On circulant matrices and rational points of Artin-Schreier’s curves

Daniela Oliveira
F. E. Brochero Martínez

Abstract. Let $\mathbb{F}_q$ be a finite field with $q$ elements, where $q$ is an odd prime power. In this paper we associated circulant matrices and quadratic forms with curves of Artin-Schreier $y^q - y = x \cdot P(x) - \lambda$, where $P(x)$ is a $\mathbb{F}_q$-linearized polynomial and $\lambda \in \mathbb{F}_q$. Our main results provide a characterization of the number of rational points in some extension $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$. In the particular case, in the case when $P(x) = x^q - x$ we given a full description of the number of rational points in term of Legendre symbol and quadratic characters.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with $q = p^e$ elements, with $p$ an odd prime and $e$ a positive integer. Algebraic curves over finite fields have many applications to several areas such as coding theory, cryptography, communications and related areas. For instance, elliptic curves over finite fields, that is a class of algebraic curves, have been used to construct cryptography codes, because their points form an appropriate group. In any case, it is important to determine the number of points of the curve in each extension of the field $\mathbb{F}_q$. For $g(x) \in \mathbb{F}_q[x]$, a plane curve with equation of the form

$$C : y^q - y = g(x),$$

is called an Artin-Schreier curve. These type of curves have been studied extensively in several contexts (see [4, 5, 10, 13]). Besides that, Artin-Schreier curves over finite fields are closely related to quadratic forms. We have some characterizations and classification in the literature about these relations (see [1, 2, 11]).

The aim of this paper is to study the number of rational points in $\mathbb{F}_{q^r}^2$ ($r \geq 1$) of $C$ when $g(x) = x \cdot f(x)$ and $f(x)$ is a $\mathbb{F}_q$-linearized polynomial. For that we associated to the curve $C$ with a quadratic form and in a more general case we associated the number of rational of $C$ with a circulant matrix. Using that relation and determining the rank of that matrix, we given an explicit formula for the number of rational points in any extension $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$ in the cases when $\gcd(r, q) = 1$. Our main result for that case provide an explicit formula for the number of rational points, given by Theorem 3.4.

Moreover, in the particular case when the curve is $y^q - y = x^{q+1} - x^2 - \lambda$, with $i$ a positive integer and $\gcd(r, p) = 1$, we determine the number of rational points in terms of Legendre symbol and $p$-adic valuation, given by the following theorem.

Theorem 1.1. Let $i, r$ be integers such that $0 < i < r$, $r = 2^b \bar{r}$ and $r = t_1^{a_1} \cdots t_u^{a_u}$ where $t_j$ are distinct odd primes such that $\gcd(t_j, p) = 1$. For $\lambda \in \mathbb{F}_q$, the number of rational points in $\mathbb{F}_{q^r}^2$ of the curve $y^q - y = x^{q+1} - x^2 - \lambda$ is

$$q^r - Dq^{(r+L)/2}$$

Key words and phrases. finite fields, circulant matrices, artin schreier curve.
where

(i) \[ D = \prod_{j=1}^{n} \left( \frac{x}{r} \right)^{\max(0,\nu_j(r) - \nu_j(i))} \quad \text{and} \quad L = \gcd(r, i), \text{ if } r \text{ is odd}; \]

(ii) \[ D = (-1)^{\nu_1^{12} + \cdots + \nu_r^{12}} \frac{L}{2^{\nu_1^{12} + \cdots + \nu_r^{12}}} \quad \text{and} \quad L = \gcd(2^i, i), \text{ if } r \text{ is even and } i \text{ is even}; \]

(iii) \[ D = \prod_{j=1}^{n} \left( \frac{x}{r} \right)^{\max(0,\nu_j(r) - \nu_j(i))} \quad \text{and} \quad L = \gcd(\tilde{r}, i), \text{ if } r \text{ is even and } i \text{ is odd}. \]

When \( i = 1 \) we obtain the curve \( y^q - y = x^{q+1} - x^2 \) that is associated to the number of monic irreducible polynomials with the two first coefficients prescribed (see [3, 9]).

The paper is organized as follows. The section 2 provides a background material and important preliminary results. In Section 3 we discuss the case when \( C : y^q - y = x \cdot P(x) - \lambda \) with \( P(x) \) a \( F_q \)-linearized polynomial. In Section 4 we give a explicitly formula for the number of rational points in \( F_q^r \) for the curve \( y^q - y = x^{q+1} - x^2 - \lambda \) and finally in Section 5 we give a alternative solution for the number of rational points when \( i = 1 \). This last section also consider the case when \( \gcd(r, p) = p \).

2. Preparation

Throughout this paper \( F_q \) denotes a finite field with \( q \) elements, where \( q \) is a power of an odd prime \( p \). An important tool used in this section is the complete homogeneous symmetric polynomials at the variables \( x_1, x_2, \ldots \), that are describe in the following definition.

Definition 2.1. The complete homogeneous symmetric polynomials of degree \( k \), denoted for \( h_k(r) \), is given by

\[ h_k(x_1, x_2, \ldots, x_r) = \sum_{0 \leq i_1 \leq \cdots \leq i_k \leq r} x_{i_1} \cdots x_{i_k}. \]

The following theorem, that can be found in [12] without prove, describe an another representation for the polynomial \( h_k \).

Theorem 2.2 ([12], Ex. 7.4). The complete homogeneous symmetric polynomial \( h_k(r) \) of degree \( k \) in the variables \( x_1, x_2, \ldots, x_r \) can be expressed as the sum of rational functions

\[ h_k(x_1, \ldots, x_r) = \sum_{i=1}^{r} \frac{x_i^{r+k-1}}{\prod_{m=1}^{r}(x_i - x_m)}. \]

That type of polynomials will be useful to determining the rank of some circulant matrices.

Definition 2.3. Given \( a_0, a_1, \ldots, a_r-1 \) elements of a field \( \mathbb{L} \), we define

a) The \( r \times r \) circulant matrix \( C = (c_{ij}) \) associated to the \( r \)-tuple \( (a_0, a_1, \ldots, a_r-1) \) by the relation \( c_{ij} = a_k \) if \( j - i \equiv k \) (mod \( r \)). Let denote by \( C(a_0, a_1, \ldots, a_r-1) \) that matrix and the vector \( (a_0, a_1, \ldots, a_r-1) \) is called the generator vector of \( C \).

b) The associated polynomial of the circulant matrix \( C \) with generator vector \( (a_0, a_1, \ldots, a_r-1) \) is \( f(x) = \sum_{i=0}^{r-1} a_i x^i \).

It is known (see for example [6]) that for a circulant matrix \( C = C(a_0, a_1, \ldots, a_r-1) \) is valid that

\[ \det C = \prod_{i=1}^{r} (a_0 + a_1 \omega_i + \cdots + a_{r-1} \omega_i^{r-1}), \]

where \( \omega_1, \ldots, \omega_r \) are the \( r \)-th roots of unity in some extension of \( F_q \), in the case when \( r \) is relatively prime with the characteristic \( p \). We will use that fact in order to calculate the
rank of \( C \). Specifically, the rank of \( C \) is related to the common roots of \( f(x) \) and \( x^r - 1 \). Before we determine the rank of \( C \) we need the following definitions.

**Definition 2.4.** For each \( 0 < j \leq k \) integers, \( A_k \) and \( A_{k,j} \) denote the polynomials

1. \( A_k(x_1, \ldots, x_k) = \prod_{1 \leq t < s \leq k} (x_s - x_t) \), for all \( k \geq 2 \).
2. \( A_{k,j}(x_1, \ldots, x_k) = (-1)^{j+1} \prod_{1 \leq t < s \leq k} (x_s - x_t) \), for all \( k \geq 3 \).

The following lemma shows a relation between the complete homogeneous symmetric polynomials and the polynomials \( A_{k,j} \), that will be useful to determine the rank of \( C \).

**Lemma 2.5.** Let \( j \leq k \) be positive integers and \( h_{r,j}(k) \) be the polynomial \( h_r(x_1, \ldots, \hat{x}_j, \ldots, x_k) \), where \( \hat{x}_j \) means to omit the variable \( x_j \). Then

\[
\sum_{j=1}^{k} x_j^{r-1} A_{k,j} h_{r-k+1,j}(k) = 0, \text{ for all } k \geq 3.
\]

**Proof.** Let denote \( \epsilon_{l,j} = \begin{cases} 
1 & \text{if } l > j \\
-1 & \text{if } l < j \\
0 & \text{if } l = j
\end{cases} \). By Theorem 2.2 it follows that

\[
\sum_{j=1}^{k} x_j^{r-1} A_{k,j} h_{r-k+1,j}(k) = \sum_{j=1}^{k} x_j^{r-1} (-1)^{j+1} \prod_{1 \leq t < s \leq k \atop t \neq j} (x_s - x_t) \sum_{l=1}^{k} \left( \prod_{m=1}^{k} (x_l - x_m) \right)
\]

\[
= \sum_{j=1}^{k} x_j^{r-1} (-1)^{j+1} \sum_{l=1}^{k} x_l^{r-1} \prod_{1 \leq t < s \leq k \atop t \neq j} (x_s - x_t) (-1)^{k-l} \epsilon_{l,j}
\]

\[
= \sum_{j=1}^{k} \sum_{l \neq j} x_j^{r-1} x_l^{r-1} \prod_{1 \leq t < s \leq k \atop t \neq j} (x_s - x_t) (-1)^{k+j-l+1} \epsilon_{l,j}.
\]

For each \( l \) and \( j \) fixed, the sum runs the term \((x_l x_j)^{r-1} = (x_j x_l)^{r-1}\) twice, then

\[
x_j^{r-1} x_l^{r-1} \prod_{1 \leq t < s \leq k \atop t \neq j} (x_s - x_t) (-1)^{k+j-l+1} (\epsilon_{l,j} + \epsilon_{j,l}) = 0.
\]

\[\square\]

**Lemma 2.6.** Let \( k \geq 2 \) be an integer and consider the polynomial

\[
F(x_1, \ldots, x_{k+1}) = \sum_{j=1}^{k+1} \frac{x_1 \ldots x_{k+1}}{x_j} A_{k+1,j}.
\]

Then \( F(x_1, \ldots, x_{k+1}) = A_{k+1} \).
Proof. We prove the result by induction on the number of variables. For \( k = 2 \) we have
\[
F(x_1, x_2, x_3) = \sum_{j=1}^{3} \frac{x_1 x_2 x_3}{x_j} (-1)^{j+1} \prod_{1 \leq s < t \leq 3, s \neq j} (x_t - x_s)
\]
\[
= x_2 x_3 (x_3 - x_2) - x_1 x_2 (x_2 - x_1) + x_1 x_3 (x_3 - x_1)
\]
\[
= (x_2 - x_1)(x_3 - x_1)(x_3 - x_2) = A_3.
\]
Let suppose that the result is true for \( k \). This equation is equivalent to \( F_1 \).

\[\square\]

We prove the result by induction on the number of variables. For \( k \) different roots of
\( g \) let \( \alpha \) be a circulant matrix over \( \mathbb{F}_q \) with generator vector \( (a_0, a_1, \ldots, a_{r-1}) \) and \( f(x) \) the associated polynomial to the matrix \( C \), where \( \gcd(r, q) = 1 \). Let \( g(x) = \gcd(f(x), x^r - 1) \) and \( \alpha_1, \alpha_2, \ldots, \alpha_m \) are the roots of \( g(x) \). Then for each positive integer \( j \leq m \) the following relation
\[
(a_0, a_1, \ldots, a_{r-j}) \cdot (1, h_1(\alpha_1, \ldots, \alpha_j), \cdots, h_{r-j}(\alpha_1, \ldots, \alpha_j)) = 0,
\]
is satisfied, where \( \cdot \) denotes the inner product.

Proof. Let denote \( \bar{\alpha}_k = (\alpha_1, \ldots, \alpha_{k+1}) \). Since \( \gcd(r, q) = 1 \) it follows that \( \alpha_i \neq \alpha_j \) for all \( i \neq j \). We proceed by induction on the number of roots. For \( \alpha \) a root of \( g \) we have
\[
a_0 + a_1 \alpha + \cdots + a_{r-1} \alpha^{r-1} = 0.
\]
Then \( (a_0, a_1, a_{r-1}) \cdot (1, \alpha, \alpha^{r-1}) = 0 \) and that relation is equivalent to the first case of the induction. If \( j = 2 \) for the pair of roots \( \alpha_1, \alpha_2 \) we have the following relations
\[
\begin{align*}
0 & = a_0 \alpha_1 + a_1 \alpha_2 + \cdots + a_{r-1} \alpha_1^{r-2} = 0 \\
a_0 \alpha_2 + a_1 \alpha_2^2 + \cdots + a_{r-1} \alpha_2^{r-2} & = 0.
\end{align*}
\]
Subtracting these equations we obtain
\[
a_0 (\alpha_2 - \alpha_1) + a_1 (\alpha_2^2 - \alpha_1^2) + \cdots + a_{r-2} (\alpha_2^{r-1} - \alpha_1^{r-1}) = 0.
\]
Since \( A_2 = \alpha_2 - \alpha_1 \neq 0 \) it follows that
\[
0 = (a_0, a_1, \ldots, a_{r-2}) \cdot (\alpha_2 - \alpha_1, a_2^2 - a_1^2, \ldots, a_{r-2} - a_1^{r-2})
\]
\[
= (a_0, a_1, \ldots, a_{r-2}) \cdot A_2 (1, \frac{h_1(\alpha_1, \alpha_2)}{A_2}, \cdots, \frac{h_{r-2}(\alpha_1, \alpha_2)}{A_2}),
\]
and that relation proved the case \( j = 2 \). Let suppose that the relation (1) is true for any choice of \( k \) different roots of \( g \). Let \( \alpha_1, \ldots, \alpha_{k+1} \) be \( k+1 \) roots of \( g \). By the induction
hypotheses, we have $k+1$ equations of the form (1), where for each one we do not consider one of the roots, i.e., the $j$-th equation is given by

\[(a_0, \ldots, a_{r-k}) \cdot (1, h_{1,j}(\bar{a}_{k+1}), \ldots, h_{r-k,j}(\bar{a}_{k+1})) = 0. \tag{2}\]

Multiplying the vector $(1, h_{1,j}(\bar{a}_{k+1}), \ldots, h_{r-k,j}(\bar{a}_{k+1}))$ for $\alpha_j^{-1}A_{k+1,j}$ and adding these vectors we get the following vector

\[u = \sum_{j=1}^{k+1} \alpha_j^{-1}(A_{k+1,j}, A_{k+1,j}h_{1,j}(\bar{a}_{k+1}), \ldots, A_{k+1,j}h_{r-k,j}(\bar{a}_{k+1})).\]

By Lemma 2.5, the last coordinate of the vector $u$ is

\[\sum_{j=1}^{k+1} \alpha_j^{-1}A_{k+1,j}h_{r-k,j}(\bar{a}_{k+1}) = 0. \tag{3}\]

Besides that, denoting $\alpha = \alpha_1 \cdots \alpha_{k+1}$, the first coordinate of $u$ is

\[a_0 \sum_{j=1}^{k+1} \alpha_j^{-1}A_{k+1,j} = a_0 \sum_{j=1}^{k+1} \alpha_j^{-1}((-1)^{j+1} \prod_{1 \leq t < k+1 \atop t \neq j} (\alpha_t - \alpha_s)) = \frac{a_0}{\alpha} A_{k+1,1}, \tag{4}\]

where in the last equality we use Lemma 2.6 and the fact that $\alpha_j's$ are $r$-th roots of unity.

For $2 \leq l \leq r - k - 1$, the $l$-th coordinate of $u$ is equal to

\[
a_l \sum_{j=1}^{k+1} \alpha_j^{-1}A_{k+1,j}h_{l,j}(\bar{a}_{k+1}) = a_l \sum_{j=1}^{k+1} \alpha_j^{-1}((-1)^{j+1} \prod_{1 \leq t < k+1 \atop t \neq j} (\alpha_t - \alpha_s) \sum_{i=1}^{k+1} \frac{\alpha_l^{i+k-1}}{\prod_{m=1 \atop m \neq l,j}^{k+1} (\alpha_t - \alpha_m)) = a_l \sum_{j=1}^{k+1} \alpha_j^{-1}((-1)^{j+1} \prod_{1 \leq t < k+1 \atop t \neq j} (\alpha_t - \alpha_s) \prod_{s,t}^{k+1} (\alpha_t - \alpha_s) e_{i,j}). \tag{5}\]

Let us denote

\[G(x_1, \ldots, x_{k+1}) = \sum_{j=1}^{k+1} \sum_{i=1}^{k+1} \frac{x_1 \cdot \ldots \cdot x_{k+1}}{x_j} x_i^{k-1}(-1)^{k+j-i+1} \prod_{1 \leq s \leq k+1 \atop s \neq i,j} (x_t - x_s) e_{i,j}. \]

We observe that for $x_i = x_j$ with $i \neq j$ we have $G(x_1, \ldots, x_{k+1}) = 0$, therefore $(x_i - x_j)$ divides $G(x_1, \ldots, x_{k+1})$ for all $i \neq j$ and then $A_{k+1}(x_1, \ldots, x_{k+1})$ divides $G(x_1, \ldots, x_{k+1})$,
which can be expressed by the following relation

\[
\frac{1}{A_{k+1}} G(x_1, \ldots, x_{k+1}) = \sum_{i=1}^{k+1} \frac{x_1 \cdots x_{k+1} x_i^{l+k-1}}{\prod_{m \neq i} (x_i - x_m)} \sum_{j=1}^{k+1} \frac{1}{\prod_{r \neq i,j} (x_r - x_j)} (x_i - x_j)
\]

Fixing \(i\), it follows by Remark 2.7 that \(\sum_{j \neq i}^{k+1} \frac{x_1 \cdots x_{k+1} x_i^{l+k}}{x_i x_j} \prod_{m \neq i} (x_i - x_m) = 1\). Therefore

\[
G(x_1, \ldots, x_{k+1}) = A_{k+1} \sum_{i=1}^{k+1} \frac{x_1 \cdots x_{k+1} x_i^{l+k}}{\prod_{m \neq i} (x_i - x_m)} = A_{k+1} h_l(k+1) \tag{6}
\]

By Equation (5) we have that \(a_i \sum_{j=1}^{k+1} a_j^{l-1} A_{k+1,j} h_{l,ij}(\tilde{g}_{k+1}) = \frac{a_i}{\alpha} A_{k+1} h_l(k+1)\). Hence by Equation (3),(4) and (6) we conclude

\[
(a_0, \ldots, a_{r-k-1}) \cdot (1, h_1(\alpha_1, \ldots, \alpha_{k+1}), \ldots, h_{n-k-1}(\alpha_1, \ldots, \alpha_{k+1})) = 0. \tag{7}
\]

\[
\text{Remark 2.9. For any } \lambda \text{ root of } g(x) \text{ and } 0 \leq i \leq m, \text{ multiplying } f(\lambda) \text{ for } \lambda^i, \text{ it follows that}
\]

\[
a_{r-i} + a_{r-i+1} \lambda + \cdots + a_{r-1} \lambda^{r-i} = 0 \tag{7a}
\]

and using Lemma 2.8 we have that the results is still true for any shift of the coefficients \(a_0, a_1, \ldots, a_{r-1}\).

\[
\text{Remark 2.10. If } g(x) \text{ has only simple roots then the result is also true in the case when } \gcd(r, q) \neq 1. \tag{7b}
\]

The following theorem shows how to find a equivalent matrix to the circulant matrix \(C\), but first we need the following definition.

\[
\text{Definition 2.11. Let } f(x) \in \mathbb{F}_q[x] \text{ be a monic polynomial of degree } n \text{ such that } f(0) \neq 0.
\]

The reciprocal polynomial \(f^*\) of the polynomial \(f\) is defined by \(f^*(x) = \frac{1}{f(0)} x^n f(1/x)\). The polynomial \(f\) is self-reciprocal if \(f = f^*\).

\[
\text{Theorem 2.12. Let } C \text{ be a } r \times r \text{ circulant matrix over } \mathbb{F}_q \text{ with generator vector } (a_0, a_1, \ldots, a_{r-1}). \text{ Let } f(x) \text{ be the polynomial associated to } C \text{ and suppose that } g(x) = \gcd(f(x), x^r - 1) \text{ is a self-reciprocal polynomial with } \deg g(x) = m. \text{ Then the rank of } C \text{ is } l = r - m \text{ and there exists an invertible matrix } M \in M_r(\mathbb{F}_q) \text{ such that } MAM^T = \begin{pmatrix} R & 0 \\ 0 & 0 \end{pmatrix}, \text{ where } R = (r_{i,j}) \text{ is the } l \times l \text{ matrix defined by } r_{ij} = a_{ij} \text{ for } 0 \leq i, j \leq l \text{ and } M^T \text{ denotes the transpose matrix of } M. \tag{7c}
\]

\[
\text{Proof. Let } \alpha_1, \ldots, \alpha_m \text{ be the roots of } g(x). \text{ Let consider the matrices } B_i \text{ formed from the identity matrix changing the entries of the } r - i + 1 \text{-th row by}
\]

\[
1, h_1(\alpha_1, \ldots, \alpha_i), \ldots, h_{r-i}(\alpha_1, \ldots, \alpha_i), 0, \ldots, 0. \tag{7d}
\]
Observe that \( B_1 = \begin{pmatrix}
1 & 0 & \cdots & 0 & 0 \\
0 & 1 & \cdots & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 1 & 0 \\
1 & \alpha_1 & \cdots & \alpha_1^{r-2} & \alpha_1^{r-1}
\end{pmatrix} \)
and since \( \alpha_1 \) and \( \alpha_1^{-1} \) are roots of \( g \), the product \( B_1 AB_1^T \) has the last row and columns with null entries. Let us denote \( M = B_mB_{m-1} \cdots B_2 B_1 \), then from Lemma 2.8 and Remark 2.9 we have that
\[
MAM^T = \begin{pmatrix} R & 0 \\ 0 & 0 \end{pmatrix},
\]
where the matrix \( R \) is the matrix \( C \) reduced to its first \( l \) rows and columns.

**Example 2.13.** Let \( q = 27 \) and \( r = 7 \). Let us denote the \( r \)-th cyclotomic polynomial by \( Q_r \). Since \( \operatorname{ord} q = 2, Q_r \) splits into 3 irreducible monic polynomials over \( \mathbb{F}_q \) of the same degree 2. Let \( (a) = \mathbb{F}_q^* \) where \( a \) has the minimal polynomial \( x^3 + 2x + 1 \). Then
\[
Q_r(x) = (x^2 + 2a^2x + 1)(x^2 + (2a^2 + a + 2)x + 1)(x^2 + (2a^2 + 2a + 2)x + 1).
\]
If
\[
f(x) = (x^2 + 2a^2x + 1)(x^2 + (2a^2 + a + 2)x + 1)(x - a)
= x^5 + x^4(a^2 + 2) + x^3(a^2 + a + 1) + x^2(2a + 1) + x(a^2 + 2a) + 2a,
\]
then
\[
g(x) = \gcd(f(x), x^r - 1) = (x^2 + 2a^2x + 1)(x^2 + (2a^2 + a + 2)x + 1)
= x^4 + x^3(a^2 + a + 2) + x^2(2a^2 + a) + x(a^2 + a + 2) + 1,
\]
is a self-reciprocal polynomial and the circulant matrix with associated polynomial \( f(x) \) is
\[
C = \begin{pmatrix}
2a & a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 & 0 \\
0 & 2a & a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 \\
a^2 + 2 & 1 & 0 & 2a & a^2 + 2a & 2a + 1 & a^2 + a + 1 \\
2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 & 0 & 2a & a^2 + 2a \\
a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 & 0 & 2a \\
a^2 + a + 1 & a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 & 0 \\
a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 & 0 & 2a
\end{pmatrix}.
\]
By Theorem 2.12 the rank of \( C \) is 3 and has reduce matrix \( C' = \begin{pmatrix} 2a & a^2 + 2a & 2a + 1 & 2a & a^2 + 2a & 1 & 0 \\
0 & 2a & a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 \\
1 & 0 & 2a & a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 \\
2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 & 0 & 2a & a^2 + 2a \\
a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 & 0 & 2a \\
a^2 + a + 1 & a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 & 0 \\
a^2 + 2a & 2a + 1 & a^2 + a + 1 & a^2 + 2 & 1 & 0 & 2a \end{pmatrix} \). In addition, \( \det C' = a^4 + 12a^3 + a = a^3 \neq 0 \).

3. The number of rational points of \( y^q - y = x \cdot P(x) - \lambda \)

In this section, we associated the number of rational points of the curve \( y^q - y = x \cdot P(x) - \lambda \) with the trace function, defined below.

**Definition 3.1.** For \( r \) a positive integer and the field \( \mathbb{F}_{q^r} \) we defined the trace function \( \mathbb{F}_{q^r} \to \mathbb{F}_q \) by
\[
\operatorname{Tr}_{\mathbb{F}_{q^r} / \mathbb{F}_q} (x) = x + x^q + \cdots + x^{q^{r-1}}.
\]
For simplicity, we denote by \( \operatorname{Tr} \).

Let \( C \) be the curve defined by the equation
\[
C : y^q - y = x \cdot P(x) - \lambda,
\]
with \( \lambda \in \mathbb{F}_q \) and \( P(x) = \sum_{j=0}^{l} a_{ij}x^j \) a \( \mathbb{F}_q \)-linearized polynomial. We are interested to find the number of rational points in \( \mathbb{F}_q^2 \) of \( C \). Applying the trace function we obtain

\[
\text{Tr}(x \cdot P(x)) = r\lambda. \tag{7}
\]

Therefore for each rational point \((x_0, y_0) \in C(\mathbb{F}_q)\) corresponds a solution of \( \text{Tr}(x_0(P(x_0))) = r\lambda \). Reciprocally for each solution of \( \text{Tr}(x_0(P(x_0))) = r\lambda \) we have \( q \) rational points of \( C(\mathbb{F}_q) \) of the form \((x_0, y_j)\) where the \( y_j \)'s are the solutions of equations \( y^q - y = x_0P(x_0) - \lambda \).

Let us denote \( N_r \) the number of solutions of \( \text{Tr}_{\mathbb{F}_q / \mathbb{F}_r}(x \cdot P(x)) = r\lambda \), then

\[
\#C_r = q \cdot N_r.
\]

Let \( P \) denote the \( r \times r \) permutation matrix \( P = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \) and \( P_l = P^l \) for each \( l \) non-negative integer. The following proposition associated the \( \mathbb{F}_q \)-linearized polynomial \( P(x) \) with a appropriated circulant matrix.

**Proposition 3.2.** Let \( P(x) = \sum_{i=0}^{l} a_i x^i \) be a \( \mathbb{F}_q \)-linearized polynomial. For \( \lambda \in \mathbb{F}_q \), the number of solutions of \( \text{Tr}(x \cdot P(x)) = r\lambda \) in \( \mathbb{F}_q^r \) is equal to the number of solutions \( \vec{z} = (z_1, z_2, \ldots, z_n)^T \in \mathbb{F}_q^r \) of the quadratic form

\[
\vec{z}^T A \vec{z} = r\lambda
\]

where \( A = \frac{1}{2} \sum_{i=0}^{l} a_i (P_i + P_i^T) \).

**Proof.** Let denote \( \Gamma = \{\beta_1, \ldots, \beta_r\} \) an arbitrary base of \( \mathbb{F}_q^r \) over \( \mathbb{F}_q \) and \( N_\Gamma = \begin{pmatrix} \beta_1 & \beta_2 & \ldots & \beta_{q-1} \\ \beta_2 & \beta_3 & \ldots & \beta_{q-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{q-1} & \beta_{q-1}^2 & \ldots & \beta_{q-1}^{q-1} \end{pmatrix} \).

Since \( \Gamma \) is a basis, then \( N_\Gamma \) is invertible and for \( x \in \mathbb{F}_q^r \) we can write \( x = \sum_{i=1}^{r} \beta_j x_i \), with \( x_1, \ldots, x_r \in \mathbb{F}_q \). The equation \( \text{Tr}(x \cdot P(x)) = r\lambda \) is equivalent to

\[
\sum_{j=0}^{r-1} x^j \cdot P(x)^j = r\lambda. \tag{8}
\]

From the fact that \( P(x) \) is a \( \mathbb{F}_q \)-linearized polynomial and trace is a linear function, it is sufficient to consider monomials of the form \( x \cdot x^j \). Let us denote \( L_l(x) = \text{Tr}(x \cdot x^j) \), then

\[
L_l(x) = \sum_{j=0}^{r-1} x^j \cdot (x^j)^j = \sum_{j=0}^{r-1} \left( \sum_{s=1}^{r} \beta_s x_s \right)^j \left( \sum_{k=1}^{r} \beta_k x_k \right)^j = \sum_{s,k=1}^{r} \left( \sum_{j=0}^{r-1} \beta_s^j \beta_k^{j+1} \right) x_s x_k.
\]

Consequently \( L_l(x) \) is a quadratic form that have the following symmetric representation

\[
L_l(x) = (x_1 \ x_2 \ \cdots \ x_r) B_l \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix}, \quad \text{with} \quad B_l = \frac{1}{2} M_l (P_l + P_l^T) M_l^T.
\]
Making the variable change \((z_1, z_2, \cdots, z_r) = (x_1 x_2 \cdots x_r)M_1\) we get a equivalent system which has the same number of solutions. Therefore
\[
L_2(y) = (z_1, z_2, \cdots, z_r) \begin{bmatrix}
\frac{1}{2}(P_1 + P_1^T) \\
\vdots \\
\frac{1}{2}(P_r + P_r^T)
\end{bmatrix}
\begin{bmatrix}
z_1 \\
z_2 \\
\vdots \\
z_r
\end{bmatrix}
\]
Using equation (8) and by definition of matrix \(A\), the result follows.

The following theorem, about number of solutions of a quadratic form, is well-known and we present without proof.

**Theorem 3.3** ([7], Theorems 6.26 and 6.27). Let \(\Phi\) be a quadratic form over \(\mathbb{F}_q\), with \(q\) a power of an odd prime. Let \(\varphi\) be the bilinear symmetric form associated to \(\Phi\), with \(v = \dim(\ker(\varphi))\). Let \(S_\chi := \{x \in \mathbb{F}_q|\chi(x) = \lambda\}\), \(\Delta\) be the determinant of the quadratic form and \(\chi\) the quadratic character of \(\mathbb{F}_q\), then

(i) If \(r + v\) is even:
\[
S_\chi = \begin{cases}
q^{r-1} + Dq^{(r+v-2)/2}(q-1) & \text{if } \lambda = 0; \\
q^{r-1} - Dq^{(r+v-2)/2} & \text{if } \lambda \neq 0,
\end{cases}
\]
where \(D = v(\lambda)\chi\((-1)^{(r-v)/2}\Delta)\) and \(v(\lambda) = \begin{cases}
-1 & \text{if } \lambda \neq 0; \\
q-1 & \text{if } \lambda = 0.
\end{cases}
\]

(ii) If \(r + v\) is odd:
\[
S_\chi = \begin{cases}
q^{r-1} & \text{if } \lambda = 0; \\
q^{r-1} - Dq^{(r+v-1)/2} & \text{if } \lambda \neq 0.
\end{cases}
\]
where \(D = v(\lambda)\chi\((-1)^{(r-v-1)/2}\lambda\Delta)\).

In particular \(D \in \{-1, 1\}\).

It is straightforward to prove that Theorems 2.12, 3.3 combined with Preposition 3.2 provide a proof of the following theorem.

**Theorem 3.4.** Let \(P(x) = \sum_{i=0}^{m} a_i x^i\) be a \(\mathbb{F}_q\)-linearized polynomial and \(f(x) = \sum_{i=0}^{l} a_i x^i\) be the associated polynomial of \(P(x)\). Let suppose that \(g(x) = \gcd(f(x), x^r-1)\) is a self-reciprocal polynomial of degree \(m\), \(R\) be a matrix as defined in Theorem 2.12 and \(a = \det R\). For each \(\lambda \in \mathbb{F}_q\), the number of rational points in \(\mathbb{F}_q^2\) of the curve \(y^2 - y = x \cdot P(x) - \lambda\) is

1. \(q^r + v(2r\lambda)q^{(r+m-2)/2}\chi((-1)^{(r-m)/2}a), \text{ if } r - m\) is even.,
2. \(q^r + q^{(r+m+1)/2}\chi((-1)^{(r-m-1)/2}2r\lambda a), \text{ if } r - m\) is odd.

**Example 3.5.** Let \(q = 27, r = 7\) and \(f(x), g(x)\) be the polynomials of Example 2.13. Put \(P(x) = x^7 + x^4(a^2 + 2) + x^3(a^2 + a + 1) + x^2(2a + 1) + x(2a^2 + 2a) + 2ax\) that have associated polynomial \(f(x)\). Since \(r - m\) is odd and \(\det C'' = a^2\), by Theorem 3.4 the number of rational points in \(\mathbb{F}_q^2\) of the curve \(y = x \cdot P(x) - \lambda\) with \(\lambda \in \mathbb{F}_q\) is \(q^7 + q^6\chi(\lambda)\).

Therefore if \(\lambda\) is a square in \(\mathbb{F}_q\) the number of rational points is \(q^7 + q^6\) and if \(\lambda\) is not a square in \(\mathbb{F}_q\) the number of rational points is \(q^7 - q^6\). Besides that, if \(\lambda = 0\) the number of rational points is \(q^7\).

In the following section we consider some special polynomials \(P(x)\) and calculate explicitly the value of \(D\) of Theorem 3.3.
4. The number of rational points of $y^q - y = x \cdot (x^{q^i} - x) - \lambda$

Throughout this section for a prime $t$ we denote $\nu_t(n)$ the $t$-adic valuation of $n$, i.e., the maximum power of $t$ that divides $n$. For any integer $a$, $\left( \frac{a}{t} \right)$ denotes the Legendre symbol. We will use that symbol in order to determine the number of rational points in $\mathbb{F}_q^2$. In previous section, the number of rational points in $\mathbb{F}_q$ of $y^q - y = x \cdot P(x) - \lambda$, with $P(x)$ a $\mathbb{F}_q$-linearized polynomial and $\lambda \in \mathbb{F}_q$, it was associated to the number of elements $x \in \mathbb{F}_q$ such that $\text{Tr}(xP(x)) = r\lambda$. For $\Phi$ a quadratic form we define the symmetric bilinear form of $\Phi$ by $\varphi(x, y) = \Phi(x + y) - \Phi(x) - \Phi(y)$. Dimension of $\Phi$ is given by $|\{x \in \mathbb{F}_q : \varphi(x, y) = 0 \text{ for all } y \in \mathbb{F}_q\}|$. Since trace function defines a quadratic form, in order to determine the number of solutions of $\text{Tr}(xP(x)) = r\lambda$ it is necessary to establish the dimension of the symmetric bilinear form associated to that quadratic form that is described by next proposition.

**Proposition 4.1.** Let $0 < i < r$ be integers and $P(x) = \sum_{j=0}^{i} a_j x^{q^j}$ a $\mathbb{F}_q$-linearized polynomial. Let $\Phi_i(x) = \text{Tr}(x \cdot P(x))$ be a quadratic form over $\mathbb{F}_q$ and $\varphi_i(x, y)$ the symmetric bilinear form associated to $\Phi_i$. If $a_0 \neq 0$, then

$$\dim \ker(\varphi_i) = \deg\left(\gcd\left(\sum_{j=0}^{i} a_j x^j + x^{q^i-j}) , x^r - 1\right)\right), \quad (11)$$

**Proof.** In order to determine the dimension of the kernel of $\varphi_i$ it is sufficient calculate the dimension of the symmetric bilinear form $\varphi(x, y)$, i.e.,

$$\dim \{x \in \mathbb{F}_q : \varphi(x, y) = 0 \text{ for all } y \in \mathbb{F}_q\}.$$  

Then

$$\varphi(x, y) = \text{Tr}\left(\sum_{j=0}^{i} a_j (x + y)^q^{j+1} - \sum_{j=0}^{i} a_j x^{q^j+1} - \sum_{j=0}^{i} a_j y^{q^j+1}\right)$$

$$= \sum_{j=0}^{i} a_j \left(\sum_{l=0}^{r-1} x^{q^{i+l}} y^{q^j} - x^{q^j} y^{q^{i+l}}\right)$$

$$= \sum_{j=0}^{i} a_j \left(\sum_{j=0}^{r-1} (x^{q^j} + x^{q^{i-j}}) y^{q^j}\right)$$

$$= \sum_{j=0}^{i} a_j \text{Tr}(x^{q^j} + x^{q^{i-j}}) y^{q^j}.$$

By later equation, the relation $\varphi(x, y) = 0$ for all $y \in \mathbb{F}_q$ is equivalent to

$$\sum_{j=0}^{i} a_j(x^{q^j} + x^{q^{i-j}}) = 0. \quad (12)$$

The $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q$ determined by Equation (12) is the set of roots of the polynomial $g(x) = \gcd(h(x), x^{q^r} - x)$ where $h(x) = \sum_{j=0}^{i} a_j(x^{q^j} + x^{q^{i-j}})$. Since $g$ is a $\mathbb{F}_q$-linearized polynomial, the degree of the associated polynomial given us the dimension of $\ker(\varphi_i)$, that correspond to the degree of $\gcd(x^r - 1, \sum_{j=0}^{i} a_j(x^j + x^{q^i-j}))$ and this fact concludes the proposition. \(\square\)
4.1. The special case $P(x) = x^{q^i} - x$. For this case we explicitly determine the dimension of the quadratic form. Besides that, we can use that information to count the number of rational points in $F_{q^r}$ of the curve $y^q - y = x^{q^i+1} - x^2 - \lambda$ with $\lambda \in F_q$. The following corollary is consequence of Proposition 4.1.

**Corollary 4.2.** Let $\Phi_i(x) = \text{Tr}(x^{q^i+1} - x^2)$, with $0 < i < r$, be a quadratic form over $F_{q^r}$ and $\varphi_i(x, y)$ the symmetric bilinear form associated to $\Phi_i$. Put $r = p^u \bar{r}$, $i = p^s \bar{i}$, where $u, s$ are non negative integers such that $u, s > 0$ are distinct odd primes satisfying $u + s < r$. Let $\tilde{\varphi}_i = \text{gcd}(\bar{r} \bar{i})$. Then

$$\dim \ker(\varphi_i) = \text{gcd}(\tilde{\varphi}_i, \tilde{\varphi}_i) \min(p^u, 2p^s).$$

**Proof.** By Proposition 4.1 we need to determine the set of roots of the following polynomial

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

Since $r = p^u \bar{r}$, $i = p^s \bar{i}$, the associated polynomial to (14) is

$$\gcd(x^{2q^i} - 2x^{q^i} + 1, x^{q^i} - 1) = \gcd((x^{2q^i} - 2x^{q^i} + 1)\min(p^u, 2p^s)).$$

Therefore, from the fact that the degree of the later polynomial given us the dimension of the kernel, it follows that $\dim \ker(\varphi_i) = \gcd(\tilde{\varphi}_i, \tilde{\varphi}_i) \min(p^u, 2p^s)$. □

Using Theorem 3.3 and previous lemma we can determine the number of solutions of $\text{Tr}(x^{q^i+1} - x^2) = r\lambda$ which will give us a complete description of the number of rationals points in $F_{q^r}$ of the curve $y^q - y = x^{q^i+1} - x^2 - \lambda$.

**Lemma 4.3.** Let $i, r$ be integers such that $0 < i < r$. Let $\Phi_i(x) = \text{Tr}(x^{q^i+1} - x^2)$ be a quadratic form over $F_{q^r}$, where $r = t_1 \ldots t_n$ and $t_j$ are distinct odd primes satisfying $\text{gcd}(t_j, p) = 1$. Let $v$ be the dimension of the bilinear symmetric form associated to $\Phi_i$. Let $\lambda$ be a non negative integer and $\text{gcd}(i, p) = 1$. Then $r + v$ is even and for $\lambda \in F_q^*$, the constant $D$ of Theorem 3.3 it is given by

$$D = \prod_{j=1}^n \left( \frac{q}{t_j} \right)^{\max\{0, \nu_{t_j}(r) - \nu_{t_j}(i)\}}.$$

**Proof.** The number of solutions $S_{\lambda}$ of $\text{Tr}(x^{q^i+1} - x^2) = \lambda$ is given by Equation (9). For each $\lambda \in F_q^*$, if $\text{Tr}(x^{q^i+1} - x^2) = \lambda$ then

$$\text{Tr}((x^{q^i})^{q^j+1} - (x^{q^i})^2) = \text{Tr}((x^{q^i+1} - x^2)^{q^j}) = \text{Tr}(x^{q^j+1} - x^2) = \lambda,$$

for all $0 \leq j \leq r - 1$. We have two cases to consider

1) $r = t^h$, $t$ an odd prime and $\text{gcd}(t, p) = 1$.

Using Equation (15), for each $x \in S_{\lambda}$ we can associated another $d - 1$ solutions, where $d$ is the minimum positive divisor of $r = t^h$ such that $x^{q^i} = x$. We have that $d > 1$, because otherwise we would have $x^q = x$ and $x^{q^i+1} - x^2 = x^2 - x^2 = 0$, which means that $\lambda = 0$, a contradiction. Then $d$ is a multiple of $t$ and Equation (9) of Theorem 3.3 module $t$ can be rewritten as

$$q^r - 1 - Dq^{(r+v-2)/2} \equiv 0 \mod t,$$

that is equivalent to

$$D \equiv (q^{(r+v-2)/2})^{-1} \equiv q^{(r+v-2)/2} \mod t,$$
where in the last congruence we use that \( D = \pm 1 \). By Lemma 4.2 we obtain
\[
D \equiv q^{(\min(b, r_1(i)))/2 - 1} \pmod{\ell}
\]
\[
\equiv q^{(\min(b, r_1(i)))(\ell - \min(b, r_1(i)) + 1)/2 - 1} \pmod{\ell}
\]
\[
\equiv q^{(\ell - \min(r, r_1(i)))/2} \pmod{\ell}
\]
\[
\equiv q^{(\max(0, b - r_1(i)))/2} \pmod{\ell}
\]
\[
\equiv (\frac{q}{\ell})^{(\max(0, b - r_1(i)))/2} \pmod{\ell}
\]

Since \((\frac{q}{\ell})\) assumes only values \([-1, 1]\) and \(\frac{\ell - 1}{2} \equiv \ell \pmod{2}\), we conclude
\[
D = \left(\frac{q}{\ell}\right)^{\max(0, b - r_1(i))}.
\]

2) Now we consider the general case \( t = t_1^{r_1} \cdots t_u^{r_u} \), with \( t_j \) being distinct odd primes satisfying \( \gcd(t_i, p) = 1 \). We will prove the result by induction on the number of distinct primes factors \( u \) of \( r \). We already proved the case when \( u = 1 \). Let suppose that the result is valid for \( u - 1 \geq 1 \) prime factors and let \( r = t_1^{r_1} \cdots t_u^{r_u} \). By Lemma 4.2 the dimension of the bilinear symmetric form associated to \( \Phi_i(x) = v = \gcd(t_1^{r_1} \cdots t_u^{r_u}, i) \) and this fact implies that \( v \) divides \( t_1^{r_1} \cdots t_u^{r_u} \) and \( r + v \) is even. Using Theorem 3.3 for \( \lambda \in \mathbb{F}_q^* \) we have
\[
S_\lambda = q^{r-1} - Dq^{(r+v-2)/2}.
\]

Let \( \lambda \) be fixed and put \( r = \tilde{r}t_u^{r_u} \) where \( \tilde{r} = t_1^{r_1} \cdots t_{u-1}^{r_{u-1}} \). For the subfield \( \mathbb{F}_{q^e} \subset \mathbb{F}_{q^r} \), applying induction hypothesis, the number of solutions of \( \text{Tr}_{\mathbb{F}_{q^e}/\mathbb{F}_q}(x^{\tilde{r}+1} - x^2) = \lambda \) is
\[
S_{\lambda, \tilde{r}} = q^{\tilde{r}-1} - \prod_{j=1}^{u-1} \left(\frac{q}{\ell}\right)^{\max(0, v_j(\tilde{r}) - v_j(i))} q^{(\tilde{r}+v_j-2)/2},
\]
where \( v_1 \) is the dimension of kernel of the bilinear symmetric form associated to \( \text{Tr}_{\mathbb{F}_{q^e}/\mathbb{F}_q}(x^{\tilde{r}+1} - x^2) \). From Lemma 4.2 \( v_1 = \gcd(\tilde{r}, i) \) that implies \( v = v_1 \cdot \gcd(t_u^{r_u}, i) \). Since \( \mathbb{F}_{q^e} \cap \mathbb{F}_{q^{r_u}} = \mathbb{F}_{q^v} \), the solutions that are not in \( \mathbb{F}_{q^e} \) can be are grouped in sets of size congruent to zero module \( t_u \), because if \( \alpha \) is a solution then \( \alpha^{t_u^\ell} \) also is a solution and since \( \alpha \in \mathbb{F}_{q^v} \) it follows that there exists \( d > 1 \) dividing \( t_u^{r_u} \) such that \( \alpha^{t_u^d} = \alpha \). Then
\[
S_\lambda = S_{\lambda, m_1} \pmod{t_u},
\]
that is equivalent to
\[
q^{\tilde{r}t_u^{r_u-1}} = Dq^{(\tilde{r}t_u^{r_u} + v - 2)/2} \equiv q^{\tilde{r}-1} - \prod_{j=1}^{u-1} \left(\frac{q}{\ell}\right)^{\max(0, v_j(\tilde{r}) - v_j(i))} q^{(\tilde{r}+v_j-2)/2} \pmod{t_u}.
\]
Using that \( q^{t_u} \equiv q \pmod{t_u} \), previous equation is equivalent to
\[
Dq^{(\tilde{r}t_u^{r_u} + v - 2)/2} \equiv \prod_{j=1}^{u-1} \left(\frac{q}{\ell}\right)^{\max(0, v_j(\tilde{r}) - v_j(i))} q^{(\tilde{r}+v_j-2)/2} \pmod{t_u}.
\] (16)
Let \( v_2 = \gcd(p_n^a, i) \). We observe that \( q^{(\alpha_n-1)/2} \equiv \left( \frac{\alpha}{t_u} \right)^{a_u} \pmod{t_u} \) and using this relation we obtain that
\[
q^{(\tilde{r} + v_1 - \tilde{r}_n - v)/2} \equiv q^{-\tilde{r}} \left( \frac{\alpha_n}{t_u} \right)^{a_u \tilde{r}} q^{(\tilde{r} - v)/2} \pmod{t_u}
\]
\[
\equiv \left( \frac{q}{t_u} \right)^{a_u \tilde{r}} q^{(\tilde{r} - v)/2} \pmod{t_u}
\]
\[
\equiv \left( \frac{q}{t_u} \right)^{a_u \tilde{r}} q^{v_1 \min \{\alpha_n, v_{t_u}(i)\} - v} \pmod{t_u}. \quad (17)
\]

Equations (16) and (17) allow us to conclude that
\[
D \equiv \prod_{j=1}^{u-1} \left( \frac{q}{t_j} \right)^{\max \{0, \nu_j(i) - \nu_j(i)\}} q^{(\tilde{r} + v_1 - \tilde{r}_n - v)/2} \pmod{t_u}
\]
\[
\equiv \prod_{j=1}^{u-1} \left( \frac{q}{t_j} \right)^{\max \{0, \nu_j(i) - \nu_j(i)\}} \left( \frac{q}{t_u} \right)^{a_u \tilde{r}} q^{v_1 \min \{\alpha_n, v_{t_u}(i)\} - v} \pmod{t_u}
\]
\[
\equiv \prod_{j=1}^{u-1} \left( \frac{q}{t_j} \right)^{\max \{0, \nu_j(i) - \nu_j(i)\}} \left( \frac{q}{t_u} \right)^{\min \{\alpha_n, v_{t_u}(i)\}} \ \pmod{t_u}
\]
\[
\equiv \prod_{j=1}^{u} \left( \frac{q}{t_j} \right)^{\max \{0, \nu_j(i) - \nu_j(i)\}} \pmod{t_u}.
\]

Consequently \( D = \prod_{j=1}^{u} \left( \frac{q}{t_j} \right)^{\max \{0, \nu_j(i) - \nu_j(i)\}} \).

\( \square \)

For extensions of degree power of 2, we have the following result.

**Lemma 4.4.** Let \( b, i, r \) be integers such that \( 0 < i < r \) and \( r = 2^k \). Let \( \Phi_i(x) = \Tr(x^{q^{r+1}} - x^2) \) be a quadratic form over \( \mathbb{F}_{q^r} \) and \( v \) be the dimension of the bilinear symmetric form associated to \( \Phi_i \). Then \( D \) defined in Theorem 3.3 is given by

(i) If \( b = 1 \), then \( D = -\chi(-\lambda) \);

(ii) If \( b \geq 2 \) and \( r + v \) is even, then \( D = (-1)^{(q-1)(2^k-v)/4} \).

(iii) If \( b = 2 \) and \( r + v \) is odd, then \( D = (-1)^{(q-1)/2} \chi \left( -\frac{1}{2^k} \right) \).

(iv) If \( b > 2 \) and \( r + v \) is odd, then \( D = (-1)^{(q+1)/2} \).

**Proof.** When \( r = 2 \) it follows that \( i = 1 \) and \( \Tr(x^{q^{r+1}} - x^2) = \lambda \), where \( x \in \mathbb{F}_{q^2} \), that is equivalent to
\[
x^{q^2+q} - x^{2q} + x^{q+1} - x^2 = \lambda
\]
and it can be written as \( (x^q - x)^2 = -\lambda \). If \( \lambda = 0 \) that relation is equivant to \( x^q - x = 0 \) and therefore \( x \in \mathbb{F}_q \). In that case we have \( q \) solutions. For \( \lambda \in \mathbb{F}_q^* \), let us consider the following maps

\[
\psi : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2} \quad \tau : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}
\]
\[
x \mapsto x^q - x \quad x \mapsto x^2
\]
In order to determine the number of solutions of Equation (18) it is enough prescribe all $x \in \mathbb{F}_{q^2}$ such that $\tau(\psi(x)) = -\lambda$. Let $\{1, \alpha\}$ be a base of $\mathbb{F}_{q^2}/\mathbb{F}_q$. The image of $\{1, \alpha\}$ by $\psi$ is $\{0, \beta\}$, where $\beta = \alpha^q - \alpha$. Since $\ker(\psi) = \mathbb{F}_q$ the image of $\psi$ is generated by $\beta$. Therefore it is enough to consider elements of the form $x = c\alpha$ with $c \in \mathbb{F}_q$. That is
\[
\tau(\psi(c\alpha)) = \tau(c\beta) = c^2\beta^2.
\]

**Claim** $\beta \notin \mathbb{F}_q$. Let suppose, by contradiction, that $\beta^q = \beta$. Then
\[
\alpha^q - \alpha^q + \alpha = 0,
\]
that only occurs if $-2(\alpha^q - \alpha) = 0$. But that later relation is not possible, because $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $p \neq 2$. Therefore $\tau(\psi(x)) = -\lambda$ if and only if $c^2\beta^2 = -\lambda$ and since $\beta \notin \mathbb{F}_q$ that equation has solution if and only if $-\lambda$ is not a square in $\mathbb{F}_q$. In this case we have $2q$ solutions for Equation (18).

Now we consider the case when $r = 2^b$ with $b > 1$. Let $i = p^r\tilde{i}$, with $\gcd(p, \tilde{i}) = 1$. From Lemma 4.2 $v = \gcd(2^b, i) \min(1, 2p^r) = \gcd(2^b, i)$, then $v$ is of the form $2^c$ with $0 \leq c \leq b$. We divide the proof in two cases.

(1) $r + v$ is even.

In this case $v$ and $i$ are even. The number of solutions of $\text{Tr}(x^{q^2+1} - x^2) = \lambda$ is given by Equation (9). If $\text{Tr}(\alpha^{q^2+1} - \alpha^2) = \lambda$, for some $\alpha \in \mathbb{F}_{q^2}^*$, then
\[
\text{Tr}((\alpha^{q^2})^{q^2+1} - (\alpha^{q^2})^2) = \text{Tr}((\alpha^{q^2+1} - \alpha^2)^{q^2}) = \text{Tr}(\alpha^{q^2+1} - \alpha^2) = \lambda, \quad (19)
\]
for each $0 \leq j \leq r-1$. Since $r = 2^b \geq 4$ and Equation (19), for each $x \in S_\lambda$ we can associated another $d - 1$ solutions, where $d$ is the minimum positive divisor of $r = 2^b$ such that $\alpha^{q^2} = \alpha$. We claim that $d > 2$. In fact if $d = 1$ then $(\alpha^{q^2+1} - \alpha^2)^{q^2} = \alpha^2 - \alpha^2 = 0$ that implies $\lambda = 0$, a contradiction. In the case when $d = 2$, for $\alpha \in \mathbb{F}_{q^2}$ it follows that $(\alpha^{q^2+1} - \alpha^2)^{q^2} = \alpha^{q^2+1} - \alpha^2 = \alpha^2 - \alpha^2 = 0$, because $i$ is even. That relation also implies $\lambda = 0$, that is also a contradiction. Then Equation (19) does not have solutions in that cases. Consequently $d > 2$, therefore $d$ is multiple of 4 and Equation (9) of Theorem 3.3 module 4 is
\[
q^{2^b-1} - Dq^{(2^b+v-2)/2} \equiv 0 \pmod{4},
\]
that is equivalent to
\[
D \equiv q^{2^b-1-(2^b+v-2)/2} \equiv q^{(2^b-v)/2} \pmod{4}.
\]
We conclude that $D = (-1)^{(q-1)(2^b-v)/4}$.

(2) $r + v$ is odd.

In this case $v$ is odd and a divisor of $2^b$, then $v = 1$. Using the same argument as in the previous case, the number of solutions of $\text{Tr}(x^{q^2+1} - x^2) = \lambda$ is given by Equation (10). Besides that, for $\lambda \in \mathbb{F}_{q^2}^*$, it follows that $\text{Tr}(x^{q^2+1} - x^2) = \lambda$ if and only if
\[
\text{Tr}((\alpha^{q^2})^{q^2+1} - (\alpha^{q^2})^2) = \text{Tr}((\alpha^{q^2+1} - \alpha^2)^{q^2}) = \text{Tr}(\alpha^{q^2+1} - \alpha^2) = \lambda, \quad (20)
\]
for all $0 \leq j \leq r-1$. Since $r = 2^b \geq 4$ and using Equation (20) for each $x \in S_\lambda$ we can associated another $d - 1$ solutions, where $d$ is the minimum divisor of $r = 2^b$ such that $\alpha^{q^2} = \alpha$. The case $d = 1$ can not occurs, otherwise we would have $\lambda = 0$. 


For $x \in \mathbb{F}_{q^2} \subset \mathbb{F}_q$, we have
\[
\lambda = \text{Tr}(x^{q^4 + 1} - x^2) = 2^{b-1} \cdot ((x^{q^4 + 1} - x) - x^2).
\]
(21)
For the same reason as in previous case, Equation (21) does not have solution in $\mathbb{F}_q$. Therefore we can suppose that $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and equation
\[
\lambda = 2^{b-1} \cdot (x^{q^4 + 1} + x q^2 - x^2)
\]
can be written as $(x^q - x)^2 = -\gamma$, with $\gamma = \frac{\lambda}{2^{b-1}}$. Using the same argument of item (i) of Lemma 4.4 it follows that $(x^q - x)^2 = -\gamma$ has solutions if and only if $-\gamma$ is not a square in $\mathbb{F}_q$, that is equivalent to $\frac{\lambda}{2^{b-1}}$ not be a square in $\mathbb{F}_q$, and in this case we have 2 solutions for Equation (18). Consequently the number of solutions of Equation (21) is $(1 - \chi(\frac{\lambda}{2^{b-1}})) q$. Then
\[
S_\lambda = \left(1 - \chi\left(\frac{-\lambda}{2^{b-1}}\right)\right) q \equiv 0 \pmod{4}.
\]
Now by Theorem 3.3 it follows that
\[
q^{2b-1} + D q^{(2b + v - 1)/2} \equiv \left(1 - \chi\left(\frac{-\lambda}{2^{b-1}}\right)\right) q \pmod{4},
\]
that is equivalent to $D \equiv (1 - \chi(\frac{-\lambda}{2^{b-1}})) q^{1 - (2b^2 + v - 1)/2} - q^{(2b^2 - v - 1)/2} \pmod{4}$. Therefore
\[
D \equiv \left(\left(1 - \chi\left(\frac{-\lambda}{2^{b-1}}\right)\right) q^{v-1} - 1\right) q^{(2b^2 - v - 1)/2} \pmod{4}.
\]
Since $v = 1$ and $q^2 \equiv 1 \pmod{4}$ we conclude that
\[
D \equiv -q^{2b - 1} \cdot \chi\left(\frac{-\lambda}{2^{b-1}}\right) \equiv -q \cdot \chi\left(\frac{-\lambda}{2^{b-1}}\right) \pmod{4}.
\]
Consequently $D = (-1)^{(q-1)/2} \cdot \chi\left(\frac{-\lambda}{2^{b-1}}\right)$.
\[\square\]
Using Theorem 3.3 and Lemma 4.4 we determine in the following theorem the value of $S_\lambda$.

**Theorem 4.5.** Let $b, i, r$ be integers such that $0 < i < r$ and $r = 2^b$. Let $\Phi_i(x) = \text{Tr}(x^{q^{4i+1}} - x^2)$ be a quadratic form over $\mathbb{F}_{q^2}$ and $v$ be the dimension of the bilinear symmetric form associated to $\Phi_i$. The number of solutions $S_\lambda$ of $\Phi_i(x) = \lambda$ in $\mathbb{F}_{q^2}$ is given by

(i) If $b = 1$: $S_\lambda = (1 - \chi(-\lambda)) q$;
(ii) If $b \geq 2$ and $r + v$ is even: $S_\lambda = q^{2b-1} - (-1)^{(q-1)(2b - v)/4} q^{2b^2 + v - 2}/2$;
(iii) If $b \geq 2$ and $r + v$ is odd: $S_\lambda = q^{2b-1} - (-1)^{(q-1)/2} \cdot \chi\left(\frac{-\lambda}{2^{b-1}}\right) q^{2b^2 + v - 2}/2$.

The results obtained in Lemmas 4.3, 4.5 can be used inductively to obtain the following result for extensions of degree $r$ with gcd($r, p) = 1$.

**Theorem 4.6.** Let $b, i, r$ be integers such that $0 < i < r$ and $r = 2^b \tilde{r}$, $r = t_1^{a_1} \cdots t_u^{a_u}$ with $t_j$ being distinct odd primes such that gcd($t_j, p) = 1$. Let $\Phi_i(x) = \text{Tr}(x^{q^{4i+1}} - x^2)$ be a quadratic form over $\mathbb{F}_{q^r}$ and $v$ the dimension of the bilinear symmetric form associated to $\Phi_i$. For $\lambda \in \mathbb{F}_{q^r}$, then

(i) $S_\lambda = (1 - \chi(-\lambda)) q^\tilde{r}$ if $i$ is even and $b = 1$.  

(ii) \( S_\lambda = q^{r-1} - (-1)^{(q^{r-1})}\frac{(b-1)(2b-v_{i})}{2} \frac{q^{(r-r_{i}-2)}}{q^{(r-r_{i}-2)}} \), if \( i \) is even and \( b \geq 2 \).

(iii) \( S_\lambda = q^{r-1} - \prod_{j=1}^{u} \left( \frac{q}{t_{j}} \right)^{\max(0,v_{ij}(r)-v_{ij}(i))} \), if \( i \) is odd.

where \( v_1 = \gcd(2^{b},i) \) and \( v_2 = \gcd(\bar{r},i) \).

**Proof.** By Lemma 4.2 it follows that \( v = \gcd(r,i) \).

(i) Using the relation of transitivity of the trace function we obtain

\[
\lambda = \text{Tr}(x^{q^{r}+1} - x^2) = \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x^{q^{r}+1} - x^2)).
\]  

(22)

Let \( \mu = \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x^{q^{r}+1} - x^2) \). Then the Equation (22) is equivalent to the system

\[
\begin{align*}
\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\mu) &= \lambda; \\
\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x^{q^{r}+1} - x^2) &= \mu.
\end{align*}
\]

Put \( Q = q^\bar{r} \) then \( Q^2 = q^r \). If \( b = 1 \), from item (i) of Lemma 4.5 it follows that the number of solutions of \( \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x^{q^{r}+1} - x^2) = \mu \) is \((1 - \chi(-\lambda))q \) for \( \lambda \in \mathbb{F}_q \). The dimension of the kernel of the quadratic form \( \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q} \) is \( v_0 = \gcd(2,i) = 2 \). The number of solutions of \( \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\mu) = \lambda \) is \( q^{\bar{r}-1} \), then for \( \lambda \in \mathbb{F}_q \)

\[
\begin{align*}
S_\lambda &= q^{\bar{r}-1} - (1 - \chi(-\lambda))q = (1 - \chi(-\lambda))q^\bar{r}.
\end{align*}
\]

Now, if \( b \geq 2 \), from item (ii) of Lemma 4.5 it follows that the number of solutions of \( \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x^{q^{r}+1} - x^2) = \mu \) is

\[
\begin{align*}
S_\mu &= Q^{2^{b-1}} - (-1)^{(Q-1)}\frac{(2b-1)}{2} Q^{(2b-1)-2} \frac{q^{(2b-1)-2}}{q^{(2b-1)-2}},
\end{align*}
\]

where \( v_1 = \gcd(2^{b},i) \) is the dimension of the kernel of the quadratic form \( \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x^{q^{r}+1} - x^2) \). Besides that, the number of solutions of \( \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\mu) = \lambda \) is \( q^{\bar{r}-1} \), then the number of solutions of \( \Phi_t(x) = \lambda \) is

\[
\begin{align*}
q^{\bar{r}-1}(Q^{2^{b-1}} - (-1)^{(Q-1)}\frac{(2b-1)}{2} Q^{(2b-1)-2}) &= q^{\bar{r}-1}(q^\bar{r} - (-1)^{(Q-1)}\frac{(2b-1)}{2} Q^{(2b-1)-2}) \\
&= q^{\bar{r}-1} - (-1)^{(Q-1)}\frac{(2b-1)}{2} Q^{(2b-1)-2}.
\end{align*}
\]

(ii) Using the relation of transitivity of the trace function we have

\[
\lambda = \text{Tr}(x^{q^{r}+1} - x^2) = \text{Tr}_{\mathbb{F}_{q^{2^b}}/\mathbb{F}_q}(\text{Tr}_{\mathbb{F}_{q^{2^b}}/\mathbb{F}_q}(x^{q^{r}+1} - x^2)).
\]  

(23)

Let \( \mu = \text{Tr}_{\mathbb{F}_{q^{2^b}}/\mathbb{F}_q}(x^{q^{r}+1} - x^2) \). The number of solutions of (23) is equal to the number of solutions of the system

\[
\begin{align*}
\text{Tr}_{\mathbb{F}_{q^{2^b}}/\mathbb{F}_q}(\mu) &= \lambda; \\
\text{Tr}_{\mathbb{F}_{q^{2^b}}/\mathbb{F}_q}(x^{q^{r}+1} - x^2) &= \mu.
\end{align*}
\]

Put \( Q = q^{2^b} \) then \( Q^\bar{r} = q^r \). Using Corollary 4.3 we have that the number of solutions of \( \text{Tr}_{\mathbb{F}_{q^{2^b}}/\mathbb{F}_q}(x^{q^{r}+1} - x^2) = \mu \) is

\[
Q^{\bar{r}-1} - \prod_{j=1}^{u} \left( \frac{q}{t_{j}} \right)^{\max(0,v_{ij}(r)-v_{ij}(i))} Q^{(2b-1)-2},
\]
where \( v_2 = \gcd(r, i) \) is the dimension of the kernel of the quadratic form \( \text{Tr}_{q^i/F_q}(x^{q^i+1} - x^2) \). Since the number of solutions of \( \text{Tr}_{q^i/F_q}(\mu) = \lambda \) is \( q^{2\lambda} - 1 \) we conclude that the number of solutions of \( \Phi_i(x) = \lambda \) is

\[
S_\lambda = q^{\nu_1 - 1} \left( q^{\nu_2 - 2} - \prod_{j=1}^u \left( \frac{q}{t_j} \right)^{\max\{0, \nu_j(r) - \nu_j(i)\}} \right) 
\]

\[
= q^{\nu_1 - 1} \left( q^{\nu_2 - 2} - \prod_{j=1}^u \left( \frac{q}{r^{t_j}} \right)^{\max\{0, \nu_j(r) - \nu_j(i)\}} \right) 
\]

\[
= q^{\nu_1 - 1} \left( q^{\nu_2 - 2} - \prod_{j=1}^u \left( \frac{q}{r^{t_j}} \right)^{\max\{0, \nu_j(r) - \nu_j(i)\}} \right) 
\]

\[
\sum_{i=0}^{r-1} f(x)^i = r\lambda. 
\]
Reordering the terms
\[ \sum_{i=0}^{r-1} f(x)^i = \sum_{i=0}^{r-1} \left( \sum_{j=1}^{r} \beta_j x_j \right)^i \left( \sum_{l=1}^{r} (\beta_l^q - \beta_l) x_l \right)^q - r\lambda \]
\[ = \sum_{j,l=1}^{r-1} \left( \sum_{i=0}^{r-1} \beta_j^q (\beta_l^{q+1} - \beta_l^q) \right) x_j x_l - r\lambda. \]

The equation (25) assures us that \( \sum_{j,l=1}^{r-1} \left( \sum_{i=0}^{r-1} \beta_j^q (\beta_l^{q+1} - \beta_l^q) \right) x_j x_l = r\lambda. \)

Denoting \((a_{j,l})_{j,l} = \frac{1}{2} \sum_{i=0}^{r-1} \beta_j^q \beta_l^q (\beta_l^{q+1} - \beta_l^q) \) for \( j \neq l \), that is
\[ a_{j,l} = \frac{1}{2} \text{Tr}(\beta_j^q \beta_l + \beta_l^q \beta_j - 2\beta_j \beta_l), \]
the result follows. □

The matrix \( A \) can be rewritten as
\[ A = \frac{1}{2} (A_1 + A_2 + A_3), \]
where \( A_1 = (\text{Tr}(\beta_j^q \beta_l))_{j,l}, A_2 = (\text{Tr}(\beta_j \beta_l^p))_{j,l} \) and \( A_3 = (\text{Tr}(\beta_j^r \beta_l))_{j,l} \). Using the permutation matrix \( P \) and the fact that \( P^{-1} = P^T \) then \( A_1 = BP^T B^T, A_2 = BPB^T \) and \( A_3 = BB^T \). It follows that \( A = \frac{1}{2} B(P^T - 2Id + P)B^T \) since \( B \) is invertible, in order to determine the number of solutions of the quadratic form with matrix \( A \) we need to determine the rank of the matrix \( P^T + P - 2Id \). The following proposition determines that rank.

**Proposition 5.2.** The rank of the matrix \( N = P^T - 2Id + P \) over \( F_q \) is
\[ \text{rank } N = \begin{cases} r - 1 & \text{if } \gcd(r,p) = 1; \\ r - 2 & \text{if } \gcd(r,p) = p. \end{cases} \]

**Proof.** The matrix \( N \in \mathcal{M}_r(F_q) \) is given by \( N = \begin{pmatrix} -2 & 1 & 0 & \cdots & 0 & 0 & 1 \\ 1 & -2 & 1 & \cdots & 0 & 0 \\ 0 & 1 & -2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -2 & 1 \\ 0 & 0 & 0 & \cdots & 1 & -2 \\ 1 & 0 & 0 & \cdots & 0 & 1 & -2 \end{pmatrix}. \)

Substituting the last row and column for the sum of all rows and then for the sum of all columns, we obtain
\[ \begin{pmatrix} 1 & -2 & 1 & \cdots & 0 & 0 & 0 \\ -2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & -2 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -2 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & -2 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}. \]

Replacing the \((r - 1)\)-th row for the sum: 1-th row more 2 times the 2-th + \( \cdots + (r - 3) \) times the \((r - 3)\)-th row more \( \frac{1}{2} \) times the \((r - 2)\)-th row minus the \((r - 1)\)-th row, we obtain
\[ \begin{pmatrix} 1 & -2 & 1 & \cdots & 0 & 0 & 0 \\ -2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & -2 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -2 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & -2 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & -2 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}. \]
we have the following theorem.

5.2

Propositions

\[
\begin{pmatrix}
-2 & 1 & 0 & \ldots & 0 & 0 & 0 \\
1 & -2 & 1 & \ldots & 0 & 0 & 0 \\
0 & 1 & -2 & \ldots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 1 & -2 & 0 \\
0 & 0 & 0 & \ldots & 0 & 0 & 1 \\
0 & 0 & 0 & \ldots & 0 & 0 & 0
\end{pmatrix}
\]

Now we consider the matrix \( N_{r-1} \), obtained after the first operation without the last column and row, that is

\[
N_{r-1} = \begin{pmatrix}
-2 & 1 & 0 & \ldots & 0 & 0 & 0 \\
1 & -2 & 1 & \ldots & 0 & 0 & 0 \\
0 & 1 & -2 & \ldots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & -2 & 1 & 0 \\
0 & 0 & 0 & \ldots & 1 & -2 & 1 \\
0 & 0 & 0 & \ldots & 0 & 1 & -2
\end{pmatrix} \in M_{r-1}(\mathbb{F}_q).
\]

**Claim 1.** Let \( L_{r-1} = \det N_{r-1} \), then \( L_{r-1} = (-1)^{(r-1)}r \).

Expanding the determinant of \( N_{r-1} \) by the first row we have

\[
L_{r-1} = -2L_{r-2} - L_{r-3}.
\]

This implies the recurrent relation \( L_{r-1} + 2L_{r-2} + L_{r-3} = 0 \), that have as characteristic polynomial \( \lambda^2 + 2\lambda + 1 = (\lambda + 1)^2 \), whose double root is \(-1\). Therefore the solution for the recurrent relation is \( L_{r-1} = A(-1)^r + B(-1)^{r-1}r \), where \( A, B \in \mathbb{F}_q \). Since \( L_2 = 3 \) and \( L_3 = -4 \), we conclude that \( A = 0 \) and \( B = -1 \) and consequently \( L_{(r-1)} = (-1)^{(r-1)}r \).

By Theorem 3.3 and Propositions 5.1 and 5.2 we have the following theorem.

**Theorem 5.3.** Let \( \lambda \in \mathbb{F}_q \) and \( r \) a positive integer. The number of rational points in \( \mathbb{F}_q \) of the curve \( y^q - y = x^{q+1} - x^2 - \lambda \), denoted by \( C_r \), is

\[
C_r = \begin{cases}
q^r + q^{(r+2)/2} \chi((-1)^{r/2}2\lambda) & \text{if } \gcd(r,p) = 1 \text{ and } r \text{ is even;}
q^r + q^{(r+1)/2}\nu(2r\lambda)\chi((-1)^{(r-1)/2}) & \text{if } \gcd(r,p) = 1 \text{ and } r \text{ is odd;}
q^r + q^{(r-4)/2}\nu(2r\lambda)\chi((-1)^{(r-2)/2}) & \text{if } \gcd(r,p) = p \text{ and } r \text{ is even;}
q^r & \text{if } \gcd(r,p) = p \text{ and } r \text{ is odd.}
\end{cases}
\]
6. Some open problems

We finished this paper by enumerating some open problems.

We note that Theorem 3.4 determine the number of rational points in \( \mathbb{F}_q^2 \) of the curve 
\[ C : y^q - y = x \cdot P(x) - \lambda \] 
when \( P(x) \) is a \( \mathbb{F}_q \)-linearized polynomial and satisfies the condition 
that \( g(x) = \gcd(f(x), x^r - 1) \) is a self-reciprocal polynomial, where \( f(x) \) is the associated polynomial of \( P(x) \). From that we have two problems:

**Problem 1.** How to determine the number of rational points of \( C \) when \( P(x) \) is not a \( \mathbb{F}_q \)-linearized polynomial?

**Problem 2.** How to determine the number of rational points of \( C \) when \( g(x) \) is not a self-reciprocal polynomial?

In Section 4, we only study extensions of degree \( r \) such that \( \gcd(r, p) = 1 \). What happens in the general case? That is:

**Problem 3.** Using similar methods or others, how to determine explicitly the number of rational points in \( \mathbb{F}_q^r \) of the curve \( y^q - y = x \cdot P(x) - \lambda \), where \( \lambda \in \mathbb{F}_q \) and \( P(x) \) is a \( \mathbb{F}_q \)-linearized polynomial, such that \( \gcd(r, p) = p \) ?

**Problem 4.** Determine the number of solutions of \( y^q - y = P(x)Q(x) \) when \( P(x), Q(x) \in \mathbb{F}_q[x] \) are \( \mathbb{F}_q \)-linearized polynomials.

In [8], the authors show that the number of monic irreducible polynomials in \( \mathbb{F}_q[x] \) of degree \( r \) and with the first and third coefficients prescribed is related to the curve

\[ y^q - y = x^{2q+1} - x^{q+2}. \]

Then, we have the following problem.

**Problem 5.** Determine the number of solution of the curve \( y^q - y = xP(x)Q(x) \) when \( P(x), Q(x) \in \mathbb{F}_q[x] \) are \( \mathbb{F}_q \)-linearized polynomials.

**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 Appl. 30 49-71, (2014).

[3] Cattell, K., Miess, C.R. Ruskey, F., Serra, M. and Sawada, J. *The number of irreducible polynomials over GF(2) with given trace and subtrace*. J. Combin. Math. Combin. Comput., 47, 31 – 64 (2003).

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

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

[6] Kra, I; Simanca S. R. *On Circulant Matrices* Notices of the AMS, (2012).

[7] Lidl, R.; Niederreiter, H. *Finite Fields*. Encyclopedia Math. Appl., Vol. 20, Addison-Wesley, Reading, MA, (1983).

[8] Lalín, Matilde and Laroque, Olivier *The number of irreducible polynomials with the first two prescribed coefficients over a finite field*. Rocky Mountain J. Math. 46 no. 5, 1587-1618 (2016).

[9] McGuire, G. and Yilmaz, E. S. *The Number of Irreducible Polynomials with the First Two Coefficients Fixed over Finite Fields of Odd Characteristic* Arxiv ID: 1609.02314.

[10] Ozbudak F., Saygi Z.: *Rational points of the curve \( y^{2^n} - y = \gamma x^{q+1} - \alpha \) over \( \mathbb{F}_q \).* Applied Algebra and Number Theory. Cambridge University Press, (2014).

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

[12] Stanley, Richard P. *Enumerative Combinatorics* Cambridge University Press, Vol 2, (1999).

[13] Van der Geer, G. and Van der Vlugt, M. *Fibre products of Artin-Schreier curves and generalized Hamming weights of codes*. J. Combin. Theory Ser. A 70, 337-348 (1995).