 1 & \text{if } b \neq 0, \end{cases}$$

$$\kappa' = \begin{cases} (2q-1)^2 & \text{if } n_x^I = 0, n_y^I = 0, \\ q^2 + q - 1 & \text{if } n_x^I = 1, n_y^I = 0 \text{ or } n_x^I = 0, n_y^I = 1 \\ 2q - 1 & \text{if } n_x^I = 1, n_y^I = 1, \\ q^2 + d_x^I & \text{if } n_x^I \geq 2, n_y^I = 0, \\ q^2 + d_y^I & \text{if } n_x^I = 0,\ n_y^I \geq 2, \\ q + d_x^I, & \text{if } n_x^I \geq 2, n_y^I = 1, \\ q + d_y^I, & \text{if } n_x^I = 1,\ n_y^I \geq 2, \\ d_x^I + d_y^I + 1 & \text{if } n_x^I \geq 2, n_y^I \geq 2, \end{cases}$$

$$\kappa'' = \begin{cases} \frac{(2q-1)^2}{q-1} & \text{if } n_x^I = 0, n_y^I = 0, \\ m_x^I + \frac{q^2}{q-1} & \text{if } n_x^I > 0, n_y^I = 0, \\ m_y^I + \frac{q^2}{q-1} & \text{if } n_x^I = 0, n_y^I > 0, \\ m_x^I + m_y^I + \frac{q^2}{q-1} & \text{if } n_x^I > 0, n_y^I > 0. \end{cases}$$

In later sections, we consider the case when I is not injective. For some special classes of curves, such as families of Fermat type curves, Hasse-Davenport curves and Artin-Schreier curves, one can obtain explicit formulae for $M_1^{S_I(\mathbf{v})}$ and $M_2^{S_I(\mathbf{v})}$ even if I is not injective.

2. Preliminaries

Let $q = p^r$ be a prime power. The canonical additive character of $\mathbb{F}_q$ is defined as

$$e_q(x) = e^{2\pi i \mathrm{Tr}(x)/p}, \tag{21}$$

where $\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{r-1}} \in \mathbb{F}_p$.
For $1 \leq d \leq r, d \mid r$, define $\mathrm{Tr}_d : \mathbb{F}_q \to \mathbb{F}_{p^d}$ by

$$\mathrm{Tr}_d(x) = x + x^{p^d} + x^{p^{2d}} + x^{p^{3d}} + \cdots + x^{q/p^d}. \tag{22}$$

By Lemma 4.2 of [5],

$$\sum_{x \in \mathbb{F}_{p^d}} e_q(xy) = \begin{cases} p^d & \text{if } \mathrm{Tr}_d(y) = 0, \\ 0 & \text{if } \mathrm{Tr}_d(y) \neq 0. \end{cases} \tag{23}$$

In particular, if we take $d = [\mathbb{F}_q : \mathbb{F}_p] = r$, then

$$\sum_{x \in \mathbb{F}_q} e_q(xy) = \begin{cases} q & \text{if } y = 0, \\ 0 & \text{if } y \neq 0. \end{cases} \tag{24}$$

It follows that the number of solutions $f(x, y) \in \mathbb{F}_q[x, y]$ in $\mathbb{F}_q^2$ can be written as

$$\frac{1}{q} \sum_{x,y \in \mathbb{F}_q} \sum_{t \in \mathbb{F}_q} e_q(tf(x, y)). \tag{25}$$

The $t = 0$ term contributes q to the total number of solutions. Thus the quantity

$$\begin{aligned} T_q(f) &= -\frac{1}{q} \sum_{x,y \in \mathbb{F}_q} \sum_{t \in \mathbb{F}_q^*} e_q(tf(x, y)) \\ &= q - \#\{(x, y) \in \mathbb{F}_q^2 : f(x, y) = 0\}. \end{aligned} \tag{26}$$

is the quantity we are interested in. For a hyperelliptic curve E over $\mathbb{F}_p$ given by $y^2 = f(x)$, where $f(x) \in \mathbb{F}_p[x]$, the quantity $T_p(f)$ can also be expressed using the Legendre symbol as

$$T_p(f) = -\sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p} \right). \tag{27}$$

Now, let $e_p(z) = \exp(2\pi i z/p)$, and

$$G_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \mod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \mod 4. \end{cases} \tag{28}$$

From Theorem 1.1.5 and Theorem 1.5.2 of [1], we have

$$\left(\frac{z}{p} \right) = \frac{1}{G_p} \sum_{d=1}^{p-1} \left(\frac{d}{p} \right) e_p \left(\frac{dz}{p} \right), \tag{29}$$

which was used in [8] to calculate the second moment in the case where the polynomial $f(x,y)$ is given by $f(x,y) = y^2 - x^3 - ax - b$.

3. Proof of theorem 1.1

We consider the family of curves parametrized by $Q = (c_i) \in \mathbb{F}_q^N$, defined in (2) as

$$f_Q(x,y) = \sum_{i=1}^{N} c_i x^{a_i} y^{b_i} = 0.$$

Given a subset $I \subseteq \{1, 2, \ldots, N\}$, $\mathbf{v} \in \mathbb{F}_q^N$ and $Q \in S_I(\mathbf{v})$ defined in (6), we set $b = \sum_{i \in I_0^c} v_i$, which gives the constant term for this family of curves. From (26), we have

$$\begin{aligned}\sum_{Q \in S_I(\mathbf{v})} T_Q &= -\frac{1}{q} \sum_{Q \in S_I(\mathbf{v})} \sum_{x,y \in \mathbb{F}_q} \sum_{\in \mathbb{F}_q^*} e_q\left(t \sum_{j=1}^{N} c_j x^{a_j} y^{b_j}\right) \\ &= -\frac{1}{q} \sum_{x,y \in \mathbb{F}_q} \sum_{t \in \mathbb{F}_q^*} e_q\left(t \sum_{\substack{j=1,\\ j \notin I}}^{N} c_j x^{a_j} y^{b_j}\right) \prod_{i \in I} \sum_{c_i \in \mathbb{F}_q} e_q(c_i t x^{a_i} y^{b_i}). \end{aligned} \tag{30}$$

Using (24), the only nonzero contributions arise from the pairs (x, y) that satisfy $x^{a_i} y^{b_i} = 0$, for all $i \in I$. If $I_0 \neq \emptyset$, then the sum becomes zero, while if $I_0 = \emptyset$, the equation (30) becomes

$$\sum_{Q \in S_I(\mathbf{v})} T_Q = -\frac{q^{|I|}}{q} \sum_{\substack{x,y \in \mathbb{F}_q \\ x^{a_i} y^{b_i} = 0,\ \forall i \in I}} \sum_{t \in \mathbb{F}_q^*} e_q\left(t \sum_{\substack{j=1,\\ j \notin I}}^{N} c_j x^{a_j} y^{b_j}\right). \tag{31}$$

Now we consider the following cases separately.

3.1. Case $n_x^I = 0,\ n_y^I = 0,\ n_x^{I^c} = 0,\ n_y^{I^c} = 0$:

The condition $x^{a_i} y^{b_i} = 0$ for all $i \in I$ becomes $xy = 0$, so we have $2q - 1$ such pairs $(x, y) \in \mathbb{F}_q^2$. By the assumption that $n_x^{I^c} = 0$ and $n_y^{I^c} = 0$, we have $x^{a_j} y^{b_j} = 0$ for all $j \notin I$ for these $2q - 1$ pairs. Thus (31) becomes

$$\begin{aligned}\sum_{Q \in S_I(\mathbf{v})} T_Q &= -\frac{q^{|I|}}{q} \sum_{\substack{x,y \in \mathbb{F}_q \\ xy=0}} \sum_{t \in \mathbb{F}_q^*} e_q(tb) \\ &= -\frac{q^{|I|}}{q} \sum_{\substack{x,y \in \mathbb{F}_q \\ xy=0}} \left(\sum_{t \in \mathbb{F}_q} e_q(tb) - 1\right) \\ &= \begin{cases} -(q-1)(2q-1)q^{|I|-1} & \text{if } b = 0, \\ (2q-1)q^{|I|-1} & \text{if } b \neq 0. \end{cases}\end{aligned} \tag{32}$$

3.2. **Case** $n_x^I > 0,\ n_y^I = 0,\ n_y^{I^c} = 0$**:**

The condition that $x^{a_i}y^{b_i} = 0$ for all $i \in I$ forces x to be zero, so there are q such pairs $(x,y) \in \mathbb{F}_q^2$. Since $n_y^{I^c} = 0$, we have $x^{a_j}y^{b_j} = 0$ for all $j \notin I$ when $x = 0$. Thus (31) becomes

$$\begin{aligned} \sum_{Q \in S_I(\mathbf{v})} T_Q &= -\frac{q^{|I|}}{q} \sum_{\substack{x,y \in \mathbb{F}_q \\ x=0}} \sum_{t \in \mathbb{F}_q^*} e_q(tb) \\ &= -\frac{q^{|I|}}{q} \sum_{\substack{x,y \in \mathbb{F}_q \\ x=0}} \left(\sum_{t \in \mathbb{F}_q} e_q(tb) - 1 \right) \\ &= \begin{cases} -(q-1)q^{|I|} & \text{if } b = 0, \\ q^{|I|} & \text{if } b \neq 0. \end{cases} \end{aligned} \tag{33}$$

3.3. **Case** $n_x^I = 0,\ n_y^I > 0,\ n_x^{I^c} = 0$ **:**

This is very similar to case (2), and is proved by switching x and y.

3.4. **Case** $n_x^I > 0,\ n_y^I > 0$ **:**

Since there exist at least one term of the form $x^{a_j}, a_j > 0$ and one term $y^{b_k}, b_k > 0$ for some $j, k \in I$, the condition $x^{a_i}y^{b_i} = 0$ for all $i \in I$ implies that $x = 0,\ y = 0$, which in turn causes $x^{a_j}y^{b_j} = 0$ for all $j \notin I$. So, there is only one term in the sum (31), which becomes

$$\begin{aligned} \sum_{Q \in S_I(\mathbf{v})} T_Q &= -\frac{q^{|I|}}{q} \sum_{\substack{x,y \in \mathbb{F}_q \\ x=0,\ y=0}} \sum_{t \in \mathbb{F}_q^*} e_q(tb) \\ &= -\frac{q^{|I|}}{q} \left(\sum_{t \in \mathbb{F}_q} e_q(tb) - 1 \right) \\ &= \begin{cases} -(q-1)q^{|I|-1} & \text{if } b = 0, \\ q^{|I|-1} & \text{if } b \neq 0. \end{cases} \end{aligned} \tag{34}$$

This completes the proof of Theorem (1.1).

4. Proof of theorem (1.2)

From (26), for $Q \in S_I(\mathbf{v})$,

$$T_Q = -\frac{1}{q} \sum_{x,y \in \mathbb{F}_q} \sum_{t \in \mathbb{F}_q^*} e_q(tf_Q(x,y)) = -\frac{1}{q} \sum_{x,y \in \mathbb{F}_q} \sum_{t \in \mathbb{F}_q^*} e_q(t \sum_{i=1}^{N} c_i x^{a_i} y^{b_i}).$$

It follows that

$$\sum_{Q\in S_I(\mathbf{v})} T_Q^2 = \frac{1}{q^2}\sum_{Q\in S_I(\mathbf{v})}\sum_{\substack{x_1,y_1\in\mathbb{F}_q\\ x_2,y_2\in\mathbb{F}_q}}\sum_{t_1,t_2\in\mathbb{F}_q^*} e_q(t_1 f_Q(x_1,y_1))e_q(t_2 f_Q(x_2,y_2))$$
$$= \sum_{t_1,t_2\in\mathbb{F}_q^*}\sum_{\substack{x_1,x_2\in\mathbb{F}_q\\ y_1,y_2\in\mathbb{F}_q}}\left(\prod_{i\in I} S_i \prod_{j\notin I} e_q(t_1 c_j x_1^{a_j} y_1^{b_j} + t_2 c_j x_2^{a_j} y_2^{b_j})\right),$$

where

$$S_i := S_i(x_1,y_1,t_1,x_2,y_2,t_2) = \sum_{c_i\in\mathbb{F}_q} e_q(c_i(t_1 x_1^{a_i} y_1^{b_i} + t_2 x_2^{a_i} y_2^{b_i})).$$

By (24), the S_i are equal to q precisely when $t_1x_1^{a_i}y_1^{b_i} + t_2x_2^{a_i}y_2^{b_i}$ vanishes. Since we have a product of S_i, we need to find the simultaneous $\mathbb{F}_q$-solutions to the following $|I|$ equations

$$t_1x_1^{a_i}y_1^{b_i} + t_2x_2^{a_i}y_2^{b_i} = 0, \text{ for } i\in I.$$

Equivalently, we have the system

$$\begin{bmatrix} x_1^{a_{i_1}}y_1^{b_{i_1}} & x_2^{a_{i_1}}y_2^{b_{i_1}} \\ x_1^{a_{i_2}}y_1^{b_{i_2}} & x_2^{a_{i_2}}y_2^{b_{i_2}} \\ \vdots & \vdots \\ x_1^{a_{i_{|I|}}}y_1^{b_{i_{|I|}}} & x_2^{a_{i_{|I|}}}y_2^{b_{i_{|I|}}} \end{bmatrix}\begin{bmatrix} t_1 \\ t_2\end{bmatrix} = \begin{bmatrix}0\\0\\ \vdots \\ 0\end{bmatrix}. \tag{35}$$

4.1. **Case:** $x_1x_2y_1y_2 \neq 0$**.** If we have that $x_1x_2y_1y_2\neq 0$, then we reduce this matrix to

$$\begin{bmatrix} 1 & u^{a_{i_1}}v^{b_{i_1}} \\ 1 & u^{a_{i_2}}v^{b_{i_2}} \\ \vdots & \vdots \\ 1 & u^{a_{i_{|I|}}}v^{b_{i_{|I|}}}\end{bmatrix},$$

where $u = \frac{x_2}{x_1}$ and $v = \frac{y_2}{y_1}$. This system has a non-zero solution only when this matrix has rank 1, that is

$$u^{a_i}v^{b_i} = u^{a_j}v^{b_j} = u^{a_k}v^{b_k},$$

for all distinct $i,j,k\in I$. Since u,v are non-zero, this further reduces to

$$u^{a_i-a_j}v^{b_i-b_j} = 1 \text{ and } u^{a_j-a_k}v^{b_j-b_k} = 1.$$

Raising the first equation to the power a_j-a_k and the second to a_i-a_j, we obtain $v^{M_{ijk}}=1$, where M_{ijk} is the determinant of the matrix

$$\begin{bmatrix} a_i-a_j & b_i-b_j \\ a_j-a_k & b_j-b_k\end{bmatrix}.$$

Denote by D the greatest common divisor of all M_{ijk}, where $i,j,k \in I$ are distinct. Then we can find integers $r_{i,j,k}$ such that $\sum_{i,j,k} r_{ijk} M_{ijk} = D$. Thus $v^D = 1$ as well.

The assumption that $\gcd(D, q-1) = 1$ guarantees that the power map $x \mapsto x^D$ is a bijection and so $v = 1$. Similarly, $u = 1$ as well.

So $x_1 = x_2$ and $y_1 = y_2$. This in turn forces $t_1 = -t_2$. Since we assume that $x_1x_2y_1y_2 \neq 0$, there are $(q-1)^3$ solutions to the simultaneous equations.

4.2. **Case:** $x_1y_1x_2y_2 = 0$**.** A more complicated scenario arises when $x_1x_2y_1y_2 = 0$. The number of solutions to the system (35) varies dramatically for different index sets I. First we consider the case when the constant term in the family $b = \sum_{i \in I_0^c} v_i = 0$. By switching x and y if necessary, we divide the problem into six manageable cases.

(1) $n_x^I = 0, n_y^I = 0, n_x^{I^c} = 0, n_y^{I^c} = 0$
   In this case, we consider sets I for which $a_ib_i \neq 0$ for all $i \in I$. Noticing that $x_1y_1 = 0$ if and only if $x_2y_2 = 0$, there are $(2q-1)^2$ tuples (x_1, x_2, y_1, y_2) that satisfy this requirement. Since t_1 and t_2 do not affect the equation, there are $(q-1)^2$ choices for (t_1, t_2). This gives a total of $(2q-1)^2(q-1)^2$ solutions to the system (35).
(2) $I_0 = \emptyset, n_x^I = 1, n_y^I = 0, n_x^{I^c} = 0, n_y^{I^c} = 0$
   This is the case where there is exactly one term $c_ix_i^{a_i}$, $i \in I$ in $f(x,y)$. Then, notice that $x_1 = 0$ if and only if $x_2 = 0$, and in this case there are q^2 choices for (y_1, y_2). If $x_1 \neq 0$, then y_1 and y_2 must be zero so that (35) has solutions with $x_1x_2y_1y_2 = 0$. Any choice of x_1, x_2, t_1 (all non-zero) determines a unique choice for t_2, yielding a total of $q^2(q-1)^2 + (q-1)^3 = (q-1)^2(q^2+q-1)$ solutions.
(3) $I_0 = \emptyset, n_x^I = 1, n_y^I = 1, n_x^{I^c} = 0, n_y^{I^c} = 0$
   In this case, there is exactly one term of the form $c_ix^{a_i}$ and one term of the form $c_jy^{b_j}$ with $i,j \in I$. Again, $x_1 = 0$ if and only if $x_2 = 0$ and in this case there are $(q-1)^3$ choices of tuples (y_1, y_2, t_1, t_2) where all the coordinates are non-zero. Similarly, the requirement that $y_1 = 0$ if and only if $y_2 = 0$ yields $(q-1)^3$ tuples (x_1, x_2, t_1, t_2) with all coordinates non-zero. If x_1, x_2, y_1, y_2 are all zero, there are $(q-1)^2$ tuples (t_1, t_2). In summary, we have $2(q-1)^3 + (q-1)^2 = (q-1)^2(2q-1)$ solutions.
(4) $I_0 = \emptyset, n_x^I \geq 2, n_y^I = 0, n_y^{I^c} = 0$
   In this case, there are at least two terms of the form say $c_ix^{a_i}$ and $c_jx^{a_j}$. As before, $x_1 = 0$ if and only if $x_2 = 0$, thus we have $q^2(q-1)^2$ solutions for (y_1, y_2, t_1, t_2). If $x_1 \neq 0$ and $y_1 = 0$, then we must have $x_2 \neq 0$ and $y_2 = 0$. If we let $u = \frac{x_1}{x_2}$, then non zeros solutions (t_1, t_2) to (35) implies $u^{d_x^I} = 1$, and any of such u's will give $d_x^I(q-1)^2$ choices of (x_1, x_2, t_1, t_2) so that (35) is satisfied. This yields a total of $(q-1)^2(q^2 + d_x^I)$ solutions.
(5) $I_0 = \emptyset, n_x^I \geq 2, n_y^I = 1, n_y^{I^c} = 0$
   Under this condition, there must be three terms in the form of x^{a_i}, x^{a_j} and y^{b_k} appearing in $f(x,y)$ with $i,j,k \in I$. We still have $x_1 = 0$ if and only if $x_2 = 0$ and $y_1 = 0$ if and only if $y_2 = 0$. For the solutions with $x_1 = 0$, we have $q(q-1)^2$ solutions for (y_1, y_2, t_1, t_2), and for the solutions with $x_1 \neq 0$, we have

$d_x^I(q-1)^2$ solutions by a similar argument as in the previous case. This gives $(q-1)^2(q+d_x^I)$ solutions in total.

(6) $I_0 = \emptyset, n_x^I \geq 2, n_y^I \geq 2$

In every other case, $f(x,y)$ contains at least four terms $c_i x^{a_i}, c_j x^{a_j}, c_k y^{a_k}$ and $c_l y^{b_l}$ with $i,j,k,l \in I$. Then as before, if only one of x_i, y_i is zero, there are $(d_x^I + d_y^I)(q-1)^2$ solutions. If $x_i = y_i = 0$, there are $(q-1)^2$ solutions. In total we obtain $(d_x^I + d_y^I + 1)(q-1)^2$ solutions.

Using our notation in (7), we summarize our discussion for $I_0 = \emptyset$ as follows:

Condition	$x_1y_1x_2y_2 \neq 0$	$x_1y_1x_2y_2 = 0$
$n_x^I = 0, n_y^I = 0$	$(q-1)^3$	$(q-1)^2(2q-1)^2$
$n_x^I = 1, n_y^I = 0$	$(q-1)^3$	$(q-1)^2(q^2+q-1)$
$n_x^I = 1, n_y^I = 1$	$(q-1)^3$	$(q-1)^2(2q-1)$
$n_x^I \geq 2, n_y^I = 0$	$(q-1)^3$	$(q-1)^2(q^2+d_x^I)$
$n_x^I \geq 2, n_y^I = 1$	$(q-1)^3$	$(q-1)^2(q+d_x^I)$
$n_x^I \geq 2, n_y^I \geq 2$	$(q-1)^3$	$(q-1)^2(d_x^I+d_y^I+1)$

For the case $I_0 \neq \emptyset$, solutions to the system (35) requires $t_1 + t_2 = 0$. We need to consider $x_1y_1x_2y_2 = 0$ in the following cases.

(1) $n_x^I = 0, n_y^I = 0, n_x^{I^c} = 0, n_y^{I^c} = 0$

Since the equations in (35) are all in the form $t_1 x_1^a y_1^b + t_2 x_2^a y_2^b = 0$, where $ab \neq 0$. Solutions with $x_1y_1 = 0$ forces $x_2y_2 = 0$, which gives $(2q-1)^2(q-1)$ solutions to the system.

(2) $I_0 \neq \emptyset, n_x^I > 0, n_y^I = 0, n_x^{I^c} = 0, n_y^{I^c} = 0$

If $x_1 = 0$, then $x_2 = 0$, which gives $q^2(q-1)$ solutions for (y_1, y_2, t_1, t_2). If $x_1 \neq 0, y_1 = 0$, then there are $m_x^I(q-1)^2$ solutions to the system.

(3) $I_0 \neq \emptyset, n_x^I = 0, n_y^I > 0, n_x^{I^c} = 0, n_y^{I^c} = 0$

By a similar argument as above, there will be $m_y^I(q-1)^2 + (q-1)q^2$ solutions to the system.

(4) $I_0 \neq \emptyset, n_x^I > 0, n_y^I > 0, n_x^{I^c} = 0, n_y^{I^c} = 0$

If $x_1 = 0$, then $x_2 = 0$, which gives $m_y^I(q-1)^2$ solutions for (y_1, y_2, t_1, t_2), where $y_1y_2 \neq 0$ and $(q-1)$ solutions with $y_1y_2 = 0$. If $x_1 \neq 0, y_1 = 0$, then there are $m_x^I(q-1)^2$ solutions to the system.

We summarize the above cases in the following table:

Condition	$x_1y_1x_2y_2 \neq 0$	$x_1y_1x_2y_2 = 0$
$n_x^I = 0, n_y^I = 0$	$(q-1)^3$	$(q-1)(2q-1)^2$
$n_x^I > 0, n_y^I = 0$	$(q-1)^3$	$m_x^I(q-1)^2 + q^2(q-1)$
$n_x^I = 0, n_y^I > 0$	$(q-1)^3$	$m_y^I(q-1)^2 + q^2(q-1)$
$n_x^I > 0, n_y^I > 0$	$(q-1)^3$	$\left(m_x^I + m_y^I\right)(q-1)^2 + (q-1)$

Next, consider the case when $b \neq 0$ in the family defined in (2). It is easy to see that the value of $M_2^{S_I(\mathbf{v})}$ is the same for all $b \neq 0$ since we can always divide the equation of the curve by b to make the constant term 1. Using the same notation as before, if we sum over b, by a similar argument we see that

$$\sum_{\substack{Q\in S_I(\mathbf{v})\\ b\in F_q}} T_Q^2 \neq 0 \implies t_1 + t_2 = 0,$$

which reduces to the case when $I_0 \neq \emptyset$. By assumptions of Theorem 1.2, the number of solutions to the system (35) with $t_1 + t_2 = 0$ is given by the above table:

Thus for each family with $b \neq 0$, the second moment $M_2^{S_I(\mathbf{v})}$ is as follows:

$I_0 = \emptyset$	$q^2 M_2^{S_I(\mathbf{v})}$
$n_x^I = 0, n_y^I = 0$	$(q-1)^3 + (2q-1)^2$
$n_x^I = 1, n_y^I = 0$	$(q-1)^3 + q(m_x^I(q-1) + q^2) - (q-1)(q^2+q-1)$
$n_x^I = 1, n_y^I = 1$	$(q-1)^3 + q(\left(m_x^I + m_y^I\right)(q-1) + 1) - (q-1)(2q-1)$
$n_x^I \geq 2, n_y^I = 0$	$(q-1)^3 + q(m_x^I(q-1) + q^2) - (q-1)(q^2 + d_x^I)$
$n_x^I \geq 2, n_y^I = 1$	$(q-1)^3 + q(\left(m_x^I + m_y^I\right)(q-1) + 1) - (q-1)(q + d_x^I)$
$n_x^I \geq 2, n_y^I \geq 2$	$(q-1)^3 + q(\left(m_x^I + m_y^I\right)(q-1) + 1) - (q-1)(d_x^I + d_y^I + 1)$

$I_0 \neq \emptyset$	$q^2 M_2^{S_I(\mathbf{v})}$
$n_x^I = 0, n_y^I = 0$	$(q-1)^3 + (q-1)(2q-1)^2$
$n_x^I = 1, n_y^I = 0$	$(q-1)^3 + (q-1)(m_x^I(q-1) + q^2)$
$n_x^I = 1, n_y^I = 1$	$(q-1)^3 + (q-1)(\left(m_x^I + m_y^I\right)(q-1) + 1)$
$n_x^I \geq 2, n_y^I = 0$	$(q-1)^3 + (q-1)(m_x^I(q-1) + q^2)$
$n_x^I \geq 2, n_y^I = 1$	$(q-1)^3 + (q-1)(\left(m_x^I + m_y^I\right)(q-1) + 1)$
$n_x^I \geq 2, n_y^I \geq 2$	$(q-1)^3 + (q-1)(\left(m_x^I + m_y^I\right)(q-1) + 1)$

This completes the proof of Theorem 1.2.

Remark: The proof shows that in the case where $n_x^I \geq 2$ and $n_y^I = 0$, we can get the same result even if $n_x^{I^c} > 0$, and for the case when $n_x^I \geq 2$ and $n_y^I \geq 2$, no restriction on I^c is necessary.

5. Fermat type curves

Consider the family of Fermat type curves over $\mathbb{F}_q$ defined by

$$y^l = x^m + ax^k + b, \tag{36}$$

where $a, b \in \mathbb{F}_q$ and l, m, k are positive integers. Let

$$T_{q,a,b} = q - \#\{(x,y) \in \mathbb{F}_q^2 |\ y^l = x^m + ax^k + b\}. \tag{37}$$

Then, we have the following result if we only average over $a \in \mathbb{F}_q$.

Theorem 5.1 *Using the above notation,*

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b} = \begin{cases} q\left(1 - \frac{(l,q-1)}{2}\left(1 + \left(\frac{b}{q}\right)_l\right)\right) & \text{if } b \neq 0, \\ 0 & \text{if } b = 0, \end{cases} \tag{38}$$

$$\sum_{b\in\mathbb{F}_q} T_{q,a,b} = 0, \tag{39}$$

where

$$\left(\frac{b}{q}\right)_l = \begin{cases} 1 & \text{if } b = y_0^l,\ y_0 \in \mathbb{F}_q^*, \\ -1 & \text{otherwise.} \end{cases}$$

Theorem 5.2 *If q is a prime power satisfying* $\gcd(q-1,l) = 2$, $\gcd(q-1,m) = 1$ *and* $\gcd(q-1,k) = 1$, *then*

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 = \begin{cases} q^2 & \text{if } b \neq 0,\ 2d \nmid q-1, \\ q\,(q - d\eta(-1)) & \text{if } b \neq 0,\ 2d | q-1, \\ 0 & \text{if } b = 0,\ 2d \nmid q-1, \\ q(q-1)d\eta(-1) & \text{if } b = 0,\ 2d | q-1, \end{cases} \tag{40}$$

where $d = \gcd(q-1, m-k)$ *and η is the quadratic character for $\mathbb{F}_q^*$.*

When $l = 2, m = 3$, and $k = 1$, Theorem 5.1 and 5.2 reduce to Theorem 3 and 4 in [8]. Notice that in the previous notation, for $N = 4$, $(a_1, a_2, a_3, a_4) = (m, k, 0, 0)$, $(b_1, b_2, b_3, b_4) = (0, 0, l, 0)$ and $I = \{2\}$, then I is injective but $n_x^{I^c} = n_y^{I^c} = 1$, thus Theorem 1.2 can not be applied in this case.

5.1. **Proof of Theorem 5.1.**

By the definition of $T_{q,a,b}$,

$$T_{q,a,b} = -\frac{1}{q} \sum_{x,y\in\mathbb{F}_q} \sum_{t\in\mathbb{F}_q^*} e_q(t(y^l - x^m - ax^k - b)). \tag{41}$$

By summing over $b \in \mathbb{F}_q$, we deduce that

$$\begin{aligned}\sum_{b\in\mathbb{F}_q} T_{q,a,b} &= -\sum_{x,y\in\mathbb{F}_q}\frac{1}{q}\sum_{b\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q^*} e_q\left(t(y^l - x^m - ax^k - b)\right)\\ &= -\sum_{x,y\in\mathbb{F}_q}\frac{1}{q}\sum_{t\in\mathbb{F}_q^*} e_q(t(y^l - x^m - ax^k))\sum_{b\in\mathbb{F}_q} e_q(-tb)\\ &= 0.\end{aligned}$$

Also, if we average over a,

$$\begin{aligned}\sum_{a\in\mathbb{F}_q} T_{q,a,b} &= -\sum_{x,y\in\mathbb{F}_q}\frac{1}{q}\sum_{a\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q^*} e_q(t(y^l - x^m - ax^k - b))\\ &= -\sum_{x,y\in\mathbb{F}_q}\frac{1}{q}\sum_{t\in\mathbb{F}_q^*} e_q(t(y^l - x^m - b))\sum_{a\in\mathbb{F}_q} e_q(t(-ax^k))\\ &= -\sum_{y\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q^*} e_q(t(y^l - b))\\ &= q - \sum_{y\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q} e_q(t(y^l - b)).\end{aligned}$$

If $b = 0$, then

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b} = 0,$$

since only the term with $y = 0$ gives contribution to the sum. If $b \neq 0$, then

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b} = q\left(1 - \frac{(l, q-1)}{2}\left(1 + \left(\frac{b}{q}\right)_l\right)\right)$$

where

$$\left(\frac{b}{q}\right)_l = \begin{cases} 1 & \text{if } b = y_0^l,\ y_0 \in \mathbb{F}_q,\\ -1 & \text{otherwise.}\end{cases}$$

This completes the proof.

5.2. **Proof of Theorem 5.2.** From (41),

$$\begin{aligned}&\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2\\ =&\frac{1}{q^2}\sum_{a\in\mathbb{F}_q}\sum_{\substack{x_1,x_2,\\ y_1,y_2\in\mathbb{F}_q}}\sum_{t_1,t_2\in\mathbb{F}_q^*} e_q\left(t_1(y_1^l - x_1^m - ax_1^k - b) + t_2(y_2^l - x_2^m - ax_2^k - b)\right)\\ =&\frac{1}{q^2}\sum_{\substack{x_1,x_2,\\ y_1,y_2\in\mathbb{F}_q}}\sum_{t_1,t_2\in\mathbb{F}_q^*} e_q\left(t_1(y_1^l - x_1^m - b) + t_2(y_2^l - x_2^m - b)\right)\sum_{a\in\mathbb{F}_q} e_q\left(-a(t_1x_1^k + t_2x_2^k)\right).\end{aligned}$$

The innermost sum is nonzero precisely when $x_2^k = -t_2^{-1}t_1x_1^k$. If $(k, q-1) = 1$, there are integers s, s' such that $sk + s'(q-1) = 1$. Thus

$$\begin{aligned}
&\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 \\
=&\frac{1}{q}\sum_{x_1,y_1,y_2\in\mathbb{F}_q}\sum_{t_1,t_2\in\mathbb{F}_q^*} e_q\left(t_1(y_1^l-b)+t_2(y_2^l-b)+(-t_1t_2^{1-sm}x_1^m(t_1^{sm-1}-t_2^{sm-1})\right) \\
=&\frac{1}{q}\sum_{y_1,y_2\in\mathbb{F}_q}\sum_{t_1,t_2\in\mathbb{F}_q^*} e_q\left(t_1(y_1^l-b)+t_2(y_2^l-b)\right)\sum_{x_1\in\mathbb{F}_q} e_q\left(x_1^m(-t_1t_2^{1-sm}(t_1^{sm-1}-t_2^{sm-1})\right).
\end{aligned}$$

By the assumption that $(m, q-1) = 1$, we see that the inner sum contributes a factor of q precisely when $t_1^{sm-1} = t_2^{sm-1}$. Raising both sides to the k-th power, we obtain $\left(\frac{t_2}{t_1}\right)^{m-k} = 1$. The number of $(m-k)^{\text{th}}$ roots of unity in $\mathbb{F}_q$ is $d = \gcd(m-k, q-1)$. For each such root u, the equality $t_2 = ut_1$ holds. Since $\gcd(l, q-1) = 2$, we can make a change of variable by replacing $y_i^{l/2}$ by y_i. Thus we rewrite our sum as

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 = \sum_{\substack{u^d=1,\\ u\in\mathbb{F}_q}}\sum_{y_1,y_2\in\mathbb{F}_q}\sum_{t_1\in\mathbb{F}_q^*} e_q\left(t_1(y_1^2-b)+ut_1(y_2^2-b)\right). \tag{42}$$

For a fixed u, we now count the number of solutions (y_1, y_2) to the equation

$$t_1y_1^2 + ut_1y_2^2 = t_1b(1+u). \tag{43}$$

Let η denote the quadratic character of $\mathbb{F}_q^*$. Using Theorem 8 of [8], which gives the number of solutions to certain quadratic forms, we see that in the case $b \neq 0$, if $u \neq -1$ there are exactly

$$q - \eta(-t_1^2u) = q - \eta(-u). \tag{44}$$

solutions to (43), and

$$q + (q-1)\eta(-t_1^2u) = 2q - 1. \tag{45}$$

solutions when $u = -1$. Since the sum over t_1 excludes 0, each solution (u, y_1, y_2) contributes $q-1$ to our sum and each non-solution (u, y_1, y_2) contributes -1. By combining this with the number of solutions to (43), (44) and (45), we find our sum in

(42) is

$$\begin{aligned}\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 &= (q-1)\left(\sum_{u^d=1,u\neq-1}(q-\eta(-u))+2q-1\right)\\ &\quad-\left(dq^2-\left(\sum_{u^d=1,u\neq-1}(q-\eta(-u))+2q-1\right)\right)\\ &= q\left(q-1-\sum_{u^d=1,u\neq-1}\eta(-u)\right)\\ &= q\left(q-\sum_{u^d=1}\eta(-u)\right).\end{aligned}$$

Similarly, if $b=0$, the number of solutions to (43) equals

$$(q-1)(1+\eta(-u))+1=q+(q-1)\eta(-u).$$

Summing over $u^d=1$,

$$\begin{aligned}\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 &= (q-1)\left(\sum_{u^d=1}(q+(q-1)\eta(-u))\right)\\ &\quad-\left(dq^2-\left(\sum_{u^d=1}(q+(q-1)\eta(-u))\right)\right)\\ &= q(q-1)\sum_{u^d=1}\eta(-u).\end{aligned}$$

In conclusion,

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 = \begin{cases} q\left(q-\sum_{u^d=1}\eta(-u)\right) & \text{if } b\neq 0,\\ q(q-1)\sum_{u^d=1}\eta(-u) & \text{if } b=0.\end{cases} \tag{46}$$

If $2d\nmid q-1$, exactly half of the u satisfying $u^d=1$ are squares in $\mathbb{F}_q$, thus the sum over all the u's is zero. In this case, (46) can be simplified as

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 = \begin{cases} q^2 & \text{if } b\neq 0,\\ 0 & \text{if } b=0.\end{cases} \tag{47}$$

If $2d\mid q-1$, every u satisfying $u^d=1$ is a square in $\mathbb{F}_q$, and since there are d such u's, one can see that (46) becomes

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 = \begin{cases} q\,(q-d\eta(-1)) & \text{if } b\neq 0,\\ q(q-1)d\eta(-1) & \text{if } b=0.\end{cases} \tag{48}$$

Moreover, the quadratic character η of the prime field $\mathbb{F}_p$ is given by the Legendre symbol $\left(\frac{\cdot}{p}\right)$. Thus (46) becomes

$$\sum_{a\in\mathbb{F}_p} T_{q,a,b}^2 = \begin{cases} p\left(p - d\left(\frac{-1}{p}\right)\right) & \text{if } b \neq 0, \\ 0 & \text{if } b = 0. \end{cases} \tag{49}$$

If $[\mathbb{F}_q : \mathbb{F}_p] \geq 2$, then $\eta(-1) = 1$, thus (46) becomes

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 = \begin{cases} q\,(q-d) & \text{if } b \neq 0, \\ q(q-1)d & \text{if } b = 0. \end{cases} \tag{50}$$

This completes the proof of Theorem 5.2.

6. Hasse-Davenport Curves

For a fixed positive integer n and $a \in \mathbb{F}_q$, the Hasse-Davenport curve is defined by

$$C_a : y^2 + y = ax^n. \tag{51}$$

When n is an odd positive integer, the number of points of curves in this family is closely related to the weight distribution of irreducible cyclic codes. A special type of binary linear code was considered by Van der Vlugt in [10], where he provided some explicit formulae for the weight distribution of such codes when $n = pq$ where p and q are primes satisfying $\gcd(p-1, q-1) = 2$ and $\operatorname{ord}_n(2) = \phi(n)/2$.

We prove a formula for the average value of the second moment of $T_{q,a,b}$ over a generalized Hasse-Davenport family $C_{a,b} : y^2 + y = ax^n + b$.

Theorem 6.1 *Let n be an integer and $T_{q,a,b} = q - \#\{(x,y) \in F_q^2 : y^2 + y = ax^n + b\}$. Let $d = \gcd(q-1, n)$. We have the following:*
When q is even,

$$\sum_{a\in\mathbb{F}_q^*} T_{q,a,b} = 0, \tag{52}$$

$$\sum_{a\in\mathbb{F}_q^*} T_{q,a,b}^2 = (d-1)q(q-1), \tag{53}$$

and when q is odd,

$$\sum_{a\in\mathbb{F}_q^*} T_{q,a,b} = 0, \tag{54}$$

$$\sum_{a\in\mathbb{F}_q^*} T_{p,a,b}^2 = \begin{cases} (d-1)q(q-1) & \textit{if} \quad 4b+1 \neq 0, \ n \ \textit{odd}, \\ (d-2)q(q-1) + (q-1) & \textit{if} \quad 4b+1 \neq 0, \ n \ \textit{even}, \\ 0 & \textit{if} \quad 4b+1 = 0, \ n \ \textit{odd}, \\ d(q-1)^3 & \textit{if} \quad 4b+1 = 0, \ n \ \textit{even}. \end{cases} \tag{55}$$

Proof. When q is even, we have

$$\begin{aligned}\sum_{a\in\mathbb{F}_q} T_{q,a,b} &= -\frac{1}{q}\sum_{a\in\mathbb{F}_q}\sum_{x,y\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q^*} e_q\left(t(y^2+y-ax^n-b)\right)\\ &= -\sum_{y\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q^*} e_q\left(t(y^2+y-b)\right)\\ &= -\sum_{t\in\mathbb{F}_q^*} e_q(-tb)\sum_{y\in\mathbb{F}_q} e_q\left(t(y^2+y)\right)\\ &= -\sum_{t\in\mathbb{F}_q^*} e_q(-tb)\sum_{y\in\mathbb{F}_q} e_q\left((t^2+t)y^2\right)\\ &= -q\ e_q(b). \end{aligned} \tag{56}$$

For the second moment, using (26), we have

$$\sum_{a\in\mathbb{F}_q} T^2_{q,a,b} = \frac{1}{q^2}\sum_{a\in\mathbb{F}_q}\sum_{\substack{x_i,y_i\in\mathbb{F}_q\\ i=1,2}}\sum_{t_1,t_2\in\mathbb{F}_q^*} e_q\left(t_1(y_1^2+y_1-ax_1^n-b)+t_2(y_2^2+y_2-ax_2^n-b)\right). \tag{57}$$

After an interchange the order of summation, the right-hand side becomes

$$\begin{aligned} &\frac{1}{q^2}\sum_{t_1,t_2\in\mathbb{F}_q^*} e_q(-(t_1+t_2)b)\sum_{x_1,x_2,a\in\mathbb{F}_q} e_q(-a(t_1x_1^n+t_2x_2^n))\\ &\qquad\times\sum_{y_1\in\mathbb{F}_q} e_q(t_1(y_1^2+y_1))\sum_{y_2\in\mathbb{F}_q} e_q(t_2(y_2^2+y_2))\\ =&\frac{1}{q^2}\sum_{t_1,t_2\in\mathbb{F}_q^*} e_q(-(t_1+t_2)b)\sum_{x_1,x_2,a\in\mathbb{F}_q} e_q(-a(t_1x_1^n+t_2x_2^n))\\ &\qquad\times\sum_{y_1\in\mathbb{F}_q} e_q((t_1+t_1^2)y_1^2)\sum_{y_2\in\mathbb{F}_q} e_q((t_2+t_2^2)y_2^2). \end{aligned} \tag{58}$$

The inner two sums are nonzero only if both t_1 and t_2 satisfy $t^2+t=0$. Since $t^2+t=0$ has $t=-1$ as its only nonzero solution, we obtain

$$\begin{aligned}\sum_{a\in\mathbb{F}_q} T^2_{q,a,b} &= \sum_{x_1,x_2\in\mathbb{F}_q}\sum_{a\in\mathbb{F}_q} e_q(-a(x_1^n+x_2^n))\\ &= q(d(q-1)+1), \end{aligned} \tag{59}$$

as there are $d(q-1)$ nonzero solutions for $x_1^n+x_2^n=0$, and $x_1=0, x_2=0$ is the only solution such that at least one of x_1, x_2 is zero. When $a=0$, the equation becomes $y^2+y=b$ and this equation has two solutions if and only if $\mathrm{Tr}(b)=0$. Thus

$$T_{q,0,b} = \begin{cases} -q & \text{if } \mathrm{Tr}(b)=0,\\ q & \text{if } \mathrm{Tr}(b)\neq 0. \end{cases} \tag{60}$$

When q is odd, by a change of variables by replacing $2y_i+1$ by y_i and $4a$ by a, we have

$$\begin{aligned}\sum_{a\in\mathbb{F}_q} T_{q,a,b} &= -\frac{1}{q}\sum_{a\in\mathbb{F}_q}\sum_{x,y\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q^*} e_q\left(t(y^2-1-ax^n-4b)\right)\\ &= -\sum_{y\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q^*} e_q\left(t(y^2-1-4b)\right)\\ &= q-\sum_{y\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q} e_q\left(t(y^2-1-4b)\right)\\ &= -\eta(4b+1)\, q. \end{aligned}\tag{61}$$

The second moment is given by

$$\begin{aligned}&\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2\\ =&\frac{1}{q^2}\sum_{\substack{x_i,y_i\in\mathbb{F}_q\\ i=1,2}}\sum_{t_1,t_2\in\mathbb{F}_q^*}\sum_{a\in\mathbb{F}_q} e_q\left(t_1(y_1^2-ax_1^n-4b-1)+t_2(y_2^2-ax_2^n-4b-1)\right)\\ =&\frac{1}{q^2}\sum_{\substack{x_i,y_i\in\mathbb{F}_q\\ i=1,2}}\sum_{t_1,t_2\in\mathbb{F}_q^*} e_q\left(t_1(y_1^2-4b-1)+t_2(y_2^2-4b-1)\right)\sum_{a\in\mathbb{F}_q} e_q\left(-a(t_1x_1^n+t_2x_2^n)\right).\end{aligned}\tag{62}$$

The only contribution to the sum is from tuples (x_1,x_2,t_1,t_2) which satisfy the equation $t_1x_1^n+t_2x_2^n=0$. If $x_2=0$ then only $x_1=0$ will contribute to the sum and there is no restriction on t_1 and t_2. If $x_1x_2\neq 0$, we write $t_2=ut_1$ and $x_1=vx_2$, then the condition becomes

$$x_2^n(u+v^n)=0.$$

We have d solutions for $v^n=1$, where $d=\gcd(q-1,n)$. So, (62) becomes

$$\begin{aligned}\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 &= \frac{1}{q}\sum_{\substack{y_i\in\mathbb{F}_q\\ i=1,2}}\sum_{t_1\in\mathbb{F}_q^*}\left(\sum_{x_2\in\mathbb{F}_q^*}\sum_{u+v^n=0}\sum_{v\in\mathbb{F}_q^*}+\sum_{u\in\mathbb{F}_q^*}\right) e_q\left(t_1(y_1^2+uy_2^2-(1+u)(4b+1))\right)\\ &= \frac{1}{q}\sum_{\substack{y_i\in\mathbb{F}_q\\ i=1,2}}\sum_{t\in\mathbb{F}_q^*}\left((q-1)\sum_{v\in\mathbb{F}_q^*}\sum_{u+v^n=0}+\sum_{u\in\mathbb{F}_q^*}\right) e_q\left(t(y_1^2+uy_2^2-(1+u)(4b+1))\right)\\ &=: \Pi_1+\Pi_2\end{aligned}$$

where

$$\Pi_1 = \frac{(q-1)}{q}\sum_{t\in\mathbb{F}_q^*}\sum_{y_1,y_2\in\mathbb{F}_q}\sum_{v\in\mathbb{F}_q^*} e_q\left(t(y_1^2-v^ny_2^2+(v^n-1)(4b+1))\right),\tag{63}$$

$$\Pi_2 = \frac{1}{q}\sum_{t\in\mathbb{F}_q^*}\sum_{y_1,y_2\in\mathbb{F}_q}\sum_{u\in\mathbb{F}_q^*} e_q\left(t(y_1^2+uy_2^2-(u+1)(4b+1))\right).\tag{64}$$

From Theorem 8 of [8], which can also be found in [9], pp 282-293, we can see that

$$\begin{aligned}\Pi_1 &= (q-1)\sum_{v\in\mathbb{F}_q^*}\left(q+\nu((1-v^n)(4b+1))\right)\eta(v^n) - q(q-1)^2\\ &= (q-1)\sum_{v\in\mathbb{F}_q^*}\nu((1-v^n)(4b+1))\eta(v^n). \qquad (65)\end{aligned}$$

From the definition of ν in (15), and the fact that

$$\sum_{v\in\mathbb{F}_q^*}\eta(v^n) = \begin{cases} 0 & \text{if } n \text{ is odd},\\ q-1 & \text{if } n \text{ is even},\end{cases} \qquad (66)$$

we obtain

$$\begin{aligned}\Pi_1 &= \begin{cases} (q-1)\left(\sum_{v^n=1} q - \sum_{v\in\mathbb{F}_q^*}\eta(v^n)\right) & \text{if } 4b+1\neq 0,\\ (q-1)^2\sum_{v\in\mathbb{F}_q^*}\eta(v^n) & \text{if } 4b+1=0,\end{cases}\\ &= \begin{cases} dq(q-1) & \text{if } 4b+1\neq 0,\ n \text{ odd},\\ dq(q-1)-(q-1)^2 & \text{if } 4b+1\neq 0,\ n \text{ even},\\ 0 & \text{if } 4b+1=0,\ n \text{ odd},\\ d(q-1)^3 & \text{if } 4b+1=0,\ n \text{ even}.\end{cases} \qquad (67)\end{aligned}$$

Similarly for Π_2, we have

$$\begin{aligned}\Pi_2 &= \sum_{u\in\mathbb{F}_q^*}\left(q+\nu((1-u)(4b+1))\right)\eta(u) - q(q-1)\\ &= \sum_{u\in\mathbb{F}_q^*}\nu((1-u)(4b+1))\eta(u)\\ &= \begin{cases} q & \text{if } 4b+1\neq 0,\\ 0 & \text{if } 4b+1=0.\end{cases} \qquad (68)\end{aligned}$$

In summary, when q is odd, we have

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 = \begin{cases} dq(q-1)+q & \text{if } 4b+1\neq 0,\ n \text{ odd},\\ dq(q-1)-(q-1)^2+q & \text{if } 4b+1\neq 0,\ n \text{ even},\\ 0 & \text{if } 4b+1=0,\ n \text{ odd},\\ d(q-1)^3 & \text{if } 4b+1=0,\ n \text{ even}.\end{cases} \qquad (69)$$

When $a=0$, the curve reduces to two lines $y(y+1)=b$, which give $q(\eta(4b+1)+1)$ points in $\mathbb{F}_q$ in total. Thus $T_{q,0,b} = -q\eta(4b+1)$, and this together with (69) completes the proof of the theorem. □

7. Artin-Schreier Curves

For a finite field $\mathbb{F}_q$ with characteristic p, the Artin-Schreier curve is defined by $y^p - y = f(x)$, where $f(x)$ is a rational function in $\mathbb{F}_q(x)$. Write $q = p^e$. Wolfmann in [12] considered the case when $e = 2t$, $f(x) = ax^n + b$, where n is a divisor of $q-1$ and has the property that there exists a divisor r of t such that $q^r \equiv -1 \pmod{n}$. Coulter in [6] considered a similar family defined by $y^{p^\alpha} - y = ax^{p^\beta+1} + bx$ and gave formulae for the number of points for several cases. More results can be found in [3], where both results are generalized. The number of points depends on the exponential sum of the type $\sum_{x\in\mathbb{F}_q} e_q(ax^n)$, and the case $n = p^\beta + 1$ has been explicitly computed in [4] and [5]. Here we consider a family of curves defined by

$$y^{p^\alpha} - y = ax^n + b,$$

where $a, b \in \mathbb{F}_q$ and $\alpha, n \in \mathbb{N}$. As before we define

$$T_{q,a,b} = -\frac{1}{q} \sum_{x,y\in\mathbb{F}_q} \sum_{t\in\mathbb{F}_q^*} e_q\left(t(y^{p^\alpha} - y - ax^n - b)\right). \tag{70}$$

We will give explicit formulae for the first and second moment for $T_{q,a,b}$, and $a \in \mathbb{F}_q^*$ for all integers n.

Theorem 7.1 *With the notation above and $d = \gcd(\alpha, e)$,*

$$\sum_{a\in\mathbb{F}_q^*} T_{q,a,b} = 0, \tag{71}$$

and

$$\sum_{a\in\mathbb{F}_q^*} T_{q,a,b}^2 = \begin{cases} (p^d-1)q(q-1)(\gcd(n(p^d-1), q-1) - (p^d-1)) & \text{if } \mathrm{Tr}_d(b) = 0, \\ q(q-1)(p^d \gcd(n, q-1) - \gcd(n(p^d-1), q-1) - 1) & \text{if } \mathrm{Tr}_d(b) \neq 0. \end{cases} \tag{72}$$

Proof. From (23), we find that

$$\begin{aligned} \sum_{a\in\mathbb{F}_q} T_{q,a,b} &= -\frac{1}{q} \sum_{a\in\mathbb{F}_q} \sum_{x,y\in\mathbb{F}_q} \sum_{t\in\mathbb{F}_q^*} e_q\left(t(y^{p^\alpha} - y - ax^n - b)\right) \\ &= -\sum_{y\in\mathbb{F}_q} \sum_{t\in\mathbb{F}_q^*} e_q\left(t(y^{p^\alpha} - y - b)\right) \\ &= -\sum_{t\in\mathbb{F}_q^*} e_q(-tb) \sum_{y\in\mathbb{F}_q} e_q\left((t - t^{p^\alpha})y^{p^\alpha}\right) \\ &= -q \sum_{t\in\mathbb{F}_{p^d}^*} e_q(-tb) \\ &= \begin{cases} -q(p^d-1) & \text{if } \mathrm{Tr}_d(b) = 0, \\ q & \text{if } \mathrm{Tr}_d(b) \neq 0. \end{cases} \end{aligned} \tag{73}$$

When $a = 0$, the equation reduces to $y^{p^\alpha} - y = b$. From Lemma 3.4 of [6], the equation has a solution only when $\mathrm{Tr}_d(b) = 0$, and there are p^d such solutions. Thus,

$$T_{q,0,b} = \begin{cases} q - p^d q & \text{if } \mathrm{Tr}_d(b) = 0, \\ q & \text{if } \mathrm{Tr}_d(b) \neq 0. \end{cases} \tag{74}$$

Combining (73) and (74), we obtain the first moment for $T_{q,a,b}, a \in \mathbb{F}_q^*$.

For the second moment, we have

$$\sum_{a\in\mathbb{F}_q} T_{q,a,b}^2 = \frac{1}{q^2} \sum_{a\in\mathbb{F}_q} \sum_{\substack{x_i,y_i\in\mathbb{F}_q\\ i=1,2}} \sum_{t_1,t_2\in\mathbb{F}_q^*} e_q\left(t_1(y_1^{p^\alpha} - y_1 - ax_1^n - b) + t_2(y_2^{p^\alpha} - y_2 - ax_2^n - b)\right).$$

Interchanging the order of summation yields

$$\begin{aligned} &\frac{1}{q^2} \sum_{t_1,t_2\in\mathbb{F}_q^*} e_q(-t_1 b - t_2 b) \sum_{a\in\mathbb{F}_q} \sum_{x_1,x_2\in\mathbb{F}_q} e_q(-a(t_1x_1^n + t_2x_2^n)) \\ &\quad\times \sum_{y_1\in\mathbb{F}_q} e_q((t_1 - t_1^{p^\alpha})y_1^{p^\alpha}) \sum_{y_2\in\mathbb{F}_q} e_q((t_2 - t_2^{p^\alpha})y_2^{p^\alpha}). \end{aligned} \tag{75}$$

The inner sum is nonzero precisely when t_1 and t_2 both satisfy the equation $t - t^{p^\alpha} = 0$, whose solutions are exactly the elements in $\mathbb{F}_{p^d}$. This simplifies the left hand side to

$$\sum_{t_1,t_2\in\mathbb{F}_{p^d}^*} e_q(-t_1 b - t_2 b) \sum_{x_1,x_2\in\mathbb{F}_q} \sum_{a\in\mathbb{F}_q} e_q(-a(t_1x_1^n + t_2x_2^n)). \tag{76}$$

The inner sum is nonzero only if

$$t_1x_1^n + t_2x_2^n = 0.$$

If we separate the zero solution which contributes q to the sum and write $x_1 = vx_2$ and $t_2 = ut_1$ for the nonzero solutions, we see that (76) becomes

$$\sum_{t_1,u\in\mathbb{F}_{p^d}^*} e_q(-t_1 b - t_1 u b) \left(\sum_{a\in\mathbb{F}_q} \sum_{x_2,v\in\mathbb{F}_q^*} e_q(-at_1x_2^n(v^n + u)) + q \right). \tag{77}$$

Only the solutions to the equation

$$v^n + u = 0, v \in \mathbb{F}_q^*, u \in \mathbb{F}_{p^d}^*$$

will contribute to the sum. For each $v \in \mathbb{F}_q^*$ satisfying

$$v^{n(p^d-1)} - 1 = 0,$$

we obtain an element u in $\mathbb{F}_{p^d}^*$, and vice versa. Also notice that

$$\sum_{t_1,u\in\mathbb{F}_{p^d}^*} e_q(-t_1(1+u)b) = \begin{cases} (p^d-1)^2 & \text{if } \mathrm{Tr}_d(b) = 0, \\ 1 & \text{if } \mathrm{Tr}_d(b) \neq 0. \end{cases} \tag{78}$$

Thus (77) becomes

$$\sum_{t_1\in\mathbb{F}_{p^d}^*}\left(q(q-1)\sum_{v^n+u=0,v\in\mathbb{F}_q^*,u\in\mathbb{F}_{p^d}^*} e_q(-t_1(1+u)b)+\sum_{u\in\mathbb{F}_{p^d}^*} q\right)$$
$$=\begin{cases} q\left((p^d-1)(q-1)\gcd(n(p^d-1),q-1)+(p^d-1)^2\right) & \text{if } \mathrm{Tr}_d(b)=0,\\ q(q-1)(-\gcd(n(p^d-1),q-1)+p^d\gcd(n,q-1))+q & \text{if } \mathrm{Tr}_d(b)\neq 0.\end{cases} \tag{79}$$

Combining 74 and 79, we complete the proof of the theorem.

□

Remark: If we average over $b\in\mathbb{F}_q$ as well, then we have

$$\sum_{a,b\in\mathbb{F}_q} T_{q,a,b}^2=(p^d-1)q(q(q-1)\gcd(n,q-1)+q) \tag{80}$$

by noticing that in (75), if we sum over b, we need to have $t_1+t_2=0$. This agrees with Theorem 7.1 since there are q/p^d elements in $\mathbb{F}_q$ with $\mathrm{Tr}_d(b)=0$.

Also, if we consider the family defined by

$$y^{p^d}-y=ax^{p^\alpha+1},$$

if e/d is even, according to [6], there will be $(q-1)/(p^d+1)$ $a's$ such that $T_{q,a,0}^2$ is $q(p^d-1)^2p^{2d}$ and for the rest of the $a's$ in $\mathbb{F}_q^*$, $T_{q,a,0}^2$ is $q(p^d-1)^2$. This agrees with Theorem 7.1, which becomes

$$\sum_{a\in\mathbb{F}_q^*} T_{q,a,b}^2=q(q-1)p^d(p^d-1)^2 \tag{81}$$

after an application of Lemma 2.3 in [6], which says that

$$\gcd(p^\alpha+1,p^e-1)=\begin{cases}1 & \text{if } p=2,\\ 2 & \text{if } e/d \text{ odd},\\ p^d+1 & \text{if } e/d \text{ even}.\end{cases} \tag{82}$$

Thus when e/d is even, $T_{q,a,b}\sim p^{d/2}(p^d-1)\sqrt{q}$ on average, while the Weil bound in this case is $p^d(p^\alpha-1)\sqrt{q}$, so not all the curves in this family are maximal or minimal.

8. Acknowledgment

The authors are grateful to the referees for many useful comments and suggestions. Also, this work was supported in part by a gift to the Mathematics Department at the University of Illinois from Gene H. Golub.

References

[1] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[2] Bryan J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[3] Herivelto Borges, Beatriz Motta, and Fernando Torres. Complete arcs arising from a generalization of the Hermitian curve. *Acta Arith.*, 164(2):101–118, 2014.

[4] Robert S. Coulter. Explicit evaluations of some Weil sums. *Acta Arith.*, 83(3):241–251, 1998.

[5] Robert S. Coulter. Further evaluations of Weil sums. *Acta Arith.*, 86(3):217–226, 1998.

[6] Robert S. Coulter. The number of rational points of a class of Artin-Schreier curves. *Finite Fields Appl.*, 8(4):397–413, 2002.

[7] Helmut Hasse. Beweis des analogons der riemannschen vermutung für die artinschen und fk schmidtschen kongruenzzetafunktionen in gewissen elliptischen fällen. vorläufie mitteilung. *Mathematisch-Physikalische Klasse*, (253-262), 1993.

[8] Saiying He and James Mc Laughlin. Some properties of the distribution of the numbers of points on elliptic curves over a finite prime field. *Bulletin of the Australian Mathematics Society*, 75(1):135–149, 2007.

[9] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[10] Marcel van der Vlugt. Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes. *J. Number Theory*, 55(2):145–159, 1995.

[11] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

[12] Jacques Wolfmann. The number of points on certain algebraic curves over finite fields. *Comm. Algebra*, 17(8):2055–2060, 1989.

Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, IL 61801, USA
E-mail address: `donepud2@illinois.edu`

Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, IL 61801, USA
E-mail address: `jli135@illinois.edu`

Simion Stoilow Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, RO-014700 Bucharest, Romania and Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, IL 61801, USA
E-mail address: `zaharesc@illinois.edu`