ON THE AUTOMORPHISM GROUP OF A FAMILY OF MAXIMAL CURVES NOT COVERED BY THE HERMITIAN CURVE

MARIA MONTANUCCI, GUILHERME TIZZIOTTI, AND GIOVANNI ZINI

ABSTRACT. In this paper we compute the automorphism group of the curves $\mathcal{X}_{a,b,n,s}$ and $\mathcal{Y}_{n,s}$ introduced in Tafazolian et al. [27] as new examples of maximal curves which cannot be covered by the Hermitian curve. They arise as subcovers of the first generalized GK curve (GGS curve). As a result, a new characterization of the GK curve, as a member of this family, is obtained.

Keywords: maximal curve, GK curve, automorphism group.
MSC 2020: 14H37, 11G20

1. Introduction

Let $\mathcal{X}$ be a nonsingular, projective, geometrically irreducible algebraic curve of positive genus g defined over a finite field $\mathbb{F}_q$ with q elements and let $\mathcal{X}(\mathbb{F}_q)$ be the set of its $\mathbb{F}_q$-rational points. The curve $\mathcal{X}$ is called $\mathbb{F}_q$-maximal if its number of $\mathbb{F}_q$-rational point attains the Hasse-Weil upper bound, namely equals $2g\sqrt{q}+q+1$. Clearly, maximal curves can only exist over fields whose cardinality is a perfect square. Apart for being of theoretical interest as extremal objects, maximal curves over finite fields have attracted a lot of attention in recent decades due to their applications to coding theory and cryptography. Maximal curves are indeed special for the structure of the so-called Weiestrass semigroup at one point, which is the main ingredient used in the literature to construct AG codes with good parameters.

The most important and well-studied example of a maximal curve is the so-called Hermitian curve $\mathcal{H}_q$ defined over $\mathbb{F}_{q^2}$ by the affine equation

$$\mathcal{H}_q : X^q + X = Y^{q+1}.$$

A well-known reason is that for fixed q, the curve $\mathcal{H}_q$ has the largest possible genus $g(\mathcal{H}_q) = q(q-1)/2$ that an $\mathbb{F}_{q^2}$-maximal curve can have. A result commonly attributed to Serre, see [18, Proposition 6], gives that any curve which is $\mathbb{F}_{q^2}$-covered by an $\mathbb{F}_{q^2}$-maximal curve is $\mathbb{F}_{q^2}$-maximal.

DEPARTMENT OF APPLIED MATHEMATICS AND COMPUTER SCIENCE, TECHNICAL UNIVERSITY OF DENMARK, 2800 KONGENS LYNGBY, DENMARK
FACULDADE DE MATEMÁTICA, UNIVERSIDADE FEDERAL DE UBERLÂNDIA, 2121 UBERLÂNDIA, BRAZIL
DEPARTMENT OF PHYSICS, INFORMATICS, AND MATHEMATICS, UNIVERSITY OF MODENA AND REGGIO EMILIA, 41125 MODENA, ITALY
E-mail addresses: marimo@dtu.dk, guilhermect@ufu.br, giovanni.zini@unimore.it.

Therefore many maximal curves can be obtained by constructing subcovers of already known maximal curves, in particular subcovers of the Hermitian curve. For a while it was speculated in the research community that perhaps all maximal curves could be obtained as subcovers of the Hermitian curve, but it was shown by Giulietti and Korchmáros that this is not the case, see [9].

Giulietti and Korchmáros constructed indeed a maximal curve over $\mathbb{F}_{q^6}$, today referred to as GK curve, which cannot be covered by the Hermitian curve whenever q is larger than 2. Garcia, Güneri, and Stichtenoth, in [8], presented a new family of maximal curves over $\mathbb{F}_{q^{2n}}$ (where n is odd), known as GGS curves, which generalizes the GK curve (when $n = 3$ the GGS curve and the GK curve coincide) and that is not Galois-covered by the Hermitian curve [8, 10]. Many applications of these curves in coding theory have been made in recent years, see e.g. [1], [2], [5], [7], [16] and [28].

Another generalization of the GK curve over $\mathbb{F}_{q^{2n}}$ (again n odd) has been introduced by Beelen and Montanucci in [3], which is now known as BM curves. These curves are not Galois-covered by the Hermitian curve as well, unless $q = 2$. Applications of the BM curves to coding theory can be found in [19] and [20].

Tafazolian, Teherán-Herrera, and Torres [27] presented two further examples of maximal curves over $\mathbb{F}_{q^{2n}}$ (n odd), denoted by $\mathcal{X}_{a,b,n,s}$ and $\mathcal{Y}_{n,s}$, that cannot be covered by the Hermitian curve. These examples are again closely related to the GK curve, as $\mathcal{Y}_{3,1}$ is exactly the GK constructed in [9]. They can be further seen as generalizations of the GGS, as $\mathcal{Y}_{n,1}$ is the GGS curve corresponding to the same parameter n.

The aim of this paper is to compute the full automorphism groups of the curves $\mathcal{X}_{a,b,n,s}$ and $\mathcal{Y}_{n,s}$ over the algebraic closure of $\mathbb{F}_{q^{2n}}$. More precisely, the following are the two central results obtained in this paper (the precise definition of the subgroups involved in the statement are in Sections 2 and 3).

Theorem 1.1. *Let q be a prime power, $n \geq 3$ odd, $m := (q^n + 1)/(q + 1)$, and s a divisor of m with $s \neq m$. If $3 \nmid n$ or $\frac{m}{s} \nmid (q^2 - q + 1)$, then $\mathrm{Aut}(\mathcal{Y}_{n,s})$ has order $q^3(q^2 - 1)m/s$ and is isomorphic to $S_{q^3} \rtimes C_{(q^2-1)\frac{m}{s}}$. If $3 \mid n$ and $\frac{m}{s} \mid (q^2 - q + 1)$, then $\mathrm{Aut}(\mathcal{Y}_{n,s})$ has order $(q^3 + 1)q^3(q^2 - 1)m/s$ and is isomorphic to $\mathrm{PGU}(3, q) \rtimes C_{m/s}$.*

Theorem 1.2. *Let $q = p^a$ be a prime power, $n \geq 3$ odd, $m := (q^n + 1)/(q + 1)$, s a divisor of m, and b a divisor of a. Assume that $b < a$ or $q^2 \nmid (\frac{m}{s} - 1)$. Then the automorphism group of $\mathcal{X}_{a,b,n,s}$ has order $\frac{q^3}{\bar{q}}(q + 1)(\bar{q} - 1)\frac{m}{s}$ and is isomorphic to $(S_{q^3}/E_{\bar{q}}) \rtimes C_{(q+1)(\bar{q}-1)m/s}$.*

Theorems 1.1 and 1.2 provide a new characterization of the GK curve as a member of the family of maximal curves $\mathcal{Y}_{n,s}$, $\mathcal{X}_{a,b,n,s}$ given in [27]. Indeed, Theorems 1.1 and 1.2 show which members in that family admit an automorphism group isomorphic to $\mathrm{PGU}(3, q)$, i.e. when the full automorphism group of the underlying Hermitian curve $\mathcal{H}_q$ can be completely lifted: they are exactly the GK curve $\mathcal{GK}$, together with its quotients $\mathcal{GK}/C$ over a subgroup C of the Galois group C_{q^2-q+1} of $\mathcal{GK} \to \mathcal{H}_q$. Theorem 1.1 also provides a different proof of the structure of the automorphism group of the GGS curve with respect to the ones given in [12] and [13].

The paper is organized as follows. In Chapter 2 the necessary background on maximal curves, their automorphism groups and general results in group theory are recalled. Chapter 3 contains the proofs of the two aforementioned theorems.

2. Preliminary results

2.1. **Automorphism groups of algebraic curves.** In this paper, $\mathcal{X}$ stands for a (projective, geometrically irreducible, non-singular) algebraic curve of genus $g = g(\mathcal{X}) \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of positive characteristic p. Let $\mathrm{Aut}(\mathcal{X})$ be the group of all automorphisms of $\mathcal{X}$. The assumption $g(\mathcal{X}) \geq 2$ ensures that $\mathrm{Aut}(\mathcal{X})$ is finite. However the classical Hurwitz bound $|\mathrm{Aut}(\mathcal{X})| \leq 84(g(\mathcal{X}) - 1)$ for complex curves fails in positive characteristic, and there exist four families of curves satisfying $|\mathrm{Aut}(\mathcal{X})| \geq 8g(\mathcal{X})^3$; see [25], [14], and [15, Section 11.12].

For a subgroup G of $\mathrm{Aut}(\mathcal{X})$, let $\bar{\mathcal{X}}$ denote a non-singular model of $\mathbb{K}(\mathcal{X})^G$, that is, a (projective, geometrically irreducible, non-singular) algebraic curve with function field $\mathbb{K}(\mathcal{X})^G$, where $\mathbb{K}(\mathcal{X})^G$ is the fixed field of G, i.e. the subfield of $\mathbb{K}(\mathcal{X})$ fixed elementwise by every element in G. Usually, $\bar{\mathcal{X}}$ is called the quotient curve of $\mathcal{X}$ by G and denoted by $\mathcal{X}/G$. The field extension $\mathbb{K}(\mathcal{X})/\mathbb{K}(\mathcal{X})^G$ is Galois of degree $|G|$.

Let Φ be the natural covering $\mathcal{X} \to \bar{\mathcal{X}}$, where $\bar{\mathcal{X}} = \mathcal{X}/G$. A point $P \in \mathcal{X}$ is a ramification point of G if the stabilizer G_P of P in G is nontrivial; the ramification index e_P is $|G_P|$; a point $\bar{Q} \in \bar{\mathcal{X}}$ is a branch point of G if there is a ramification point $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$; the ramification (branch) locus of G is the set of all ramification (branch) points. The G-orbit of $P \in \mathcal{X}$ is the subset $o = \{g(P) \in \mathcal{X} \colon g \in G\}$ of $\mathcal{X}$, and it is *long* if $|o| = |G|$, otherwise o is *short*. For a point $\bar{Q} \in \bar{\mathcal{X}}$, the G-orbit o lying over $\bar{Q}$ consists of all points $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$. If $P \in o$ then $|o| = |G|/|G_P|$ and hence $\bar{Q}$ is a branch point if and only if o is a short G-orbit. It may be that G has no short orbits. This is the case if and only if every non-trivial element in G is fixed–point-free on $\mathcal{X}$, that is, the covering Φ is unramified. On the other hand, G has a finite number of short orbits.

For a non-negative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $G_P^{(i)}$ (or $G_i(P)$ as in [23, Chapter IV]) and defined to be

$$G_P^{(i)} = \{\alpha \in G_P : \ v_P(\alpha(t) - t) \geq i + 1\},$$

where t is a uniformizing element (local parameter) at P. The main properties of the subgroup chain $G_P^{(0)} \supseteq G_P^{(1)} \supseteq G_P^{(2)} \supseteq \ldots$ are collected in the following lemma.

Lemma 2.1. [15, Theorem 11.49 and Theorem 11.74]

(1) $G_P^{(0)} = G_P = S \rtimes H$, *where* S *is a* p*-group and* H *is a cyclic group of order not divisible by* p.
(2) $G_P^{(1)} = S$ *is the unique Sylow* p*-subgroup (and maximal normal subgroup) of* G_P.
(3) For every $i \geq 1$, $G_P^{(i)}$ *is normal in* G_P *and the quotient group* $G_P^{(i+1)}/G_P^{(i)}$ *is elementary abelian.*

Let $\bar{g}$ be the genus of the quotient curve $\mathcal{X}/G$. The *Hurwitz genus formula* (also called Riemann-Hurwitz formula, see [24, Theorem 3.4.13]) gives the following equation:

$$2g-2=|G|(2\bar{g}-2)+\sum_{P\in\mathcal{X}} d_P, \tag{1}$$

where the different d_P at P is given by

$$d_P=\sum_{i\geq 0}(|G_P^{(i)}|-1), \tag{2}$$

see [15, Theorem 11.70]. Clearly the above contribution $\sum_{P\in\mathcal{X}}\sum_{i\geq 0}(|G_P^{(i)}|-1)$ can be re-written by summing with respect to the elements of $\alpha\in G$ and counting the number of $P's$ and $i's$ such that $\alpha\in G_P^{(i)}$. Doing so one can re-write the formula above as

$$2g-2=|G|(2\bar{g}-2)+\sum_{\alpha\in G\setminus\{id\}} i(\alpha), \tag{3}$$

where $i(\alpha)$ is called the contribution of the automorphism α to the covering Φ.

Let γ be the p-rank of $\mathcal{X}$, and let $\bar{\gamma}$ be the p-rank of the quotient curve $\mathcal{X}/G$. A formula relating γ and $\bar{\gamma}$ is known whenever G is a p-group: in this case, the *Deuring-Shafarevich formula* states that

$$\gamma-1=|G|(\bar{\gamma}-1)+\sum_{i=1}^{k}(|G|-\ell_i), \tag{4}$$

where $\ell_1,\dots,\ell_k$ are the sizes of the short orbits of G; see [26] or [15, Theorem 11.62].

A subgroup of $\mathrm{Aut}(\mathcal{X})$ is a prime-to-p group, or a p'-group, if its order is prime to p. A subgroup G of $\mathrm{Aut}(\mathcal{X})$ is *tame* if the 1-point stabilizer in G of any point of $\mathcal{X}$ is a p'-group. Otherwise, G is *non-tame* (or *wild*). By [15, Theorem 11.56], if $|G|>84(g(\mathcal{X})-1)$ then G is non-tame. An orbit o of G is *tame* if G_P is a p'-group for every $P\in o$.

The following lemma gives a strong restriction to the action of the Sylow p-subgroup of the 1-point stabilizer when $\mathcal{X}$ is a maximal curve. Actually, it holds for the class of curves with p-rank $\gamma=0$, which contains the maximal curves, see e.g. [15, Theorem 9.76].

Lemma 2.2. [11, Proposition 3.8, Theorem 3.10] *Let $\mathcal{X}$ be an $\mathbb{F}_{q^2}$-maximal curve of genus $g\geq 2$. Then the automorphism group $\mathrm{Aut}(\mathcal{X})$ fixes the set $\mathcal{X}(\mathbb{F}_{q^2})$ of $\mathbb{F}_{q^2}$-rational points. Also, automorphisms of $\mathcal{X}$ over the algebraic closure of $\mathbb{F}_{q^2}$ are always defined over $\mathbb{F}_{q^2}$.*

We can use Lemma 2.2 to ensure that a Sylow p-subgroup of a non-tame automorphism group of an $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ fixes exactly one $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$.

Corollary 2.3. *Let p denote the characteristic of the finite field $\mathbb{F}_{q^2}$ where $q=p^t$ and let $\mathcal{X}$ be an $\mathbb{F}_{q^2}$-maximal curve with genus $g=g(\mathcal{X})\geq 2$ such that $p\mid|\mathrm{Aut}(\mathcal{X})|$. If H is a p-subgroup of $\mathrm{Aut}(\mathcal{X})$, then H fixes exactly one point $P\in\mathcal{X}(\mathbb{F}_{q^2})$ and acts semiregularly on the set of the remaining $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$.*

Proof. Assume first that H is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$. Then from Lemma 2.2, H acts on the set $\mathcal{X}(\mathbb{F}_{q^2})$ of $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$. Since $|\mathcal{X}(\mathbb{F})| \equiv 1 \pmod p$, H must fix at least one point $P \in \mathcal{X}(\mathbb{F}_{q^2})$. Also, $\mathcal{X}$ has zero p-rank and hence the claim follows from [15, Lemma 11.129]. Now assume that H is an arbitrary p-subgroup of $\mathrm{Aut}(\mathcal{X})$. Since H is contained in at least one Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$, and the property of fixing a point $P \in \mathcal{X}$ and being semiregular elsewhere is preserved by subgroups, the claim follows for H as well. □

If the bound $|G| > 84(g(\mathcal{X}) - 1)$ is satisfied, a lot can be said about the structure of the short orbits of G on $\mathcal{X}$. The following theorem lists all the possibilities.

Theorem 2.4. [15, Theorem 11.56 and Lemma 11.111] Let $\mathcal{X}$ be an irreducible curve of genus $g \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of characteristic p.

- If G has at least five short orbits then $|G| \leq 4(g-1)$.
- If G has four short orbits then $|G| \leq 12(g-1)$.
- If G has exactly one short orbit, then the length of this orbit divides $2g-2$.
- If $p > 0$ and $|G| > 84(g-1)$ then the fixed field $\mathbb{K}(\mathcal{X})^G$ is rational and G has at most three short orbits, namely:
  (1) exactly three short orbits, two tame of length $|G|/2$ and one non-tame, with $p \geq 3$; or
  (2) exactly two short orbits, both non-tame; or
  (3) only one short orbit, which is non-tame, whose length divides $2g-2$; or
  (4) exactly two short orbits, one tame and one non-tame.
- In any case $|G| < 8g^3$ unless one of the following cases occurs up to isomorphism over $\mathbb{K}$:
  - $p = 2$ and $\mathcal{X}$ is a non-singular model of $Y^2 + Y = X^{2k+1}$, with $k > 1$;
  - $p > 2$ and $\mathcal{X}$ is a non-singular model of $Y^2 = X^n - X$, where $n = p^h$ and $h > 0$;
  - $\mathcal{X}$ is the Hermitian curve $\mathcal{H}_q : Y^{q+1} = X^q + X$ where $q = p^h$ and $h > 0$;
  - $\mathcal{X}$ is the non-singular model of the Suzuki curve $\mathcal{S}_q : X^{q_0}(X^q + X) = Y^q + Y$, where $q_0 = 2^r$, $r \geq 1$ and $q = 2q_0^2$.

A tool we will use to compute automorphism groups is the so-called Weierstrass semigroup $H(P)$ at a point $P \in \mathcal{X}$:

$$H(P) := \{i \in \mathbb{N} \colon \exists f \in \mathbb{K}(\mathcal{X}), (f)_\infty = iP\}.$$

It is well-known that the set $H(P)$ is a numerical semigroup and that from the Weierstrass gap theorem the set of gaps $G(P) := \mathbb{N} \setminus H(P)$ has cardinality g, see e.g. [24, Theorem 1.6.8]. Points that are in the same orbit under the action of an automorphism group of $\mathcal{X}$ have the same Weierstrass semigroup, see [24, Lemma 3.5.2]. The following lemma provides a tool to compute gaps.

Lemma 2.5. [29, Corollary 14.2] *Let $\mathcal{X}$ be an algebraic curve of genus g defined over $\mathbb{K}$. Let P be a point of $\mathcal{X}$ and ω be a regular differential on $\mathcal{X}$. Then $v_P(\omega) + 1$ is a gap at P.*

In the following section the first generalized GK curve will be introduced, and with that also the protagonists of this paper, namely the curves $\mathcal{Y}_{n,s}$ and $\mathcal{X}_{a,b,n,s}$.

2.2. **The first generalized GK curve $\mathcal{C}_n$ (GGS curve).** As mentioned in the introduction, from a result commonly attributed to Serre [17], we know that every curve which is $\mathbb{F}_{q^2}$-covered by an $\mathbb{F}_{q^2}$-maximal curve is itself also $\mathbb{F}_{q^2}$-maximal. The most important example of $\mathbb{F}_{q^2}$-maximal curve is the Hermitian curve $\mathcal{H}_q$, with affine equation $Y^{q+1} = X^{q+1} - 1$ or $Y^{q+1} = X^q + X$. The automorphisms group of $\mathcal{H}_q$ is very large compared to $g(\mathcal{H}_q)$. Indeed it is isomorphic to $\mathrm{PGU}(3,q)$ and its order is larger than $16g(\mathcal{H}_q)^4$. Moreover $\mathcal{H}_q$ has the largest genus admissible for an $\mathbb{F}_{q^2}$-maximal curve and it is the unique curve having this property up to birational isomorphism, see [22].

Few examples of maximal curves not covered by $\mathcal{H}_q$ are known in the literature. In [9] Giulietti and Korchmáros constructed an $\mathbb{F}_{q^6}$-maximal curve, nowadays known as the GK curve, which is not a subcover of the Hermitian curve $\mathcal{H}_{q^3}$ whenever $q \geq 3$. An affine space model for it is

$$\mathcal{GK} : \begin{cases} Z^{q^2-q+1} = Y\frac{X^{q^2}-X}{X^q+X} \\ Y^{q+1} = X^q + X \end{cases} .$$

The full automorphism group of $\mathcal{GK}$ has order $(q^3+1)q^3(q^2-1)(q^2-q+1)$. It is generated by two normal subgroups, one isomorphic to $\mathrm{PGU}(3,q)$ and the other cyclic of order q^2-q+1, and contains $\mathrm{PGU}(3,q) \times C_{\frac{q^2-q+1}{\gcd(3,q+1)}}$ as a normal subgroup of index $\gcd(3,q+1)$; see [9, Section 5].

Two generalizations of the GK curve into infinite families of maximal curves are known in the literature and they are not Galois subcovers of the corresponding maximal Hermitian curve. The first generalization $\mathcal{C}_n$ was introduced by Garcia, Güneri and Stichtenoth in [8], whence the name of GGS curve. For any prime power q and odd $n \geq 3$, the GGS curve $\mathcal{C}_n$ is given by the affine space model

$$\mathcal{C}_n : \begin{cases} Z^m = Y\frac{X^{q^2}-X}{X^q+X} \\ Y^{q+1} = X^q + X \end{cases} \tag{5}$$

where $m := \frac{q^n+1}{q+1}$; $\mathcal{C}_n$ is equivalently defined by the equations

$$\mathcal{C}_n : \quad Z^m = Y^{q^2} - Y, \quad Y^{q+1} = X^q + X.$$

Notice that $\mathcal{C}_3$ is the GK curve $\mathcal{GK}$. The curve $\mathcal{C}_n$ is $\mathbb{F}_{q^{2n}}$-maximal of genus $g(\mathcal{C}_n) = (q-1)(q^{n+1}+q^n-q^2)/2$. Whenever $n \geq 5$, $\mathcal{C}_n$ is not a Galois subcover of $\mathcal{H}_{q^n}$; see [6] for $q \geq 3$ and [10] for $q = 2$.

For any $n \geq 5$, the automorphism group of $\mathcal{C}_n$ was determined independently in [12] and [13]. It has order $q^3(q^2-1)m$ and it is a semidirect product $\mathrm{Aut}(\mathcal{C}_n) = S_{q^3} \rtimes \Sigma$, where

$$\begin{aligned} S_{q^3} &= \left\{(x,y,z) \mapsto (x + b^q y + c, y + b, z) \,:\, b,c \in \mathbb{F}_{q^2}, c^q + c = b^{q+1}\right\} \cong E_q \,.\, E_{q^2} \,, \\ \Sigma &= \left\{(x,y,z) \mapsto (x,y,z) \mapsto (\zeta^{q^n+1}x, \zeta^m y, \zeta z) \,:\, \zeta^{(q^n+1)(q-1)} = 1\right\} \cong C_{(q^n+1)(q-1)} \,. \end{aligned}$$

Let x, y, z be the coordinate functions. The function field $\mathbb{F}_{q^{2n}}(x,y,z)$ of $\mathcal{C}_n$ is a Kummer extension of degree m of the Hermitian function field $\mathbb{F}_{q^{2n}}(x,y)$, the Galois group of $\mathbb{F}_{q^{2n}}(x,y,z)/\mathbb{F}_{q^{2n}}(x,y)$ being the subgroup of order m in Σ. In this extension, the places

centered at the q^3+1 $\mathbb{F}_{q^2}$-rational points of $\mathcal{H}_q$ are the unique ramified places, and they are totally ramified.

The group $\mathrm{Aut}(\mathcal{C}_n)$ has exactly two short orbits on $\mathcal{C}_n$, namely the singleton $\{P_\infty\}$, where P_∞ is an $\mathbb{F}_{q^2}$-rational point of $\mathcal{C}_n$ (common pole of x, y and z), and the set $\mathcal{O}$ of the remaining q^3 $\mathbb{F}_{q^2}$-rational points of $\mathcal{C}_n$. The principal divisor of the variable z is

$$(z) = \sum_{P\in\mathcal{O}} P - q^3 P_\infty.$$

2.3. **The curves $\mathcal{Y}_{n,s}$ and $\mathcal{X}_{a,b,n,s}$.** Two families of subcovers $\mathcal{Y}_{n,s}$ and $\mathcal{X}_{a,b,n,s}$ of the GGS curve $\mathcal{C}_n$ were introduced and studied by Tafazolian, Tehéran-Herrera and Torres in [27].

Let q be a prime power, $n\geq 3$ be an odd integer and $s\geq 1$ be a divisor of $m=\frac{q^n+1}{q+1}$. We always assume $s\neq m$ (otherwise, $\mathcal{Y}_{n,s}$ is the Hermitian curve $\mathcal{H}_q$). The curve $\mathcal{Y}_{n,s}$ is defined over $\mathbb{F}_{q^{2n}}$ by the affine equations

$$\mathcal{Y}_{n,s}: \begin{cases} Z^{m/s} = Y^{q^2}-Y \\ Y^{q+1} = X^q + X \end{cases}. \tag{6}$$

It is an $\mathbb{F}_{q^{2n}}$-maximal curve and it has genus

$$g(\mathcal{Y}_{n,s}) = \frac{q^{n+2}-q^n-sq^3+q^2+s-1}{2s}.$$

The curve $\mathcal{Y}_{n,s}$ is clearly a subcover of the GGS curve, but it is also a generalization of the GGS, as it provides a larger family of maximal curves in which $\mathcal{C}_n$ lives from $\mathcal{Y}_{n,1}=\mathcal{C}_n$.

Let x,y,z be the coordinate functions of $\mathcal{Y}_{n,s}$, P_∞ be the unique common pole of x,y,z, and $P_{(\alpha,\beta,\gamma)}$ denote the $\mathbb{F}_{q^{2n}}$-rational point of $\mathcal{Y}_{n,s}$ which is a zero of $x-\alpha, y-\beta, z-\gamma$. Then, for any $\alpha,\beta\in\mathbb{F}_{q^{2n}}$, we have the following principal divisors:

$$(x-\alpha) = (q+1)m/sP_{(\alpha,0,0)} - (q+1)m/sP_\infty\ ; \tag{7}$$

$$(y-\beta) = \sum_{i=1}^{q} m/sP_{(\alpha_i,\beta,0)} - qm/sP_\infty,\ \text{with } \alpha_i^q+\alpha_i=\beta^{q+1}\ ; \tag{8}$$

$$(z) = \sum_{j=1}^{q^2}\sum_{i=1}^{q} P_{(\alpha_i,\beta_j,0)} - q^3P_\infty,\ \text{with } \alpha_i,\beta_j\in\mathbb{F}_{q^2} \text{ and } \beta_j^{q+1}=\alpha_i^q+\alpha_i \text{ for all } i,j. \tag{9}$$

We will denote with O the set $O:=\{P_{(\alpha_i,\beta_j,0)}:\ \alpha_i,\beta_j\in\mathbb{F}_{q^2},\ \beta_j^{q+1}=\alpha_i^q+\alpha_i\}$ of cardinality q^3 given by the totally ramified points in $\mathbb{F}_{q^2}(x,y,z)/\mathbb{F}_{q^2}(x,y)$ other than P_∞. From [27, Proposition 5.1] we have that $H(P_\infty)=\langle qm/s, q^3, (q+1)m/s\rangle$, and $H(P_\infty)$ is a telescopic semigroup.

The following lemma will be used to determine the full automorphism group of $\mathcal{Y}_{n,s}$.

Lemma 2.6. *Denote with dz the differential of the function z in the function field of $\mathcal{Y}_{n,s}$. Then (dz) is equal to*

$$K = (2g(\mathcal{Y}_{n,s})-2)P_\infty.$$

In particular, the canonical differential K is exact.

Proof. Denote with F the function field of $\mathcal{Y}_{n,s}$ over the algebraic closure $\mathbb{K}$ of $\mathbb{F}_{q^{2n}}$. By Equation (9), the function field extension $F/\mathbb{K}(z)$ is of degree q^3. More precisely, $F/\mathbb{K}(z)$ is a Galois extension whose Galois group $G \subseteq \mathrm{Aut}(\mathcal{Y}_{n,s})$ is $G = \{\theta_{b,c} : b, c \in \mathbb{F}_{q^2}, c^q + c = b^{q+1}\}$, where

$$\theta_{b,c}(x) = x + b^q y + c, \quad \theta_{b,c}(y) = y + b, \quad \theta_{b,c}(z) = z.$$

Since G fixes the function z, it fixes its divisor. This implies that G acts on the support of both zero and pole divisors of z given in (9). In particular, G fixes P_∞. Since $\mathcal{Y}_{n,s}$ is $\mathbb{F}_{q^{2n}}$-maximal it has p-rank zero. From [15, Lemma 11.129] P_∞ is the only ramified point in $F/\mathbb{K}(z)$, as elements of order a power of the characteristic p can only fix P_∞ and no other places in F. From [24, Theorem 3.4.6],

$$(\mathrm{Cotr}F/\mathbb{K}(z)(dz)) = (dz)_F = \mathrm{Con}F/\mathbb{K}(z)((dz)) + \mathrm{Diff}(F|\mathbb{K}(z)).$$

Since the support of both $\mathrm{Con}F|\mathbb{K}(z)((dz))$ and $\mathrm{Diff}(F|\mathbb{K}(z))$ is just P_∞, while the degree of the divisor $(dz)_F$ is $2g(\mathcal{Y}_{n,s}) - 2$, we get that $(dz) = K$. □

The maximality of $\mathcal{Y}_{n,s}$, the fact that each point of $O \cup \{P_\infty\}$ is totally ramified in the covering $\mathcal{Y}_{n,s} \to \mathcal{H}_q$ with $P \mapsto \bar{P}$ and the fact that $O \cup \{P_\infty\}$ is exactly where the ramification occurs, yield the existence of special functions on the function fields of both $\mathcal{Y}_{n,s}$ and the Hermitian curve $\mathcal{H}_q$, that can be arbitrarily difficult to construct by hands. This is a consequence of the so-called *Fundamental equation*, see [15, Section 9.8]. These functions are summarized in the following lemma.

Lemma 2.7. *Let $P = P_{(\alpha,\beta,\gamma,1)}$ be an $\mathbb{F}_{q^{2n}}$-rational point of $\mathcal{Y}_{n,s}$. Then there exists a function f_P in the function field of $\mathcal{Y}_{n,s}$ such that*

$$(\pi_P) = (q^n + 1)P - (q^n + 1)P_\infty,$$

that is the order of the equivalence class $[P - P_\infty]$ in the Picard group of $\mathcal{Y}_{n,s}$ divides $q^n + 1$. If $\gamma \neq 0$, that is $P \notin O$, then there exists a function $\xi_{\bar{P}}$ on the Hermitian curve $\mathcal{H}_q$ such that

$$(\xi_{\bar{P}})_{\mathcal{H}_q} = q\bar{P} + \Phi(\bar{P}) - (q + 1)\bar{P}_\infty,$$

where $\Phi(\bar{P})$ denotes the $\mathbb{F}_{q^2}$-Frobenius image of $\bar{P}$. In particular, seeing the function $\xi_{\bar{P}}$ on $\mathcal{Y}_{n,s}$ gives

$$(\xi_{\bar{P}}) = qP + E_P - (q + 1)m/sP_\infty,$$

where E_P is an effective divisor whose support does not contain P nor P_∞.

The curve $\mathcal{X}_{a,b,n,s}$ is defined for any odd integer $n \geq 3$ and prime power q where $q = p^a$ with p prime, $b \geq 1$ is a divisor of a, $\bar{q} := p^b$, and $s \geq 1$ is a divisor of $m = \frac{q^n+1}{q+1}$. Choose $c \in \mathbb{F}_{q^2}$ such that $c^{q-1} = -1$. The $\mathbb{F}_{q^{2n}}$-rational curve $\mathcal{X}_{a,b,n,s}$ is given by the affine equations

$$\mathcal{X}_{a,b,n,s} : \begin{cases} Z^{m/s} = Y^{q^2} - Y \\ cY^{q+1} = \mathrm{Tr}_{q/\bar{q}}(X) \end{cases}, \tag{10}$$

where $\mathrm{Tr}_{q/\bar{q}}(X) = X + X^{\bar{q}} + \cdots + X^{q/\bar{q}}$ is the trace map of the extension $\mathbb{F}_q/\mathbb{F}_{\bar{q}}$.

The curve $\mathcal{X}_{a,b,n,s}$ is $\mathbb{F}_{q^{2n}}$-maximal and it has genus

$$g(\mathcal{X}_{a,b,n,s}) = \frac{q^{n+2} - \bar{q}q^n - sq^3 + q^2 + (s-1)\bar{q}}{2s\bar{q}}.$$

Furthermore, $\mathcal{X}_{a,b,n,s}$ is a subcover of the GGS curve $\mathcal{C}_n$.

Let x, y, z be the coordinate functions of $\mathcal{Y}_{n,s}$, P_∞ be the unique common pole of x, y, z, and $P_{(\alpha,\beta,\gamma)}$ denote the $\mathbb{F}_{q^{2n}}$-rational point of $\mathcal{Y}_{n,s}$ which is a zero of $x-\alpha, y-\beta, z-\gamma$. Then, for any $\alpha, \beta \in \mathbb{F}_{q^{2n}}$, we have the following principal divisors:

$$(x-\alpha) = (q+1)m/sP_{(\alpha,0,0)} - (q+1)m/sP_\infty \ ; \tag{11}$$

$$(y-\beta) = \sum_{i=1}^{q/\bar{q}} m/sP_{(\alpha_i,\beta,0)} - \frac{q}{\bar{q}}m/sP_\infty, \text{ with } \mathrm{Tr}_{q/\bar{q}}(\alpha_i) = \beta^{q+1} \ ; \tag{12}$$

$$(z) = \sum_{j=1}^{q^2}\sum_{i=1}^{q/\bar{q}} P_{(\alpha_i,\beta_j,0)} - \frac{q^3}{\bar{q}}P_\infty, \text{ with } \beta_j \in \mathbb{F}_{q^2} \text{ and } c\beta_j^{q+1} = \mathrm{Tr}_{q/\bar{q}}(\alpha_i), \text{ for all } i,j. \tag{13}$$

From [27, Proposition 5.1] we have that $H(P_\infty) = \langle \frac{q}{\bar{q}}m/s, \frac{q^3}{\bar{q}}, (q+1)m/s\rangle$, which is a telescopic semigroup.

3. The automorphism group of $\mathcal{Y}_{n,s}$ and $\mathcal{X}_{a,b,n,s}$

In this section the automorphism groups of of $\mathcal{Y}_{n,s}$ and $\mathcal{X}_{a,b,n,s}$ are computed.

3.1. The automorphism group of $\mathcal{Y}_{n,s}$.

We aim to prove the following theorem.

Theorem 3.1. *If $3 \nmid n$ or $\frac{m}{s} \nmid (q^2-q+1)$, then the full automorphism group $\mathrm{Aut}(\mathcal{Y}_{n,s})$ of $\mathcal{Y}_{n,s}$ has order $q^3(q^2-1)m/s$ and is isomorphic to $S_{q^3} \rtimes C_{(q^2-1)\frac{m}{s}}$.*

If $3 \mid n$ and $\frac{m}{s} \mid (q^2-q+1)$, then $\mathrm{Aut}(\mathcal{Y}_{n,s})$ has order $(q^3+1)q^3(q^2-1)m/s$ and is isomorphic to $\mathrm{PGU}(3,q) \rtimes C_{m/s}$.

The case $s = 1$, that is the GGS curve $\mathcal{C}_n$, has been analyzed independently in [13] and [12]. Recall that if $(n,s) = (3,1)$ then the curve $\mathcal{Y}_{n,s}$ is the so-called GK-curve, whose full automorphism group is well-known, see [9]. From this point of view Theorem 3.1 can be seen as a new characterization of the GK curve, in terms of its automorphism group, in the family of maximal curves $\mathcal{Y}_{n,s}$ constructed in [27].

We start by observing that an automorphism group G of order $q^3(q^2-1)m/s$ and isomorphic to $S_{q^3} \rtimes C_{(q^2-1)\frac{m}{s}}$ can be found by hands, independently from the condition $3 \nmid n$ or $\frac{m}{s} \nmid (q^2-q+1)$. It is readily seen indeed that the following are automorphism groups of $\mathcal{Y}_{n,s}$

$$S_{q^3} = \left\{(x,y,z) \mapsto (x + b^q y + c, y + b, z) \ : \ b,c \in \mathbb{F}_{q^2}, c^q + c = b^{q+1}\right\} \cong E_q \,.\, E_{q^2}$$

where

$$E_q = \{(x,y,z) \mapsto (x+c, y, z) \ : \ c \in \mathbb{F}_{q^2}, c^q + c = 0\}$$

is the center of S_{q^3}. Also, if a is a primitive element of $\mathbb{F}_{q^2}$ and $\lambda_a \in \mathbb{F}_{q^{2n}}$ satisfies $\lambda_a^{\frac{m}{s}} = a$, another automorphism group of $\mathcal{Y}_{n,s}$ is given by

$$C := \langle \tau : (x, y, z) \mapsto (a^{q+1}x, ay, \lambda_a z) \rangle \cong C_{(q^2-1)\frac{m}{s}}.$$

We remark that C contains the cyclic group $C_{m/s} = \mathrm{Gal}(\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(y, z))$.

Since S_{q^3} and C are of co-prime order and C normalizes S_{q^3}, we get that $G := \langle S_{q^3}, C \rangle$ has order $q^3(q^2-1)m/s$ and is equal to $S_{q^3} \rtimes C_{(q^2-1)\frac{m}{s}}$.

Note that the group G has exactly one fixed point, namely P_∞. This follows from the fact that S_{q^3} has $\{P_\infty\}$ as its unique short orbit from Lemma 2.2, and S_{q^3} is normal in G. Theorem 3.1 is proven by first showing that the stabilizer of P_∞ in $\mathrm{Aut}(\mathcal{Y}_{n,s})$ is exactly G. To this aim, some preliminary technical lemmas are needed.

Lemma 3.2. *Let $\alpha \in E_q \setminus \{id\}$. Then $i(\alpha) = (q^n + 1)/s + 1$.*

Proof. Note that α is of prime order p since E_q is elementary abelian, and α acts non-trivially on x, while both y and z are fixed by α. This means that the fixed field of E_q contains $\mathbb{F}_{q^{2n}}(y, z)$, where $z^{m/S} = y^{q^2} - y$. Actually the fixed field of E_q coincides with $\mathbb{F}_{q^{2n}}(y, z)$, as the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(y, z)$ has degree $q = |E_q|$.

All the elements of $E_q \setminus \{id\}$ are conjugate in G, because the subgroup $\langle \tau^{m(q+1)/s} \rangle \subset C$ of order $q-1$ acts transitively on $E_q \setminus \{id\}$ by conjugation. Hence each $\alpha \in E_q \setminus \{id\}$ gives the same contribution $A := i(\alpha)$ to the different divisor of the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(y, z)$. Since $g(\mathbb{F}_{q^{2n}}(y, z)) = (m/s - 1)(q^2 - 1)/2$, we get from the Hurwitz genus formula that

$$2g(\mathcal{Y}_{n,s}) - 2 = \frac{(q^2-1)(q^n+1)}{s} - (q^3+1) = |E_q|\left(2g(\mathbb{F}_{q^{2n}}(y, z)) - 2\right) + \sum_{\alpha \in E_q \setminus \{0\}} i(\alpha)$$

$$= q\left((q^2-1)(m/s+1) - 2\right) + A(q-1),$$

from which one gets the claim $i(\alpha) = (q^n + 1)/s + 1$. □

Lemma 3.3. *Let $\beta \in S_{q^3} \setminus E_q$. Then $i(\beta) = m/s + 1$.*

Proof. We first observe that the fixed field F_{q^3} of S_{q^3} is the rational function field $\mathbb{F}_{q^{2n}}(z)$. In fact, z is fixed by S_{q^3}, and the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(z)$ has degree $\deg((z)_\infty) = \deg(q^3 P_\infty) = |S_{q^3}|$. Since E_q is the only proper normal subgroup in S_{q^3}, the ramification groups $S_{q^3}^{(i)}$ either coincide with S_{q^3}, or with E_q, or are trivial. This implies that the degree of the different divisor of the extension $\mathbb{F}_{q^{2n}}(x, y, z)/F_{q^3}$ can be written as $(n-j)(q-1)+j(q^3-1) = n(q-1)+j(q^3-q)$ where n is the number of non-trivial ramification groups (including the 0th ramification group), and j the number of ramification groups coinciding with S_{q^3}. From Lemma 3.2 each element of $E_q \setminus \{id\}$ is contained in exactly $(q^n+1)/s+1$ ramification groups, which implies that $n = (q^n + 1)/s + 1$ (because all the higher ramification groups contained properly in E_q need to be trivial). From the Hurwitz genus formula and Lemma

3.2 we obtain

$$2g(\mathcal{Y}_{n,s}) - 2 = |S_{q^3}|\left(2g(\mathbb{F}_{q^{2n}}(z)) - 2\right) + \left(\frac{q^n+1}{s} + 1\right)(q-1) + j(q^3-q),$$

which yields $j = m/s + 1$ by direct computation. Since we have only 2 possible higher ramification groups, the elements of $S_{q^3} \setminus E_q$ give all the same contribution to the different divisor, namely $m/s + 1$. □

Recall that from Lemma 2.1, $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty} = \tilde{S} \rtimes \tilde{C}$, where $\tilde{S}$ is the Sylow p-subgroup of $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty}$ and $\tilde{C}$ is a cyclic p'-group. Our first aim is to show that $\tilde{C}$ coincides with C.

We denote by $\bar{P}_\infty$ the point of $\mathcal{H}_q$ lying below P_∞.

Lemma 3.4. *Let $G \subseteq \mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty} = \tilde{S} \rtimes \tilde{C}$, where $\tilde{S}$ is the Sylow p-subgroup of $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty}$ and $\tilde{C}$ is cyclic of order d where $(d,p) = 1$. Then $|\tilde{C}| = |C| = (q^2-1)\frac{m}{s}$.*

Proof. Up to conjugation we can choose $\tilde{C}$ such that $C \subseteq \tilde{C}$. Since $\tilde{C}$ is cyclic, $C_{m/s} \subseteq C$ is a normal subgroup of $\tilde{C}$. The quotient group $\tilde{C}/C_{m/s}$ is an automorphism group of $\mathcal{Y}_{n,s}/C_{m/s} = \mathcal{H}_q$ fixing $\bar{P}_\infty$. Since the stabilizer of $\bar{P}_\infty$ in $\mathrm{Aut}(\mathcal{H}_q)$ has order $q^3(q^2-1)$ and $\tilde{C}/C_{m/s}$ is a p'-group, we get that $|\tilde{C}/C_{m/s}| \leq q^2 - 1$. However since $\tilde{C}$ contains C we have $q^2 - 1 = |C/C_{m/s}| \leq |\tilde{C}/C_{m/s}|$, which yields $C = \tilde{C}$. □

To complete the proof of our intermediate statement $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty} = G$, we need to show that $\tilde{S} = S_{q^3}$.

Lemma 3.5. *Let $\gamma \in \tilde{S} \setminus S_{q^3}$. Then $i(\gamma) = 2$. In particular both E_q and S_{q^3} are normal subgroups of $\tilde{S}$.*

Proof. Since the fixed field of S_{q^3} is rational and $S_{q^3} \subseteq \tilde{S}$, the fixed field of $\tilde{S}$ is also rational. From Lemmas 3.2 and 3.3 we know that $i(\alpha) = (q^n+1)/s + 1$ and $i(\beta) = m/s + 1$ for all $\alpha \in E_q \setminus \{id\}$ and $\beta \in S_{q^3} \setminus E_q$. Furthermore for all $\gamma \in \tilde{S} \setminus S_{q^3}$ one has $i(\gamma) \geq 2$ as $\tilde{S} = \tilde{S}^{(0)}_{P_\infty} = \tilde{S}^{(1)}_{P_\infty}$. Then the Hurwitz genus formula applied to $\mathcal{Y}_{n,s} \to \mathcal{Y}_{n,s}/\tilde{S}$ gives

$$\frac{(q^n+1)(q^2-1)}{s} - (q^3+1) \geq -2|\tilde{S}| + \left(\frac{(q^n+1)}{s} + 1\right)(q-1) + \left(\frac{m}{s} + 1\right)(q^3-q) + 2(|\tilde{S}| - q^3).$$

Since the right and left hand-sides coincide, we deduce that equality must hold, that is $i(\gamma) = 2$ for all $\gamma \in \tilde{S} \setminus S_{q^3}$. In particular $\tilde{S} = \tilde{S}^{(0)}_{P_\infty} = \tilde{S}^{(1)}_{P_\infty}$, $S_{q^3} = \tilde{S}^{(2)}_{P_\infty} = \ldots = \tilde{S}^{(m/s)}_{P_\infty}$, $E_q = \tilde{S}^{(m/s+1)}_{P_\infty} = \ldots = \tilde{S}^{(q^n+1)/s}_{P_\infty}$ and $\tilde{S}^{(i)}_{P_\infty} = \{id\}$ for all $i \geq (q^n+1)/s + 1$. Now, S_{q^3} is normal in $\tilde{S}$ by Lemma 2.1 item 2. The subgroup E_q is hence also normal in $\tilde{S}$, being the center of S_{q^3} and hence a characteristic subgroup of S_{q^3}. □

Remark 3.6. *The statement about the normality of E_q and S_{q^3} can be strengthened by looking at the entire stabilizer $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty}$ and not only at $\tilde{S}$. Since Lemma 2.1 implies that higher ramification groups are normal in the entire stabilizer of a point and $\tilde{S} = \mathrm{Aut}(\mathcal{Y}_{n,s})^{(1)}_{P_\infty}$, we have that S_{q^3} and E_q are normal in $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty}$.*

With the previous lemmas and remarks, we are in a position to prove our aimed intermediate statement $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty} = G$, which we observe being true independently from the condition $3 \nmid n$ or $\frac{m}{s} \nmid (q^2-q+1)$ (that indeed we have never used so far).

Proposition 3.7. *The stabilizer* $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty}$ *of* P_∞ *in* $\mathrm{Aut}(\mathcal{Y}_{n,s})$ *is* G.

Proof. By Lemma 3.5 and Remark 3.6, E_q is a normal subgroup of $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty}$. Hence $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty}/E_q$ is an automorphism group of the fixed field of E_q, that is, $\mathbb{F}_{q^{2n}}(y,z)$ with $y^{q^2}-y = z^{m/s}$. Since $\gcd(q^2+1, q^n+1) = 2$ for n odd, we get from [4, Theorem 3.2] that

$$\frac{m}{s}q^2(q^2-1) = |G/E_q| \le |\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty}/E_q| \le |\mathrm{Aut}(\mathbb{F}_{q^{2n}}(y,z))| = \frac{m}{s}q^2(q^2-1),$$

which implies $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty} = G$. □

Define the following set of rational points of $\mathcal{Y}_{n,s}$:

$$O = \{P_{(\alpha_i,\beta_j,0)} \in \mathcal{Y}_{n,s} : \ \alpha_i, \beta_j \in \mathbb{F}_{q^2},\ \beta_j^{q+1} = \alpha_i^q + \alpha_i\}.$$

The following is an easy but useful lemma.

Lemma 3.8. *The group* $C_{m/s}$ *is normal in* $\mathrm{Aut}(\mathcal{Y}_{n,s})$ *if and only if* $\mathrm{Aut}(\mathcal{Y}_{n,s})$ *acts on the set* $O \cup \{P_\infty\}$. *Furthermore, if* $C_{m/s}$ *is normal in* $\mathrm{Aut}(\mathcal{Y}_{n,s})$, *then* $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s}$ *is an automorphism group of the Hermitian function field* $\mathbb{F}_{q^{2n}}(x,y)$ *and either* $\mathrm{Aut}(\mathcal{Y}_{n,s}) = G$ *or* $|\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s}| = q^3(q^2-1)(q^3+1)$. *In the latter case,* $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s}$ *is isomorphic to* $\mathrm{PGU}(3,q)$ *and acts on* $\mathbb{F}_{q^{2n}}(x,y)$ *as* $\mathrm{PGU}(3,q)$ *in its natural action.*

Proof. Recall that $O \cup \{P_\infty\}$ consists exactly of the fixed points of $C_{m/s}$ on $\mathcal{Y}_{n,s}$, and $C_{m/s}$ has no other short orbits. This immediately implies that if $C_{m/s}$ is normal in $\mathrm{Aut}(\mathcal{Y}_{n,s})$ then $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on $O \cup \{P_\infty\}$: in fact, if $\alpha \in \mathrm{Aut}(\mathcal{Y}_{n,s})$, $\beta \in C_{m/s}$ and $P \in O \cup \{P_\infty\}$, then $\alpha(P) = \alpha(\beta(P)) = \beta'(\alpha(P))$ for some $\beta' \in C_{m/s}$ and hence $\alpha(P)$ is fixed by β', i.e. $\alpha(P) \in O \cup \{P_\infty\}$.

Conversely, suppose that $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on the set $O \cup \{P_\infty\}$ and consider the subgroup

$$T = \{\sigma \in \mathrm{Aut}(\mathcal{Y}_{n,s}) \mid \sigma(P) = P, \text{ for all } P \in O \cup \{P_\infty\}\}$$

of $\mathrm{Aut}(\mathcal{Y}_{n,s})$. Let $g \in \mathrm{Aut}(\mathcal{Y}_{n,s})$ and $\sigma \in T$. For all $P \in O \cup \{P_\infty\}$ it holds that $g(P) \in O \cup \{P_\infty\}$ and hence $\sigma(g(P)) = g(P)$, which implies $g^{-1}\sigma g(P) = P$ for all $P \in O \cup \{P_\infty\}$, that is, $g\sigma g^{-1} \in T$. Thus, T is a normal subgroup of $\mathrm{Aut}(\mathcal{Y}_{n,s})$. Moreover, the characteristic p does not divide the order of T, because $|S| > 1$ and the curve has p-rank zero, see [15, [Lemma 11.129]. Then, by Lemma 2.1, T is cyclic. Therefore $C_{m/s} \subseteq T$ is a characteristic subgroup of T and hence a normal subgroup of $\mathrm{Aut}(\mathcal{Y}_{n,s})$.

To prove the second part of the statement recall that the fixed field of $C_{m/s}$ is the Hermitian function field $\mathbb{F}_{q^{2n}}(x,y)$ and that $\mathrm{Aut}(\mathbb{F}_{q^{2n}}(x,y)) = \mathrm{PGU}(3,q)$, see [15, Proposition 11.30]. Thus, $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s}$ is a subgroup of $\mathrm{PGU}(3,q)$ containing $G/C_{m/s}$, which is a group of order $q^3(q^2-1)$ fixing the point $\bar{P}_\infty$ below P_∞. Since $\mathrm{PGU}(3,q)_{\bar{P}_\infty}$ is a maximal subgroup of $\mathrm{PGU}(3,q)$ of order $q^3(q^2-1)$ (see [15, Theorem A.10]), we get either $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s} = G/C_{m/s}$ (in this case, $\mathrm{Aut}(\mathcal{Y}_{n,s})$ fixes P_∞) or $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s} = \mathrm{PGU}(3,q)$. □

Lemma 3.8 is a key ingredient, because it defines the strategy we are going to use to complete the proof of the theorem. First we prove that if $C_{m/s}$ is normal, then $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s} \cong \mathrm{PGU}(3,q)$ if and only if $3 \mid n$ and $\frac{m}{s} \mid (q^2-q+1)$. Then we prove, independently from n, that $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on $O \cup \{P_\infty\}$. In this way, whenever $3 \nmid n$ or $\frac{m}{s} \nmid (q^2-q+1)$, the claim $\mathrm{Aut}(\mathcal{Y}_{n,s}) = \mathrm{Aut}(\mathcal{Y}_{n,s})_{P_\infty}$ will follow immediately from Lemma 3.8.

Lemma 3.9. *Assume that $C_{m/s}$ is normal in $\mathrm{Aut}(\mathcal{Y}_{n,s})$. Then $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s} \cong \mathrm{PGU}(3,q)$ if and only if $3 \mid n$ and $\frac{m}{s} \mid (q^2-q+1)$.*

Proof. The automorphism group $\mathrm{PGU}(3,q)$ of the function field $\mathbb{F}_{q^{2n}}(x,y)$ is 2-transitive on the rational places of $\mathbb{F}_{q^{2n}}(x,y)$, and hence can be generated as $\mathrm{PGU}(3,q) = \langle \mathrm{PGU}(3,q)_{Q_\infty}, \tau \rangle$, where $\tau(x) = 1/x$ and $\tau(y) = y/x$; see [15, Page 664, item 9]. Since $C_{m/s}$ is normal in $\mathrm{Aut}(\mathcal{Y}_{n,s})$, we apply Lemma 3.8. From $G/C_{m/s} = \mathrm{PGU}(3,q)_{\bar{P}_\infty}$ we get that $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s} \cong \mathrm{PGU}(3,q)$ if and only if τ can be lifted to an automorphism $\tilde{\tau}$ of $\mathbb{F}_{q^{2n}}(x,y,z)$ having the same action of τ on the totally ramified points in $O \cup \{P_\infty\}$.

Suppose that $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s} \cong \mathrm{PGU}(3,q)$, i.e. such $\tilde{\tau}$ exists. Then $\tilde{\tau}(P_\infty) = P_{(0,0,0)}$ and $O \setminus \{P_{(0,0,0)}\}$ is fixed setwise by $\tilde{\tau}$. From Equations (7) and (8), this implies that the divisors of $\tilde{\tau}(x)$ and $1/x$ coincide, and the same holds for those of $\tilde{\tau}(y)$ and y/x. Therefore $\tilde{\tau}(x) = \lambda/x$ and $\tilde{\tau}(y) = \mu y/x$ for some non-zero constants $\lambda, \mu \in \mathbb{F}_{q^{2n}}$. Since the equality $y^{q+1} = x^q + x$ is preserved by $\tilde{\tau}$, we get that $\lambda = \mu^{q+1}$. Also from Equation (9) we have that

$$(\tilde{\tau}(z)) = \left(\sum_{P \in O,\ P \neq P_{(0,0,0)}} P \right) + P_\infty - q^3 P_{(0,0,0)}$$

and

$$(z/\tilde{\tau}(z)) = (q^3+1)(P_{(0,0,0)} - P_\infty).$$

By Equation (11), this implies that the order $o_{P_{(0,0,0)}}$ of $[P_{(0,0,0)} - P_\infty]$ in the Picard group of $\mathcal{Y}_{n,s}$ divides $\gcd((q+1)m/s, q^3+1) = (q+1) \cdot \gcd(m/s, q^2-q+1) \leq (q+1)m/s$. Also, $o_{P_{(0,0,0)}} \in H(P_\infty)$ and $o_{P_{(0,0,0)}}$ is coprime with q. By [27, Proposition 5.1], the semigroup $H(P_\infty)$ satisfies $H(P_\infty) = \langle qm/s, (q+1)m/s, q^3 \rangle$; thus, the smallest element of $H(P_\infty)$ coprime with q is $(q+1)m/s$. Therefore, $o_{P_{(0,0,0)}} = (q+1)m/s = \gcd((q+1)m/s, q^3+1)$, that is, m/s divides q^2-q+1. By Lemma 2.7, also $\gcd(q^n+1, q^3+1)$ is an element of $H(P_\infty)$ which is coprime with q, and hence not smaller than $(q+1)m/s$. Since $m/s > 1$, this implies $\gcd(q^n+1, q^3+1) > q+1$ and hence $3 \mid n$.

Conversely, suppose that m/s divides q^2-q+1 and 3 divides n. Then the $\mathbb{F}_{q^{2n}}$-maximal curve $\mathcal{Y}_{n,s}$ is a quotient $\mathcal{GK}/C_{\frac{q^2-q+1}{m/s}}$ of the $\mathbb{F}_{q^6}$-maximal curve $\mathcal{GK}$; thus, $\mathcal{Y}_{n,s}$ is also $\mathbb{F}_{q^6}$-maximal. The fundamental equation [15, Page xix Item (ii)] implies that there exists a function ρ_0 such that $(\rho_0) = (q^3+1)(P_\infty - P_{(0,0,0)})$. Our aim is to show that τ can be lifted to an automorphism $\tilde{\tau}$ of $\mathcal{Y}_{n,s}$ by defining

$$\tilde{\tau} : (x,y,z) \mapsto \left(\frac{1}{x}, \frac{y}{x}, \xi \cdot \rho_0 \cdot z \right),$$

for some suitable constant ξ.

To this aim, note first that the equation $y^{q+1} = x^q + x$ is trivially preserved by $\tilde{\tau}$, as τ is an automorphism of $\mathbb{F}_{q^{2n}}(x, y)$ and $\tilde{\tau}$ acts as τ on x and y. Moreover, choosing ξ carefully, we can force also the other equation of $\mathcal{Y}_{n,s}$ to be preserved by $\tilde{\tau}$. Indeed, we have

$$\begin{aligned}((\rho_0 z)^{m/s}) &= \frac{m}{s}(\rho_0 z) = \frac{m}{s}(z) + \frac{m}{s}(q^3+1)(P_\infty - P_{(0,0,0)}) \\ &= \frac{m}{s}\sum_{P\in O} P - \frac{m}{s}q^3 P_\infty + \frac{m}{s}(q^3+1)P_\infty - \frac{m}{s}(q^3+1)P_{(0,0,0)} \\ = \frac{m}{s}\left(\sum_{P\in O\cup\{P_\infty\},\ P\neq P_{(0,0,0)}} P - q^3 P_{(0,0,0)}\right) &= (\tau(y^{q^2}-y)) = (\tilde{\tau}(y^{q^2}-y)),\end{aligned}$$

and hence there exists a nonzero constant $\eta \in \mathbb{F}_{q^{2n}}$ such that $(\rho_0 z)^{m/s} = \eta(\tilde{\tau}(y^{q^2}-y))$. Choosing ξ such that $\xi^{m/s} = \eta^{-1}$ we get

$$\tilde{\tau}(z^{m/s}) = \tilde{\tau}(z)^{m/s} = \xi^{m/s}(\rho_0 z)^{m/s} = \eta^{-1}\cdot\eta(\tilde{\tau}(y^{q^2}-y)) = \tilde{\tau}(y^{q^2}-y),$$

so that also the second equation of $\mathcal{Y}_{n,s}$ is preserved by $\tilde{\tau}$, yielding $\tilde{\tau} \in \mathrm{Aut}(\mathcal{Y}_{n,s})$. Since $\tilde{\tau}$ acts as τ on $\mathbb{F}_{q^{2n}}(x, y)$ and $\tau \notin \mathrm{PGU}(3, q)_{\bar{P}_\infty} = G/C_{m/s}$, we get $\tau \notin G$ and hence $\mathrm{Aut}(\mathcal{Y}_{n,s}) \neq G$. By Lemma 3.8, this implies $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s} \cong \mathrm{PGU}(3, q)$. □

At this point we are left with proving that $C_{m/s}$ is normal in $\mathrm{Aut}(\mathcal{Y}_{n,s})$, or equivalently $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on $O \cup \{P_\infty\}$; then Lemmas 3.8, 3.9 will complete the proof of Theorem 3.1.

In some cases this property can be obtained almost for free.

Lemma 3.10. *If $q^3(q^3-1) \leq (q^n+1)(q^2-1)/s - (q^3+1)$ then $C_{m/s}$ is normal in $\mathrm{Aut}(\mathcal{Y}_{n,s})$.*

Proof. We start by proving that a point $P \in \mathcal{Y}_{n,s} \setminus (O \cup \{P_\infty\})$ cannot have the same Weierstrass semigroup as P_∞. As $q^3 \in H(P_\infty)$ by [27, Proposition 5.1], it is enough to show that $q^3 \notin H(P)$. We can write $P = P_{(a,b,c)}$ as $P \neq P_\infty$, and $c \neq 0$ as $P \notin O$. Consider the differential $w := (z-c)^{q^3-1}dz$ on $\mathcal{Y}_{n,s}$. By Equation (9) and Lemma 2.6, the valuation of w at P_∞ is $v_{P_\infty}(w) = -q^3(q^3-1) + 2g(\mathcal{Y}_{n,s}) - 2$, and hence $v_{P_\infty}(w) \geq 0$ by the assumption. Then w is a regular differential, with valuation q^3-1 at P. Lemma 2.5 implies that $q^3 = (q^3-1)+1 \notin H(P)$.

Since the Weierstrass semigroup of a point is invariant under automorphisms, we have proved for any $P \in \mathcal{Y}_{n,s} \setminus (O \cup \{P_\infty\})$ that P is not in the same orbit as P_∞ under $\mathrm{Aut}(\mathcal{Y}_{n,s})$. We now prove that any $P \in \mathcal{Y}_{n,s} \setminus (O \cup \{P_\infty\})$ is not in the same orbit of any point of O. Suppose on the contrary that some point of O is in the orbit O_P of $P \in \mathcal{Y}_{n,s}(O \cup \{P_\infty\})$ under $\mathrm{Aut}(\mathcal{Y}_{n,s})$. Then $O \subseteq O_P$, because O is an orbit under $G \subseteq \mathrm{Aut}(\mathcal{Y}_{n,s})$. Since $P_\infty \notin O_P$, this implies that P is not in the same orbit of any point of O under $\mathrm{Aut}(\mathcal{Y}_{n,s})$. Therefore $\{P_\infty\}$ is an orbit under $\mathrm{Aut}(\mathcal{Y}_{n,s})$, i.e. $\mathrm{Aut}(\mathcal{Y}_{n,s})$ fixes P_∞ and $\mathrm{Aut}(\mathcal{Y}_{n,s}) = G$ by Proposition 3.7. Thus $C_{m/s}$ is normal in $\mathrm{Aut}(\mathcal{Y}_{n,s})$, and hence $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on $O \cup \{P_\infty\}$ by Lemma 3.8, in contradiction with $O \subseteq O_P$ with $P \notin O \cup \{P_\infty\}$.

We have then proved that points of $O \cup \{P_\infty\}$ and points out of $O \cup \{P_\infty\}$ cannot be in the same orbit under $\mathrm{Aut}(\mathcal{Y}_{n,s})$, that is, $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on $O \cup \{P_\infty\}$. By Lemma 3.8, this is equivalent to $C_{m/s}$ being normal in $\mathrm{Aut}(\mathcal{Y}_{n,s})$. □

Remark 3.11. *An equivalent proof for Lemma 3.10 can be proposed by showing that the gap sequences at $P \notin O \cup \{P_\infty\}$ and $Q \in O$ are different, using the generalized Weierstrass semigroup $H(Q, P_\infty)$. This semigroup has been computed in [21].*

In the following we can then assume that $q^3(q^3-1) > (q^n+1)(q^2-1)/s - (q^3+1)$; to unify the cases $q = 2$ and $q > 2$, we will assume $m/s \leq q^3 - q^2 + 2q - 1$.

We denote by O_∞ the orbit of P_∞ under $\mathrm{Aut}(\mathcal{Y}_{n,s})$.

Lemma 3.12. *The short orbit O_∞ is the only non-tame orbit of $\mathrm{Aut}(\mathcal{Y}_{n,s})$.*

Proof. We know already that O_∞ is a non-tame short orbit of $\mathrm{Aut}(\mathcal{Y}_{n,s})$, because G fixes P_∞ and has order divisible by p. If S is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{Y}_{n,s})$ containing the Sylow p-subgroup S_{q^3} of G, then $S = S_{q^3}$, because S fixes P_∞ by Corollary 2.3 and G is the full stabilizer of P_∞ in $\mathrm{Aut}(\mathcal{Y}_{n,s})$.

Let O' be a non-tame short orbit of $\mathrm{Aut}(\mathcal{Y}_{n,s})$, and P'. By Lemma 2.1 we can write the stabilizer of P' as $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P'} = S' \rtimes C'$, where S' is the Sylow p-subgroup of $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P'}$. Arguing as above, S' is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{Y}_{n,s})$. Then the Sylow p-subgroups S_{q^3}, S' are conjugate, say $\alpha^{-1} S' \alpha = S_{q^3}$ with $\alpha \in \mathrm{Aut}(\mathcal{Y}_{n,s})$. This implies $\alpha(P_\infty) = P'$, and hence their orbits coincide, i.e. $O' = O_\infty$. The claim is proved. □

Remark 3.13. *By the properties of p-groups and Sylow p-subgroups, it can be noted that Lemma 3.12 holds also for other curves: if $\mathcal{X}$ is a curve in characteristic p such that p divides $|\mathrm{Aut}(\mathcal{X})|$ and every p-element of $\mathrm{Aut}(\mathcal{X})$ has exactly one fixed point, then $\mathrm{Aut}(\mathcal{X})$ has exactly one non-tame orbit.*

Remark 3.14. *Since G is the full stabilizer of P_∞ in $\mathrm{Aut}(\mathcal{Y}_{n,s})$ by Proposition 3.7, we get from the orbit-stabilizer theorem that*

$$|\mathrm{Aut}(\mathcal{Y}_{n,s})| = |O_\infty| \cdot |G|.$$

If $O_\infty = \{P_\infty\}$ then $\mathrm{Aut}(\mathcal{Y}_{n,s}) = G$, and hence $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on $O \cup \{P_\infty\}$, which proves Theorem 3.1. We can then assume in the rest of this section that $|O_\infty| > 1$.

Since $\{P_\infty\}$ and O are the only short orbits of G, we get that either $O_\infty = \{P_\infty\} \cup O$ or O_∞ contains at least one long orbit of G. In the first case we get immediately that $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on $O \cup \{P_\infty\}$, whence Theorem 3.1 follows. In the latter case we have that

$$|\mathrm{Aut}(\mathcal{Y}_{n,s})| = |O_\infty| \cdot |G| > |G|^2 > 84(g(\mathcal{Y}_{n,s}) - 1),$$

and hence we can apply Theorem 2.4 to investigate the short orbits of $\mathrm{Aut}(\mathcal{Y}_{n,s})$. Since there are automorphisms fixing points in $O \cup \{P_\infty\}$, we know that $O \cup \{P_\infty\}$ is contained in the union of short orbits of $\mathrm{Aut}(\mathcal{Y}_{n,s})$. Since G fixes P_∞ and has order divisible by p, we also know that P_∞ is contained in a non-tame short orbit of $\mathrm{Aut}(\mathcal{Y}_{n,s})$.

By Remark 3.14, the cases $O_\infty = \{P_\infty\}$ and $O_\infty = \{P_\infty\} \cup O$ have already been worked out. Therefore we can assume from now on that O_∞ contains $k \geq 1$ long orbits of G.

This implies $|\mathrm{Aut}(\mathcal{Y}_{n,s})| > 84(g-1)$, so that Theorem 2.4 applies for the short orbits of $\mathrm{Aut}(\mathcal{Y}_{n,s})$. Note that if $q \geq 7$, then already $|G| > 84(g-1)$, and Theorem 2.4 applies for $\mathrm{Aut}(\mathcal{Y}_{n,s})$ without any assumption on O_∞.

Lemma 3.15. $\mathrm{Aut}(\mathcal{Y}_{n,s})$ *has exactly two short orbits: the non-tame orbit* O_∞*, and a tame short orbit* O_1*.*

Proof. By Theorem 2.4, $\mathrm{Aut}(\mathcal{Y}_{n,s})$ has at most three short orbits, in particular:

(1) exactly three short orbits, two tame of length $|\mathrm{Aut}(\mathcal{Y}_{n,s})|/2$ and one non-tame, with $p \geq 3$; or
(2) exactly two short orbits, both non-tame; or
(3) only one short orbit, which is non-tame, oflength dividing $2g-2$; or
(4) exactly two short orbits, one tame and one non-tame.

We start by observing that Case (2) cannot occur by Lemma 3.12. If Case (3) occurs then $|O_\infty|$ must divide $2g-2$, which is impossible since $|O_\infty| \geq 1 + |G| > 2g-2$. Thus, the proof is complete once we show that Case (1) cannot occur.

Suppose that Case (1) occurs, and let O_1, O_2 be the tame orbits of $\mathrm{Aut}(\mathcal{Y}_{n,s})$ of the same length $|\mathrm{Aut}(\mathcal{Y}_{n,s})|/2$. Recall that P_∞ is in the non-tame orbit O_∞ of $\mathrm{Aut}(\mathcal{Y}_{n,s})$, O is an orbit of G, and G acts semiregularly out of $O \cup \{P_\infty\}$. If $O \subseteq O_1$, this implies that the length of O_1 is congruent to $|O|$ modulo $|G|$ while the length of O_2 is divisible by $|G|$, a contradiction to $|O_1| = |O_2|$; therefore $O \not\subseteq O_1$ and analogously $O \not\subseteq O_2$. Thus, $O \subseteq O_\infty$. Write $|O_\infty| = 1 + |O| + k|G| = q^3 + 1 + k|G|$ for some $k \geq 1$. The Hurwitz genus formula applied to $\mathrm{Aut}(\mathcal{Y}_{n,s})$, together with Lemmas 3.2 and 3.3, gives

$$\frac{(q^n+1)(q^2-1)}{s} - (q^3+1) =$$

$$-2|\mathrm{Aut}(\mathcal{Y}_{n,s})| + 2\frac{|\mathrm{Aut}(\mathcal{Y}_{n,s})|}{2}(2-1) + |O_\infty|\left(|G| - 1 + (q^3-1)\frac{m}{s} + (q-1)q\frac{m}{s}\right).$$

By the orbit-stablizer theorem $|O_\infty||G| = |\mathrm{Aut}(\mathcal{Y}_{n,s})|$, whence

$$\frac{(q^n+1)(q^2-1)}{s} - (q^3+1) = (q^3+1+k|G|)\left(|G| - 1 + (q^3-1)\frac{m}{s} + (q-1)q\frac{m}{s}\right).$$

Using $|G| = q^3(q^2-1)m/s$, this yields a contradiction to $k \geq 1$. □

We are now in the position of proving that the assumption $k \geq 1$ yields a contradiction, which in turn gives that $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on $O \cup \{P_\infty\}$ as shown above.

Proposition 3.16. $\mathrm{Aut}(\mathcal{Y}_{n,s})$ *acts on* $O \cup \{P_\infty\}$*.*

Proof. Suppose by contradiction that $\mathrm{Aut}(\mathcal{Y}_{n,s})$ does not act on $O \cup \{P_\infty\}$. By Lemma 3.15, $\mathrm{Aut}(\mathcal{Y}_{n,s})$ has exactly two short orbits: the non-tame orbit O_∞ of length $|O_\infty| = 1 + \ell|O| +$

$k|G|$ where $k \geq 1$ and $\ell \in \{0,1\}$, and the tame orbit O_1 of length $|O_1| = (1-\ell)|O| + k_1|G|$ where $k_1 \geq 0$. The Hurwtiz genus formula applied to $\mathrm{Aut}(\mathcal{Y}_{n,s})$ gives

$$\frac{(q^n+1)(q^2-1)}{s} - (q^3+1) = -2|\mathrm{Aut}(\mathcal{Y}_{n,s})| + |O_1|\left(\frac{|\mathrm{Aut}(\mathcal{Y}_{n,s})|}{|O_1|} - 1\right)$$

$$+(\ell q^3 + 1 + k|G|)\left(|G| - 1 + (q^3-1)\frac{m}{s} + (q-1)q\frac{m}{s}\right).$$

We analyze the cases $\ell = 1$ and $\ell = 0$ separately.

- **The case $\ell = 0$.** In this case $O \subseteq O_1$. Then the stabilizer of any point in O_1 is conjugate to the stabilizer of a point in O, which contains C and hence has order divisible by $(q^2-1)m/s$. Thus, there exists some $h \geq 1$ such that $|\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_1}| = h(q^2-1)m/s$ for any $P_1 \in O_1$. By the orbit-stabilizer theorem,

$$(1+k|G|)|G| = |\mathrm{Aut}(\mathcal{Y}_{n,s})| = (q^3 + k_1|G|)h(q^2-1)m/s,$$

and hence

$$1 + kq^3(q^2-1)m/s = (1 + k_1(q^2-1)m/s)h.$$

In particular, h is congruent to 1 modulo $(q^2-1)m/s$.

If $h = 1$, then $|\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_1}| = (q^2-1)m/s$ and $k_1 = kq^3$. The Hurwitz genus formula now gives

$$\frac{(q^n+1)(q^2-1)}{s} - (q^3+1) = -(q^3 + kq^3|G|) + (1+k|G|)\left(-1 + (q^3-1)\frac{m}{s} + (q-1)q\frac{m}{s}\right),$$

and so

$$0 = -kq^3|G| + k|G|\left(-1 + (q^3-1)\frac{m}{s} + (q-1)q\frac{m}{s}\right) = k|G|\left(-q^3 - 1 + (q^3+q^2-q-1)\frac{m}{s}\right) > 0,$$

a contradiction.

Hence $h = t(q^2-1)m/s + 1$ with $t \geq 1$. This implies $kq^3 = (1 + k_1(q^2-1)m/s)t + k_1$. The orbit-stabilizer theorem now gives

$$|\mathrm{Aut}(\mathcal{Y}_{n,s})| = (q^3 + k_1|G|)h(q^2-1)m/s > (q^3 + k_1|G|)\left((q^2-1)m/s\right)^2.$$

If $k_1 > 0$ then

$$|\mathrm{Aut}(\mathcal{Y}_{n,s})| > (q^3 + |G|)\left((q^2-1)m/s\right)^2 > 8g^3,$$

and a contradiction is obtained from Theorem 2.4. If $k_1 = 0$ then $t = kq^3$ and

$$|\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_1}| = \left(kq^3(q^2-1)m/s + 1\right)(q^2-1)m/s. \tag{14}$$

Since the orbit of $P_1$is tame, the stabilizer $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_1}$ is cyclic of order prime-to-p. Then, by [15, Theorem 11.79], $\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_1}$ has order at most $4g+4 = 2(q^2-1)(q+1)m/s - 2q^3 + 6$, which is a contradiction to Equation (14).

- **The case $\ell = 1$.** In this case $O \subseteq O_\infty$. From the orbit-stabilizer theorem we have
$$(1 + q^3 + k|G|)|G| = |\mathrm{Aut}(\mathcal{Y}_{n,s})| = k_1|G||\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_1}|,$$
and hence
$$|\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_1}| = \left(1 + q^3 + k|G|\right)/k_1. \tag{15}$$
On the other hand, the Hurwitz genus formula gives
$$0 = -k_1|G| - k|G| + (q^3 + k|G|)(q^2 - 1)(q + 1)m/s,$$
that is
$$k_1 = q + 1 + k\left((q^2 - 1)(q + 1)m/s - 1\right). \tag{16}$$
Using Equations (15) and (16) together we get
$$\begin{aligned}|\mathrm{Aut}(\mathcal{Y}_{n,s})_{P_1}| &= \frac{1 + q^3 + k\frac{q^3(q^2-1)m}{s}}{q + 1 + k\left(\frac{m(q^2-1)(q+1)}{s} - 1\right)} \\ &= q^2 - q + 1 + \frac{k\left(-\frac{m(q^2-1)}{s} + q^2 - q + 1\right)}{k\left(\frac{m(q^2-1)(q+1)}{s} - 1\right) + q + 1},\end{aligned}$$
which is not an integer because $k \geq 1$. This contradiction completes the proof.

□

The proof of Theorem 3.1 is now complete. Indeed, by Proposition 3.16 $\mathrm{Aut}(\mathcal{Y}_{n,s})$ acts on $O \cup \{P_\infty\}$. From Lemma 3.8 either $\mathrm{Aut}(\mathcal{Y}_{n,s}) = G$ or $\mathrm{Aut}(\mathcal{Y}_{n,s})/C_{m/s}$ is isomorphic to $\mathrm{PGU}(3, q)$. From Lemma 3.9 the latter case happens if and only if 3 divides n and m/s divides $q^2 - q + 1$.

3.2. **The automorphism group of $\mathcal{X}_{a,b,n,s}$.** Consider the curve
$$\mathcal{Y}_{n,s} : \begin{cases} W^{m/s} = V^{q^2} - V \\ V^{q+1} = U^q + U \end{cases}$$
with coordinate functions u, v, w, and the automorphism group
$$E_{\bar{q}} = \left\{(u, v, w) \mapsto \left(u + \frac{\lambda}{c}, v, w\right) : \lambda \in \mathbb{F}_{\bar{q}}\right\} \subset \mathrm{Aut}(\mathcal{Y}_{n,s}),$$
which is elementary abelian of order $\bar{q}$ and is contained in S_{q^3}. The aim of this section is to prove the following theorem.

Theorem 3.17. *Assume that $b < a$ or $q^2 \nmid (\frac{m}{s} - 1)$. Then the automorphism group of $\mathcal{X}_{a,b,n,s}$ has order $\frac{q^3}{\bar{q}}(q + 1)(\bar{q} - 1)\frac{m}{s}$ and is isomorphic to $(S_{q^3}/E_{\bar{q}}) \rtimes C_{(q+1)(\bar{q}-1)m/s}$.*

Remark 3.18. *Suppose that $b = a$, that is $\bar{q} = q$. Then $\mathcal{X}_{a,a,n,s}$ is the plane curve $Z^{m/s} = Y^{q^2} - Y$. If $q^2 \nmid (\frac{m}{s} - 1)$, then we can apply [4, Theorem 3.2], whose case (ii) holds. This immediately yields the claim of Theorem 3.17. Therefore, we can assume from now on that $b < a$.*

We start by noting that $\mathcal{X}_{a,b,n,s}$ is the quotient curve of $\mathcal{Y}_{n,s}$ over $E_{\bar{q}}$. Indeed, define $x = cu - (cu)^{\bar{q}}$, $y = v$, $z = w$. Then the function field of $\mathcal{X}_{a,b,n,s}$ is exactly $\mathbb{F}_{q^{2n}}(x, y, z)$; see [27, Definition 3.1]. By direct computation $E_{\bar{q}}$ fixes x, y, z, i.e. $\mathbb{K}(\mathcal{X}_{a,b,n,s}) \subseteq \mathbb{K}(\mathcal{Y}_{n,s})^{E_{\bar{q}}}$. Since $|E_{\bar{q}}| = [\mathbb{K}(\mathcal{Y}_{n,s}) : \mathbb{K}(\mathcal{X}_{a,b,n,s})]$, equality holds and $\mathcal{X}_{a,b,n,s} = \mathcal{Y}_{n,s}/E_{\bar{q}}$.

Therefore, an automorphism group G of $\mathcal{X}_{a,b,n,s}$ is given by

$$G := \frac{\mathrm{N}_{\mathrm{Aut}(\mathcal{Y}_{n,s})}(E_{\bar{q}})}{E_{\bar{q}}} = \frac{S_{q^3}}{E_{\bar{q}}} \rtimes C_{(q+1)(\bar{q}-1)\frac{m}{s}}.$$

The group G has exactly one fixed point, namely P_∞. We want to prove that G is the whole stabilizer of P_∞ in $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$.

To this aim, we compute in the next propositions the contribution of the p-elements $\alpha \in G$ to the covering $\mathcal{X}_{a,b,n,s} \to \mathcal{X}_{a,b,n,s}/H$, where H is any subgroup of $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$ containing α.

Proposition 3.19. *Let $\alpha \in E_q/E_{\bar{q}}$. Then $i(\alpha) = (q^n + 1)/s + 1$.*

Proof. Differently from the proof of Lemma 3.2, the non-trivial elements of $E_q/E_{\bar{q}}$ are not in a unique orbit under conjugation in G. However, they still give the same contribution. To see this, let $\alpha_1, \alpha_2 \in (E_q/E_{\bar{q}}) \setminus \{id\}$, and let $\beta_1, \beta_2 \in E_q \setminus E_{\bar{q}}$ be such that α_1, α_2 are the cosets respectively of β_1, β_2 in $E_q/E_{\bar{q}}$. Define $H_i = \langle \beta_i, E_{\bar{q}} \rangle = \langle \beta_i \rangle \times E_{\bar{q}}$, for $i = 1, 2$. By Lemma 3.2, the curves $\mathcal{Y}_{n,s}/H_1$ and $\mathcal{Y}_{n,s}/H_2$ have the same genus. Clearly, $\mathcal{Y}_{n,s}/H_i \cong \mathcal{X}_{a,b,n,s}/\langle \alpha_i \rangle$ for $i = 1, 2$. Thus, $g(\mathcal{X}_{a,b,n,s}/\langle \alpha_1 \rangle) = g(\mathcal{X}_{a,b,n,s}/\langle \alpha_2 \rangle)$. As $\langle \alpha_i \rangle$ is cyclic of prime order, this implies $i(\alpha_1) = i(\alpha_2)$.

Since α fixes y and z, and the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(y, z)$ has degree $q/\bar{q} = |E_q/E_{\bar{q}}|$, the fixed field of $E_q/E_{\bar{q}}$ is exactly $\mathbb{F}_{q^{2n}}(y, z)$, whose genus is $g(\mathbb{F}_{q^{2n}}(y, z)) = \frac{(m/s-1)(q^2-1)}{2}$. Now the claim follows by applying the Hurwitz genus formula to $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(y, z)$. □

Proposition 3.20. *Let $\alpha \in (S_{q^3}/E_{\bar{q}}) \setminus (E_q/E_{\bar{q}})$. Then $i(\alpha) = m/s + 1$.*

Proof. The proof generalizes the one of Lemma 3.3. Since z is fixed by $S_{q^3}/E_{\bar{q}}$ and $(z)_\infty = q^3/\bar{q}P_\infty$ by Equation (13), we have that the fixed field of $S_{q^3}/E_{\bar{q}}$ is $\mathbb{F}_{q^{2n}}(z)$ and hence is rational. As $E_{\bar{q}}$ is central in S_{q^3} and E_q is the only proper normal subgroup of S_{q^3} containing $E_{\bar{q}}$, we have that $E_q/E_{\bar{q}}$ is the only proper normal subgroup of $S_{q^3}/E_{\bar{q}}$. Therefore, as in the proof of Lemma 3.3, the only possible non-trivial higher ramification groups $(S_{q^3}/E_{\bar{q}})^{(i)}$ are $S_{q^3}/E_{\bar{q}}$ and $E_q/E_{\bar{q}}$. Then the degree of the different divisor in $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(z)$ is $(n - j)(q/\bar{q} - 1) + j(q^3/\bar{q} - 1)$, where j is the number of ramification groups coinciding with $S_{q^3}/E_{\bar{q}}$ and $n = (q^n + 1)/s + 1$ by Lemma 3.19. From the Hurwitz genus formula applied to $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(z)$, it follows that $j = m/s + 1$. The claim follows. □

By Lemma 2.1, we can write $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_\infty} = \tilde{S} \rtimes \tilde{C}$, where $\tilde{S}$ is the Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$ and $\tilde{C}$ is a cyclic p'-group. Clearly $S_{q^3}/E_{\bar{q}} \leq \tilde{S}$ and, up to conjugation, we can assume $C_{(q+1)(\bar{q}-1)m/s} \leq \tilde{C}$.

Lemma 3.21. *The equality $\tilde{C} = C_{(q+1)(\bar{q}-1)m/s}$ holds.*

Proof. From $C_{m/s} \lhd \tilde{C}$ it follows that $\tilde{C}/C_{m/s}$ is an automorphism group of the fixed field $\mathbb{F}_{q^{2n}}(x,y)$ of $C_{m/s}$, of order at least $|C_{(q+1)(\bar{q}-1)\frac{m}{s}}/C_{m/s}| = (q+1)(\bar{q}-1)$. By [4, Theorem 3.3], the p'-part of $|\mathrm{Aut}(\mathbb{F}_{q^{2n}}(x,y))_{P_\infty}|$ is at most $(q+1)(\bar{q}-1)$. Then equality holds and the claim follows. □

Lemma 3.22. *The equality $\tilde{S} = S_{q^3}/E_{\bar{q}}$ holds.*

Proof. The first step is to prove that $i(\sigma) = 2$ for all $\sigma \in \tilde{S} \setminus (S_{q^3}/E_{\bar{q}})$. Since $i(\sigma) \geq 2$ for all $\sigma \in \tilde{S}$ and $i(\alpha)$ has been computed in Propositions 3.19, 3.20 for all $\alpha \in S_{q^3}/E_{\bar{q}}$, the claim $i(\sigma) = 2$ follows by direct computation from the Hurwitz genus formula, in analogy with the proof of Lemma 3.5. Therefore $i(\alpha) \geq i(\beta)$ for any non-trivial $\alpha \in E_q/E_{\bar{q}}$ and $\beta \in \mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_\infty}$, so that $E_q/E_{\bar{q}}$ is the last non-trivial higher ramification group at P_∞. By Lemma 2.1, this implies that $E_q/E_{\bar{q}}$ is normal in $\tilde{S}$. Therefore $\tilde{S}/(E_q/E_{\bar{q}})$ is an automorphism group of the fixed field of $E_q/E_{\bar{q}}$, which clearly coincides with $\mathbb{F}_{q^{2n}}(y,z)$ where $z^{m/s} = y^{q^2} - y$. By [4, Theorem 3.2], a Sylow p-subgroup of the automorphism group of $\mathbb{F}_{q^{2n}}(y,z)$ has order q^2. This is equal to the size of $(S_{q^3}/E_{\bar{q}})/(E_q/E_{\bar{q}})$, and the claim follows. □

Lemmas 3.21 and 3.22 complete the proof of the following result.

Corollary 3.23. *The full stabilizer of P_∞ in $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$ is*

$$G = (S_{q^3}/E_{\bar{q}}) \rtimes C_{(q+1)(\bar{q}-1)m/s}.$$

Define $O = \left\{P_{(\alpha,\beta,0)} \mid \beta \in \mathbb{F}_{q^2},\, c\beta^{q+1} = \mathrm{Tr}_{q/\bar{q}}(\alpha)\right\}$, and consider the set $O \cup \{P_\infty\} \subset \mathcal{X}_{a,b,n,s}(\mathbb{F}_{q^{2n}})$, which is stabilized pointwise by $C_{m/s}$.

Lemma 3.24. *The pointwise stabilzer of $O \cup \{P_\infty\}$ in $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$ is $C_{m/s}$.*

Proof. If α stabilizes $O \cup \{P_\infty\}$ pointwise, then α preserves the principal divisors of the coordinate functions x, y, z. Thus $\alpha : (x,y,z) \mapsto (\lambda x, \mu y, \rho z)$ for some $\lambda, \mu, \rho \in \mathbb{F}_{q^{2n}}$. By direct checking with the equations of $\mathcal{X}_{a,b,n,s}$, this implies $\lambda = \mu = 1$ and $\rho^{m/s} = 1$, that is $\alpha \in C_{m/s}$. □

Corollary 3.25. *If $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$ acts on $O \cup \{P_\infty\}$, then $\mathrm{Aut}(\mathcal{X}_{a,b,n,s}) = \mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_\infty}$.*

Proof. By Lemma 3.24, $C_{m/s}$ is normal in $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$. Then $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})/C_{m/s}$ is an automorphism group of the fixed field $\mathbb{F}_{q^{2n}}(x,y)$ of $C_{m/s}$. By [15, Theorem 12.11] (see also [4, Lemma 2.3]), $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})/C_{m/s}$ stabilizes the unique point at infinity of $\mathbb{F}_{q^{2n}}(x,y)$, which is totally ramified under P_∞. Since $C_{m/s}$ fixes P_∞, this implies that $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$ fixes P_∞. □

By Corollaries 3.23 and 3.25, Theorem 3.17 is proved once we show that $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$ acts on $O \cup \{P_\infty\}$. By contradiction, assume from now on that this is not the case.

Suppose first that no point in $\mathcal{X}_{a,b,n,s} \setminus (O \cup \{P_\infty\})$ is in the same orbit O_∞ of P_∞ under $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$. Since $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$ does not act on $O \cup \{P_\infty\}$, there exist two points $P \in \mathcal{X}_{a,b,n,s} \setminus (O \cup \{P_\infty\})$ and $Q \in O$ lying in the same orbit O_P. Then $O \subseteq O_P$, because O is an orbit under G. As $P_\infty \notin O_P$, this implies that $O_\infty = \{P_\infty\}$; in this case, the claim follows from Corollary 3.23.

Therefore there exists $P \in \mathcal{X}_{a,b,n,s} \setminus (O \cup \{P_\infty\})$ with $P \in O_\infty$. Also, P is $\mathbb{F}_{q^{2n}}$-rational, because the automorphism group of the $\mathbb{F}_{q^{2n}}$-maximal curve $\mathcal{X}_{a,b,n,s}$ is defined over $\mathbb{F}_{q^{2n}}$, and P lies in the same orbit of the $\mathbb{F}_{q^{2n}}$-rational point P_∞.

Lemma 3.26. *The short orbit O_∞ is the only non-tame orbit of* $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$.

Proof. The proof is analogous to the one of Lemma 3.12. It relies on the fact that all Sylow p-subgroups are conjugate, together with the correspondence between a point in a non-tame orbit and the Sylow p-subgroup made by the p-elements fixing that point. □

Write

$$|O_\infty| = 1 + \ell|O| + k|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_\infty}| = 1 + i\frac{q^3}{\bar{q}} + k\frac{q^3}{\bar{q}}(q+1)(\bar{q}-1)\frac{m}{s}, \tag{17}$$

where ℓ is 1 or 0 according to $O \subset \mathcal{O}_\infty$ or $O \not\subset O_\infty$, and $k \geq 1$ is the number of long orbits of $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_\infty}$ contained in O_∞. Since $k \geq 1$, the orbit-stabilizer theorem yields

$$|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})| = |O_\infty| \cdot |G| > |G|^2 > 84(g-1).$$

Then, by Theorem 2.4, one of the following cases holds for the short orbits of $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$:

(A) exactly one short orbit O_∞, non-tame, of length dividing $2g(\mathcal{X}_{a,b,n,s}) - 2$;
(B) exactly one non-tame orbit O_∞ and two tame orbits, both of length $|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})|2$, with $p \geq 3$;
(C) exactly one non-tame orbit O_∞ and one tame orbit.

The case (A) cannot occur, because $k \geq 1$ implies $|O_\infty| > 2g(\mathcal{X}_{a,b,n,s}) - 2$. In the next lemmas we find a contradiction also to the cases (B) and (C).

Lemma 3.27. *The case (B) does not occur.*

Proof. Suppose that the case (B) occurs. In analogy with Lemma 3.15, we apply the Hurwitz genus formula to $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})$. By Lemmas 3.19 and 3.20, we obtain

$$2g(\mathcal{X}_{a,b,n,s}) - 2 = -2|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})|$$
$$+2\frac{|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})|}{2}(2-1) + |O_\infty|\left(|G| - 1 + \left(\frac{q}{\bar{q}} - 1\right)(q+1)\frac{m}{s} + \left(\frac{q^3}{\bar{q}} - \frac{q}{\bar{q}}\right)\frac{m}{s}\right).$$

Since $|O_\infty| \cdot |G| = |\mathrm{Aut}(\mathcal{X}_{a,b,n,s})|$, we get

$$\left(\frac{q^2}{\bar{q}} - 1\right)(q+1)\frac{m}{s} - \left(\frac{q^3}{\bar{q}} + 1\right) = \left(1 + \ell\frac{q^3}{\bar{q}} + k|G|\right) \cdot \left(\left(\frac{q^2}{\bar{q}} - 1\right)(q+1)\frac{m}{s} - 1\right).$$

Since $k \geq 1$, this is a contradiction. □

Lemma 3.28. *The case (C) does not occur.*

Proof. The proof is analogous to the one of Proposition 3.16. Suppose that the case (C) occurs, and let O_1 be the tame short orbit. Then O is contained in O_∞ or $\mathcal{O}_1$ according to $\ell = 1$ or $\ell = 0$. Thus, O_1 has size $(1-\ell)|O| + k_1|G|$, where $k_1 \geq 0$ is the number of long orbits of G contained in O_1. By the Hurwitz genus formula we obtain

$$2g(\mathcal{X}_{a,b,n,s}) - 2 =$$

$$-2|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})| + |O_\infty| \left(|G| - 1 + \left(\frac{q^2}{\bar{q}} - 1 \right) (q+1) \frac{m}{s} \right) + |O_1| \left(\frac{|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})|}{|O_1|} - 1 \right),$$

which yields

$$k_1 = k \left(\left(\frac{q^2}{\bar{q}} - 1 \right) (q+1) \frac{m}{s} - 1 \right) + \ell \left(\frac{q^2/\bar{q} - 1}{\bar{q} - 1} \right). \tag{18}$$

By the orbit-stabilizer theorem,

$$|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_1}| \cdot |O_1| = |G| \cdot |O_\infty|, \tag{19}$$

where P_1 is a point of O_1. We analyze the cases $\ell = 0$ and $\ell = 1$ separately.

- Let $\ell = 0$. Then $O \subseteq O_1$ and $\mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_1}$ has a subgroup conjugate to $C_{(q+1)(\bar{q}-1)m/s}$. We can then write $|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_1}| = h(q+1)(\bar{q}-1)m/s$ for some $h \geq 1$. By direct computation with Equations (18) and (19), we get

$$h \left(1 + k(q+1)(\bar{q}-1) \frac{m}{s} \left(\left(\frac{q^2}{\bar{q}} - 1 \right) (q+1) \frac{m}{s} - 1 \right) \right) = 1 + k(q+1)(\bar{q}-1) \frac{m}{s}. \tag{20}$$

  In particular, $h \equiv 1 \pmod{(q+1)(\bar{q}-1)\frac{m}{s}}$.

  Suppose that $h > 1$. Then $h > (q+1)(\bar{q}-1)\frac{m}{s}$, so that

$$|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_1}| > \left((q+1)(\bar{q}-1) \frac{m}{s} \right)^2$$

  and hence

$$|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})| = |\mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_1}| \cdot |O_1| >$$

$$\left((q+1)(\bar{q}-1) \frac{m}{s} \right)^2 \cdot \left(\frac{q^3}{\bar{q}} + k \left(\left(\frac{q^2}{\bar{q}} - 1 \right) (q+1) \frac{m}{s} - 1 \right) \frac{q^3}{\bar{q}} (q+1)(\bar{q}-1) \frac{m}{s} \right).$$

  Since $k > 0$, this implies

$$|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})| > 8g^3,$$

  a contradiction to Theorem 2.4. Therefore $h = 1$. Now Equation (20), together with $h = 1$ and $k \geq 1$, provides a contradiction.

- Let $\ell = 1$. By direct computation using Equations (18) and (19), one gets

$$|\mathrm{Aut}(\mathcal{X}_{a,b,n,s})_{P_1}| = q\bar{q} - q + \frac{kq(q+1)(\bar{q}-1)\frac{m}{s} - \left(\frac{q^3}{\bar{q}} - q\bar{q} - 1\right)}{k\left((q+1)\left(\frac{q^2}{\bar{q}} - 1\right)\frac{m}{s} - 1\right) + \frac{q^2/\bar{q}-1}{\bar{q}-1}}. \tag{21}$$

Consider the fraction on the right-hand side of Equation (21), and recall $k \geq 1$. The denominator is positive and greater than the absolute value of the numerator. Also, the numerator is non-zero, being congruent to 1 modulo q. Thus, the right-hand side of Equation (21) is not an integer, a contradiction.

□

The proof of Theorem 3.17 is now complete.

Acknowledgments

The first author would like to acknowledge the support from The Danish Council for Independent Research (DFF-FNU) for the project *Correcting on a Curve*, Grant No. 8021-00030B. The third author was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

References

[1] D. Bartoli, M. Montanucci and G. Zini, *Multi point AG codes on the GK maximal curve*, Designs, Codes and Cryptography, 86, pp. 161–177 (2018).

[2] D. Bartoli, M. Montanucci, and G. Zini, *AG codes and AG quantum codes from the GGS curve*, Des. Codes Cryptogr. **86** (2018), no. 10, 2315–2344.

[3] P. Beelen and M. Montanucci. A new family of maximal curves. *Journal of the London Math. Soc.* **2** (2018), 1–20.

[4] M. Bonini, M. Montanucci and G. Zini, On plane curves given by separated polynomials and their automorphisms. *Adv. Geom.* **20** (2020), no. 1, 61–70.

[5] A. S. Castellanos, G. Tizziotti, *Two-Point AG Codes on the GK Maximal Curves*. IEEE Transactions on Information Theory, v. 62, p. 681-686, 2016.

[6] I. M. Duursma and K.-H. Mak, *On maximal curves which are not Galois subcovers of the Hermitian curve*, Bull. Braz. Math. Soc (N.S.) **43 (3)** (2012), 453–465.

[7] S. Fanali and M. Giulietti, *One-point AG Codes on the GK Maximal Curves*, IEEE Trans. on Information Theory, vol. 56, no. 1, pp. 202 - 210, 2010.

[8] A. Garcia, C. Güneri, and H. Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Adv. Geom. 10 (2010), no. 3, 427–434.

[9] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. 343 (2009), 229–245.

[10] M. Giulietti, M. Montanucci and G. Zini, *On maximal curves that are not quotients of the Hermitian curve*, Finite Fields Appl. **41** (2016), 72–88.

[11] B. Gunby, A. D. Smith and A. Yuan, *Irreducible canonical representations in positive characteristic*, Res. Number Theory 1, 3 (2015). https://doi.org/10.1007/s40993-015-0004-8

[12] C. Güneri, M. Özdemir and H. Stichtenoth, *The automorphism group of the generalized Giulietti–Korchmáros function field* , Adv. Geom. vol. 13, no. 2, 2013, pp. 369-380.

[13] R. Guralnick, B. Malmskog, R. Pries, *The automorphism group of a family of maximal curves*, J. Algebra 361 (2012), 92–116.
[14] H.W. Henn, Funktionenkörper mit großer Automorphismengruppe, *J. Reine Angew. Math.* **302** (1978), 96–115.
[15] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics, Princeton (2008).
[16] C. Hu and S. Yang, *Multi-point Codes from the GGS Curves*, Advances in Mathematics of Communications, to appear.
[17] S.L. Kleiman.*Algebraic cycles and the Weil conjectures*, in: Dix exposés sur la cohomologie des schémas, in: Adv. Stud. Pure Math. **3**, (1968) 359–386 .
[18] G. Lachaud, *Sommes d' Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris 305 (Serie I) (1987), 729–732.
[19] L. Landi and L. Vicino, *Two-point AG codes from the Beelen-Montanucci maximal curve*, Finite Fields Appl. **80** (2022), Paper No. 102009, 17 pp.
[20] M. Montanucci and V. Pallozzi Lavorante, *AG codes from the second generalization of the GK maximal curve*, Discrete Math. 343 (2020), 111810.
[21] M. Montanucci and G. Tizziotti, *Generalized Weierstrass semigroups at several points on certain maximal curves which cannot be covered by the Hermitian curve*, Des. Codes Cryptogr. (2022). https://doi.org/10.1007/s10623-022-01130-3.
[22] H.G. Rück and H. Stichtenoth. A characterization of the Hermitian function fields over finite fields. *J. Reine Angew. Math.* **457** (1994), 185–188.
[23] J.P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979, viii+241 pp.
[24] H. Stichtenoth, *Algebraic Function Fields and Codes*, Berlin, Germany: Springer, 1993.
[25] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern, *Arch. Math.* **24** (1973), 615–631.
[26] F. Sullivan, p-torsion in the class group of curves with many automorphisms, *Arch. Math.* **26** (1975), 253–261.
[27] S. Tafazolian, A. Teherán-Herrera, and F. Torres, *Further examples of maximal curves which cannot be covered by the Hermitian curve*. J. Pure Appl. Algebra, 220(3) : 1122–1132, 2016.
[28] G. Tizziotti and A. S. Castellanos, *Weierstrass Semigroup and Pure Gaps at Several Points on the GK Curve*. Bulletin Brazilian Mathematical Society, v. 49, p. 419–429, 2018.
[29] G. D. Villa Salvador, Topics in the theory of algebraic function fields, Mathematics: Theory and Applications. Birkhäuser Boston, Inc., Boston, MA, (2006).