ON THE NUMBER OF RATIONAL POINTS OF ARTIN-SCHREIER'S CURVES AND HYPERSURFACES

F.E. BROCHERO MARTÍNEZ AND DANIELA OLIVEIRA

ABSTRACT. Let $\mathbb{F}_{q^n}$ represent the finite field with q^n elements. In this paper, our focus is on determining the number of $\mathbb{F}_{q^n}$-rational points for two specific objects: an affine Artin-Schreier curve given by the equation $y^q - y = x(x^{q^i} - x) - \lambda$, and an Artin-Schreier hypersurface given by the equation $y^q - y = \sum_{j=1}^r a_j x_j (x_j^{q^{i_j}} - x_j) - \lambda$.

Additionally, we establish that the Weil bound is only achieved in these cases when the trace of the element $\lambda \in \mathbb{F}_{q^n}$ over the subfield $\mathbb{F}_q$ is equal to zero.

1. INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field with $q = p^s$ elements, where p is an odd prime. One important class of curves over finite fields is known as Artin-Schreier's curves. These curves are defined by the equation $y^q - y = f(x)$, where $f(x) \in \mathbb{F}_q[x]$. Extensive research has been conducted on these curves in various contexts, including references such as [6, 7, 8, 10, 16].

This class of curves can be generalized to multiple variables, resulting in hypersurfaces of the form $y^q - y = f(X)$, where $f(X) \in \mathbb{F}_q[X]$ and $X = (x_1, \ldots, x_r)$. The study of the number of affine rational points on algebraic hypersurfaces over finite fields has significant applications in coding theory, cryptography, communications, and related fields, as evidenced by works such as [3, 9, 15, 16].

The first aim of this paper is to calculate the number of $\mathbb{F}_{q^n}$-rational points on the Artin-Schreier curve $\mathcal{C}_i$ defined by the equation:

$$\mathcal{C}_i : y^q - y = x(x^{q^i} - x) - \lambda,$$

where $i \in \mathbb{N}$ and $\lambda \in \mathbb{F}_{q^n}$. We denote the number of affine $\mathbb{F}_{q^n}$-rational points of $\mathcal{C}_i$ as $N_n(\mathcal{C}_i)$.

For each $i \in \mathbb{N}$, we introduce the map $Q_i : \mathbb{F}_{q^n} \to \mathbb{F}_q$ defined as follows

$$Q_i : \mathbb{F}_{q^n} \to \mathbb{F}_q$$

$$\alpha \mapsto \mathrm{Tr}(\alpha(\alpha^{q^i} - \alpha) - \lambda),$$

where $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ denotes the trace function. We define $N_n(Q_i)$ as the number of zeroes of Q_i in $\mathbb{F}_{q^n}$. According to Hilbert's Theorem 90, we can establish the relationship

$$N_n(\mathcal{C}_i) = q \cdot N_n(Q_i).$$

Thus, determining $N_n(\mathcal{C}_i)$ is equivalent to calculate $N_n(Q_i)$. Additional details regarding this fact can be found in [1, 2, 13].

The study of the number of $\mathbb{F}_{q^n}$-rational points on Artin-Schreier's curves has attracted the attention of many authors. For instance, Wolfmann determined in [17] the number of rational points on the curve defined over $\mathbb{F}_{q^k}$, given by the equation $y^q - y = ax^s + b$, where $a \in \mathbb{F}_{q^k}^*$, $b \in \mathbb{F}_{q^k}$, k is an even special integer, and s has specific properties. Coulter, in [7], determined the number of $\mathbb{F}_q$-rational points on the curve $y^{p^n} - y = ax^{p^\alpha+1} + L(x)$, where $a \in \mathbb{F}_q^*$, $L(x)$ is a $\mathbb{F}_{p^t}$-linearized polynomial, and $t = \gcd(n, s)$ divides $d = \gcd(\alpha, s)$.

In [6], the authors determined the number of $\mathbb{F}_{q^m}$-rational points on the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$, in specific cases when h, n, m are positive integers with n dividing m, and $\gamma, a \in \mathbb{F}_{q^m}$ ($\gamma \neq 0$). In [4], they provided specific examples of maximal and minimal curves over finite fields in odd characteristic. They studied the Artin-Schreier curves of the form $y^q - y = xS(x)$, where $S(x)$ represents a $\mathbb{F}_q$-linearized polynomial, and established a connection with quadratic forms. In our prior research [5], we obtained a formula for $N_n(\mathcal{C}_i)$ when $\gcd(n,p) = 1$, using the fact that Q_i defines a quadratic form to find a connection between the number of affine rational points with the rank of an appropriate circulant matrix. This provides an explicit formula for $N_n(\mathcal{C}_i)$ when $\gcd(n,p) = 1$.

In this paper, we employ an alternative method that involves determining the solutions of the quadratic form Q_i using appropriate permutation matrices. With this approach, we compute the number $N_n(\mathcal{C}_i)$ without imposing any conditions on $\gcd(n,p)$. Additionally, we establish conditions for the Artin-Schreier curve $\mathcal{C}_i$ in order to be maximal or minimal with respect to the Hasse-Weil bound.

The second objective of this paper is to determine the number of $\mathbb{F}_{q^n}$-rational points on the affine Artin-Schreier hypersurface $\mathcal{H}_r$, which is given by the equation

$$\mathcal{H}_r : y^q - y = \sum_{j=1}^{r} a_j x_j (x_j^{q^{i_j}} - x_j) - \lambda, \tag{1}$$

where $a_j \in \mathbb{F}_q^*$ and $0 < i_j < n$ for $1 \leq j \leq r$ (see section 7.1.4 in [12]). We denote by $N_n(\mathcal{H}_r)$ the number of $\mathbb{F}_{q^n}$-rational points on the hypersurface $\mathcal{H}_r$. The well-known Weil bound assures us that

$$|N_n(\mathcal{H}_r) - q^{rn}| \leq (q-1) \prod_{j=1}^{r} q^{i_j} q^{\frac{nr}{2}} = (q-1) q^{\frac{nr+2I}{2}}, \tag{2}$$

where $I = \sum_{j=1}^{r} i_j$.

In this paper, we present necessary and sufficient conditions in order to the hypersurface $\mathcal{H}_r$ to be $\mathbb{F}_{q^n}$-maximal or $\mathbb{F}_{q^n}$-minimal, i.e. $N_n(\mathcal{H}_r)$ achieves the upper or lower bound specified in (2). Currently, in the literature is always interesting to give a description of the number of rational points for Artin-Schreier's hypersurfaces, as well as the conditions under which these hypersurfaces satisfy the bound given in (2) or other known bounds.

Using the results obtained for the curve $\mathcal{C}_i$, we can explicitly determine the number of rational points $N_n(\mathcal{H}_r)$ and to identify the conditions to achieve the maximality or minimality of this hypersurface.

The organization of this paper is as follows: Section 2 provides background material and preliminary results. In Section 3, we compute the number of $\mathbb{F}_{q^n}$-rational points on the Artin-Schreier curves $\mathcal{C}_i$ and establish necessary and sufficient conditions for these curves to be maximal or minimal. In Section 4, we determine the number of $\mathbb{F}_{q^n}$-rational points on the hypersurfaces $\mathcal{H}_r$ in (1) and derive explicit conditions for these hypersurfaces to be maximal or minimal.

2. Preliminary results

In this paper, we use the symbols ψ and $\tilde{\psi}$ to represent the canonical additive characters of $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$, respectively. The quadratic character of $\mathbb{F}_q$ is denoted as χ. The trace function Tr maps elements from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and is defined as follows:

$$\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$$
$$x \mapsto x + x^q + \cdots + x^{q^{n-1}}.$$

We set τ to represent the function $\tau = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ i & \text{if } p \equiv 3 \pmod 4. \end{cases}$

To determine the number of rational points on the curve $\mathcal{C}_i$, we associate the quadratic form $\mathrm{Tr}(x(x^{q^i} - x))$ with this curve. By fixing a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, we can provide its associated matrix and the dimension of its radical. To achieve this, we need to recall the following definitions.

Definition 2.1. *Consider a quadratic form $Q : \mathbb{F}_{q^n} \to \mathbb{F}_q$. The associated symmetric bilinear form $B : \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_q$ of Q is defined as follows*

$$B(\alpha, \beta) = \frac{1}{2}\left(Q(\alpha + \beta) - Q(\alpha) - Q(\beta)\right).$$

The radical of the quadratic form $Q : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is the $\mathbb{F}_q$-subspace defined as

$$rad(Q) = \{\alpha \in \mathbb{F}_{q^n} : B(\alpha, \beta) = 0 \text{ for all } \beta \in \mathbb{F}_{q^n}\}.$$

Furthermore, Q is considered non-degenerate if $rad(Q) = \{0\}$.

Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The $n \times n$ matrix $A = (a_{ij})$, defined as $a_{ij} = B(v_i, v_j)$, represents the associated matrix of the quadratic form Q with respect to the basis $\mathcal{B}$. Notably, the dimension of $rad(Q)$ is given by $n - \mathrm{rank}(A)$.

Consider the quadratic forms $Q_1 : \mathbb{F}_{q^m} \to \mathbb{F}_q$ and $Q_2 : \mathbb{F}_{q^n} \to \mathbb{F}_q$, where $m \geq n$. Let U and V be the associated matrices of Q_1 and Q_2, respectively. We say that Q_1 is equivalent to Q_2 if there exists $M \in \mathrm{GL}_m(\mathbb{F}_q)$ such that

$$M^T U M = \left(\begin{array}{c|c} V & 0 \\ \hline 0 & 0 \end{array}\right) \in M_m(\mathbb{F}_q),$$

where $\mathrm{GL}_m(\mathbb{F}_q)$ represents the group of invertible $m \times m$ matrices over $\mathbb{F}_q$, and $M_m(\mathbb{F}_q)$ denotes the set of $m \times m$ matrices over $\mathbb{F}_q$. Furthermore, Q_2 is said to be a *reduced form* of Q_1 if $rad(Q_2) = \{0\}$. The following theorem is a well-known result about the number of solutions of quadratic forms over finite fields.

Theorem 2.2 ([11], Theorems 6.26 and 6.27). *Let Q be a quadratic form over $\mathbb{F}_{q^n}$, where q is power of an odd prime. Let B_Q be the bilinear symmetric form associated to Q, $v = \dim(rad(B_Q))$ and $\tilde{Q}$ a reduced nondegenerate quadratic form equivalent to Q. Set $S_\alpha = |\{x \in \mathbb{F}_{q^n} | Q(x) = \alpha\}|$ and let Δ be the determinant of the quadratic form $\tilde{Q}$. Then*

(i) If $n + v$ is even

$$S_\alpha = \begin{cases} q^{n-1} + Dq^{(n+v-2)/2}(q-1) & \text{if } \alpha = 0, \\ q^{n-1} - Dq^{(n+v-2)/2} & \text{if } \alpha \neq 0, \end{cases} \tag{3}$$

where $D = \chi((-1)^{(n-v)/2}\Delta)$.

(ii) If $n + v$ is odd

$$S_\alpha = \begin{cases} q^{n-1} & \text{if } \alpha = 0, \\ q^{n-1} + Dq^{(n+v-1)/2} & \text{if } \alpha \neq 0. \end{cases} \tag{4}$$

where $D = \chi((-1)^{(n-v-1)/2}\alpha\Delta)$.

In particular $D \in \{-1, 1\}$.

We end this section with some basics definitions and results on Gauss sums.

Definition 2.3. *Let Ψ be an additive character of $\mathbb{F}_q$ and Φ a multiplicative character of $\mathbb{F}_q^*$. The Gauss sum of Ψ and Φ is defined by*

$$G(\Psi, \Phi) = \sum_{x \in \mathbb{F}_q^*} \Psi(x)\Phi(x).$$

Theorem 2.4. [11, Theorem 5.15] *Let χ be the quadratic character of $\mathbb{F}_q^*$. Then*

$$G(\tilde{\psi}, \chi) = -(-\tau)^s \sqrt{q}.$$

The following lemma establishes a connection between quadratic forms and character sums, providing valuable insights for our results. It can be derived through a straightforward computation using Theorem 2.2.

Lemma 2.5. *Let H be a $n \times n$ non null symmetric matrix over $\mathbb{F}_q$ and $l = rank(H)$. Then there exists $M \in GL_n(\mathbb{F}_q)$ such that $D = MHM^T$ is a diagonal matrix, i.e., $D = diag(a_1, a_2, \ldots, a_l, 0, \ldots, 0)$ where $a_i \in \mathbb{F}_q^*$ for all $i = 1, \ldots, l$. For the quadratic form*

$$F : \mathbb{F}_q^n \to \mathbb{F}_q, \quad F(X) = XHX^T \quad (X = (x_1, \ldots, x_n) \in \mathbb{F}_q^n),$$

it follows that

$$\sum_{X \in \mathbb{F}_q^n} \tilde{\psi}\big(F(X)\big) = (-1)^{l(s+1)} \tau^{ls} \chi(\delta) q^{n-l/2},$$

where $\delta = a_1 \cdots a_l$.

3. The curve $y^q - y = x(x^{q^i} - x) - \lambda$

In [5], we establish a formula for computing the number $N_n(\mathcal{C}_1)$ when $\gcd(n, p) = 1$. In this section, we introduce a method that enables us to compute the number $N_n(\mathcal{C}_i)$ without imposing any conditions on n and an odd prime p. Consider the basis $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and

$$B = \begin{pmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} \\ \vdots & \cdots & \ddots & \vdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} \end{pmatrix}. \tag{5}$$

We utilize the Hilbert's Theorem 90 to establish a connection between $N_n(\mathcal{C}_i)$ and the number of solutions of the equation

$$\mathrm{Tr}(\alpha(\alpha^{q^i} - \alpha)) = \mathrm{Tr}(\lambda), \tag{6}$$

where $\alpha \in \mathbb{F}_{q^n}$ and λ is a fixed element. Here, $N_n(Q_i)$ represents the number of solutions of $\mathrm{Tr}(\alpha(\alpha^{q^i} - \alpha)) = \mathrm{Tr}(\lambda)$ for $\alpha \in \mathbb{F}_{q^n}$. By Hilbert's Theorem 90, we know that

$$N_n(\mathcal{C}_i) = q N_n(Q_i).$$

The following proposition establishes a connection between $\mathrm{Tr}(x^{q^i+1} - x^2 - \lambda)$ and a quadratic form.

Proposition 3.1. *Let $f(x) = x^{q^i+1} - x^2 - \lambda$, where $\lambda \in \mathbb{F}_{q^n}$. The number of solutions of $\mathrm{Tr}(f(x)) = 0$ in $\mathbb{F}_{q^n}$ is equal to the number of solutions in $\mathbb{F}_q^n$ of the quadratic form*

$$(x_1 \ x_2 \ \cdots \ x_n) A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \mathrm{Tr}(\lambda),$$

where $A = (a_{j,l})$ is the $n \times n$ matrix defined by the relations $a_{j,l} = \frac{1}{2}\mathrm{Tr}(\beta_j^{q^i}\beta_l + \beta_l^{q^i}\beta_j - 2\beta_j\beta_l)$.

Proof. Given $x \in \mathbb{F}_{q^n}$, we can express it as $x = \sum_{j=1}^n \beta_j x_j$, where $x_1, \ldots, x_n \in \mathbb{F}_q$ are coefficients with respect to the basis $\mathcal{B}$. The equation $\mathrm{Tr}(f(x)) = 0$ is equivalent to

$$\sum_{k=0}^{n-1} f(x)^{q^k} = 0. \tag{7}$$

Expanding this expression, we obtain

$$\sum_{k=0}^{n-1} f(x)^{q^k} = \sum_{k=0}^{n-1}\Big(\sum_{j=1}^n \beta_j x_j\Big)^{q^k}\Big(\sum_{l=1}^n (\beta_l^{q^i} - \beta_l)x_l\Big)^{q^k} - \operatorname{Tr}(\lambda)$$

$$= \sum_{j,l=1}^n \Big(\sum_{k=0}^{n-1} \beta_j^{q^k}(\beta_l^{q^{i+k}} - \beta_l^{q^k})\Big)x_j x_l - \operatorname{Tr}(\lambda).$$

The relation $\displaystyle\sum_{j,l=1}^n \left(\sum_{k=0}^{n-1} \beta_j^{q^k}(\beta_l^{q^{i+k}} - \beta_l^{q^k})\right)x_j x_l = \operatorname{Tr}(\lambda)$ is obtained from (7). By symmetrizing this expression, we observe that

$$\frac{1}{2}\sum_{k=0}^{n-1} \beta_j^{q^k}\beta_l^{q^k}(\beta_l^{q^{i+k}-q^k} + \beta_j^{q^{i+k}-q^k} - 2) = \frac{1}{2}\operatorname{Tr}\big(\beta_j^{q^i}\beta_l + \beta_l^{q^i}\beta_j - 2\beta_j\beta_l\big) = a_{j,l},$$

and the result follows.   □

The matrix A in Proposition 3.1 can be expressed as

$$A = \frac{1}{2}(A_1 + A_2 - 2A_3),$$

where $A_1 = (\operatorname{Tr}(\beta_j^{q^i}\beta_l))_{j,l}$, $A_2 = (\operatorname{Tr}(\beta_j\beta_l^{q^i}))_{j,l}$ and $A_3 = (\operatorname{Tr}(\beta_j\beta_l))_{j,l}$. Let $\mathcal{P}$ be the $n \times n$ cyclic permutation matrix defined by

$$\mathcal{P} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \cdots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

and note that $\mathcal{P}^{-1} = \mathcal{P}^T$. It follows that $A_1 = B(\mathcal{P}^i)^T B^T$, $A_2 = B(\mathcal{P}^i)B^T$, and $A_3 = BB^T$, where B is defined in (5). Hence, we have $A = \frac{1}{2}BM_{n,i}B^T$, where

$$M_{n,i} = \big(\mathcal{P}^i\big)^T - 2Id + \mathcal{P}^i, \tag{8}$$

i.e., the matrix $M_{n,i} = (m_{j,l})$ is given by

$$m_{j,l} = \begin{cases} -2 & \text{if } j = l; \\ 1 & \text{if } |j - l| = i; \\ 0 & \text{otherwise,} \end{cases}$$

with the convention that the rows and columns of the matrix are indexed from 0 to $n-1$, i.e., $0 \le j, l \le n-1$.

In order to compute the number of solutions of the quadratic form defined by matrix A, we will consider an equivalent matrix obtained by using the matrix $M_{n,i}$. We will then compute the character of the determinant of this equivalent matrix. We begin by considering the case $i = 1$.

3.1. **The case $i = 1$.** The following proposition provides us a method to choose a suitable basis $\mathcal{B}$ that simplifies the calculation of $\chi(\det(A'))$, where A' is a reduced matrix of A.

Proposition 3.2. *Suppose that $p | n$. Then there exists an element $\beta \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ such that*

$$\beta^q + \beta^{q^{n-1}} - 2\beta = 0.$$

Proof. In fact, we are going to prove that there exists $\beta \in \mathbb{F}_{q^p} \subset \mathbb{F}_{q^n}$. For that, it is enough to show that the dimension of the subspace consisting of the roots of the polynomial

$$L(x) = \gcd(x^{q^p} - x, x^q + x^{q^{p-1}} - 2x)$$

is at least two. From Theorem 3.62 in [11], it suffices to show that

$$l(x) = \gcd(x^p - 1, x + x^{p-1} - 2),$$

has degree 2, because $\deg(L(x)) = q^{\deg(l(x))}$. We have

$$\deg(\gcd(x^p - 1, x + x^{p-1} - 2)) = \deg(\gcd(x^p - 1, x^2 - 2x + 1))$$
$$= \deg(\gcd((x - 1)^p, (x - 1)^2)) = 2$$

This proves the proposition.   □

According to Proposition 3.2, we can choose the basis $\mathcal{B}$ in such a way that $\beta_n = 1$ and $\beta_{n-1} = \beta$, where β satisfies

$$\beta^q + \beta^{q^{n-1}} - 2\beta = 0,$$

which is equivalent to

$$\beta^{q^2} - 2\beta^q + \beta = 0. \tag{9}$$

The above equation implies

$$(\beta^q - \beta)^q = \beta^q - \beta. \tag{10}$$

In particular, we have $\beta^q - \beta \in \mathbb{F}_q$. From now on, we fix the basis $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_{n-2}, \beta, 1\}$. The following proposition determines the rank of $M_{n,1}$ and the determinant of one of its reduced matrices.

Proposition 3.3. *The rank of the $n \times n$ matrix $M_{n,1} = \mathcal{P}^T - 2Id + \mathcal{P}$ over $\mathbb{F}_q$ is given by*

$$\text{rank } M_{n,1} = \begin{cases} n - 1 & \text{if } \gcd(n, p) = 1; \\ n - 2 & \text{if } \gcd(n, p) = p. \end{cases}$$

In addition, if $M'_{n,1}$ denotes the principal submatrix of $M_{n,1}$ constructed from the first $\text{rank}(M_{n,1})$ rows and columns, then $M'_{n,1}$ is a reduced matrix of $M_{n,1}$ and

$$\det M'_{n,1} = \begin{cases} (-1)^{n-1} n & \text{if } \gcd(n, p) = 1; \\ (-1)^{n-1} & \text{if } \gcd(n, p) = p. \end{cases}$$

Proof. Let us denote M_n as the matrix:

$$M_n = \begin{pmatrix} -2 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & -2 & 1 & \ldots & 0 & 0 & 0 \\ 0 & 1 & -2 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & -2 & 1 & 0 \\ 0 & 0 & 0 & \ldots & 1 & -2 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & -2 \end{pmatrix}.$$

We observe that $M_{n,1} = M_n + R_n$, where $R_n = (r_{i,j})$ with $r_{i,j} = \begin{cases} 1 & \text{if } (i, j) \in \{(1, n), (n, 1)\}; \\ 0 & \text{otherwise.} \end{cases}$

If we define

$$U = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 1 & 1 & 1 & \ldots & 1 & 1 \end{pmatrix}$$

then we have

$$U M_{n,1} U^T = \begin{pmatrix} -2 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & -2 & 1 & \ldots & 0 & 0 & 0 \\ 0 & 1 & -2 & \ldots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & -2 & 1 & 0 \\ 0 & 0 & 0 & \ldots & 1 & -2 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 \end{pmatrix} = \left(\begin{array}{c|c} M_{n-1} & 0 \\ \hline 0 & 0 \end{array} \right).$$

We claim that $L_{n-1} = \det(M_{n-1}) = (-1)^{n-1} n$ for $n > 1$. To prove this, we expand the determinant of M_{n-1} along the first row and obtain the recursive relation

$$L_{n-1} = -2L_{n-2} - L_{n-3} \text{ for all } n \geq 4. \tag{11}$$

This implies that the sequence $L_{n\{n\geq 2\}}$ satisfies the recurrence relation (11). Since $L_2 = 3$ and $L_3 = -4$, it follows by induction in n that $L_{n-1} = (-1)^{n-1}n$.

Furthermore, if $\gcd(n, p) = 1$, it follows that $L_{n-1} = (-1)^{n-1}n \neq 0$, which means that the rank of M_{n-1} is $n - 1$. This implies that the rank of $M_{n,1}$ is also $n - 1$.

In the case $\gcd(n, p) = p$, we define the matrix V as

$$
V = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\
1 & 2 & 3 & \cdots & n-3 & -2 & -1 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1
\end{pmatrix}.
$$

We observe that V is invertible, and by matrix operations, we have

$$
VUM_{n,1}U^TV^T = \left(\begin{array}{c|cc}
M_{n-2} & 0 & 0 \\
\hline
0\cdots 0 & 0 & 0 \\
0\cdots 0 & 0 & 0
\end{array}\right).
$$

Therefore, $L_{n-2} = (-1)^{n-2}(n-1) \neq 0$, and the rank of $M_{n,1}$ is $n - 2$. Thus, the result follows.

$\square$

Using the notation in Proposition 3.3, we can express A as follows

$$
A = \begin{cases}
\frac{1}{2}BU^{-1}\left(\begin{array}{c|c} M_{n-1} & 0 \\ \hline 0 & 0 \end{array}\right)(U^{-1})^T B^T & \text{if } \gcd(n, p) = 1; \\[3em]
\frac{1}{2}BU^{-1}V^{-1}\left(\begin{array}{c|cc} M_{n-2} & 0 & 0 \\ \hline 0\cdots 0 & 0 & 0 \\ 0\cdots 0 & 0 & 0 \end{array}\right)(V^{-1})^T(U^{-1})^T B^T & \text{if } \gcd(n, p) = p.
\end{cases}
$$

Now, we will determine the determinant of a reduced matrix of A. This requires the use of the following proposition, which tell us about the quadratic character of the determinant of BB^T.

Proposition 3.4. *Let $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_{n-2}, \beta, 1\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and B the matrix defined in (5). Then*

$$
\chi(\det(BB^T)) = \begin{cases} 1 & \text{if } n \text{ is odd;} \\ -1 & \text{if } n \text{ is even.} \end{cases}
$$

Proof. We want to determine the determinant of BB^T. The matrix BB^T can be expressed as

$$
BB^T = \begin{pmatrix}
\text{Tr}(\beta_1^2) & \text{Tr}(\beta_1\beta_2) & \cdots & \text{Tr}(\beta_1\beta_n) \\
\text{Tr}(\beta_2\beta_1) & \text{Tr}(\beta_2^2) & \cdots & \text{Tr}(\beta_2\beta_n) \\
\vdots & \cdots & \ddots & \vdots \\
\text{Tr}(\beta_n\beta_1) & \text{Tr}(\beta_n\beta_2) & \cdots & \text{Tr}(\beta_{n-1}^2)
\end{pmatrix}.
$$

Since $\text{Tr}(\beta_i\beta_j) \in \mathbb{F}_q$ for $1 \leq i, j \leq n$, we have that $BB^T \in GL_n(\mathbb{F}_q)$. It is important to note that while $BB^T \in GL(\mathbb{F}_q)$, the individual matrices B and B^T do not necessarily belong to $GL(\mathbb{F}_q)$. Hence, we cannot directly compare the quadratic character $\chi(\det(BB^T))$ with $\chi(\det(B))^2$, because the latter does not make sense if $\det(B)$ is not in $\mathbb{F}_q$. Let $\sigma : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$ be the Frobenius map, that is $\sigma(\alpha) = \alpha^q$, and let $B = (c_{i,j})$ with $1 \leq i, j \leq n$, where

$c_{i,j} = \beta_i^{q^{j-1}}$. We have

$$\det(B) = \sum_{\tau \in S_n} (-1)^{\text{sign}(\tau)} c_{1\tau(1)} \cdots c_{n\tau(n)}$$

$$= \sum_{\tau \in S_n} (-1)^{\text{sign}(\tau)} \beta_1^{q^{\tau(1)-1}} \cdots \beta_n^{q^{\tau(n)-1}}$$

Then

$$\sigma(\det(B)) = \sum_{\tau \in S_n} (-1)^{\text{sign}(\tau)} \beta_1^{q^{\tau(1)}} \cdots \beta_n^{q^{\tau(n)}}$$

$$= \sum_{\tau \in S_n} (-1)^{\text{sign}(\tau)} \beta_1^{q^{\rho(\tau(1))-1}} \cdots \beta_n^{q^{\rho(\tau(n))-1}}$$

$$= (-1)^{\text{sign}(\rho)} \det(B)$$

where ρ^{-1} is the permutation $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \end{pmatrix}$. Since

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \end{pmatrix} = (1\,n)(1\,n-1)\cdots(1\,3)(1\,2),$$

we have that $(-1)^{\text{sign}(\rho)} = (-1)^{n-1}$. Therefore, $\det(B) \in \mathbb{F}_q$ if and only if n is odd. In conclusion

$$\chi(\det(BB^T)) = \begin{cases} 1 & \text{if } n \text{ is odd;} \\ -1 & \text{if } n \text{ is even.} \end{cases}$$

$\square$

Proposition 3.5. *The rank of the $n \times n$ matrix A over $\mathbb{F}_q$ is given by*

$$rank\ A = \begin{cases} n-1 & \text{if } \gcd(n,p) = 1; \\ n-2 & \text{if } \gcd(n,p) = p, \end{cases}$$

and a reduced matrix of A is given by $A' = \frac{1}{2} \begin{cases} B_{11} M_{n-1} B_{11}^T & \text{if } \gcd(n,p) = 1; \\ \tilde{B}_{11} M_{n-2} \tilde{B}_{11}^T & \text{if } \gcd(n,p) = p, \end{cases}$ *where the matrices $B_{11} = (b_{l,k})$ and $\tilde{B}_{11} = (\tilde{b}_{l,k})$ are given by*

$$b_{l,k} = \beta_l^{q^{k-1}} - \beta_l^{q^{n-1}} \quad \text{for} \quad 1 \le l, k \le n-1$$

and

$$\tilde{b}'_{l,k} = \beta_l^{q^{k-1}} + k\beta_l^{q^{n-2}} - (k+1)\beta_l^{q^{n-1}} \quad \text{for } 1 \le l, k \le n-2.$$

In addition,

$$\chi(\det A') = \begin{cases} (-1)^{n-1} \cdot \chi((-2)^{n-1}n) & \text{if } \gcd(n,p) = 1; \\ (-1)^{n-1}\chi\left((-1)^{n-1}2^{n-2}\right) & \text{if } \gcd(n,p) = p. \end{cases}$$

Proof. We will divide the proof into two cases, based on the value of $\gcd(n,p)$, using the notation introduced in the proof of Proposition 3.3 for the matrices M_n, U, and V.

(1) If $\gcd(n,p) = 1$. In this case, we have that

$$A = \frac{1}{2} BU^{-1} \left(\begin{array}{c|c} M_{n-1} & 0 \\ \hline 0 & 0 \end{array} \right) (U^{-1})^T B^T$$

and

$$
BU^{-1} = \begin{pmatrix}
\beta_1 - \beta_1^{q^{n-1}} & \beta_1^q - \beta_1^{q^{n-1}} & \cdots & \beta_1^{q^{n-2}} - \beta_1^{q^{n-1}} & \beta_1^{q^{n-1}} \\
\beta_2 - \beta_2^{q^{n-1}} & \beta_2^q - \beta_2^{q^{n-1}} & \cdots & \beta_2^{q^{n-2}} - \beta_2^{q^{n-1}} & \beta_2^{q^{n-1}} \\
\vdots & \cdots & \ddots & \cdots & \vdots \\
\beta - \beta^{q^{n-1}} & \beta^q - \beta^{q^{n-1}} & \cdots & \beta^{q^{n-2}} - \beta^{q^{n-1}} & \beta^{q^{n-1}} \\
0 & 0 & \cdots & 0 & 1
\end{pmatrix}
$$

$$
= \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & 1 \end{pmatrix}, \tag{12}
$$

where $B_{12} = \begin{pmatrix} \beta_1^{q^{n-1}} \\ \beta_2^{q^{n-1}} \\ \vdots \\ \beta^{q^{n-1}} \end{pmatrix}$ and $B_{21} = \begin{pmatrix} 0 & 0 & \cdots & 0 \end{pmatrix}$. From (12), it follows that

$\det(BU^{-1}) = \det(B_{11})$ and we have that

$$
\chi\left(\det(B_{11} M_{n-1} B_{11}^T)\right) = \chi(\det(BB^T)\det(M_{n-1}))
$$

$$
= (-1)^{n-1} \cdot \chi((-1)^{n-1} n) \tag{13}
$$

Since

$$
A = \frac{1}{2} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & \beta_n^{q^{n-1}} \end{pmatrix} \begin{pmatrix} M_{n-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} B_{11}^T & B_{21}^T \\ B_{12}^T & \beta_n^{q^{n-1}} \end{pmatrix}
$$

$$
= \frac{1}{2} \begin{pmatrix} B_{11} M_{n-1} B_{11}^T & 0 \\ 0 & 0 \end{pmatrix},
$$

it follows that A has $\frac{1}{2} B_{11} M_{n-1} B_{11}^T$ as a reduced matrix. Additionally, we have

$$
\chi(\det(B_{11} M_{n-1} B_{11}^T) = (-1)^{n-1} \cdot \chi((-2)^{n-1} n),
$$

where the last step follows from (13).

(2) If $\gcd(n, p) = p$, we have the expression for the matrix A as follows

$$
A = \frac{1}{2} BU^{-1} V^{-1} \left(\begin{array}{c|cc} M_{n-2} & 0 & 0 \\ \hline 0 \cdots 0 & 0 & 0 \\ 0 \cdots 0 & 0 & 0 \end{array} \right) (V^{-1})^T (U^{-1})^T B^T,
$$

where the matrices $U^{-1} V^{-1}$ and $BU^{-1} V^{-1}$ are given by

$$
U^{-1} V^{-1} = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\
1 & 2 & 3 & \cdots & -3 & -2 & -1 & 0 \\
-2 & -3 & -4 & \cdots & -(n-2) & 1 & 1 & 1
\end{pmatrix}
$$

and $BU^{-1} V^{-1} = (b_{l,k})$ where

$$
b_{l,k} = \begin{cases}
\beta_l^{q^{k-1}} + k\beta_l^{q^{n-2}} - (k+1)\beta_l^{q^{n-1}} & \text{if } 1 \le l \le n, 1 \le k \le n-2; \\
-\beta_l^{q^{n-2}} + \beta_l^{q^{n-1}} & \text{if } 1 \le l \le n, k = n-1; \\
\beta_l^{q^{n-1}} & \text{if } 1 \le l \le n, k = n.
\end{cases}
$$

We observe that the only non-zero entry in the last row is $b_{n,n} = 1$. In order to determine the entries in the $(n-1)$-th row, we need the following result.

Claim: $\beta^{q^l} = l\beta^q - (l-1)\beta$, for $l \ge 2$.

We will prove this by induction. For $l = 2$, the result follows from (9). Let us assume that the claim is true for some $k \geq 2$. Then, for $l = k + 1$, we have:

$$\beta^{q^{k+1}} = (\beta^{q^k})^q = (k\beta^q - (k-1)\beta)^q$$
$$= k\beta^{q^2} - (k-1)\beta^q$$
$$= 2k\beta^q - k\beta - (k-1)\beta^q$$
$$= (k+1)\beta^q - k\beta,$$

Thus, the claim holds for $l = k + 1$, completing the induction step and proving the claim.

From this relation, we can prove that the only entries non-null of the $(n-1)$-th row of the matrix $BU^{-1}V^{-1}$ are $b_{n-1,n-1}$ and $b_{n-1,n}$. In fact, using that $\gcd(n, p) = p$, we have that

$$\beta^{q^{n-2}} = (n-2)\beta^q - (n-3)\beta = -2\beta^q + 3\beta$$

and

$$\beta^{q^{n-1}} = (n-1)\beta^q - (n-2)\beta = -\beta^q + 2\beta.$$

Therefore the entries $b_{n-1,k}$ for $1 \leq k \leq n-2$ are given by

$$b_{n-1,k} = \beta^{q^{k-1}} + l\beta^{q^{n-2}} - (k+1)\beta^{q^{n-1}}$$
$$= (k-1)\beta^q - (k-2)\beta + k(-2\beta^q + 3\beta) - (k+1)(-\beta^q + 2\beta)$$
$$= 0,$$

and the entry $b_{n-1,n-2}$ is

$$b_{n-1,n-1} = -\beta^{q^{n-2}} + \beta^{q^{n-1}}$$
$$= 2\beta^q - 3\beta - \beta^q + 2\beta$$
$$= \beta^q - \beta.$$

Consequently

$$b_{n-1,k} = \begin{cases} 0 & \text{if } 1 \leq k \leq n-2; \\ \beta^q - \beta & \text{if } k = n-1; \\ \beta & \text{if } k = n, \end{cases}$$

and we obtain that

$$A = \frac{1}{2}BU^{-1}V^{-1}\left(\begin{array}{c|cc} M_{n-2} & 0 & 0 \\ \hline 0\cdots 0 & 0 & 0 \\ 0\cdots 0 & 0 & 0 \end{array}\right)(V^{-1})^T(U^{-1})^T B^T$$

$$= \frac{1}{2}\left(\begin{array}{c|cc} \tilde{B}_{11} & \tilde{B}_{12} & \\ \hline \tilde{B}_{21} & \beta^q - \beta & \beta \\ & 0 & 1 \end{array}\right)\left(\begin{array}{c|cc} M_{n-2} & 0 & 0 \\ \hline 0\cdots 0 & 0 & 0 \\ 0\cdots 0 & 0 & 0 \end{array}\right)\left(\begin{array}{c|cc} \tilde{B}_{11}^T & \tilde{B}_{21}^T & \\ \hline \tilde{B}_{12}^T & \beta^q - \beta & \beta \\ & 0 & 1 \end{array}\right)$$

$$= \frac{1}{2}\left(\begin{array}{c|cc} \tilde{B}_{11}M_{n-2}\tilde{B}_{11}^T & 0 & 0 \\ & \vdots & \vdots \\ & 0 & 0 \\ \hline 0\cdots 0 & 0 & 0 \\ 0\cdots 0 & 0 & 0 \end{array}\right),$$

where $(\tilde{B}_{12})^T = \begin{pmatrix} \beta_1^{q^{n-1}} - \beta_1^{q^{n-2}} & \beta_1^{q^{n-1}} \\ \vdots & \vdots \\ \beta_{n-2}^{q^{n-1}} - \beta_{n-2}^{q^{n-2}} & \beta_{n-2}^{q^{n-1}} \end{pmatrix}$ and $\tilde{B}_{21} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}$. This

implies that

$$\chi(\det(\tilde{B}_{11})) = \chi\left(\frac{1}{\beta^q - \beta} \det\left(\begin{array}{c|cc} \tilde{B}_{11} & * & * \\ \hline 0 & \beta^q - \beta & \beta \\ 0 & 0 & 1 \end{array}\right)\right)$$

$$= \chi\left(\frac{1}{\beta^q - \beta} \det(BU^{-1}V^{-1})\right)$$

$$= \chi\left(\frac{-1}{\beta^q - \beta} \det(B)\right).$$

From the previous analysis, we can conclude that a reduced matrix of A is given by $\tilde{B}_{11} M_{n-2} \tilde{B}_{11}^T$, which has a rank of $n-2$. We can now evaluate the quadratic character of the determinant of this matrix, i.e.,

$$\chi\left(\det\left(\tilde{B}_{11} M_{n-2} \tilde{B}_{11}^T\right)\right) = \chi\left(\left(\frac{1}{\beta^q - \beta}\right)^2 \det(BB^T) \det(M_{n-2})\right)$$

$$= (-1)^{n-1} \chi\left((-1)^{n-1}\right),$$

where we use Propositions 3.3 and 3.4. Therefore, the proposition is proven. $\qquad\square$

The following definition will be useful to determine $N_n(\mathcal{C}_i)$.

Definition 3.6. *For each $\alpha \in \mathbb{F}_q$ we define*

$$\varepsilon_\alpha = \begin{cases} q-1 & \text{if } \alpha = 0; \\ -1 & \text{otherwise.} \end{cases}$$

From Theorem 2.2 and Proposition 3.5 we have the following theorem.

Theorem 3.7. *Let $\lambda \in \mathbb{F}_{q^n}$ and n a positive integer. The number $N_n(\mathcal{C}_1)$ of affine rational points in $\mathbb{F}_{q^n}^2$ of the curve determined by the equation $y^q - y = x^{q+1} - x^2 - \lambda$ is*

$$N_n(\mathcal{C}_1) = \begin{cases} q^n - \chi(2(-1)^{\frac{n}{2}} n \operatorname{Tr}(\lambda)) q^{(n+2)/2} & \text{if } \gcd(n,p) = 1 \text{ and } n \text{ is even;} \\ q^n + \varepsilon_{\operatorname{Tr}(\lambda)} \chi((-1)^{(n-1)/2} n) q^{(n+1)/2} & \text{if } \gcd(n,p) = 1 \text{ and } n \text{ is odd;} \\ q^n - \varepsilon_{\operatorname{Tr}(\lambda)} \chi((-1)^{n/2}) q^{(n+2)/2} & \text{if } \gcd(n,p) = p \text{ and } n \text{ is even;} \\ q^n + \chi(2(-1)^{\frac{n-3}{2}} \operatorname{Tr}(\lambda)) q^{(n+3)/2} & \text{if } \gcd(n,p) = p \text{ and } n \text{ is odd.} \end{cases}$$

This theorem allows us to determine when $\mathcal{C}_1$ is minimal or maximal with respect the Hasse-Weil bound, as we show in the following corollary.

Theorem 3.8. *Consider the curve $\mathcal{C}_1$ given by*

$$\mathcal{C}_1 : y^q - y = x^{q+1} - x^2 - \lambda.$$

Then $\mathcal{C}_1$ is minimal in $\mathbb{F}_{q^n}$ if and only if one of the following holds:
a) $\operatorname{Tr}(\lambda) = 0$, $2p$ divides n and $q \equiv 1 \pmod 4$;
b) $\operatorname{Tr}(\lambda) = 0$, $4p$ divides n and $q \equiv 3 \pmod 4$.
Moreover, $\mathcal{C}_1$ is maximal in $\mathbb{F}_{q^n}$ if and only if $\operatorname{Tr}(\lambda) = 0$, $2p$ divides n, 4 does not divide n and $q \equiv 3 \pmod 4$.

Proof. The result follows from Theorem 3.7 and the fact that the genus of $\mathcal{C}_1$ is $g = \frac{q(q-1)}{2}$. $\square$

3.2. **The curve** $y^q - y = x(x^{q^i} - x) - \lambda$ **with** $i \geq 1$. The following proposition provides information about the rank of the matrices $M_{n,i}$ and the quadratic character of the determinant of one of its reduced matrices.

Proposition 3.9. *Let* i, n *be integers such that* $0 < i < n$ *and* $M_{n,i}$ *as defined in* (8). *Set* $d = \gcd(i,n)$ *and* $l = \frac{n}{d}$. *The rank of the* $n \times n$ *matrix* $M_{n,i}$ *is*

$$\text{rank } M_{n,i} = \begin{cases} n - d & \text{if } \gcd(l,p) = 1; \\ n - 2d & \text{if } \gcd(l,p) = p. \end{cases}$$

In addition, the matrices

$$\tilde{M}_{n,i} = \begin{pmatrix} M_{l,1} & 0 & 0 & 0 \\ 0 & M_{l,1} & 0 & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & 0 & M_{l,1} \end{pmatrix} \quad \text{and} \quad \tilde{M}'_{n,i} = \begin{pmatrix} M'_{l,1} & 0 & 0 & 0 \\ 0 & M'_{l,1} & 0 & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & 0 & M'_{l,1} \end{pmatrix} \quad (14)$$

are an equivalent matrix and a reduced matrix of $M_{n,i}$, *respectively, where* $M'_{l,1}$ *is as the matrix given in Proposition 3.3.*

The determinant of the matrix $\tilde{M}_{n,i}$ *is* $(-1)^i 2^i$ *if* $n = 2i$ *and, otherwise we have that*

$$\det \tilde{M}'_{n,i} = \begin{cases} (-1)^{n-d} l^d & \text{if } \gcd(l,p) = 1; \\ (-1)^n & \text{if } \gcd(l,p) = p. \end{cases}$$

Proof. For convenience, let us enumerate the rows and columns of the matrix $M_{n,i}$ from 0 to $n-1$. Suppose that n is even and $i = \frac{n}{2}$. In this case, the matrix $M_{n,i}$ can be expressed as follows

$$a_{k,l} = \begin{cases} -2 & \text{if } k = l, \\ 2 & \text{if } k - l \equiv 0 \pmod{\frac{n}{2}}, \\ 0 & \text{otherwise.} \end{cases}$$

Let us denote $D_{\frac{n}{2}} = 2 \cdot \text{Id}_{\frac{n}{2}}$, where $\text{Id}_{\frac{n}{2}}$ is the $\frac{n}{2} \times \frac{n}{2}$ identity matrix. It follows that

$$M_{n,n/2} = \left(\begin{array}{c|c} -D_{n/2} & D_{n/2} \\ \hline D_{n/2} & -D_{n/2} \end{array} \right) \text{ that is equivalent to } \left(\begin{array}{c|c} -D_{n/2} & 0 \\ \hline 0 & 0 \end{array} \right).$$

Therefore

$$\text{rank } M_{n,\frac{n}{2}} = \frac{n}{2} = i \quad \text{and} \quad \det \tilde{M}'_{n,\frac{n}{2}} = (-2)^{\frac{n}{2}} = (-2)^i \neq 0.$$

This completes the proof for the case $n = 2i$. For the remaining cases, we will first establish that it suffices to consider the case where $i = d$. Subsequently, we will construct a block diagonal matrix consisting of d matrices of the form $M_{l,1}$, where $n = ld$.

We observe that any permutation $\rho : \mathbb{Z}_n \to \mathbb{Z}_n$ induces a natural action on $\mathbb{F}_q^n$ through the following map:

$$\rho : \quad \begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ (v_0, \ldots, v_{n-1}) & \mapsto & (v_{\rho(0)}, \ldots, v_{\rho(n-1)}). \end{array}$$

This action is associated with an invertible matrix M_ρ defined by

$$M_\rho \begin{pmatrix} v_0 \\ \vdots \\ v_{n-1} \end{pmatrix} = \begin{pmatrix} v_{\rho(0)} \\ \vdots \\ v_{\rho(n-1)} \end{pmatrix}.$$

Conversely, for any permutation matrix R, there exists a permutation $\rho' : \mathbb{Z}_n \to \mathbb{Z}_n$ such that $M_{\rho'} = R$. In particular, we observe that the map $\mathcal{P}^i$ determines the permutation

$$\begin{array}{rccc} \pi_i : & \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & z & \mapsto & z + i. \end{array}$$

Consider the map

$$\delta : \mathbb{Z}_n \to \mathbb{Z}_n$$
$$a \mapsto ai$$

where $a \in \mathbb{Z}_n$ is an element satisfying $\gcd(a, n) = 1$. Since a and n are coprime, δ is a permutation. Furthermore, δ induces a matrix M_σ, and the matrix $M_\sigma \mathcal{P}^i M_\sigma^{-1}$ corresponds to a permutation of $\mathbb{Z}_n$ given by

$$\begin{aligned} \delta \circ \pi_i \circ \delta^{-1}(z) &= \delta(\pi_i(\delta^{-1}(z))) \\ &= \delta(\pi_i(a^{-1}z)) \\ &= \delta(a^{-1}z + i) \\ &= z + ai. \end{aligned}$$

We know that the congruence $ai \equiv u \pmod{n}$ has a solution if and only if d divides u. Since $d = \gcd(i, n)$, there exists $a \in \mathbb{Z}_n$ such that $\delta \circ \pi_i \circ \delta^{-1}(z) = z + \gcd(i, n)$. Therefore, we can replace i with d without loss of generality. For each $z \in \mathbb{Z}_n$, by the Euclidean Division Algorithm, there exist unique integers r and s such that $0 \leq s \leq l - 1$ and $0 \leq r \leq d - 1$ satisfying $z = sd + r$. Let us consider the map

$$\begin{array}{rccc} \varphi : & \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & sd + r & \mapsto & s + lr. \end{array} \tag{15}$$

Claim: The map φ is a permutation of the elements of $\mathbb{Z}_n$. Let us suppose that there exist distinct elements z_1 and z_2 in $\mathbb{Z}_n$ such that $\varphi(z_1) = \varphi(z_2)$. By the Euclidean Division, there exist $0 \leq s_1, s_2 \leq l - 1$ and $0 \leq r_1, r_2 \leq d - 1$ with $z_1 = s_1 d + r_1$ and $z_2 = s_2 d + r_2$. Then we have

$$\varphi(s_1 d + r_1) = \varphi(s_2 d + r_2) \Leftrightarrow s_1 + lr_1 = s_2 + lr_2 \Leftrightarrow s_1 - s_2 = l(r_2 - r_1).$$

Since $0 \leq s_1, s_2 \leq l - 1$, the above equation implies that $s_1 = s_2 = 0$ and $r_1 = r_2 = 0$. However, this contradicts the fact that $z_1 \neq z_2$. Therefore, φ is a permutation.

We will utilize the permutation φ to rearrange the rows and columns of $\mathcal{P}^d - 2Id + \left(\mathcal{P}^d\right)^T$ and obtain the block diagonal matrix $\tilde{M}_{n,i}$ with d blocks. Applying the permutation φ to this matrix, we obtain the permuted matrix $\varphi(\mathcal{P}^d - 2Id + \left(\mathcal{P}^d\right)^T)$.

Let us observe that $\varphi \circ \pi_d \circ \varphi^{-1}$ defines a permutation $\theta : \mathbb{Z}_n \to \mathbb{Z}_n$ given by

$$\begin{aligned} \theta(z) = \varphi \circ \pi_d \circ \varphi^{-1}(z) &= \varphi \circ \pi_d(\varphi^{-1}(s + rl)) \\ &= \varphi \circ \pi_d(sd + r) \\ &= \varphi((s + 1)d + r) \\ &= (s + 1) + rl, \end{aligned}$$

where $z = sl + r$ with $0 \leq s \leq l - 1$ and $0 \leq r \leq d - 1$. We obtain that

$$M_\varphi \left(\left(\mathcal{P}^d\right)^T - 2Id + \mathcal{P}^d \right) M_\varphi^{-1} = \tilde{M}_{n,d}.$$

In fact, the product of the permutation matrix M_φ for $\left(\mathcal{P}^d\right)^T - 2Id + \mathcal{P}^d$ and M_φ^{-1} maps the nonzero entries of $M_{n,d}$ to the nonzero entries of $\tilde{M}_{n,d}$. In the case when $k = j$, writing $k = s + rl$ with $0 \leq s \leq l - 1$ and $0 \leq r \leq d - 1$, we have

$$\theta(a_{k,k}) = a_{(s+1)+rl,(s+1)+rl} = a_{\theta(k),\theta(k)},$$

which implies that the new matrix will have $a_{k,k} = -2$. If $a_{k,k+d} = 1$, with $k = s + rl$ and $0 \le s \le l - 1$, we have

$$\theta(a_{k,k+d}) = a_{(s+1)+rl,(s+2)+rl} = a_{\theta(k),\theta(k+d)},$$

which implies that $a_{k,k+1} = 1$ when considering the indices modulo l. The same procedure applies to $a_{k+d,k}$, as it is the transpose of $a_{k,k+d}$. The other entries are zero and their images are also zero. Therefore, we obtain the matrix in (14).

Using Proposition 3.3 and the fact that the matrix $\tilde{M}_{n,i}$ is a block diagonal matrix with d blocks equal to the matrix $M_{l,1}$, we can determine the rank of $M_{n,i}$ and the determinant of the reduced matrix $\tilde{M}'_{n,i}$. In conclusion, we obtain that

$$\text{rank } M_{n,i} = \begin{cases} (l-1)d = n - d & \text{if } \gcd(l,p) = 1; \\ (l-2)d = n - 2d & \text{if } \gcd(l,p) = p, \end{cases}$$

and

$$\det \tilde{M}'_{n,i} = \begin{cases} \left((-1)^{l-1}l\right)^d = (-1)^{n-d}l^d & \text{if } \gcd(l,p) = 1; \\ \left((-1)^{l-1}\right)^d = (-1)^{n-d} & \text{if } \gcd(l,p) = p. \end{cases}$$

$\square$

From Proposition 3.1, we know that the matrix associated with the quadratic form $\text{Tr}(x(x^{q^i} - x))$ is given by

$$A = \frac{1}{2}B((\mathcal{P}^i)^T - 2Id + \mathcal{P}^i)B^T = \frac{1}{2}BM_{n,i}B^T$$

where B is defined in (5). By applying Propositions 3.5 and 3.9, we obtain the following result.

Corollary 3.10. *Let i be an integer such that $0 < i < n$. Set $d = \gcd(i,n)$ and $l = \frac{n}{d}$. The rank of the $n \times n$ matrix $A = \frac{a}{2}B((\mathcal{P}^i)^T - 2Id + \mathcal{P}^i)B^T$, where $a \in \mathbb{F}_{q^n}^*$, is given by*

$$\text{rank } A = \begin{cases} n - d & \text{if } \gcd(l,p) = 1; \\ n - 2d & \text{if } \gcd(l,p) = p. \end{cases}$$

Let A' be a reduced matrix of A. Then

$$\chi(\det(A')) = \begin{cases} (-1)^{n-d}\chi((-2a)^{n-d}l^d) & \text{if } \gcd(l,p) = 1; \\ (-1)^{n-d}\chi((-a)^{n-d}2^n) & \text{if } \gcd(l,p) = p. \end{cases}$$

Proof. Let suppose that $\gcd(l,p) = 1$, because step for the other case is essentially the same. The result follows from

$$\det(A') = \det\left(\frac{a}{2}\tilde{M}_{l,1}\right)^d \det(BB^T),$$

and

$$\chi(\det(A')) = \chi\left((2a)^{ld-d}\det(\tilde{M}_{l,1})^d\right)\chi(\det(BB^T)).$$

By applying Propositions 3.5 and 3.9, we obtain the result. $\square$

By Theorem 2.2 and Propositions 3.1 and 3.9 we have the following theorem.

Theorem 3.11. *Let n, i be integers such that $0 < i < n$ and put $d = \gcd(i,n)$ and $l = \frac{n}{d}$. If $n = 2i$, the number $N_n(\mathcal{C}_i)$ of affine rational points in $\mathbb{F}_{q^n}^2$ of the curve determined by the equation $y^q - y = x^{q^i+1} - x^2 - \lambda$ is*

$$N_n(\mathcal{C}_i) = \begin{cases} q^n - \chi((-1)^{(i+1)/2}\text{Tr}(\lambda))q^{(3i+1)/2} & \text{if } i \text{ is odd;} \\ q^n + \varepsilon_{\text{Tr}(\lambda)}\chi((-1)^{i/2})q^{3i/2} & \text{if } i \text{ is even.} \end{cases}$$

If $n \neq 2i$, the number of affine rational points of $\mathcal{C}_i$ is

$$N_n(\mathcal{C}_i) = \begin{cases} q^n - \chi(2(-1)^{(n-d+1)/2}\mathrm{Tr}(\lambda)l^d)q^{(n+d+1)/2} & \text{if } \gcd(l,p) = 1 \text{ and } n+d \text{ is odd;} \\ q^n + \varepsilon_{\mathrm{Tr}(\lambda)}\chi((-1)^{(n-d)/2}l^d)q^{(n+d)/2} & \text{if } \gcd(l,p) = 1 \text{ and } n+d \text{ is even;} \\ q^n - (-1)^d\chi(2(-1)^{(n+1)/2}\mathrm{Tr}(\lambda))q^{(n+2d+1)/2} & \text{if } \gcd(l,p) = p \text{ and } n \text{ is odd;} \\ q^n + (-1)^d\varepsilon_{\mathrm{Tr}(\lambda)}\chi((-1)^{n/2})q^{(n+2d)/2} & \text{if } \gcd(l,p) = p \text{ and } n \text{ is even.} \end{cases}$$

Remark 3.12. *The curve $\mathcal{C}_i$ has genus $g = \frac{(q-1)q^i}{2}$. The Hasse-Weil bound of $\mathcal{C}_i$ is given by*

$$|N_n(\mathcal{C}_i) - q^n| \leq (q-1)q^{\frac{n+2i}{2}}.$$

Using Theorem 3.11, we can determine the conditions when the curve $\mathcal{C}_i$ is maximal (or minimal) with respect the Hasse-Weil bound.

Theorem 3.13. *Let n, i be integers such that $0 < i < n$, set $d = \gcd(i,n)$ and $l = \frac{n}{d}$ and $n \neq 2i$. The curve*

$$\mathcal{C}_i : y^q - y = x(x^{q^i} - x) - \lambda$$

is maximal in $\mathbb{F}_{q^n}$ if and only if $\mathrm{Tr}(\lambda) = 0$, n is even p divides l, i divides n, $n \neq 2i$ and $(-1)^d\chi((-1)^{n/2}) = 1$. The curve $\mathcal{C}_i$ is minimal in $\mathbb{F}_{q^n}$ if and only if $\mathrm{Tr}(\lambda) = 0$, n is even, p divides l, i divides n, $n \neq 2i$ and $(-1)^d\chi((-1)^{n/2}) = -1$.

4. THE NUMBER OF AFFINE RATIONAL POINTS OF THE HYPERSUFARCE
$$y^q - y = \sum_{j=1}^{r} a_j x_j(x_j^{q^{i_j}} - x_j) - \lambda$$

Using the results derived in the previous section, we can now determine the number of affine rational points of Artin-Schreier's hypersurface $\mathcal{H}_r$ defined by the equation:

$$\mathcal{H}_r : y^q - y = \sum_{j=1}^{r} a_j x_j(x_j^{q^{i_j}} - x_j) - \lambda,$$

where $a_j \in \mathbb{F}_q^*$ and $0 < i_j < n$ for $j \in \{1, \ldots, r\}$. According to Theorem 5.4 in [11], we have the following result for a character ψ of $\mathbb{F}_{q^n}$

$$\sum_{c \in \mathbb{F}_{q^n}} \psi(uc) = \begin{cases} 0 & \text{if } u \neq 0; \\ q^n & \text{if } u = 0. \end{cases}$$

Using this result we can compute the number $N_n(\mathcal{H}_r)$ as follows

$$q^n N_n(\mathcal{H}_r) = \sum_{c \in \mathbb{F}_{q^n}} \sum_{x_1 \in \mathbb{F}_{q^n}} \cdots \sum_{x_r \in \mathbb{F}_{q^n}} \sum_{y \in \mathbb{F}_{q^n}} \psi\left(c\left(\sum_{j=1}^{r} a_j x_j(x_j^{q^{i_j}} - x_j) - y^q + y - \lambda\right)\right)$$

$$= q^{(r+1)n} + \sum_{c \in \mathbb{F}_{q^n}^*} \sum_{x_1 \in \mathbb{F}_{q^n}} \cdots \sum_{x_r \in \mathbb{F}_{q^n}} \psi\left(c\left(\sum_{i=1}^{r} a_j x_j(x_j^{q^{i_j}} - x_j) - \lambda\right)\right) \sum_{y \in \mathbb{F}_{q^n}} \psi\left(c(-y^q + y)\right)$$

$$= q^{(r+1)n} + \sum_{c \in \mathbb{F}_{q^n}^*} \psi(-c\lambda) \prod_{j=1}^{r} \sum_{x_j \in \mathbb{F}_{q^n}} \psi\left(c\left(a_j x_j(x_j^{q^{i_j}} - x_j)\right)\right) \sum_{y \in \mathbb{F}_{q^n}} \psi\left(c(-y^q + y)\right)$$

$$= q^{(r+1)n} + \sum_{c \in \mathbb{F}_{q^n}^*} \psi(-c\lambda) \prod_{j=1}^{r} \sum_{x_j \in \mathbb{F}_{q^n}} \psi\left(c\left(a_j x_j(x_j^{q^{i_j}} - x_j)\right)\right) \sum_{y \in \mathbb{F}_{q^n}} \psi\left(y\left(-c^{q^{n-1}} + c\right)\right).$$

$$(16)$$

We observe that

$$\sum_{y\in\mathbb{F}_{q^n}} \psi\left(y\left(-c^{q^{n-1}}+c\right)\right) = \begin{cases} q^n & \text{if } c^{q^{n-1}}-c=0; \\ 0 & \text{otherwise.} \end{cases}$$

Since $c^{q^{n-1}}-c=0$ if and only if $c\in\mathbb{F}_{q^{n-1}}$, we can conclude that the inner sum in (16) has non-null terms only if $c\in\mathbb{F}_q$. From the theory of characters over finite fields, we have that $\psi(-c\lambda)=\tilde{\psi}(\text{Tr}(-c\lambda))=\tilde{\psi}(-c\text{Tr}(\lambda))$ (see [11] equation (5.7) in page 191), therefore, we have that

$$N_n(\mathcal{H}_r) = q^{rn} + \sum_{c\in\mathbb{F}_q^*} \tilde{\psi}(-c\text{Tr}(\lambda)) \prod_{j=1}^{r} \sum_{x_j\in\mathbb{F}_{q^n}} \psi\left(ca_j\left(x_j(x_j^{q^{i_j}}-x_j)\right)\right). \qquad (17)$$

The following theorem gives explicit formulas for $N_n(\mathcal{H}_r)$.

Theorem 4.1. *Let $i_1,\ldots,i_r$ be positive integers such that $0 < i_j < n$. We define $d_j = \gcd(i_j,n)$ and $l_j = \frac{n}{d_j}$. Let $X = \{l_1,\ldots,l_{\tilde{r}}\}$ and $Y = \{l_{\tilde{r}+1},\ldots,l_r\}$, where $\gcd(l_k,p) = 1$ for $l_k\in X$ and $\gcd(l_k,p) = p$ for $l_k\in Y$.*

Let $\mathcal{H}_r$ be the hypersurface given by the expression

$$y^q - y = \sum_{j=1}^{r} a_j x_j(x_j^{q^{i_j}}-x_j) - \lambda,$$

where $\lambda\in\mathbb{F}_{q^n}$ and $a_j\in\mathbb{F}_q$. Let us define

$$D_1 = \sum_{j=1}^{\tilde{r}} d_j, \quad D_2 = \sum_{j=\tilde{r}+1}^{r} d_j, \quad L_1 = \prod_{j=1}^{\tilde{r}} l_j^{d_j}. \quad A_1 = \prod_{j=1}^{\tilde{r}} a_j^{n-d_j} \quad \text{and} \quad A_2 = \prod_{\tilde{r}}^{r} a_j^n.$$

Let $A = A_1 A_2$. In the case $X = \varnothing$ we set $L_1 = 1$, $A_1 = 1$, and in the case $Y = \varnothing$ we set $A_2 = 1$. The number $N_n(\mathcal{H}_r)$ of affine rational points of $\mathcal{H}_r$ in $\mathbb{F}_q^{r+1}$ is given by

$$N_n(\mathcal{H}_r) = \begin{cases} q^{rn} + (-1)^{D_2}\tau^{s(nr-D_1-2D_2)}\chi((-1)^{D_2}AL_1)\varepsilon_{\text{Tr}(\lambda)}q^{\frac{nr+D_1+2D_2}{2}} & \text{if } nr-D_1 \text{ is even;} \\ q^{rn} + (-1)^{D_2+1}\tau^{s(nr-D_1-2D_2+1)}\chi(2(-1)^{D_2}AL_1\text{Tr}(\lambda))q^{\frac{nr+D_1+2D_2+1}{2}} & \text{if } nr-D_1 \text{ is odd.} \end{cases}$$

Proof. From (17) we obtain that

$$N_n(\mathcal{H}_r) = q^{rn} + \sum_{c\in\mathbb{F}_q^*} \tilde{\psi}(-c\text{Tr}(\lambda)) \prod_{j=1}^{r} \sum_{x_j\in\mathbb{F}_{q^n}} \psi\left(ca_j\left(x_j(x_j^{q^{i_j}}-x_j)\right)\right). \qquad (18)$$

We can divide this product into two parts: one from 1 to $\tilde{r}$ and the other from $\tilde{r}+1$ to r. We use Corollary 3.10, for the matrices $A_j = \frac{ca_j}{2}B((\mathcal{P}^i)^T - 2Id + \mathcal{P}^i)B^T$, $1\leq j\leq r$. In this case,

$$\text{rank } A_j = \begin{cases} n-d_j & \text{if } \gcd(l_j,p) = 1; \\ n-2d_j & \text{if } \gcd(l_j,p) = p. \end{cases}$$

Let A_j' be a reduced matrix of A_j. Then

$$\chi(\det(A_j')) = \begin{cases} (-1)^{n-d_j}\chi((-2)^{n-d_j}l_j^{d_j}) & \text{if } \gcd(l_j,p) = 1; \\ (-1)^{n-d_j}\chi((-1)^{n-d_j}2^n) & \text{if } \gcd(l_j,p) = p. \end{cases}$$

Combining this result with Lemma 2.5, we can obtain the following expressions

$$\prod_{j=1}^{\tilde{r}} \sum_{x_j \in \mathbb{F}_{q^n}} \psi\left(ca_j\left(x_j(x_j^{q^{i_j}} - x_j)\right)\right) = \prod_{j=1}^{\tilde{r}} (-1)^{(s+1)(n-d_j)} \tau^{s(n-d_j)} \left((-1)^{n-d_j} \chi((-2ca_j)^{n-d_j} l_j^{d_j})\right) q^{n-(n-d_j)/2}$$

$$= (-1)^{s(n\tilde{r}-D_1)} \tau^{s(n\tilde{r}-D_1)} \chi((-2c)^{n\tilde{r}-D_1} A_1 L_1) q^{\frac{n\tilde{r}+D_1}{2}}$$

and

$$\prod_{j=\tilde{r}+1}^{r} \sum_{x_j \in \mathbb{F}_{q^n}} \psi\left(ca_j\left(x_j(x_j^{q^{i_j}} - x_j)\right)\right) = \prod_{j=\tilde{r}+1}^{r} (-1)^{(s+1)(n-2d_j)} \tau^{s(n-2d_j)} \left((-1)^{n-d_j} \chi((-1)^{n-d_j}(2ca_j)^{n-2d_j})\right) q^{n-(n-2d_j)/2}$$

$$= (-1)^{sn(r-\tilde{r})-D_2} \tau^{sn(r-\tilde{r})-2sD_2} \chi((-1)^{n(r-\tilde{r})-D_2}(2c)^{n(r-\tilde{r})} A_2) q^{\frac{n(r-\tilde{r})+2D_2}{2}}.$$

Using the given expressions in (18), we obtain the following result

$$N_n(\mathcal{H}_r) - q^{rn} = (-1)^{s(nr-D_1)-D_2} \tau^{s(nr-D_1-2D_2)} \sum_{c \in \mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \chi((-1)^{D_2}(-2c)^{nr-D_1} AL_1) q^{\frac{nr+D_1+2D_2}{2}}$$

$$(19)$$

We will now proceed with the proof by considering two cases.

(1) If $nr - D_1$ is even, then $\chi((-2c)^{nr-D_1}) = 1$. Substituting this in (19), we have

$$N_n(\mathcal{H}_r) - q^{rn} = (-1)^{D_2} \tau^{s(nr-D_1-2D_2)} \chi((-1)^{D_2} AL_1) q^{\frac{nr+D_1+2D_2}{2}} \sum_{c \in \mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda))$$

$$= \begin{cases} (-1)^{D_2} \tau^{s(nr-D_1-2D_2)} \chi((-1)^{D_2} AL_1) q^{\frac{nr+D_1+2D_2}{2}}(q-1) & \text{if } \mathrm{Tr}(\lambda) = 0 \\ (-1)^{D_2} \tau^{s(nr-D_1-2D_2)} \chi((-1)^{D_2} AL_1) q^{\frac{2nr+D_1+2D_2}{2}}(-1) & \text{if } \mathrm{Tr}(\lambda) \neq 0 \end{cases}$$

$$= (-1)^{D_2} \tau^{s(nr-D_1-2D_2)} \chi((-1)^{D_2} AL_1) \varepsilon_{\mathrm{Tr}(\lambda)} q^{\frac{nr+D_1+2D_2}{2}}.$$

(2) If $nr - D_1$ is odd, then $\chi((-2c)^{nr-D_1}) = \chi(-2c)$. Substituting this in (19), we have

$$N_n(\mathcal{H}_r) - q^{rn} = (-1)^{s-D_2} \tau^{s(nr-D_1-2D_2)} \chi(2(-1)^{D_2+1} AL_1) q^{\frac{nr+D_1+2D_2}{2}} \sum_{c \in \mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \chi(c)$$

$$= \begin{cases} (-1)^{s-D_2} \tau^{s(nr-D_1-2D_2)} \chi(2(-1)^{D_2+1} AL_1) q^{\frac{nr+D_1+2D_2}{2}} \sum_{c \in \mathbb{F}_q^*} \chi(c) & \text{if } \mathrm{Tr}(\lambda) = 0 \\ (-1)^{s-D_2} \tau^{s(nr-D_1-2D_2)} \chi(2(-1)^{D_2} AL_1 \mathrm{Tr}(\lambda)) q^{\frac{nr+D_1+2D_2}{2}} \sum_{c \in \mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \chi(-c\mathrm{Tr}(\lambda)) & \text{if } \mathrm{Tr}(\lambda) \neq 0 \end{cases}$$

$$= \begin{cases} 0 & \text{if } \mathrm{Tr}(\lambda) = 0; \\ (-1)^{s-D_2} \tau^{s(nr-D_1-2D_2)} \chi(2(-1)^{D_2} AL_1 \mathrm{Tr}(\lambda)) q^{\frac{nr+D_1+2D_2}{2}} G_1(\tilde{\psi}, \chi) & \text{if } \mathrm{Tr}(\lambda) \neq 0. \end{cases}$$

Applying Theorem 2.4, which states that $G_1(\tilde{\psi}, \chi) = -(-\tau)^s \sqrt{q}$, we obtain the following expression

$$N_n(\mathcal{H}_r) - q^{rn} = (-1)^{D_2+1} \tau^{s(nr-D_1-2D_2+1)} \chi(2(-1)^{D_2} AL_1 \mathrm{Tr}(\lambda)) q^{\frac{nr+D_1+2D_2+1}{2}}.$$

$$\square$$

The well-known Weil bound tells us that

$$|N_n(\mathcal{H}_r) - q^{nr}| \leq (q-1) \prod_{j=1}^{r} q^{i_j} q^{nr/2} = (q-1) q^{\frac{rn+2I}{2}},$$

where $I = \sum_{j=1}^{r} i_j$. By Theorem 4.1 this bound can be attained only if in the case $nr - D_1$ is even and $\mathrm{Tr}(\lambda) = 0$. Besides that, we would need that $2I = D_1 + 2D_2$, that only occurs if $D_1 = 0$ and $i_j = d_j$ for $j \in Y$. Using this fact, we obtain the following result, that assures us when the hypersurface $\mathcal{H}_r$ is maximal or minimal.

Theorem 4.2. *Let* $\mathcal{H}_r : y^q - y = \sum_{j=1}^{r} a_j x_j(x_j^{q^{i_j}} - x_j) - \lambda$ *with* $\lambda \in \mathbb{F}_{q^n}$, $a_j \in \mathbb{F}_q^*$ *and* $0 < i_j < n$ *and satisfying the same conditions as in Theorem 4.1.*

The hypersurface $\mathcal{H}_r$ *attains the upper Weil bound if and only if one of the following holds*

- $\text{Tr}(\lambda) = 0$, $D_1 = 0$, nr *is even,* $i_j = d_j$ *for all* $j \in Y$, $(nr - 2D_2)s \equiv 0 \pmod 4$ *and* $(-1)^{D_2}\chi((-1)^{D_2}AL_1) = 1$;
- $\text{Tr}(\lambda) = 0$, $D_1 = 0$, nr *is even,* $i_j = d_j$ *for all* $j \in Y$, $(nr - 2D_2)s \equiv 2 \pmod 4$ *and* $(-1)^{D_2}\chi((-1)^{D_2}AL_1) = -1$.

The hypersurface $\mathcal{H}_r$ *attains the lower bound if and only if one of the following holds*

- $\text{Tr}(\lambda) = 0$, $D_1 = 0$, nr *is even,* $i_j = d_j$ *for all* $j \in Y$, $(nr - 2D_2)s \equiv 2 \pmod 4$ *and* $(-1)^{D_2}\chi((-1)^{D_2}AL_1) = 1$;
- $\text{Tr}(\lambda) = 0$, $D_1 = 0$, nr *is even,* $i_j = d_j$ *for all* $j \in Y$, $(nr - 2D_2)s \equiv 0 \pmod 4$ *and* $(-1)^{D_2}\chi((-1)^{D_2}AL_1) = -1$.

Example 4.3. *Let* $q = 5^2$, $n = 30$. *We consider the Artin-Schreier hypersurface given by*

$$\mathcal{H} : y^q - y = x_1(x_1^{q^2} - x_1) + x_2(x_2^{q^3} - x_2) + x_3(x_3^{q^6} - x_3).$$

Following the notation of Theorem 4.2, we have that $i_1 = d_1 = 2, i_2 = d_2 = 3, i_3 = d_3 = 6,$ $l_1 = 15, l_2 = 10, l_3 = 5$, $D_2 = 2 + 3 + 6 = 11$, $A = 1$ *and* $L_1 = 1$. *Moreover,*

$$(nr - 2D_2)s \equiv (90 - 22) \cdot 2 \equiv 0 \pmod 4,$$

$$(-1)^{D_2}\chi((-1)^{D_2}AL_1) = (-1)^{11}\chi((-1)^{11}) = -1.$$

It follows from Theorem 4.2 that $\mathcal{H}$ *is* $\mathbb{F}_{q^{30}}$-*minimal.*

5. Declaration of competing interest

The authors certify that they have NO affiliations with or involvement in any organization or entity with any financial interest (such as honoraria; educational grants; participation in speakers' bureaus; membership, employment, consultancies, stock ownership, or other equity interest; and expert testimony or patent-licensing arrangements), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

6. Acknowledgements

References

[1] Anbar, N. and Meidl, W. *More on quadratic functions and maximal Artin-Schreier curves.* Applicable Algebra in Engineering, Communication and Computing **26(5)** 409-426, (2015).

[2] Anbar, N. and Meidl, W. *Quadratic functions and maximal Artin-Schreier curves.* Finite Fields and Their Applications **30** 49-71, (2014).

[3] Aubry, Y. *Reed-Muller codes associated to projective algebraic varieties.* Coding theory and algebraic geometry. Springer 4-17, (1992).

[4] Bartoli, D., Quoos, L., Saygı, Z. and Yılmaz, E. S. *Explicit maximal and minimal curves of Artin–Schreier type from quadratic forms.* Applicable Algebra in Engineering, Communication and Computing **32** 507-520 (2021).

[5] Brochero Martínez, F. E. and Oliveira, D. *Artin-Schreier curves given by* $\mathbb{F}_q$-*linearized polynomials.* Discrete Mathematics **346** 113630, (2023).

[6] Coşgun, A., Özbudak, F. and Saygi, Z. *Further results on rational points of the curve* $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ *over* $\mathbb{F}_{q^m}$. Designs, Codes and Cryptography **79.3** 423-441 (2016).

[7] Coulter, R. S. *The number of rational points of a class of Artin-Schreier curves.* Finite Fields and Their Applications **8.4** 397-413, (2002).

[8] Farnell, S. and Pries, R. *Families of Artin–Schreier curves with Cartier–Manin matrix of constant rank.* Linear Algebra and its Applications **439**(7) 2158-2166, (2013).

[9] Güneri, C. and Özbudak, F. *Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields.* Finite Fields and Their Applications **14.1** 44-058 (2008).

[10] Hefez, A. and Kakuta, N. *Polars of Artin-Schreier curves.* Acta Arithmetica. **77**, 57-70 (1996).

[11] Lidl, R.; Niederreiter, H. *Finite Fields.* Encyclopedia of Mathematics and its Applications, Vol. **20**, Addison-Wesley, Reading, MA, (1983).

[12] Mullen G.L.; Panario, D. *Handbook of Finite Fields.* Discrete Mathematics and its applications, (2013).

[13] Ozbudak, F. and Saygi, Z. *Explicit maximal and minimal curves over finite fields of odd characteristics.* Finite Fields and Their Applications, **42**, 81-92 (2016).

[14] Rojas-León, A. and Wan, D. *Improvements of the Weil bound for Artin–Schreier curves.* Mathematische Annalen **351.2** 417-442 (2011).

[15] Stepanov, S. A. *Codes on algebraic curves.* Springer Science & Business Media (2012).

[16] Van der Geer, G. and Van der Vlugt, M. *Fibre products of Artin-Schreier curves and generalized Hamming weights of codes.* Journal of Combinatorial Theory, Series A **70**, 337-348 (1995).

[17] Wolfmann, J. *The number of points on certain algebraic curves over finite fields.* Communications in Algebra **17.8** 2055-2060 (1989).

Departamento de Matemática, UNIVERSIDADE FEDERAL DE MINAS GERAIS, UFMG, Belo Horizonte MG (Brazil)
Email address: `fbrocher@mat.ufmg.br`

Instituto de Ciências Matemáticas e de Computação, UNIVERSIDADE DE SÃO PAULO (USP) São Carlos (Brazil)
Email address: `danielaalvesoliveira@gmail.com`