ON THE ZETA FUNCTION AND THE AUTOMORPHISM GROUP OF THE GENERALIZED SUZUKI CURVE

HERIVELTO BORGES AND MARIANA COUTINHO

ABSTRACT. For p an odd prime number, $q_0 = p^t$, and $q = p^{2t-1}$, let $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ be the nonsingular model of

$$Y^q - Y = X^{q_0}(X^q - X).$$

In the present work, the number of $\mathbb{F}_{q^n}$-rational points and the full automorphism group of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ are determined. In addition, the L-polynomial of this curve is provided, and the number of $\mathbb{F}_{q^n}$-rational points on the Jacobian $J_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}$ is used to construct étale covers of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$, some with many rational points.

1. INTRODUCTION

Algebraic curves over finite fields is a significant research topic, in particular because of its connection with other areas of mathematics. In this context, determining the number of rational points on a curve is a classical, but often challenging, problem. While a general method to compute such numbers is out of reach, effective bounds can be found in the literature. For instance, if $\mathcal{Y}$ is a (projective, nonsingular, geometrically irreducible, algebraic) curve of genus g defined over the finite field $\mathbb{F}_q$, then the remarkable Hasse-Weil bound gives

$$|\mathrm{N}_q(\mathcal{Y}) - (q+1)| \leqslant 2gq^{1/2},$$

where q is a power of a prime p, and $\mathrm{N}_q(\mathcal{Y})$ is the number of $\mathbb{F}_q$-rational points on $\mathcal{Y}$.

Curves attaining the previous upper (resp. lower) bound are called $\mathbb{F}_q$-maximal (resp. $\mathbb{F}_q$-minimal). For $p = 2$, an important example is the Deligne-Lusztig curve associated with the Suzuki group $\mathrm{Sz}(q)$ [9], [24], [25], here for simplicity called the Suzuki curve, which is the nonsingular model $\mathcal{Y}_\mathcal{S}$ of

$$\mathcal{S} : Y^q - Y = X^{q_0}(X^q - X),$$

where $q_0 = 2^t$, $q = 2^{2t-1}$, and $t \geqslant 2$[(1)]. Indeed in [24, Proposition 4.3], together with the expression for the Zeta function of $\mathcal{Y}_\mathcal{S}$, the explicit formula for the number of rational points on $\mathcal{Y}_\mathcal{S}$ shows that it is $\mathbb{F}_{q^4}$-maximal.

2020 *Mathematics Subject Classification.* Primary 11G20, 14G05, 14G10, 14H37.

The authors would like to thank Felipe Voloch for the discussion regarding the content of Section 6.

The first author was supported by FAPESP (Brazil), grant 2017/04681–3, and partially funded by the 2019 IMPA Post-doctoral Summer Program.

The second author was financed in part by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001, CNPq (Brazil), grant 154359/2016–5, and FAPESP (Brazil), grant 2018/23839–0.

(1)This is an alternative plane model for the Suzuki curve, which is usually given by $Y^q - Y = X^{q_0}(X^q - X)$, with $q_0 = p^t$ and $q = p^{2t+1}$ (see [17, Proposition 4.2]).

The Suzuki curve is optimal in the sense that its number of $\mathbb{F}_q$-rational points coincides with the maximum number of $\mathbb{F}_q$-rational points that a curve of its genus can have [25, Proposition 2.1]. Moreover, in [16, Theorem 5.1], it is shown that this curve can be characterized by its genus and number of $\mathbb{F}_q$-rational points.

In addition to its maximality and optimality, the Suzuki curve is known for its large automorphism group. Specifically, it is one of four examples of curves of genus $g \geqslant 2$ which have an automorphism group of order greater than or equal to $8g^3$ [26], [27, Theorem 11.127]. Furthermore, in [4] and [23], the investigation of genera and plane models for quotients of the Suzuki curve is addressed. Past studies also examined embeddings in $\mathbb{P}^N$ [2], [11], class field theory [29], the invariant a-number [15], and Weierstrass semigroups and coding theory [3], [8], [12], [14], [21], [28], [32]. More recently, the construction of a Galois cover of the Suzuki curve in [38] raised a number of other issues to be investigated [20], [34].

Most of the aforementioned applications were based on knowledge of the number of $\mathbb{F}_{q^n}$-rational points and the automorphism group of the Suzuki curve. Motivated by this, for $p > 2$, $q_0 = p^t$, and $q = p^m$, where m, t are positive integers satisfying $m = 2t - 1$, let $\mathcal{G}_{\mathcal{S}}$ be the projective geometrically irreducible plane curve (see Proposition 2.6) defined over $\mathbb{F}_q$ given in affine coordinates by

$$\mathcal{G}_{\mathcal{S}} : Y^q - Y = X^{q_0}(X^q - X), \tag{1.1}$$

and let $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ be its nonsingular model, called herein the generalized Suzuki curve.

The objective of this work is twofold. First, the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ is investigated for all $n \geqslant 1$[(2)]. In addition, the L-polynomial of $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ is determined. An explicit description of the L-polynomial $L_{\mathcal{Y}}(T)$ of a curve $\mathcal{Y}$ of genus g is highly desirable since it encodes significant information such as the number of rational points on the Jacobian $J_{\mathcal{Y}}$ of $\mathcal{Y}$. Using this fact, some constructions of curves with many rational points are presented in [39]. Moreover, considering the Frobenius endomorphism Φ on $J_{\mathcal{Y}}$, then the characteristic polynomial of Φ is described precisely by $T^{2g}L_{\mathcal{Y}}(T^{-1})$, and from its factorization, the Frobenius linear series on $\mathcal{Y}$ is obtained. For further details, see [27, Sections 9.7 and 9.8].

Second, the full automorphism group of $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ is presented. Additionally, considering the more general curve $\mathcal{X}$ given by the nonsingular model of

$$Y^q - Y = X^{q_0}(X^q - X),$$

where $q = p^m$ and $q_0 = p^t$, with m, t being positive integers satisfying $2t > m \geqslant t$, and $2t - 1 > m \geqslant t$ if $p = 2$, one can easily verify that the proof of Theorem 1.3 below also holds for $\mathcal{X}$. Consequently, the curves $\mathcal{X}$ and $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ have isomorphic automorphism groups when $p > 2$. Further, for $p = 2$, this extension of Theorem 1.3 answers a question raised by Giulietti and Korchmáros, completing their description of the full automorphism group of $\mathcal{X}$ in [22].

Let p be an odd prime. For each integer k, define

$$\eta(k) \coloneqq \left(\frac{k}{p}\right) = \begin{cases} 1, & \text{if } p \nmid k \text{ and } k \text{ is a square modulo } p \\ 0, & \text{if } p \mid k \\ -1, & \text{otherwise,} \end{cases} \tag{1.2}$$

[(2)]For $n = 1$, the number $\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_{\mathcal{S}}})$ was previously studied in [35] in connection with geometric Goppa codes. Also, for $p = 3$, and considering [17, Proposition 4.2], the curve $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ is $\mathbb{F}_q$-covered by the so-called Ree curve, and then the information on its maximality given by Theorem 1.1 could be recovered by Serre's result (see Theorem 2.2).

where $\left(\frac{*}{p}\right)$ is the Legendre symbol, and for $\mathbf{i}$ a chosen square root of -1, consider

$$\tilde{p}^{1/2} \coloneqq \begin{cases} p^{1/2}, & \text{if } \eta(-1)=1 \\ \mathbf{i}p^{1/2}, & \text{if } \eta(-1)=-1. \end{cases} \tag{1.3}$$

The main results are the following.

Theorem 1.1. *If g denotes the genus of $\mathcal{X}_{\mathcal{G}_S}$, then the number $\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_S})$ of $\mathbb{F}_{q^n}$-rational points on $\mathcal{X}_{\mathcal{G}_S}$ is described as follows.*

1. *If $p \mid n$, then*

$$\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_S}) = \begin{cases} q^n+1, & \text{if } n \text{ is odd} \\ q^n+1-\eta((-1)^{n/2})\cdot 2gq^{n/2}, & \text{if } n \text{ is even.} \end{cases}$$

2. *If $p \nmid n$, then*

$$\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_S}) = \begin{cases} q^n+1+\eta((-1)^{(n-1)/2}n)\cdot 2gq^{n/2}p^{-1/2}, & \text{if } n \text{ is odd} \\ q^n+1, & \text{if } n \text{ is even.} \end{cases}$$

In particular, $\mathcal{X}_{\mathcal{G}_S}$ is $\mathbb{F}_{q^n}$-maximal if and only if $p \mid n$, $n \equiv 2 \pmod 4$, and $p \equiv 3 \pmod 4$.

Theorem 1.2. *Let g be the genus of $\mathcal{X}_{\mathcal{G}_S}$, and let $\mathcal{M}_p(T)$ be the minimal polynomial of $-\zeta_p/\tilde{p}^{1/2}$ over $\mathbb{Q}$, where ζ_p is the primitive p-th root of unity $\mathbf{e}^{\frac{2\pi\mathbf{i}}{p}}$. Then, the L-polynomial $L_{\mathcal{X}_{\mathcal{G}_S}/\mathbb{F}_q}(T)$ of $\mathcal{X}_{\mathcal{G}_S}$ is given by*

$$L_{\mathcal{X}_{\mathcal{G}_S}/\mathbb{F}_q}(T) = \left(p^{p-1}\cdot(qT^2-\eta(-1))\cdot \mathcal{M}_p(p^{t-1}T)^2\right)^{\frac{g}{p}}. \tag{1.4}$$

Moreover:

1. *If $p \mid n$, then $L_{\mathcal{X}_{\mathcal{G}_S}/\mathbb{F}_{q^n}}(T)$ is given by*
   a) $\left(q^nT^2-\eta(-1)\right)^g$, *if n is odd.*
   b) $\left(q^{n/2}T-\eta((-1)^{n/2})\right)^{2g}$, *if n is even.*
2. *If $p \nmid n$, then $L_{\mathcal{X}_{\mathcal{G}_S}/\mathbb{F}_{q^n}}(T)$ is given by*
   a) $\left(p^{p-1}\cdot(q^nT^2-\eta(-1))\cdot \mathcal{M}_p(\eta((-1)^{(n-1)/2}n)\cdot p^{t-1}q^{(n-1)/2}T)^2\right)^{\frac{g}{p}}$, *if n is odd.*
   b) $\left(q^{\frac{np}{2}}T^p-\eta((-1)^{n/2})\right)^{\frac{2g}{p}}$, *if n is even.*

Finally, if $\overline{\mathbb{F}}_q(\mathcal{X}_{\mathcal{G}_S})$ is the function field of $\mathcal{X}_{\mathcal{G}_S}$, and $x, y \in \overline{\mathbb{F}}_q(\mathcal{X}_{\mathcal{G}_S})$ are such that $\overline{\mathbb{F}}_q(\mathcal{X}_{\mathcal{G}_S}) = \overline{\mathbb{F}}_q(x,y)$ and $y^q - y = x^{q_0}(x^q - x)$, then the automorphism group of $\mathcal{X}_{\mathcal{G}_S}$ is described as follows.

Theorem 1.3. *The automorphism group $\mathrm{Aut}(\mathcal{X}_{\mathcal{G}_S})$ of $\mathcal{X}_{\mathcal{G}_S}$ has order $q^2(q-1)$ and is given by the maps*

$$(x,y) \mapsto (\alpha x+\beta, \alpha\beta^{q_0}x + \alpha^{q_0+1}y + \gamma),$$

where $\alpha \in \mathbb{F}_q^*$ and $\beta, \gamma \in \mathbb{F}_q$. Moreover,

$$\mathrm{Aut}(\mathcal{X}_{\mathcal{G}_S}) = \mathbb{G} \rtimes \mathbb{H},$$

where $\mathbb{G}$ *is the Sylow* p*-subgroup of* $\mathrm{Aut}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$ *consisting of the maps*

$$(x, y) \mapsto (x + \beta, \beta^{q_0} x + y + \gamma),$$

with $\beta, \gamma \in \mathbb{F}_q$*, and* $\mathbb{H}$ *is the cyclic complement of* $\mathbb{G}$ *in* $\mathrm{Aut}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$*, which can be described by the maps*

$$(x, y) \mapsto (\alpha x, \alpha^{q_0+1} y),$$

with $\alpha \in \mathbb{F}_q^*$.

This paper is organized as follows. Section 2 provides the general background used to prove Theorems 1.1, 1.2, and 1.3, which is done in Sections 3, 4, and 5, respectively. Finally, in Section 6 some examples and applications of Theorems 1.1 and 1.2 are considered.

Notation

Together with (1.2) and (1.3), the following notation is used throughout this text.

- p is a prime number, $q = p^m$, and $q_0 = p^t$ for some positive integers m, t.
- For each positive integer n, $\mathbb{F}_{q^n}$ is the finite field with q^n elements, $\mathbb{F}_{q^n}^* \coloneqq \mathbb{F}_{q^n} \setminus \{0\}$, $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_{q^n}$, and $\overline{\mathbb{F}}_q^* \coloneqq \overline{\mathbb{F}}_q \setminus \{0\}$.
- $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}$ and $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_p}$ denote the absolute trace and norm functions of $\mathbb{F}_{q^n}$, respectively.
- The term *curve* (resp. *plane curve*) means a projective, nonsingular, geometrically irreducible, algebraic curve (resp. a projective plane algebraic curve).
- For a curve $\mathcal{Y}$ defined over $\mathbb{F}_q$
  - $\overline{\mathbb{F}}_q(\mathcal{Y})$ is the function field of $\mathcal{Y}$, and $\mathbb{F}_{q^n}(\mathcal{Y})$ is the $\mathbb{F}_{q^n}$-rational function field of $\mathcal{Y}$;
  - $\mathcal{Y}(\mathbb{F}_{q^n})$ is the set of $\mathbb{F}_{q^n}$-rational points on $\mathcal{Y}$, and $\mathrm{N}_{q^n}(\mathcal{Y}) = \#\mathcal{Y}(\mathbb{F}_{q^n})$;
  - $L_{\mathcal{Y}/\mathbb{F}_{q^n}}(T)$ is the L-polynomial of $\mathcal{Y}$ viewed as a curve defined over $\mathbb{F}_{q^n}$;
  - $J_\mathcal{Y}$ is the Jacobian of $\mathcal{Y}$, and $J_\mathcal{Y}(\mathbb{F}_{q^n})$ is the group of $\mathbb{F}_{q^n}$-rational points on $J_\mathcal{Y}$. Also, assuming that $\mathcal{Y}$ has a rational point $P_0 \in \mathcal{Y}(\mathbb{F}_q)$, and considering $\mathcal{Y}$ embedded in $J_\mathcal{Y}$ via

    $$P_0 \mapsto 0,$$

    $\langle \mathcal{Y}(\mathbb{F}_{q^n}) \rangle$ is the subgroup of $J_\mathcal{Y}(\mathbb{F}_{q^n})$ generated by $\mathcal{Y}(\mathbb{F}_{q^n})$.
- $\mathbf{e}$ is the Euler's number, $\mathbf{i}$ is a fixed square root of -1, and $\zeta_k \coloneqq \mathbf{e}^{\frac{2\pi\mathbf{i}}{k}}$ for each positive integer k.
- For each positive integer k,

  $$\mu_k^{prim} \coloneqq \left\{ \zeta_k^i \ : \ 1 \leqslant i \leqslant k \text{ and } \gcd(i, k) = 1 \right\}$$

  is the set of roots of the k-th cyclotomic polynomial $\Phi_k(T)$.

2. Preliminaries

2.1. **L-Polynomials and Supersingular Curves.** Let $\mathcal{Y}$ be a curve of genus g defined over the finite field $\mathbb{F}_q$, and consider its L-polynomial

$$L_{\mathcal{Y}/\mathbb{F}_q}(T) \coloneqq \exp\left(\sum_{n=1}^{\infty} (\mathrm{N}_{q^n}(\mathcal{Y}) - q^n - 1) \frac{T^n}{n} \right),$$

which is the numerator of the Zeta function of $\mathcal{Y}$.

It is well known that $L_{\mathcal{Y}/\mathbb{F}_q}(T) \in \mathbb{Z}[T]$ has degree $2g$ and satisfies $L_{\mathcal{Y}/\mathbb{F}_q}(0) = 1$ [27, Chapter 9]. Further, if $\omega_1, \ldots, \omega_{2g} \in \mathbb{C}$ are the roots of

$$T^{2g} L_{\mathcal{Y}/\mathbb{F}_q}(T^{-1}),$$

then the following holds:

$$\mathrm{N}_{q^n}(\mathcal{Y}) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n. \tag{2.1}$$

From the Hasse-Weil theorem, $|\omega_i| = q^{1/2}$ for all $i = 1, \ldots, 2g$, and then $\omega_i = q^{1/2}\xi_i$, with $|\xi_i| = 1$ for each i. In particular, (2.1) can be rewritten as

$$\mathrm{N}_{q^n}(\mathcal{Y}) = q^n + 1 - q^{n/2} \sum_{i=1}^{2g} \xi_i^n,$$

and thus $\mathcal{Y}$ is $\mathbb{F}_{q^n}$-maximal (resp. $\mathbb{F}_{q^n}$-minimal) if and only if $\xi_i^n = -1$ (resp. $\xi_i^n = 1$) for each $i \in \{1, \ldots, 2g\}$.

The curve $\mathcal{Y}$ is supersingular if ξ_i is a root of unity for all $i = 1, \ldots, 2g$. In this case, the number

$$s \coloneqq \min\left\{ n \ : \ \xi_i^n = 1 \text{ for all } i = 1, \ldots, 2g \right\}$$

is called the period of $\mathcal{Y}$ over $\mathbb{F}_q$.

The following result is used in the proof of Theorem 1.1.

Theorem 2.1 (33, Theorem 1)**.** *For q odd, let $\mathcal{Y}$ be a curve defined over $\mathbb{F}_q$. If $\mathcal{Y}$ is supersingular with period s over $\mathbb{F}_q$, and $n = n_1 k$, where $n_1 = \gcd(n, s)$, then the following occurs:*

1. *If $n_1 m$ is even, then*

$$\mathrm{N}_{q^n}(\mathcal{Y}) - (q^n + 1) = q^{(n-n_1)/2}\Big[\mathrm{N}_{q^{n_1}}(\mathcal{Y}) - (q^{n_1} + 1)\Big].$$

2. *If $n_1 m$ is odd and $p \mid k$, then*

$$\mathrm{N}_{q^n}(\mathcal{Y}) - (q^n + 1) = q^{(n-n_1)/2}\Big[\mathrm{N}_{q^{n_1}}(\mathcal{Y}) - (q^{n_1} + 1)\Big].$$

3. *If $n_1 m$ is odd and $p \nmid k$, then*

$$\mathrm{N}_{q^n}(\mathcal{Y}) - (q^n + 1) = \eta((-1)^{(k-1)/2}k) \cdot q^{(n-n_1)/2}\Big[\mathrm{N}_{q^{n_1}}(\mathcal{Y}) - (q^{n_1} + 1)\Big].$$

Finally, if $\mathcal{Z}$ is a curve defined over $\mathbb{F}_q$ which is $\mathbb{F}_q$-covered by $\mathcal{Y}$, then the following theorem [1, Proposition 5] provides a relation between $L_{\mathcal{Y}/\mathbb{F}_q}(T)$ and $L_{\mathcal{Z}/\mathbb{F}_q}(T)$.

Theorem 2.2 (Serre)**.** *Let $\mathcal{Z}$ be a curve defined over $\mathbb{F}_q$, and let $\varphi : \mathcal{Y} \to \mathcal{Z}$ be an $\mathbb{F}_q$-rational covering. Then, $L_{\mathcal{Z}/\mathbb{F}_q}(T)$ divides $L_{\mathcal{Y}/\mathbb{F}_q}(T)$.*

2.2. **On the Number of $\mathbb{F}_{q^n}$-Rational Points of $Y^p - Y = XR(X)$.** Suppose that p is an odd prime number. For each positive integer n, we study the number of $\mathbb{F}_{q^n}$-rational points on a nonsingular model $\mathcal{Y}_R$ of the plane curve given in affine coordinates by

$$\mathcal{F}_R : Y^p - Y = XR(X),$$

where $R(X)$ is a p-polynomial defined over $\mathbb{F}_q$; that is,

$$R(X) = \alpha_k X^{p^k} + \alpha_{k-1} X^{p^{k-1}} + \cdots + \alpha_1 X^p + \alpha_0 X,$$

with $\alpha_0, \ldots, \alpha_k \in \mathbb{F}_q$ and $\alpha_k \neq 0$.

The following proposition presents some properties of $\mathcal{F}_R$.

Proposition 2.3 (27, Lemma 12.1)**.** *The plane curve $\mathcal{F}_R$ is geometrically irreducible. Moreover:*

1. *The genus g of $\mathcal{F}_R$ is given by*
$$g = \frac{p^k(p-1)}{2}.$$
2. *$P = (0 : 1 : 0) \in \mathbb{P}^2(\overline{\mathbb{F}}_q)$ is the unique point at infinity of $\mathcal{F}_R$. If $k = 1$, then $\mathcal{F}_R$ is nonsingular. Otherwise, P is the unique singular point of $\mathcal{F}_R$. In both cases, P has multiplicity $p^k + 1 - p$ and is the center of only one $\mathbb{F}_q$-rational branch of $\mathcal{F}_R$.*

Therefore, the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{Y}_R$ is given by the number of solutions in $\mathbb{F}_{q^n}^2$ of the equation

$$Y^p - Y = XR(X) \tag{2.2}$$

plus 1.

To count the number of solutions in $\mathbb{F}_{q^n}^2$ of (2.2), set

$$\begin{array}{rccc} B_R^{(n)} : & \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} & \to & \mathbb{F}_p \\ & (\alpha, \beta) & \mapsto & \frac{1}{2}\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\alpha R(\beta) + \beta R(\alpha)) \end{array}.$$

One can check that $B_R^{(n)}$ is an $\mathbb{F}_p$-symmetric bilinear form on $\mathbb{F}_{q^n}$, with associated quadratic form

$$\begin{array}{rccc} Q_R^{(n)} : & \mathbb{F}_{q^n} & \to & \mathbb{F}_p \\ & \alpha & \mapsto & \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\alpha R(\alpha)) \end{array},$$

which satisfies $Q_R^{(n)}(\gamma\alpha) = \gamma^2 Q_R^{(n)}(\alpha)$ for all $\gamma \in \mathbb{F}_p$, and also

$$B_R^{(n)}(\alpha, \beta) = \frac{1}{2}Q_R^{(n)}(\alpha + \beta) - \frac{1}{2}Q_R^{(n)}(\alpha) - \frac{1}{2}Q_R^{(n)}(\beta)$$

for all $(\alpha, \beta) \in \mathbb{F}_{q^n}^2$.

Considering the radical (kernel) of $B_R^{(n)}$

$$W_R^{(n)} = \left\{ \alpha \in \mathbb{F}_{q^n} \ : \ B_R^{(n)}(\alpha, \beta) = 0 \text{ for each } \beta \in \mathbb{F}_{q^n} \right\},$$

which is an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{q^n}$, the following expressions give the number of solutions in $\mathbb{F}_{q^n}^2$ of (2.2).

Proposition 2.4 (18, Proposition 13.4)**.** *The number of solutions in $\mathbb{F}_{q^n}^2$ of* (2.2) *is*

1. q^n, *if* $mn - \dim_{\mathbb{F}_p}(W_R^{(n)})$ *is odd.*
2. $q^n \pm (p-1)p^{\dim_{\mathbb{F}_p}(W_R^{(n)})/2}q^{n/2}$, *if* $mn - \dim_{\mathbb{F}_p}(W_R^{(n)})$ *is even.*

The following result provides an important tool to determine the dimension of $W_R^{(n)}$.

Proposition 2.5 (18, Proposition 13.1)**.** $W_R^{(n)}$ *consists of the roots in* $\mathbb{F}_{q^n}$ *of the polynomial*

$$E_R(T) = R(T)^{p^k} + \sum_{i=0}^{k} (\alpha_i T)^{p^{k-i}}.$$

2.3. **The Curve $\mathcal{G}_\mathcal{S}$.** Let $\mathcal{G}_\mathcal{S}$ be given as in (1.1). From [35, Theorem 1], [17, Proposition 4.1], and a straightforward calculation, the following holds.

Proposition 2.6. $\mathcal{G}_\mathcal{S}$ *is a geometrically irreducible plane curve of genus* g *given by*

$$g = \frac{q_0(q-1)}{2}.$$

Further, $P = (0:1:0) \in \mathbb{P}^2(\overline{\mathbb{F}}_q)$ *is the unique point at infinity of* $\mathcal{G}_\mathcal{S}$*, which is also its only singular point, having multiplicity equal to* q_0*.*

Considering the nonsingular model $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ of $\mathcal{G}_\mathcal{S}$, let $x, y \in \overline{\mathbb{F}}_q(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$ be such that $\overline{\mathbb{F}}_q(\mathcal{X}_{\mathcal{G}_\mathcal{S}}) = \overline{\mathbb{F}}_q(x,y)$ and $y^q - y = x^{q_0}(x^q - x)$. Then, the following occurs.

Proposition 2.7 (10, Theorem 3.3)**.** *The extension* $\overline{\mathbb{F}}_q(x,y)/\overline{\mathbb{F}}_q(x)$ *is a Galois extension of degree* q*. Moreover, the only ramified place of* $\overline{\mathbb{F}}_q(x)$ *is the infinite place* $\mathcal{P}_\infty$*, which is totally ramified in* $\overline{\mathbb{F}}_q(x,y)$*.*

Let Q_∞ be the $\mathbb{F}_q$-rational point of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ corresponding to the unique place $\mathcal{Q}_\infty$ of $\overline{\mathbb{F}}_q(x,y)$ lying over the infinity place $\mathcal{P}_\infty$ of $\overline{\mathbb{F}}_q(x)$. Then, the following holds.

Corollary 2.8. $P = (0:1:0)$ *is the center of a unique* $\mathbb{F}_q$*-rational branch of* $\mathcal{G}_\mathcal{S}$*, namely the branch of* $\mathcal{G}_\mathcal{S}$ *corresponding to the point* $Q_\infty \in \mathcal{X}_{\mathcal{G}_\mathcal{S}}$*.*

This subsection ends with the following result.

Proposition 2.9 (35, Theorem 7)**.** *The sets* $\{1, x\}$ *and* $\{1, x, y\}$ *are bases for the Riemann-Roch spaces* $\mathscr{L}(qQ_\infty)$ *and* $\mathscr{L}((q+q_0)Q_\infty)$*, respectively.*

2.4. **Automorphism Group.** Let $\mathcal{Y}$ be a curve of genus g defined over the finite field $\mathbb{F}_q$. The automorphism group $\mathrm{Aut}(\mathcal{Y})$ of $\mathcal{Y}$ is defined as the group of $\overline{\mathbb{F}}_q$-automorphisms of the function field $\overline{\mathbb{F}}_q(\mathcal{Y})$.

Considering the action of $\mathrm{Aut}(\mathcal{Y})$ on the points of $\mathcal{Y}$, the stabilizer of $\mathrm{Aut}(\mathcal{Y})$ at $Q \in \mathcal{Y}$, denoted by $\mathrm{Aut}_Q(\mathcal{Y})$, is the subgroup of $\mathrm{Aut}(\mathcal{Y})$ consisting of all automorphisms fixing Q. Further, for each non-negative integer i, the i-th ramification group $\mathrm{Aut}_Q^{(i)}(\mathcal{Y})$ at Q is defined by

$$\mathrm{Aut}_Q^{(i)}(\mathcal{Y}) = \left\{ \sigma \in \mathrm{Aut}_Q(\mathcal{Y}) \ : \ v_Q(\sigma(\mathfrak{t}) - \mathfrak{t}) \geqslant i+1 \right\},$$

where v_Q is the discrete valuation associated to Q, $\mathfrak{t} \in \overline{\mathbb{F}}_q(\mathcal{Y})$ is a local parameter at Q, and $\mathrm{Aut}_Q^{(i)}(\mathcal{Y}) \supseteq \mathrm{Aut}_Q^{(i+1)}(\mathcal{Y})$ for all $i \geqslant 0$. The following result summarizes properties of these subgroups.

Proposition 2.10 (27, Lemma 11.44 and Theorem 11.74)**.** $\mathrm{Aut}_Q^{(0)}(\mathcal{Y}) = \mathrm{Aut}_Q(\mathcal{Y})$. *Moreover,* $\mathrm{Aut}_Q^{(1)}(\mathcal{Y})$ *is the unique Sylow* p*-subgroup of* $\mathrm{Aut}_Q(\mathcal{Y})$*, and* $\mathrm{Aut}_Q(\mathcal{Y}) = \mathrm{Aut}_Q^{(1)}(\mathcal{Y}) \rtimes \mathbb{H}$*, where* $\mathbb{H}$ *is a cyclic subgroup of* $\mathrm{Aut}_Q(\mathcal{Y})$ *of order coprime to* p*.*

The following result is used to prove Theorem 1.3.

Theorem 2.11 (27, Theorem 11.140)**.** *Suppose that* $g \geqslant 2$*, and let* $Q \in \mathcal{Y}$ *be a point satisfying*

$$|\mathrm{Aut}_Q^{(1)}(\mathcal{Y})| > 2g + 1.$$

Then, one of the following cases occurs:

1. $\mathrm{Aut}(\mathcal{Y}) = \mathrm{Aut}_Q(\mathcal{Y})$.
2. $\mathcal{Y}$ *is birationally equivalent to one of the following curves:*
   a) *the Hermitian curve*

$$Y^\ell + Y = X^{\ell+1} \tag{2.3}$$

   where $p \geqslant 2$ *and* $\ell = p^k$*.*
   b) *the Suzuki curve, given by the nonsingular model of*

$$Y^\ell + Y = X^{\ell_0}(X^\ell + X), \tag{2.4}$$

   where $p = 2$*,* $\ell_0 = 2^k$*, and* $\ell = 2\ell_0^2$*.*
   c) *the Ree curve, given by the nonsingular model of*

$$Y^{\ell^2} = [1 + (X^\ell - X)^{\ell-1}]Y^\ell - (X^\ell - X)^{\ell-1}Y + X^\ell(X^\ell - X)^{\ell+3\ell_0}, \tag{2.5}$$

   where $p = 3$*,* $\ell_0 = 3^k$*, and* $\ell = 3\ell_0^2$*.*

3. Proof of Theorem 1.1

We prove Theorem 1.1 using the concepts and notation introduced in Subsection 2.3.

3.1. Elementary Abelian p-Extension.

The following result summarizes properties of the extension $\overline{\mathbb{F}}_q(x,y)/\overline{\mathbb{F}}_q(x)$.

Proposition 3.1 (17, Propositions 1.1 and 1.2)**.** $\overline{\mathbb{F}}_q(x,y)/\overline{\mathbb{F}}_q(x)$ *is an elementary abelian* p*-extension of degree* q*. The set of intermediate fields* $\overline{\mathbb{F}}_q(x) \subseteq E \subseteq \overline{\mathbb{F}}_q(x,y)$ *such that* $[E : \overline{\mathbb{F}}_q(x)] = p$ *is given by*

$$\left\{ E_\alpha \ : \ \alpha \in \mathbb{F}_q^* \right\},$$

where for each $\alpha \in \mathbb{F}_q^*$*,* E_α *is the intermediate field of* $\overline{\mathbb{F}}_q(x,y)/\overline{\mathbb{F}}_q(x)$ *given by*

$$E_\alpha \coloneqq \overline{\mathbb{F}}_q(x, y_\alpha),$$

with $y_\alpha \coloneqq (\alpha y)^{p^{m-1}} + (\alpha y)^{p^{m-2}} + \cdots + (\alpha y)^p + \alpha y$ *satisfying the equation* $y_\alpha^p - y_\alpha = \alpha x^{q_0}(x^q - x)$*. Further,* $E_{\alpha_1} = E_{\alpha_2}$ *if and only if* $\alpha_1 = \alpha\alpha_2$ *for some* $\alpha \in \mathbb{F}_p^*$*. Therefore, there are exactly* $\frac{q-1}{p-1}$ *intermediate fields* E *of* $\overline{\mathbb{F}}_q(x,y)/\overline{\mathbb{F}}_q(x)$ *such that* $[E : \overline{\mathbb{F}}_q(x)] = p$*.*

Based on Proposition 3.1, for each $\alpha \in \mathbb{F}_q^*$, consider the plane model $(\mathcal{F}_\alpha, (x, y_\alpha))$ for E_α, where $\mathcal{F}_\alpha$ is the geometrically irreducible plane curve defined over $\mathbb{F}_q$ given in affine coordinates by[3]

$$\mathcal{F}_\alpha : Y^p - Y = \alpha X^{q_0}(X^q - X).$$

Also, let $\mathcal{X}_\alpha$ be the nonsingular model of $\mathcal{F}_\alpha$. If $\left\{\alpha_i \ : \ i = 1, \ldots, \frac{q-1}{p-1}\right\} \subseteq \mathbb{F}_q^*$ is such that

$$\left\{E_\alpha \ : \ \alpha \in \mathbb{F}_q^*\right\} = \left\{E_{\alpha_i} \ : \ i = 1, \ldots, \frac{q-1}{p-1}\right\},$$

then the following result relates the L-polynomial of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ to the L-polynomials of $\mathcal{X}_{\alpha_i}$, for $i = 1, \ldots, \frac{q-1}{p-1}$. Thus the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ can be expressed as a function of the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{X}_{\alpha_i}$, with $i = 1, \ldots, \frac{q-1}{p-1}$, for each positive integer n.

Proposition 3.2 (13, Corollary 6.7)**.** *Considering the previous notation, then*

$$L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(T) = \prod_{i=1}^{\frac{q-1}{p-1}} L_{\mathcal{X}_{\alpha_i}/\mathbb{F}_q}(T).$$

In particular,

$$\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{S}}) - (q^n + 1) = \sum_{i=1}^{\frac{q-1}{p-1}} \left(\mathrm{N}_{q^n}(\mathcal{X}_{\alpha_i}) - (q^n + 1)\right) \tag{3.1}$$

for each positive integer n.

The following lemmas describe the number $\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$ for each positive integer n.

Lemma 3.3. *For each $\alpha \in \mathbb{F}_q^*$, $\mathbb{F}_q(x, y_\alpha)$ is $\mathbb{F}_q$-isomorphic to $\mathbb{F}_q(x, y_1)$. In particular, from* (3.1)*,*

$$\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{S}}) - (q^n + 1) = \frac{q-1}{p-1}\left(\mathrm{N}_{q^n}(\mathcal{X}_1) - (q^n + 1)\right)$$

for each positive integer n.

Proof. Recall that $q = p^m$ and $q_0 = p^t$, where $m = 2t - 1$; that is, $m - t = t - 1$. For $\alpha \in \mathbb{F}_q^*$, let $\beta := \alpha^{p^{m-t}+p^{m-t-1}+\cdots+p+1} \in \mathbb{F}_q$ and $\gamma := \mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \in \mathbb{F}_p$. Then,

$$\begin{aligned}
\beta^{q_0}\beta &= \left(\alpha^{p^{m-t}+p^{m-t-1}+\cdots+p+1}\right)^{p^t} \alpha^{p^{m-t}+p^{m-t-1}+\cdots+p+1} \\
&= \alpha^{p^m+p^{m-1}+\cdots+p^{t+1}+p^t} \cdot \alpha^{p^{t-1}+p^{t-2}+\cdots+p+1} \\
&= \alpha^{p^m}\alpha^{p^{m-1}+\cdots+p+1} \\
&= \alpha\gamma,
\end{aligned}$$

[3]The geometric irreducibility of $\mathcal{F}_\alpha$ for each $\alpha \in \mathbb{F}_q^*$ follows from the geometric irreducibility of $\mathcal{G}_\mathcal{S}$ [17, Lemma 1.3].

and $\mathbb{F}_q(x, y_\alpha) = \mathbb{F}_q(\beta x, \gamma y_\alpha)$, with

$$\begin{aligned}(\beta x)^{q_0}((\beta x)^q - (\beta x)) &= \beta^{q_0}\beta x^{q_0}(x^q - x)\\ &= \alpha\gamma x^{q_0}(x^q - x)\\ &= (\gamma y_\alpha)^p - (\gamma y_\alpha).\end{aligned}$$

Therefore,

$$\begin{array}{ccc}\mathbb{F}_q(x, y_\alpha) & \to & \mathbb{F}_q(x, y_1)\\ \frac{A(\beta x,\gamma y_\alpha)}{B(\beta x,\gamma y_\alpha)} & \mapsto & \frac{A(x,y_1)}{B(x,y_1)}\end{array}$$

is an $\mathbb{F}_q$-isomorphism between $\mathbb{F}_q(x, y_\alpha)$ and $\mathbb{F}_q(x, y_1)$, where $A(X, Y), B(X, Y) \in \mathbb{F}_q[X, Y]$ and $B(\beta x, \gamma y_\alpha) \neq 0$. □

Lemma 3.4. *For each $\alpha \in \mathbb{F}_q^*$, $E_1 = \overline{\mathbb{F}}_q(x, z_1)$ and $\mathbb{F}_q(x, y_1) = \mathbb{F}_q(x, z_1)$, where*

$$z_1 \coloneqq y_1 - x^{\frac{q}{p}}x^{\frac{q_0}{p}} - x^{\frac{q}{p^2}}x^{\frac{q_0}{p^2}} - \cdots - x^{\frac{q}{p^{t-1}}}x^{\frac{q_0}{p^{t-1}}} - x^{\frac{q}{q_0}}x^{\frac{q_0}{q_0}} \in \mathbb{F}_q(x, y_1)$$

satisfies $z_1^p - z_1 = x(x^{\frac{q}{q_0}} - x^{q_0})$. In particular, if $\tilde{\mathcal{F}}_1$ is the geometrically irreducible plane curve given in affine coordinates by

$$\tilde{\mathcal{F}}_1 : Y^p - Y = X(X^{\frac{q}{q_0}} - X^{q_0}),$$

and $\tilde{\mathcal{X}}_1$ is its nonsingular model, then $(\tilde{\mathcal{F}}_1, (x, z_1))$ is another plane model for E_1, and

$$\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{S}}) - (q^n + 1) = \frac{q-1}{p-1}\left(\mathrm{N}_{q^n}(\tilde{\mathcal{X}}_1) - (q^n + 1)\right)$$

for each positive integer n.

Proof. The equalities $E_1 = \overline{\mathbb{F}}_q(x, z_1)$ and $\mathbb{F}_q(x, y_1) = \mathbb{F}_q(x, z_1)$ follow immediately from the definition of z_1. Further,

$$\begin{aligned}z_1^p - z_1 &= y_1^p - y_1 - x^q x^{q_0} + x^{\frac{q}{q_0}}x^{\frac{q_0}{q_0}}\\ &= x^{q_0}(x^q - x) - x^q x^{q_0} + x^{\frac{q}{q_0}}x\\ &= x(x^{\frac{q}{q_0}} - x^{q_0})\end{aligned}$$

as desired, and the other statements follow from the geometric irreducibility of $\tilde{\mathcal{F}}_1$ given in Proposition 2.3. □

3.2. **The Number of $\mathbb{F}_{q^n}$-Rational Points on $\tilde{\mathcal{F}}_1 : Y^p - Y = X(X^{\frac{q}{q_0}} - X^{q_0})$.** Considering the notation as in Subsection 2.2, let $\tilde{\mathcal{F}}_1 = \mathcal{F}_R$, where

$$R(X) = X^{\frac{q}{q_0}} - X^{q_0}.$$

To apply Proposition 2.4, let us determine the dimension of $W_R^{(n)}$ over $\mathbb{F}_p$ based on the characterization provided in Proposition 2.5. For this, we first note that

$$E_R(T) = (T - T^q)^p - (T - T^q).$$

Thus the following statements are equivalent for an element $\alpha \in \mathbb{F}_{q^n}$:

1. $\alpha \in W_R^{(n)}$
2. $E_R(\alpha) = 0$
3. $\alpha^q - \alpha \in \mathbb{F}_p$,

and from a straightforward calculation, we obtain the subsequent result.

Lemma 3.5. *Let $\beta \in \mathbb{F}_p$ be fixed. Then,*

$$\#\left\{\alpha \in \mathbb{F}_{q^n} \ : \ \alpha^q - \alpha - \beta = 0\right\} = \begin{cases} q, & \text{if } n\beta = 0 \\ 0, & \text{otherwise.} \end{cases}$$

In particular, the splitting field of $E_R(T)$ is $\mathbb{F}_{q^p}$,

$$\#W_R^{(n)} = \begin{cases} pq, & \text{if } p \mid n \\ q, & \text{otherwise,} \end{cases}$$

and

$$\dim_{\mathbb{F}_p}(W_R^{(n)}) = \begin{cases} m+1, & \text{if } p \mid n \\ m, & \text{otherwise.} \end{cases}$$

Recall that m is odd. Therefore, since Proposition 2.3 provides that the genus of $\tilde{\mathcal{X}}_1$ is given by

$$g(\tilde{\mathcal{X}}_1) \coloneqq \frac{p^t(p-1)}{2},$$

as a consequence of Proposition 2.4, Lemma 3.5, and the considerations in Subsection 2.2, the following holds.

Lemma 3.6. *The number of $\mathbb{F}_{q^n}$-rational points on $\tilde{\mathcal{X}}_1$ can be described as follows.*

1. *If $p \mid n$, then*

$$\mathrm{N}_{q^n}(\tilde{\mathcal{X}}_1) = \begin{cases} q^n + 1, & \text{if } n \text{ is odd} \\ q^n + 1 \pm 2g(\tilde{\mathcal{X}}_1)q^{n/2}, & \text{if } n \text{ is even.} \end{cases} \tag{3.2}$$

2. *If $p \nmid n$, then*

$$\mathrm{N}_{q^n}(\tilde{\mathcal{X}}_1) = \begin{cases} q^n + 1 \pm 2g(\tilde{\mathcal{X}}_1)q^{n/2}p^{-1/2}, & \text{if } n \text{ is odd} \\ q^n + 1, & \text{if } n \text{ is even.} \end{cases} \tag{3.3}$$

In particular, $\mathrm{N}_q(\tilde{\mathcal{X}}_1) = qp + 1$, and $\tilde{\mathcal{X}}_1$ is $\mathbb{F}_{q^n}$-maximal or minimal if and only if $p \mid n$ and n is even.

Therefore, to determine the sign $\pm$ in (3.2) and (3.3), the analysis is separated in two cases.

3.2.1. *The Case $p \mid n$.* The following result is used to determine the sign in (3.2).

Theorem 3.7 (6, Comments on page 105 and Theorem 7.4)**.** *There exist $\beta \in \mathbb{F}_{q^p}$ and an $\mathbb{F}_{q^p}$-rational morphism $\varphi : \tilde{\mathcal{X}}_1 \to \mathfrak{X}_\beta$, where $\mathfrak{X}_\beta$ is the nonsingular model defined over $\mathbb{F}_{q^p}$ of*

$$Y^p - Y = \beta X^2.$$

Based on the previous result, consider $\tilde{\mathcal{X}}_1$, $\mathfrak{X}_\beta$, and φ defined over the extensions $\mathbb{F}_{q^n}$ of $\mathbb{F}_{q^p}$, where n is even. In particular, β is a square in all these extensions, and since m is odd, the following occurs.

Proposition 3.8 (6, Lemma 9.1)**.** *Let n be an even positive integer such that $p \mid n$. Then, $\mathfrak{X}_\beta$ is $\mathbb{F}_{q^n}$-maximal if and only if $\eta((-1)^{n/2}) = -1$; that is, if and only if*

$$p \equiv 3 \pmod 4 \text{ and } n \equiv 2 \pmod 4.$$

Note that the essential part of Proposition 3.8 is given by the information over the extension $\mathbb{F}_{q^{2p}}$. Indeed, it follows from (2.1) that if $\mathfrak{X}_\beta$ is $\mathbb{F}_{q^{2p}}$-maximal, then it is $\mathbb{F}_{q^n}$-maximal for $p \mid n$ and $n \equiv 2 \pmod 4$.

Therefore, from Theorem 2.2, the sign in (3.2) is obtained.

Lemma 3.9. *Let n be an even positive integer such that $p \mid n$. The curve $\tilde{\mathcal{X}}_1$ is $\mathbb{F}_{q^n}$-maximal if and only if $p \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$. In particular,* (3.2) *can be rewritten in the form*

$$\mathrm{N}_{q^n}(\tilde{\mathcal{X}}_1) = \begin{cases} q^n+1, & \text{if } n \text{ is odd} \\ q^n+1-\eta((-1)^{n/2})\cdot 2g(\tilde{\mathcal{X}}_1)q^{n/2}, & \text{if } n \text{ is even.} \end{cases}$$

3.2.2. *The Case $p \nmid n$.* Let s be the period of $\tilde{\mathcal{X}}_1$ over $\mathbb{F}_q$. From Lemmas 3.6 and 3.9,

$$s = \begin{cases} 2p, & \text{if } \eta(-1)=1 \\ 4p, & \text{if } \eta(-1)=-1. \end{cases} \tag{3.4}$$

Since $\gcd(n,s)=1$, for each odd positive integer n such that $p \nmid n$, and $\mathrm{N}_q(\tilde{\mathcal{X}}_1) = qp+1$ from Lemma 3.6, the sign in (3.3) is obtained via a straightforward application of Theorem 2.1.

Lemma 3.10. *If $p \nmid n$, then*

$$\mathrm{N}_{q^n}(\tilde{\mathcal{X}}_1) = \begin{cases} q^n+1+\eta((-1)^{(n-1)/2}n)\cdot 2g(\tilde{\mathcal{X}}_1)q^{n/2}p^{-1/2}, & \text{if } n \text{ is odd} \\ q^n+1, & \text{if } n \text{ is even.} \end{cases}$$

3.3. **Conclusion.** Theorem 1.1 follows from Lemmas 3.4, 3.9, and 3.10. ∎

4. Proof of Theorem 1.2

From Proposition 3.2 and Lemma 3.4,

$$L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(T) = \left(L_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T)\right)^{\frac{q-1}{p-1}}, \tag{4.1}$$

which shows that $L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(T)$ is essentially determined by $L_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T)$. Defining

$$M_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T) \coloneqq T^{2g(\tilde{\mathcal{X}}_1)} L_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(q^{-1/2}T^{-1}) \in \mathbb{Q}(p^{1/2})[T],$$

then

$$M_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T) = \prod_{i=1}^{2g(\tilde{\mathcal{X}}_1)} (T-\xi_i),$$

where, for $i=1,\dots,2g(\tilde{\mathcal{X}}_1)$, the elements $\xi_i \in \mathbb{C}$ satisfy

$$-q^{-n/2}\left[\mathrm{N}_{q^n}(\tilde{\mathcal{X}}_1) - (q^n+1)\right] = \sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i^n. \tag{4.2}$$

Note that

$$M_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T) = L_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(q^{-1/2}T).$$

Thus to determine the L-polynomial $L_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T)$, it is sufficient to describe the polynomial $M_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T)$. Further, since $\tilde{\mathcal{X}}_1$ is a supersingular curve with period s given by (3.4), the following holds

$$\min\left\{n \ : \ \xi_i^n = 1 \text{ for all } i=1,\dots,2g(\tilde{\mathcal{X}}_1)\right\} = \begin{cases} 2p, \text{ if } \eta(-1)=1 \\ 4p, \text{ if } \eta(-1)=-1. \end{cases} \tag{4.3}$$

From (4.3) and Lemma 3.9,

$$\xi_i^2 \in \begin{cases} \mu_p^{prim} \cup \{1\}, & \text{if } \eta(-1)=1 \\ \mu_{2p}^{prim} \cup \{-1\}, & \text{if } \eta(-1)=-1, \end{cases}$$

and so

$$\sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i^2 = r_0\Big(\eta(-1)\cdot 1\Big) + r_1\Big(\eta(-1)\cdot \zeta_p\Big) + \cdots + r_{p-1}\Big(\eta(-1)\cdot \zeta_p^{p-1}\Big),$$

with $r_i \in \mathbb{N}$ being such that $\sum_{i=0}^{p-1} r_i = 2g(\tilde{\mathcal{X}}_1) = p^t(p-1)$. Also, (4.2) and Lemma 3.10 imply that

$$\sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i^2 = 0,$$

and then $r_0 = r_1 = \cdots = r_{p-1} = p^{t-1}(p-1)$. Thus

$$M_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T) = \prod_{i=1}^{2g(\tilde{\mathcal{X}}_1)} (T-\xi_i) = \prod_{i=0}^{p-1} (T-\lambda_i)^{m_i}(T+\lambda_i)^{n_i}, \tag{4.4}$$

where $m_i, n_i \in \mathbb{N}$ are such that $m_i + n_i = p^{t-1}(p-1)$, and $\pm\lambda_i$ are the square roots of the p elements in

$$\begin{cases} \mu_p^{prim} \cup \{1\}, & \text{if } \eta(-1) = 1 \\ \mu_{2p}^{prim} \cup \{-1\}, & \text{if } \eta(-1) = -1 \end{cases}$$

for each $i = 0, \ldots, p-1$. Label the elements λ_i in a way that

$$\lambda_i = \begin{cases} \zeta_p^i, & \text{if } \eta(-1) = 1 \\ \mathbf{i}\zeta_p^i, & \text{if } \eta(-1) = -1. \end{cases}$$

Furthermore, from (4.2) and Lemmas 3.9, 3.10, $\sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i^p = 0$ and

$$\sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i = -p^{t-1}(p-1)p^{1/2}.$$

Since (4.3) and Lemma 3.9 imply that

$$\xi_i^p = \begin{cases} \pm 1, & \text{if } \eta(-1) = 1 \\ \pm\mathbf{i}, & \text{if } \eta(-1) = -1, \end{cases}$$

by the choice of λ_i and equation (4.4),

$$g(\tilde{\mathcal{X}}_1) = \sum_{i=0}^{p-1} m_i = \sum_{i=0}^{p-1} n_i \tag{4.5}$$

$$-p^{t-1}(p-1)p^{1/2} = \sum_{i=0}^{p-1} (m_i - n_i)\lambda_i. \tag{4.6}$$

From the Quadratic Gauss Sum [31, Theorem 5.15],

$$p^{1/2} = \sum_{i=0}^{p-1} \eta(-i)\lambda_i. \tag{4.7}$$

Hence (4.5) and $m_i + n_i = p^{t-1}(p-1)$ yield $n_0 = m_0 = \frac{p^{t-1}(p-1)}{2}$, and considering $1 \leqslant i \leqslant p-1$,

$$(m_i, n_i) = \begin{cases} (0, p^{t-1}(p-1)), & \text{if } \eta(-i) = 1 \\ \\ (p^{t-1}(p-1), 0), & \text{if } \eta(-i) = -1. \end{cases}$$

In particular, $M_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T)$ in (4.4) becomes

$$(T^2 - \eta(-1))^{\frac{p^{t-1}(p-1)}{2}} \left(\prod_{\eta(i)=1} (T + \eta(-1)\lambda_i) \prod_{\eta(i)=-1} (T - \eta(-1)\lambda_i) \right)^{p^{t-1}(p-1)}.$$

Let $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be such that $\sigma_i(\zeta_p) = \zeta_p^i$, with $1 \leqslant i \leqslant p-1$. Then, from the Quadratic Gauss Sum

$$\sigma_i(\tilde{p}^{1/2}) = \eta(i) \cdot \tilde{p}^{1/2},$$

where $\tilde{p}^{1/2} \in \mathbb{Q}(\zeta_p)$ is defined as in (1.3), and

$$\sigma_i(-\zeta_p/\tilde{p}^{1/2}) = -\eta(-i)\lambda_i/p^{1/2} = -\eta(i) \cdot \eta(-1)\lambda_i/p^{1/2}$$

for each $i \in \{1, \ldots, p-1\}$ yields

$$\begin{aligned} & \prod_{\eta(i)=1} (p^{1/2}T + \eta(-1)\lambda_i) \prod_{\eta(i)=-1} (p^{1/2}T - \eta(-1)\lambda_i) \\ = \; & p^{(p-1)/2} \prod_{\eta(i)=1} (T + \eta(-1)\lambda_i/p^{1/2}) \prod_{\eta(i)=-1} (T - \eta(-1)\lambda_i/p^{1/2}) \\ = \; & p^{(p-1)/2} \prod_{i=1}^{p-1} \left(T - \sigma_i(-\zeta_p/\tilde{p}^{1/2}) \right) \\ = \; & p^{(p-1)/2} \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})} \left(T - \sigma(-\zeta_p/\tilde{p}^{1/2}) \right) \\ = \; & p^{(p-1)/2} \mathcal{M}_p(T), \end{aligned}$$

where $\mathcal{M}_p(T)$ is the minimal polynomial over $\mathbb{Q}$ of $-\zeta_p/\tilde{p}^{1/2}$. Therefore, (1.4) follows from (4.1) and the equalities

$$L_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(T) = M_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(q^{1/2}T) = M_{\tilde{\mathcal{X}}_1/\mathbb{F}_q}(p^{t-1}p^{1/2}T).$$

Further, (4.2),

$$M_{\tilde{\mathcal{X}}_1/\mathbb{F}_{q^n}}(T) = \prod_{i=1}^{2g(\tilde{\mathcal{X}}_1)} (T - \xi_i^n),$$

where $M_{\tilde{\mathcal{X}}_1/\mathbb{F}_{q^n}}(T) = T^{2g(\tilde{\mathcal{X}}_1)} L_{\tilde{\mathcal{X}}_1/\mathbb{F}_{q^n}}(q^{-n/2}T^{-1})$, and a straightforward calculation give the second part of Theorem 1.2. ∎

5. Proof of Theorem 1.3

Consider the notation as in Subsections 2.3 and 2.4. Let $\mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$ be the stabilizer of $Q_\infty \in \mathcal{X}_{\mathcal{G}_\mathcal{S}}$, $\mathrm{Aut}^{(1)}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$ be the unique Sylow p-subgroup of $\mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$, and $\mathbb{H}$ be the cyclic complement of $\mathrm{Aut}^{(1)}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$ in $\mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$.

Let $\mathfrak{G}$ be the set of maps on $\overline{\mathbb{F}}_q(\mathcal{X}_{\mathcal{G}_\mathcal{S}}) = \overline{\mathbb{F}}_q(x, y)$ given by

$$(x, y) \mapsto (\alpha x + \beta, \alpha\beta^{q_0} x + \alpha^{q_0+1} y + \gamma),$$

where $\alpha \in \mathbb{F}_q^*$ and $\beta, \gamma \in \mathbb{F}_q$. One can check that $\mathfrak{G}$ is a subgroup of $\mathrm{Aut}(\mathcal{X}_{\mathcal{G}_S})$ of order $q^2(q-1)$. Moreover, the following lemma holds.

Lemma 5.1. $\mathfrak{G} = \mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})$.

Proof. The inclusion $\mathfrak{G} \subseteq \mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})$ is straightforward. To show the other inclusion, let $\sigma \in \mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})$. From Proposition 2.9, $\{1, x\}$ and $\{1, x, y\}$ are bases for the Riemann–Roch spaces $\mathscr{L}(qQ_\infty)$ and $\mathscr{L}((q+q_0)Q_\infty)$, respectively. Therefore, $\sigma(x) \in \mathscr{L}(qQ_\infty)$, $\sigma(y) \in \mathscr{L}((q+q_0)Q_\infty)$, and

$$\sigma(x) = \alpha x + \gamma \text{ and } \sigma(y) = \alpha_1 x + \beta_1 y + \gamma_1$$

for some $\alpha, \alpha_1, \beta_1, \gamma, \gamma_1 \in \overline{\mathbb{F}}_q$, with $\alpha\beta_1 \neq 0$. Since σ is an $\overline{\mathbb{F}}_q$-automorphism,

$$0 = \sigma(0) = \sigma(y^q - y - x^{q_0}(x^q - x)) = \sigma(y)^q - \sigma(y) - \sigma(x)^{q_0}(\sigma(x)^q - \sigma(x)),$$

and thus

$$\begin{gathered}(\alpha_1 X + \beta_1 Y + \gamma_1)^q - (\alpha_1 X + \beta_1 Y + \gamma_1) - (\alpha X + \gamma)^{q_0}((\alpha X + \gamma)^q - (\alpha X + \gamma)) \\ = \delta(Y^q - Y - X^{q_0}(X^q - X))\end{gathered}$$

for some $\delta \in \overline{\mathbb{F}}_q^*$. Therefore, comparing the coefficients on both sides of the previous equality, the following is obtained

- $\alpha \in \mathbb{F}_q^*$
- $\gamma \in \mathbb{F}_q$
- $\alpha_1 = \alpha\gamma^{q_0} \in \mathbb{F}_q$
- $\beta_1 = \alpha^{q_0+1}$
- $\gamma_1 \in \mathbb{F}_q$,

which completes the proof. □

Consider the subgroup of $\mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})$ consisting of the maps

$$(x, y) \mapsto (x + \beta, \beta^{q_0} x + y + \gamma),$$

where $\beta, \gamma \in \mathbb{F}_q$, which is a Sylow p-subgroup of $\mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})$ (of order q^2). From Proposition 2.10, this describes the subgroup $\mathrm{Aut}^{(1)}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})$. Also, the cyclic complement $\mathbb{H}$ of $\mathrm{Aut}^{(1)}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})$ in $\mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})$ can be given by the maps

$$(x, y) \mapsto (\alpha x, \alpha^{q_0+1} y),$$

where $\alpha \in \mathbb{F}_q^*$, which has order $q-1$, and

$$\mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S}) = \mathrm{Aut}^{(1)}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S}) \rtimes \mathbb{H}.$$

Finally, from Theorem 2.11, $\mathrm{Aut}(\mathcal{X}_{\mathcal{G}_S}) = \mathrm{Aut}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})$, which completes the proof. Indeed $|\mathrm{Aut}^{(1)}_{Q_\infty}(\mathcal{X}_{\mathcal{G}_S})| = q^2 > q_0(q-1) + 1 = 2g + 1$, where g is the genus of $\mathcal{X}_{\mathcal{G}_S}$, and also, since $p \neq 2$, a comparison of genus (when $t > 1$) and inflection points (when $m = t = 1$) shows that $\mathcal{X}_{\mathcal{G}_S}$ is not birationally equivalent to any of the curves (2.3), (2.4), and (2.5). ■

6. Applications, Examples, and Remarks

The following result regarding Hilbert class fields of curves can be found in [36, p. 367] and [37, Ch. VI, Sect. 2(8)].

Theorem 6.1. *Let $\mathcal{Y}$ be a curve defined over $\mathbb{F}_q$ of genus $g(\mathcal{Y}) \geqslant 2$. Assume that $\mathcal{Y}$ has a rational point $P_0 \in \mathcal{Y}(\mathbb{F}_q)$, and suppose that $\mathcal{Y}$ is embedded in its Jacobian $J_{\mathcal{Y}}$ by considering*

$$P_0 \mapsto 0.$$

If $\langle \mathcal{Y}(\mathbb{F}_q)\rangle \subsetneq J_{\mathcal{Y}}(\mathbb{F}_q)$, then, for each divisor i of $[J_{\mathcal{Y}}(\mathbb{F}_q) : \langle \mathcal{Y}(\mathbb{F}_q)\rangle]$, there exists an étale cover $\mathcal{Z}$ of $\mathcal{Y}$ of degree i and genus $g(\mathcal{Z}) = i \cdot (g(\mathcal{Y}) - 1) + 1$, which satisfies $\mathrm{N}_q(\mathcal{Z}) \geqslant i \cdot \mathrm{N}_q(\mathcal{Y})$.

The following example remarkably illustrates Theorem 6.1.

Example 6.2. Let $p = 7$ and $t = 1$, and consider $\mathcal{X}_{\mathcal{G}_S}$ embedded in $J_{\mathcal{X}_{\mathcal{G}_S}}$ via

$$Q_\infty \mapsto 0.$$

Using Magma [5], it is possible to check that

$$\begin{aligned} J_{\mathcal{X}_{\mathcal{G}_S}}(\mathbb{F}_7) &= \frac{\mathbb{Z}}{1822\mathbb{Z}} + \frac{\mathbb{Z}}{1822\mathbb{Z}} + \frac{\mathbb{Z}}{1822\mathbb{Z}} + \frac{\mathbb{Z}}{1822\mathbb{Z}} + \frac{\mathbb{Z}}{3644\mathbb{Z}} + \frac{\mathbb{Z}}{3644\mathbb{Z}} + \frac{\mathbb{Z}}{3644\mathbb{Z}} \\ &= \frac{\mathbb{Z}}{1822\mathbb{Z}} + \frac{\mathbb{Z}}{1822\mathbb{Z}} + \frac{\mathbb{Z}}{1822\mathbb{Z}} + \frac{\mathbb{Z}}{1822\mathbb{Z}} + \langle a_1\rangle + \langle a_2\rangle + \langle a_3\rangle, \end{aligned}$$

where a_i has order $3644 = 4 \cdot 911$ for all $i = 1, 2, 3$, and that the order of each $\mathbb{F}_7$-rational point of $\mathcal{X}_{\mathcal{G}_S}$ is $1822 = 2 \cdot 911$. In particular, the order of any element of $\langle \mathcal{X}_{\mathcal{G}_S}(\mathbb{F}_7)\rangle$ divides 1822, which shows that $a_i \notin \langle \mathcal{X}_{\mathcal{G}_S}(\mathbb{F}_7)\rangle$ for each $i = 1, 2, 3$, and $[J_{\mathcal{X}_{\mathcal{G}_S}}(\mathbb{F}_7) : \langle \mathcal{X}_{\mathcal{G}_S}(\mathbb{F}_7)\rangle] > 1$. Further, $911a_i + \langle \mathcal{X}_{\mathcal{G}_S}(\mathbb{F}_7)\rangle$ has order 2 or 4 in

$$\frac{J_{\mathcal{X}_{\mathcal{G}_S}}(\mathbb{F}_7)}{\langle \mathcal{X}_{\mathcal{G}_S}(\mathbb{F}_7)\rangle}$$

for each $i = 1, 2, 3$, and so these elements generate a subgroup of order 8.

From Theorem 6.1, there exists an étale cover $\mathcal{Z}^{(8)}_{\mathcal{X}_{\mathcal{G}_S}}$ (resp. $\mathcal{Z}^{(4)}_{\mathcal{X}_{\mathcal{G}_S}}$) of $\mathcal{X}_{\mathcal{G}_S}$ with genus $161 = 8 \cdot (g(\mathcal{X}_{\mathcal{G}_S}) - 1) + 1$ (resp. $81 = 4 \cdot (g(\mathcal{X}_{\mathcal{G}_S}) - 1) + 1$) and at least $400 = 8 \cdot \mathrm{N}_7(\mathcal{X}_{\mathcal{G}_S})$ (resp. $200 = 4 \cdot \mathrm{N}_7(\mathcal{X}_{\mathcal{G}_S})$) rational points. We point out here that from Oesterlé's bound, a curve of genus 161 (resp. 81) defined over $\mathbb{F}_7$ has at most 410 (resp. 226) $\mathbb{F}_7$-rational points.

Moreover, also from Theorem 6.1, there exists an étale cover $\mathcal{Z}^{(2)}_{\mathcal{X}_{\mathcal{G}_S}}$ of $\mathcal{X}_{\mathcal{G}_S}$ with genus $41 = 2 \cdot (g(\mathcal{X}_{\mathcal{G}_S}) - 1) + 1$ and at least $100 = 2 \cdot \mathrm{N}_7(\mathcal{X}_{\mathcal{G}_S})$ rational points, which shows that

$$\mathrm{N}_{41}(7) \coloneqq \max\left\{ \mathrm{N}_7(\mathcal{Y}) \ : \ \mathcal{Y} \text{ is a curve of genus 41 defined over } \mathbb{F}_7 \right\} \geqslant 100$$

and gives a new entry in [19]. ■

Deciding whether or not the set of $\mathbb{F}_q$-rational points on a curve $\mathcal{Y}$ defined over $\mathbb{F}_q$ generates the group $J_{\mathcal{Y}}(\mathbb{F}_q)$ is not an easy task. However, in some cases this can be done using information on the number of $\mathbb{F}_q$-rational points on $\mathcal{Y}$ and on its L-polynomial. For instance, the following result can be found in [39].

Theorem 6.3 (Voloch)**.** *Let $\mathcal{Y}$ be a curve defined over $\mathbb{F}_q$ of genus $g(\mathcal{Y}) \geqslant 2$, and assume that $\mathcal{Y}$ has an $\mathbb{F}_q$-rational point. If $\mathrm{N}_q(\mathcal{Y}) = \mathrm{N}_{q^n}(\mathcal{Y})$ and $L_{\mathcal{Y}/\mathbb{F}_q}(1) < L_{\mathcal{Y}/\mathbb{F}_{q^n}}(1)$, then, for each divisor i of $L_{\mathcal{Y}/\mathbb{F}_{q^n}}(1)/L_{\mathcal{Y}/\mathbb{F}_q}(1)$, there exists an étale cover $\mathcal{Z}$ of $\mathcal{Y}$ of degree i and genus $g(\mathcal{Z}) = i \cdot (g(\mathcal{Y}) - 1) + 1$, which satisfies $\mathrm{N}_{q^n}(\mathcal{Z}) \geqslant i \cdot \mathrm{N}_{q^n}(\mathcal{Y})$.*

As a consequence of the previous result, the following occurs.

Corollary 6.4. *For each divisor i of $L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_{q^2}}(1)/L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(1)$, there exists an étale cover of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ of degree i with at least $i(q^2+1)$ rational points over $\mathbb{F}_{q^2}$ and genus $i(g-1)+1$. Moreover, if $p > 3$ and $p \equiv -1 \pmod 3$, then for each divisor i of $L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_{q^3}}(1)/L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(1)$, there exists an étale cover of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ of degree i with at least $i(q^2+1)$ rational points over $\mathbb{F}_{q^3}$ and genus $i(g-1)+1$.*

To prove Corollary 6.4, the following lemma, whose proof is straightforward, is used.

Lemma 6.5. *Consider the notation as in Section 4. Then,*

$$p^{p-1}\mathcal{M}_p(T)\mathcal{M}_p(-T) = \Phi_p(\eta(-1)\cdot pT^2),$$

and $\mathcal{M}_p(T)$ corresponds to the irreducible factor of $\Phi_p(\eta(-1)\cdot pT^2)$ with positive linear coefficient. In particular,

$$L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(1) < L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_{q^n}}(1)$$

for each positive integer n.

Proof of Corollary 6.4. From Theorem 1.1, $\mathrm{N}_q(\mathcal{X}_{\mathcal{G}_\mathcal{S}}) = \mathrm{N}_{q^2}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$. Further, if $p > 3$ and $p \equiv -1 \pmod 3$, then $\mathrm{N}_q(\mathcal{X}_{\mathcal{G}_\mathcal{S}}) = \mathrm{N}_{q^3}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$. Therefore, the result follows from Theorem 6.3 and Lemma 6.5. ∎

Example 6.6. To apply Corollary 6.4, an explicit description of the well-known equality

$$\frac{L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_{q^2}}(1)}{L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(1)} = L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(-1)$$

is desirable. Based on Theorem 1.2, the following examples illustrate the cases $p = 5, 7$.

***p* = 5.** Here,

$$5^2 \cdot \mathcal{M}_5(T) = 25T^4 + 25T^3 + 15T^2 + 5T + 1,$$

where $\mathcal{M}_5(T)$ is the minimal polynomial of $-\zeta_5/5^{1/2}$ over $\mathbb{Q}$. Therefore,

$$5^2 \cdot \mathcal{M}_5(5^{t-1}T) = q^2T^4 + qq_0T^3 + 3qT^2 + q_0T + 1,$$

which gives that

$$L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(T) = \left((qT^2-1)\cdot(q^2T^4 + qq_0T^3 + 3qT^2 + q_0T + 1)^2\right)^{\frac{g}{5}}.$$

In particular,

$$L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(1) = (q-1)^{\frac{g}{5}} \cdot \left(q^2 + qq_0 + 3q + q_0 + 1\right)^{\frac{2g}{5}}$$

and

$$L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(-1) = (q-1)^{\frac{g}{5}} \left(q^2 - qq_0 + 3q - q_0 + 1\right)^{\frac{2g}{5}}.$$

$p = 7$. Analogous to the previous case,

$$L_{\mathcal{X}_{\mathcal{G}_S}/\mathbb{F}_q}(T) = \left((qT^2+1)\cdot(q^3T^6+q^2q_0T^5+3q^2T^4+qq_0T^3+3qT^2+q_0T+1)^2\right)^{\frac{g}{7}}.$$

In particular,

$$L_{\mathcal{X}_{\mathcal{G}_S}/\mathbb{F}_q}(1) = (q+1)^{\frac{g}{7}}\cdot(q^3+q^2q_0+3q^2+qq_0+3q+q_0+1)^{\frac{2g}{7}}$$

and

$$L_{\mathcal{X}_{\mathcal{G}_S}/\mathbb{F}_q}(-1) = (q+1)^{\frac{g}{7}}\cdot(q^3-q^2q_0+3q^2-qq_0+3q-q_0+1)^{\frac{2g}{7}}.$$

References

1. AUBRY, Y.; PERRET, M. Divisibility of zeta functions of curves in a covering. *Archiv der Mathematik*, v. 82, p. 205–213, 2004.
2. BALLICO, E.; RAVAGNANI, A. Embedding Suzuki curves in $\mathbb{P}^4$. *Journal of Commutative Algebra*, v. 7, p. 149–166, 2015.
3. BARTOLI, D.; MONTANUCCI, M.; ZINI, G. Weierstrass semigroups at every point of the Suzuki curve. `https://arxiv.org/abs/1811.07890`, 2018.
4. BASSA, A. et al. Towards a characterization of subfields of the Deligne–Lusztig function fields. *Journal of Combinatorial Theory, Series A*, v. 120, p. 1351–1371, 2013.
5. BOSMA, W.; CANNON, J.; PLAYOUST, C. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, v. 24, p. 235–265, 1997.
6. BOUW, I. et al. Zeta Functions of a Class of Artin–Schreier Curves with Many Automorphisms. In: EISCHEN, E. et al. (Eds.) *Directions in Number Theory: Proceedings of the 2014 WIN3 Workshop*. Cham: Springer, 2016. p. 87–124.
7. COULTER, R.; HENDERSON, M. A note on the roots of trinomials over a finite field. *Bulletin of the Australian Mathematical Society*, v. 69, p. 429–432, 2004.
8. CHEN, C. Y.; DUURSMA, I. Geometric Reed-Solomon codes of length 64 and 65 over $\mathbb{F}_8$. *IEEE Transactions on Information Theory*, v. 49, p. 1351–1353, 2003.
9. DELIGNE, P.; LUSZTIG, G. Representations of reductive groups over finite fields. *Annals of Mathematics*, v. 103, p. 103–161, 1976.
10. DEOLALIKAR, V. Determining irreducibility and ramification groups for an additive extension of the rational function fields. *Journal of Number Theory*, v. 97, p.269–286, 2002.
11. DUURSMA, I.; EID, A. Smooth embeddings for the Suzuki and Ree curves. In: Ballet, S. et al. (Eds.) *Algorithmic arithmetic, geometry, and coding theory*. Providence: American Mathematical Society, 2015. p. 251–291.
12. DUURSMA, I.; PARK, S. Delta sets for divisors supported in two points. *Finite Fields and Their Applications*, v. 18, p. 865–885, 2012.
13. DUURSMA, I.; STICHTENOTH, H.; VOSS, C. Generalized Hamming weights for duals of BCH codes, and maximal algebraic function fields. In: PELLIKAAN, R.; PERRET, M.; VLADUT, S. G. (Eds.) *Arithmetic, Geometry and Coding Theory: Proceedings of the International Conference held at Centre International de Rencontres de Mathématiques (CIRM), Luminy, France, June 28 - July 2, 1993*. Berlin, Boston: De Gruyter, 1996. p. 53–66.

14. EID, A. et al. Suzuki-invariant codes from the Suzuki curve. *Designs, Codes and Cryptography*, v. 81, p. 413–425, 2016.
15. FRIEDLANDER, H. et al. The a-numbers of Jacobians of Suzuki curves. *Proceedings of the American Mathematical Society*, v. 141, p. 3019–3028, 2013.
16. FUHRMANN, R.; TORRES, F. On Weierstrass points and optimal curves. *Supplemento ai Rendiconti del Circolo matematico di Palermo*, v. 51, p. 25–46, 1998.
17. GARCIA, A.; STICHTENOTH, H. Elementary abelian p-extensions of algebraic function fields. *Manuscripta Mathematica*, v. 72, p. 67–79, 1991.
18. van der GEER, G.; van der VLUGT, M. Reed–Muller codes and supersingular curves. I. *Compositio Mathematica*, v. 84, p. 333–367, 1992.
19. van der GEER, G. et al. Tables of Curves with Many Points. `http://www.manypoints.org`, 2009.
20. GIULIETTI, M. et al. On some Galois covers of the Suzuki and Ree curves. *Journal of Number Theory*, v. 189, p. 220–254, 2018.
21. GIULIETTI, M.; KORCHMÁROS, G. On automorphism groups of certain Goppa codes. *Designs, Codes and Cryptography*, v. 47, p. 177–190, 2008.
22. GIULIETTI, M.; KORCHMÁROS, G. Garden of curves with many automorphisms. In: NIEDERREITER, H. et al. (Eds.) *Algebraic Curves and Finite Fields: Cryptography and Other Applications*. Berlin, Boston: De Gruyter, 2014. p. 93–120.
23. GIULIETTI, M.; KORCHMÁROS, G.; TORRES, F. Quotients curves of the Suzuki curve. *Acta Arithmetica*, v. 122, p. 245–274, 2006.
24. HANSEN, J. P. Deligne-Lusztig varieties and group codes. In: STICHTENOTH, H.; TSFASMAN, M. A. (Eds.) *Coding Theory and Algebraic Geometry: Proceedings of the International Workshop held in Luminy, France, June 17-21, 1991*. Berlin, Heidelberg: Springer-Verlag, 1992. p. 63–81.
25. HANSEN, J. P.; STICHTENOTH, H. Group codes on certain algebraic curves with many rational points. *Applicable Algebra in Engineering, Communication and Computing*, v. 1, p. 67–77, 1990.
26. HENN, H. W. Funktionenkörper mit groβer Automorphismengruppe. *Journal für die reine und angewandte Mathematik*, v. 302, p. 96–115, 1978.
27. HIRSCHFELD, J. W. P.; KORCHMÁROS, G.; TORRES, F. *Algebraic Curves over a Finite Field*. Princeton: Princeton University Press, 2008.
28. KIRFEL, C.; PELLIKAAN, R. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE Transactions on Information Theory*, v. 41, p. 1720–1732, 1995.
29. LAUTER, K. Deligne-Lusztig curves as ray class fields. *Manuscripta Mathematica*, v. 98, p. 87–96, 1999.
30. LIANG, J. On the solutions of trinomial equations over finite fields. *Bulletin of the Calcutta Mathematical Society*, v. 70, p. 379–382, 1978.
31. LIDL, R.; H. NIEDERREITER, H. *Finite Fields*, Cambridge: Cambridge University Press, 1997.
32. MATTHEWS, G. L. Codes from the Suzuki function field. *IEEE Transactions on Information Theory*, v. 50, p. 3298–3302, 2004.
33. MCGUIRE, G.; YILMAZ, E. On the zeta functions of supersingular curves. *Finite Fields and Their Applications*, v. 54, p. 65–79, 2018.

34. MONTANUCCI, M.; TIMPANELLA, M.; ZINI, G. AG codes and AG quantum codes from cyclic extensions of the Suzuki and Ree curves. *Journal of Geometry*, v. 109: 23, 2018.
35. PEDERSEN, J. P.; S∅RENSEN, A. B. Codes from certain Algebraic Function Fields with many Rational Places. *Mat-Report 1990-11*, Technical University of Denmark.
36. ROSEN, M. The Hilbert class field in function fields. *Expositiones Mathematicae*, v. 5, p. 365–378, 1987.
37. SERRE, J. –P. *Algebraic groups and class fields.* New York: Springer, 1988.
38. SKABELUND, D. C. New maximal curves as ray class fields over Deligne–Lusztig curves. *Proceedings of the American Mathematical Society*, v. 146, p. 525–540, 2018.
39. VOLOCH, J. F. Jacobians of curves over finite fields. *Rocky Mountain Journal of Mathematics*, v. 30, p. 755–759, 2000.

Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, Avenida Trabalhador São-carlense, 400, CEP 13566–590, São Carlos, SP, Brazil
Email address: hborges@icmc.usp.br

Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, Rua Sérgio Buarque de Holanda, 651, CEP 13083–859, Campinas, SP, Brazil
Email address: mariananery@alumni.usp.br