GENERALIZED ARTIN-MUMFORD CURVES OVER FINITE FIELDS

MARIA MONTANUCCI AND GIOVANNI ZINI

Abstract. Let $\mathbb{F}_q$ be the finite field of order $q = p^h$ with $p > 2$ prime and $h > 1$, and let $\mathbb{F}_\bar{q}$ be a subfield of $\mathbb{F}_q$. From any two $\bar{q}$-linearized polynomials $L_1, L_2 \in \mathbb{F}_q[T]$ of degree $q$, we construct an ordinary curve $X_{(L_1, L_2)}$ of genus $g = (q - 1)^2$ which is a generalized Artin-Schreier cover of the projective line $\mathbb{P}^1$. The automorphism group of $X_{(L_1, L_2)}$ over the algebraic closure $\mathbb{F}_q$ of $\mathbb{F}_q$ contains a semidirect product $\Sigma \rtimes \Gamma$ of an elementary abelian $p$-group $\Sigma$ of order $q^2$ by a cyclic group $\Gamma$ of order $\bar{q} - 1$. We show that for $L_1 \neq L_2$, $\Sigma \rtimes \Gamma$ is the full automorphism group $\text{Aut}(X_{(L_1, L_2)})$ over $\mathbb{F}_\bar{q}$; for $L_1 = L_2$ there exists an extra involution and $\text{Aut}(X_{(L_1, L_2)}) = \Sigma \rtimes \Delta$ with a dihedral group $\Delta$ of order $2(\bar{q} - 1)$ containing $\Gamma$. Two different choices of the pair $(L_1, L_2)$ may produce birationally isomorphic curves, even for $L_1 = L_2$. We prove that any curve of genus $(q - 1)^2$ whose $\mathbb{F}_q$-automorphism group contains an elementary abelian subgroup of order $q^2$ is birationally equivalent to $X_{(L_1, L_2)}$ for some separable $\bar{q}$-linearized polynomials $L_1, L_2$ of degree $q$. We produce an analogous characterization in the special case $L_1 = L_2$. This extends a result on the Artin-Mumford curves, due to Arakelian and Korchmáros [1].

1. INTRODUCTION

The Artin-Mumford curve $\mathcal{M}_c$ of genus $(p - 1)^2$ defined over a field $\mathbb{F}$ of odd characteristic $p$ is the nonsingular model of the plane curve with affine equation

$$(X^p - X)(Y^p - Y) = c, \quad c \in \mathbb{F}^*.$$  

Artin-Mumford curves, especially over non-Archimedean valued fields of positive characteristic, have been investigated in several papers; see [3], [2], and [4]. By a result of Cornelissen, Kato and Kontogeorgis [2] valid over any non-Archimedean valued field $(\mathbb{F}, | \cdot |)$ of positive characteristic, if $|c| < 1$ then $\text{Aut}_{\mathbb{F}}(\mathcal{M}_c)$ is the semidirect product

$$(C_p \times C_p) \rtimes D_{p-1},$$  

where $C_p$ is a cyclic group of order $p$ and $D_{p-1}$ is a dihedral group of order $2(p - 1)$. This result holds over any algebraically closed field; see [12].

The interesting question whether the genus $(p - 1)^2$ together with an automorphism group as in [2] characterize the Artin-Mumford curve has been solved so far only for curves defined over $\mathbb{F}_p$; see [1].

A natural generalization of Artin-Mumford curves arises when the polynomials $X^p - X$ and $Y^p - Y$ in [1] are replaced by separable linearized polynomials $L_1, L_2$ of equal degree. Our aim is to investigate such generalized Artin-Mumford curves, especially their automorphism groups. To present our results, we need some notation that will also be used throughout the paper.

For an odd prime $p$ and powers $\bar{q} = p^h$ and $\bar{q} = \bar{q}^m$, $\mathbb{F}_p = \mathbb{F}_\bar{q}$, $\mathbb{F}_q$ are the finite fields of order $p$, $\bar{q}$, $q$; $\mathbb{K}$ is the algebraic closure of $\mathbb{F}_p$; $L_1(T), L_2(T) \in \mathbb{K}[T]$ are separable polynomials of degree $q$ which are $\bar{q}$-linearized. We admit that one, but not both, is $\bar{q}$-linearized, for some $k \geq 2$. With this notation, the generalized Artin-Mumford curve $X_{(L_1, L_2)}$ is the nonsingular model of the plane curve with affine equation

$$(3) \quad X_{(L_1, L_2)}: \quad L_1(X) \cdot L_2(Y) = 1.$$  

The family of generalized Artin-Mumford curves is denoted by:

$$S_{\bar{q} | \bar{q}} = \{ X_{(L_1, L_2)} \mid L_1(T), L_2(T) \in \mathbb{K}[T], \deg(L_1) = \deg(L_2) = q, L_1, L_2 \text{ are separable} \}.$$
\[ \bar{q} \text{-linearized, not both } q^k \text{-linearized for any } k \geq 2 \].

An interesting feature of a generalized Artin-Mumford curve \( \mathcal{X}_{(L_1, L_2)} \) is that its genus only depends on \( q \), namely \( g(\mathcal{X}_{(L_1, L_2)}) = (q - 1)^2 \). Also, \( \mathcal{X}_{(L_1, L_2)} \) is an ordinary curve, that is, its genus and \( p \)-rank are equal. A complete description of the automorphism group of any generalized Artin-Mumford curve is given in the following two theorems.

**Theorem 1.1.** The full automorphism group of \( \mathcal{X}_{(L, L)} \) is the semidirect product
\[
\Sigma \rtimes \Delta,
\]
where
- \( \Sigma = \{ (X, Y) \mapsto (X + \alpha, Y + \beta) \mid L(\alpha) = L(\beta) = 0 \} \) is an elementary abelian \( p \)-group of order \( q^2 \);
- \( \Delta = \langle \theta, \xi \rangle \) is a dihedral group of order \( 2(\bar{q} - 1) \), where \( \theta : (X, Y) \mapsto (\lambda X, \lambda^{-1} Y) \) with \( \lambda \) a primitive \( (\bar{q} - 1) \)-th root of unity, and \( \xi : (X, Y) \mapsto (Y, X) \).

**Theorem 1.2.** If \( L_1 \neq L_2 \), the full automorphism group of \( \mathcal{X}_{(L_1, L_2)} \) is the semidirect product
\[
\Sigma \rtimes \Gamma,
\]
where
- \( \Sigma = \{ (X, Y) \mapsto (X + \alpha, Y + \beta) \mid L_1(\alpha) = L_2(\beta) = 0 \} \) is an elementary abelian \( p \)-group of order \( q^2 \);
- \( \Gamma = \langle \theta \rangle \) is a cyclic group of order \( \bar{q} - 1 \), where \( \theta : (X, Y) \mapsto (\lambda X, \lambda^{-1} Y) \) with \( \lambda \) a primitive \( (\bar{q} - 1) \)-th root of unity.

For \( \bar{q} = q \), the size of \( \text{Aut}(\mathcal{X}_{(L_1, L_2)}) \) is approximately \( 2(g(\mathcal{X}_{(L_1, L_2)}) + 1)^{3/2} \). Since the groups given in Theorems 1.1 and 1.2 are solvable, \( \mathcal{X}_{(L_1, L_2)} \) attains, up to the constant, the bound given in [8].

Our main result is that \( \text{Aut}(\mathcal{X}_{(L_1, L_2)}) \) together with \( g(\mathcal{X}_{(L_1, L_2)}) \) characterize the curves in \( S_{\bar{q} q} \). This result can be viewed as a generalization of [1] Theorem 1.1] on Artin-Mumford curves.

**Theorem 1.3.** Let \( X \) be a (projective, non-singular, geometrically irreducible, algebraic) curve of genus \( g = (q - 1)^2 \) defined over \( \mathbb{K} \). If \( \text{Aut}(X) \) contains an elementary abelian subgroup \( E_{q^2} \) of order \( q^2 \), then \( X \) is birationally equivalent over \( \mathbb{K} \) to some \( X_{(L_1, L_2)} \in S_{\bar{q} q} \), where \( \bar{q} \) is the largest power of \( p \) such that \( \text{Aut}(X) \) contains a cyclic subgroup \( C_{\bar{q} - 1} \) of order \( \bar{q} - 1 \).

In the case \( L_1 = L_2 \), the assumption on the genus can be weakened under a stronger assumption on the automorphism group, as follows.

**Theorem 1.4.** Let \( X \) be a curve of genus \( g \leq (q - 1)^2 \) defined over \( \mathbb{K} \). If \( \text{Aut}(X) \) contains a semidirect product \( E_{q^2} \rtimes (C_2 \times C_2) \) (where \( E_{q^2} \) is elementary abelian of order \( q^2 \) and \( C_2 \times C_2 \) is a Klein four-group), then \( X \) is birationally equivalent over \( \mathbb{K} \) to some \( X_{(L_1, L_2)} \in S_{\bar{q} q} \), where \( \bar{q} \) is the largest power of \( p \) such that \( \text{Aut}(X) \) contains a cyclic subgroup \( C_{\bar{q} - 1} \) of order \( \bar{q} - 1 \).

In Section 2 preliminary results on automorphism groups of ordinary curves and curves of even genus are collected. In Section 3 we give the proofs of Theorems 1.1 and 1.2 doing so we also show the relevant properties of generalized Artin-Mumford curves; see Lemma 3.1. The proof of Theorems 1.3 and 1.4 is given in Section 4 where additional classification results of independent interest are found, as well. Here we only mention that Theorem 1.5 gives the following characterization.

**Theorem 1.5.** Let \( Y \) be a curve of genus \( q - 1 \) defined over \( \mathbb{K} \) whose automorphism group \( \text{Aut}(Y) \) contains an elementary abelian subgroup \( E_q \) of order \( q \). Then one of the following holds.
(I) \( \mathcal{Y} \) is birationally equivalent over \( \mathbb{K} \) to the curve \( \mathcal{Y}_{L,a} \) with affine equation
\[
L(y) = ax + \frac{1}{x},
\]
for some \( a \in \mathbb{K}^* \) and \( L(T) \in \mathbb{K}[T] \) a separable \( p \)-linearized polynomial of degree \( q \). For the curve \( \mathcal{Y}_{L,a} \) the following properties hold:
(i) \( \mathcal{Y}_{L,a} \) is ordinary and hyperelliptic;
(ii) \( \mathcal{Y}_{L,a} \) has exactly \( 2q \) Weierstrass places, which are the fixed places of the hyperelliptic involution \( \mu \).
(iii) The full automorphism group \( \text{Aut}(\mathcal{Y}_L) \) of \( \mathcal{Y}_{L,a} \) has order \( 4q \) and is a direct product \( \text{Dih}(E_q) \times \langle \mu \rangle \).

(II) \( p \neq 3 \) and \( \mathcal{Y} \) is birationally equivalent over \( \mathbb{K} \) to the curve \( Z_{L,b} \) with affine equation
\[
L(y) = x^3 + bx,
\]
for some \( a \in \mathbb{K} \) and \( L(T) \in \mathbb{K}[T] \) a separable \( p \)-linearized polynomial of degree \( q \). For the curve \( Z_{L,b} \) the following properties hold:
(i) \( Z_{L,b} \) has zero \( p \)-rank;
(ii) \( \text{Aut}(Z_{L,b}) \) contains a generalized dihedral subgroup \( \text{Dih}(E_q) = E_q \times \langle \nu \rangle \).

Theorem 1.5 provides a generalization of [13, Proposition (2.2) and Corollary (2.3)].

Our proof uses function field theory, especially the Hurwitz genus formula and the Deuring-Shafarevich Theorem 1.5, together with deeper results on finite groups, especially the classification theorem on finite non-abelian simple groups whose Sylow 2-subgroups are dihedral or semidihedral. In doing so we adopt the approach worked out by Giulietti and Korchmáros in [3].

2. Background and Preliminary Results

We keep the notation used in Introduction. Also, \( \mathcal{X} \) is a (projective, non-singular, geometrically irreducible, algebraic) curve of genus \( g \geq 2 \) defined over \( \mathbb{K} \), \( \mathbb{K}(\mathcal{X}) \) is the function field of \( \mathcal{X} \), and \( \text{Aut}(\mathcal{X}) \) is its full automorphism group over \( \mathbb{K} \).

For a subgroup \( G \) of \( \text{Aut}(\mathcal{X}) \), let \( \tilde{\mathcal{X}} \) denote a non-singular model of \( \mathbb{K}(\mathcal{X})^G \), that is, a curve with function field \( \mathbb{K}(\mathcal{X})^G \), where \( \mathbb{K}(\mathcal{X})^G \) consists of all elements of \( \mathbb{K}(\mathcal{X}) \) fixed by every element in \( G \). Usually, \( \tilde{\mathcal{X}} \) 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 \( \Phi \) be the cover of \( \mathcal{X}/\tilde{\mathcal{X}} \) where \( \tilde{\mathcal{X}} = \mathcal{X}/G \). A place \( P \) of \( \mathbb{K}(\mathcal{X}) \) is a ramification place of \( G \) if the stabilizer \( G_P \) of \( P \) in \( G \) is nontrivial; the ramification index \( e_P \) is \( |G_P| \). The \( G \)-orbit of \( P \) in \( \mathbb{K}(\mathcal{X}) \) is the subset \( o_P = \{ R \mid R = g(P), g \in G \} \) of the set of the places of \( \mathbb{K}(\mathcal{X}) \), and it is long if \( |o_P| = |G| \), otherwise \( o_P \) is short. For a place \( Q \), the \( G \)-orbit \( o \) lying over \( Q \) consists of all places \( P \) of \( \mathbb{K}(\mathcal{X}) \) such that \( \Phi(P) = Q \). If \( P \in o \) then \( |o| = |G|/|G_P| \) and hence \( P \) is a ramification place if and only if \( o \) is a short \( G \)-orbit.

If every non-trivial element in \( G \) is fixed–point-free on the set of the places of \( \mathbb{K}(\mathcal{X}) \), the cover \( \Phi \) is unramified. For a non-negative integer \( i \), the \( i \)-th ramification group of \( \mathcal{X} \) at \( P \) is denoted by \( G_P^{(i)} \) and defined to be
\[
G_P^{(i)} = \{ \alpha \in G_P \mid v_P(\alpha(t) - t) \geq i + 1 \},
\]
where \( t \) is a local parameter at \( P \); see [11]. Here \( G_P^{(0)} = G_P \).

Let \( \tilde{g} \) be the genus of the quotient curve \( \tilde{\mathcal{X}} = \mathcal{X}/G \). The Hurwitz genus formula [6] Theorem 7.27] gives the following equation
\[
2\tilde{g} - 2 = |G|(2\tilde{g} - 2) + \sum_{P \in \mathcal{X}} d_P,
\]
where the different \( d_P \) at \( P \) is given by

\[
d_P = \sum_{i \geq 0} (|G_P^{(i)}| - 1),
\]

see [6, Theorem 11.70]. Let \( \gamma \) and \( \bar{\gamma} \) be the \( p \)-ranks of \( \cal{X} \) and \( \bar{\cal{X}} \) respectively. The Deuring-Shafarevich formula [6, Theorem 11.62] states that

\[
\gamma - 1 = |G| (\bar{\gamma} - 1) + \sum_{i=1}^{k} (|G| - \ell_i)
\]

where \( \ell_1, \ldots, \ell_k \) are the sizes of the short orbits of \( G \).

A subgroup \( G \) of \( \text{Aut}(\cal{X}) \) is tame if \( \gcd(p, |G|) = 1 \), otherwise \( G \) is non-tame. The stabilizer \( G_P \) of a place \( P \in \cal{X} \) in \( G \) is a semidirect product \( G_P = Q_P \rtimes U \) where the normal subgroup \( Q_P \) is a \( p \)-group while the complement \( U \) is a tame cyclic group; see [6, Theorem 11.49].

The following result is due to Nakajima; see [10, Theorems 1, 2 and 3] and [6, Lemma 11.75].

**Theorem 2.1.** Let \( \cal{X} \) be a curve with \( g(\cal{X}) \geq 2 \) defined over an algebraically closed field of characteristic \( p \geq 3 \), and \( H \) be a Sylow \( p \)-subgroup of \( \text{Aut}(\cal{X}) \). Then the following hold.

(I) When \( g(\cal{X}) \geq 2 \), we have

\[
|H| \leq \frac{p}{p-2} (\gamma(\cal{X}) - 1) \leq \frac{p}{p-2} (g(\cal{X}) - 1).
\]

(II) If \( \cal{X} \) is ordinary \( (i.e. \ g(\cal{X}) = \gamma(\cal{X})) \) and \( G \leq \text{Aut}(\cal{X}) \), then \( G_P^{(2)} = \{1\} \) and \( G_P^{(1)} \) is elementary abelian, for every \( P \in \cal{X} \).

(III) If \( \cal{X} \) is ordinary then \( |\text{Aut}(\cal{X})| \leq 84(g(\cal{X}) - 1)g(\cal{X}) \).

(IV) If \( g(\cal{X}) = 1 \) then \( H \) is cyclic.

The following results are due to Giulietti and Korchmáros; see [5].

**Lemma 2.2.** Let \( H \) be a solvable automorphism group of an algebraic curve \( \cal{X} \) of genus \( g(\cal{X}) \geq 2 \) containing a normal \( d \)-subgroup \( Q \) of odd order such that \( |Q| \) and \( [H : Q] \) are coprime. Suppose that a complement \( U \) of \( Q \) in \( H \) is abelian, and that \( N_H(U) \cap Q = \{1\} \). If

\[
|H| \geq 30(g(\cal{X}) - 1),
\]

then \( d = p \) and \( U \) is cyclic.

The odd core \( O(G) \) of a group \( G \) is its maximal normal subgroup of odd order. If \( O(G) \) is trivial, then \( G \) is an odd core-free group.

**Lemma 2.3.** Let \( \cal{X} \) be a curve of even genus, and \( G \) be an odd core-free automorphism group of \( \cal{X} \) with a non-abelian simple minimal normal subgroup \( M \). Up to isomorphism, one of the following cases occurs for some prime \( d \) and odd \( k \):

(i) \( M = \text{PSL}(2, d^k) \leq G \leq \text{PGL}(2, d^k) \) with \( d^k \geq 5 \);

(ii) \( M = \text{PSL}(3, d^k) \leq G \leq \text{PGL}(3, d^k) \) with \( d^k \equiv 3 \pmod{4} \);

(iii) \( M = \text{PSU}(3, d^k) \leq G \leq \text{PGU}(3, d^k) \) with \( d^k \equiv 1 \pmod{4} \);

(iv) \( M = G = A_7, \) the alternating group on 7 letters;

(v) \( M = G = M_{11}, \) the Mathieu group on 11 letters.

**Lemma 2.4.** If \( \cal{X} \) is a curve of even genus then \( \text{Aut}(\cal{X}) \) has no elementary abelian \( 2 \)-subgroup of order 8.

**Lemma 2.5.** Let \( \cal{X} \) be a curve of even genus and \( G \leq \text{Aut}(\cal{X}) \). If \( G \) has a minimal normal subgroup of order 2 then \( G = O(G) \rtimes S_2 \), where \( S_2 \) is Sylow 2-subgroup of \( G \), unless \( S_2 \) is a generalized quaternion group.
For a positive integer $d$, $C_d$ stands for a cyclic group of order $d$, $D_d$ for a dihedral group of order $2d$, $E_d$ for an elementary abelian group of order $d$, and $Dih(E_d)$ for a generalized dihedral group $E_d \rtimes C_2$ of order $2d$.

3. THE AUTOMORPHISM GROUP OF $X_{L_1, L_2}$

Lemma 3.1. For the curve $X_{L_1, L_2}$ as in [3], $X_\infty = (1 : 0 : 0)$ and $Y_\infty = (0 : 1 : 0)$, the following properties hold:

i) $X_\infty$ and $Y_\infty$ are $q$-fold ordinary points;
ii) $X_{L_1, L_2}$ is ordinary with $g(X_{L_1, L_2}) = \gamma(X_{L_1, L_2}) = (q - 1)^2$;
iii) If $L_1 \neq L_2$, $\text{Aut}(X_{L_1, L_2})$ contains the subgroup $\Sigma \times \Gamma$ defined in [3];
iv) If $L_1 = L_2 = L$, $\text{Aut}(X_{L_1, L_2})$ contains the subgroup $\Sigma \times \Delta$ defined in [3];

v) In both cases iii) and iv), the group $\Sigma$ is a Sylow $p$-subgroup of $\text{Aut}(X_{L_1, L_2})$.

vi) The quotient curves $X_{L_1, L_2}/x_1$ and $X_{L_1, L_2}/y_0$ are rational curves, where $x_1 = \{\tau_{\alpha, \beta} \in \Sigma | \beta = 0\}$ and $y_0 = \{\tau_{\alpha, \beta} \in \Sigma | \alpha = 0\}$.

Proof. Let $\tilde{P}_{x=\alpha}$, with $L_1(\alpha) = 0$, be the $q$ distinct zeros and $\tilde{P}_{x=\alpha}$ be the unique pole of $L(x)$ in $\mathbb{K}(x)$. Then

$$v_{\tilde{P}_{x=\alpha}}(1/L_1(x)) = -1, \quad v_{\tilde{P}_{x=\alpha}}(1/L_1(x)) = q,$$

and $1/L_1(x)$ has valuation zero at any other place of $\mathbb{K}(x)$. Thus, the function field $\mathbb{K}(X_{L_1, L_2}) = \mathbb{K}(x, y)$ with $L_1(x) \cdot L_2(y) = 1$, is a generalized Artin-Schreier extension of $\mathbb{K}(x)$ of degree $q$; see [11, Proposition 3.7.10]. The places $\tilde{P}_{x=\alpha}$ are totally ramified while any other place is unramified. The genus of $X_{L_1, L_2}$ is given by

$$g(X_{L_1, L_2}) = q \cdot g(\mathbb{K}(x)) + \frac{q - 1}{2} \cdot (-2 + 2q) = (q - 1)^2.$$ 

The places $P_{x=\alpha}$, lying over $\tilde{P}_{x=\alpha}$, $i = 1, \ldots, q$, are the poles of $y$ and they are centered at $Y_\infty$. The unique zero of $y$ is place $P_{x=\infty}$ lying over $\tilde{P}_{x=\infty}$. Analogously, $x$ has $q$ distinct poles $P_{y=\beta}$, with $L_2(\beta) = 0$, which are simple and centered at $X_\infty$, and a unique zero $P_{y=\infty}$. Note that $P_{x=\infty} = P_{y=0}$ and $P_{y=\infty} = P_{x=0}$. Let $\Sigma = \{\tau_{\alpha, \beta} : (X, Y) \mapsto (X + \alpha, Y + \beta) | L_1(\alpha) = L_2(\beta) = 0\}$. By direct computation $\Sigma$ is an elementary abelian $p$-subgroup of $\text{Aut}(X_{L_1, L_2})$ of order $q^2$. From Theorem [2.11], $\Sigma$ is a Sylow $p$-subgroup of $\text{Aut}(X_{L_1, L_2})$. Thus the Galois group of $\mathbb{K}(x, y) / \mathbb{K}(x)$ is contained in $\Sigma$ up to conjugation, and hence $\mathbb{K}(x, y)^\Sigma$ is rational. By direct computation $\Sigma$ has at least two short orbits of length $q$, namely

$$\Omega_x = \{P_{y=\beta} | L_2(\beta) = 0\}, \quad \Omega_y = \{P_{x=\alpha} | L_1(\alpha) = 0\}.$$ 

From the Deuring-Shafarevich formula [3] applied to the extension $\mathbb{K}(x, y) / \mathbb{K}(x, y)^\Sigma$,

$$q^2 - 2q = g(X_{L_1, L_2}) - 1 \geq \gamma(X_{L_1, L_2}) - 1 \geq q^2(0 - 1) + 2(q^2 - q) = q^2 - 2q.$$ 

Therefore the curve $X_{L_1, L_2}$ is ordinary. By direct checking, if $L_1 \neq L_2$, then $\Sigma$ and $\Gamma$ are subgroups of $\text{Aut}(X_{L_1, L_2})$, $\Gamma$ normalizes $\Sigma$, and $\Gamma \cap \Sigma = \{1\}$. Analogously, if $L_1 = L_2$, then $\Sigma$ and $\Delta$ are subgroups of $\text{Aut}(X_{L_1, L_2})$, $\Delta$ normalizes $\Sigma$, and $\Delta \cap \Sigma = \{1\}$.

In order to prove vi), set $\eta = L_1(x)$. Then $\mathbb{K}(\eta, y) \subset \mathbb{K}(X_{L_1, L_2})^{\Sigma_y}$. Since $[\mathbb{K}(X_{L_1, L_2}) : \mathbb{K}(\eta, y)] \leq q$, this implies $\mathbb{K}(X_{L_1, L_2})^{\Sigma_x} = \mathbb{K}(\eta, y)$ and

$$X_{L_1, L_2}/x_1 : \ L_2(y) = \frac{1}{\eta}.$$ 

This shows that $X_{L_1, L_2}/x_1$ is rational, and the same holds for $X_{L_1, L_2}/y_0$.

The following result follows from the proof of Lemma 3.1.
Corollary 3.2. The group $\Sigma$ has exactly two short orbit $\Omega_x$ and $\Omega_y$, both of length $q$. Namely,
\[ \Omega_x = \{ P_y = \beta \mid L_2(\beta) = 0 \}, \quad \Omega_y = \{ P_x = \alpha \mid L_1(\alpha) = 0 \}. \]
Moreover $\kappa(x, y)^\Sigma$ is rational and the principal divisors of the coordinate functions are given by
\[ (x) = q P_y = 0 - \sum_{P \in \Omega_y} P, \quad (y) = q P_x = 0 - \sum_{P \in \Omega_x} P. \]

Lemma 3.3. Let $C$ be a cyclic subgroup of $\text{Aut}(X_{(L_1, L_2)})$ containing $\Gamma = (\theta)$, where $\theta : (X, Y) \mapsto (\lambda X, \lambda^{-1} Y)$ with $\lambda$ a primitive $(\bar{q} - 1)$-th root of unity. Suppose that $C$ is contained in the normalized $N$ of $\Sigma$ in $\text{Aut}(X_{(L_1, L_2)})$. Then $C = \Gamma$.

Proof. First of all we observe that $C \cap \Sigma = \{1\}$. In fact by direct checking $\Gamma$ does not commute with any non trivial $p$-element $\tau_{x, y} \in \Sigma$. From Lemma 3.1(v), $C$ is tame. Since $C \leq N$, $C$ is isomorphic to an automorphism group $C$ of $X_{(L_1, L_2)}/\Sigma$. Denote by $\Gamma$ the subgroup of $PGL(2, \kappa)$ which is isomorphic to $\Gamma$. Moreover, from Corollary 3.2 $C$ acts on $\Omega_x \cup \Omega_y$, and $C \leq PGL(2, \kappa)$ as $X_{(L_1, L_2)}/\Sigma$ is rational. From [7, Hauptsatz 8.27] both $C$ and $\Gamma$ fix exactly two places on $X_{(L_1, L_2)}/\Sigma$ which are then the two places $P_x$ and $P_y$ lying under $\Omega_x$ and $\Omega_y$, respectively. Hence, from Corollary 3.2 $C$ fixes the pole divisors of $x$ and $y$. From the Orbit stabilizer theorem $C$ fixes at least one place in $\Omega_x$ and one place in $\Omega_y$. By direct computation $\Gamma$ fixes $P_x = 0 \in \Omega_y$ and $P_y = 0 \in \Omega_x$, acting semiregularly on $\Omega_x \setminus \{ P_y = 0 \}$ and $\Omega_y \setminus \{ P_x = 0 \}$. Thus, $C$ fixes $P_y = 0$ and $P_x = 0$ and hence the zero divisors of $x$ and $y$ are preserved by $C$ from Corollary 3.2. This implies that the generator $c$ of $C$ has the form $c : (x, y) \mapsto (\gamma x, \delta y)$, for some $\gamma, \delta \in \kappa$. By direct computation $\gamma^{\bar{q} - 1} = \delta^{\bar{q} - 1} = 1$, and so $C = \Gamma$. \hfill \Box

Corollary 3.4. Let $C$ be a cyclic subgroup of the normalizer $N$ of $\Sigma$ in $\text{Aut}(X_{(L_1, L_2)})$ such that $(\bar{q} - 1) \mid |C|$ and $(\bar{q} - 1) \mid (\bar{q} - 1)$. Then $C = \Gamma$.

3.1. Proof of Theorem [1.1]

In this section, $L_1 = L_2 = L$ and we refer to $\Sigma$ and $\Delta$ as defined in Theorem [1.1] For $q = p$ Theorem [1.1] was proved in [1, Theorem 1.1]. Thus, we suppose that $q > p$.

Lemma 3.5. The normalizer $N$ of $\Sigma$ in $\text{Aut}(X_{(L_1, L_2)})$ is $N = \Sigma \rtimes \Delta$.

Proof. From Corollary 3.2 $\bar{N} = N/\Sigma$ is a tame subgroup of $PGL(2, \kappa)$ containing a dihedral group $\bar{\Delta}$ which is isomorphic to $\Delta = \Gamma \rtimes \xi$, where $\Gamma = (\theta)$. Now we show that there are no involutions in $N \setminus (\Sigma \rtimes \Delta)$. Let $\iota \in N$ be an involution and let $\bar{\iota}$ be the induced involution in $PGL(2, \kappa)$. Denote by $P_x$ and $P_y$ the places lying under $\Omega_x$ and $\Omega_y$, respectively. From [7, Hauptsatz 8.27] there exists a unique involution in $PGL(2, \kappa)$ fixing $P_x$ and $P_y$, and it is induced by $\theta^{(\bar{q} - 1)/2}$. Thus, if $\iota \not\in \Gamma$ then $\iota$ switches $\Omega_x$ and $\Omega_y$. From Corollary 3.2 $\iota$ maps $x$ to $a(x + \alpha)$ and $y$ to $b(x + \beta)$ where $a, b \in \kappa$ and $L(\alpha) = L(\beta) = 0$. Since the order of $\iota$ is equal to 2, we have that $\alpha = \beta = 0$ and $\alpha = \beta \in \{-1, 1\}$. Hence, $\iota = \xi$ or $\iota = \theta^{(\bar{q} - 1)/2} \cdot \xi$, and so $\iota \in \Delta$. From [7, Hauptsatz 8.27], one of the following holds:

1. $\bar{N}$ is isomorphic either to $\text{A}_4$ or $\text{S}_4$ or $\text{A}_5$.
2. $\bar{N}$ is isomorphic to a dihedral group $D_d$ of order $2d$.

Suppose $\bar{N} \cong \text{A}_4$. If $\bar{q} \neq 3$, $\Delta$ is not contained in $\bar{N}$. If $\bar{q} = 3$ then $\bar{N}$ is not tame, a contradiction.

Suppose $\bar{N} \cong \text{S}_4$. In this case $\bar{q} = 3$, which is impossible as $\bar{N}$ is tame, or $\bar{q} = 5$, which is impossible as $\bar{N}$ contains more than the 5 involutions contained in $\bar{\Delta} \cong D_5$.

Suppose that $\bar{N} \cong \text{A}_5$. Then as before $\bar{q} = 3$ which is not possible.

Therefore, case (2) occurs. From Lemma 3.3 $d = \bar{q} - 1$ and the claim follows. \hfill \Box
In order to prove that \( \text{Aut}(X_{L,L}) = N \), several cases are distinguished according to the structure of the minimal normal subgroups of \( \text{Aut}(X_{L,L}) \). Recall that every finite group admits a minimal normal subgroup, which is either elementary abelian or a direct product of isomorphic simple groups.

**Lemma 3.6.** If \( \text{Aut}(X_{L,L}) \) has a minimal normal subgroup \( E_{dk} \) which is an elementary abelian \( d \)-group, then \( \text{Aut}(X_{L,L}) \) admits an elementary abelian minimal normal subgroup \( M \) which is a \( p \)-group.

**Proof.** Assume that \( d \neq p \). Since \( \Sigma \) normalizes \( E_{dk} \), from Lemma 3.2, \( |E_{dk} \times \Sigma| < 30(\sigma(X_{L,L}) - 1) \) or \( N_H(\Sigma) \cap E_{dk} = E_{dh} = \{1\} \) with \( 0 < h \leq k \).

- Assume that \( N_H(\Sigma) \cap E_{dk} = E_{dh} = \{1\} \) with \( 0 < h \leq k \). From Lemma 3.5, \( E_{dk} \leq \Delta \) up to conjugation, and hence \( d^h = 4 \) or \( h = 1 \). If \( d^h = 4 \), then \( \text{Aut}(\omega) = E_{dk} = \langle \xi \rangle \times \langle \theta \rangle \rangle \) from Lemma 2.4. By direct checking \( E_{dk} \) does not commute with \( \Sigma \), a contradiction. Hence \( E_{dk} = C_d \leq C_{q-1} \).

If \( d = 2 \) then \( \text{Aut}(X_{L,L}) = O(\text{Aut}(X_{L,L})) \times S_2 \) by Lemma 2.6. Thus \( O(\text{Aut}(X_{L,L})) \) contains a minimal normal subgroup of \( \text{Aut}(X_{L,L}) \), and we can assume \( d \) to be odd. Assume that \( d \neq p \) is odd. Since \( C_d \leq \Gamma \) and \( E_{dk} \) is abelian, we have that \( E_{dk} \) fixes \( P_{y=0} \) and \( P_{x=0} \), acts on \( \Omega_x \setminus \{P_{y=0}\} \) and \( \Omega_y \setminus \{P_{x=0}\} \).

- Assume that \( |E_{dk} \times \Sigma| < 30(\sigma(X_{L,L}) - 1) \). By direct computation \( d^k < 30 \). Since no subgroup of \( \Sigma \) commutes with \( E_{dk} \), we have that \( \Sigma \) is isomorphic to a subgroup of \( \text{GL}(k,d) \).

If \( d^k \neq 27 \) then \( GL(k,d) \) has no elementary abelian subgroup of odd square order. If \( d^k = 27 \) then \( d = p = 3 \), a contradiction.

**Remark 3.7.** We have shown in Lemma 2.6 that \( \text{Aut}(X_{L,L}) \) does not admit elementary abelian normal \( d \)-subgroups for \( d \neq p \) odd. If \( \text{Aut}(X_{L,L}) \) admits an elementary abelian minimal normal subgroup then it also admits a minimal normal \( p \)-subgroup.

**Proposition 3.8.** If \( \text{Aut}(X_{L,L}) \) admits an elementary abelian minimal normal subgroup \( M \), then \( \text{Aut}(X_{L,L}) = \Sigma \times \Delta \).

**Proof.** From Lemma 3.6 we can assume that \( M \leq \Sigma \). Let \( \Sigma \) be a Sylow \( p \)-subgroup of \( \text{Aut}(X_{L,L}) \). Then \( M \subseteq \Sigma \cap \Sigma \). For any \( \tau_{\alpha\beta} \in M \) and \( \sigma \in \text{Aut}(X_{L,L}) \), we have \( \sigma(\tau_{\alpha\beta}) = \tau_{\alpha'\beta'} \) for some \( \alpha', \beta' \). Therefore \( \sigma \) acts on the poles of \( x \) and \( y \), that is, \( \sigma \) acts on \( \Omega_y \) and on \( \Omega_x \). Suppose by contradiction that there exists \( \omega \) in \( \Sigma \setminus \Sigma \) fixing a place \( P \in \Omega_x \cup \Omega_y \). Then \( \text{Aut}(X_{L,L}) \) admits a Sylow \( p \)-subgroup \( \Sigma \) containing \( \omega \) and the stabilizer \( \Sigma_P \) of \( P \) in \( \Sigma \). Thus the order of \( \Sigma_P \) is strictly greater than the order of \( \Sigma \), a contradiction. This proves that \( \Sigma_P = \Sigma_P \) for all \( P \in \Omega_x \cup \Omega_y \), and hence \( \Sigma = \Sigma \). The claim follows from Lemma 3.6.

**Proposition 3.9.** \( \text{Aut}(X_{L,L}) \) admits an elementary abelian minimal normal subgroup.

**Proof.** Suppose by contradiction that \( \text{Aut}(X_{L,L}) \) admits no elementary abelian minimal normal subgroup. Thus, \( \text{Aut}(X_{L,L}) \) is odd-core free. In fact if \( O(\text{Aut}(X_{L,L})) \neq \{1\} \) then \( O(\text{Aut}(X_{L,L})) \) contains a minimal normal subgroup which is then elementary abelian by the Feit-Thompson theorem. From Lemma 2.3 one of the following cases occurs:

(i) \( M := \text{PSL}(2, d^k) \subseteq \text{Aut}(X_{L,L}) \leq \text{PGL}(2, d^k) \). In this case \( \Sigma/(\Sigma \cap M) \) is isomorphic to a subgroup of \( \text{PGL}(2, d^k) \). Since \( [\text{PGL}(2, d^k) : \text{PSL}(2, d^k)] = 2 \) and \( \text{PGL}(2, d^k) \) is cyclic of order \( k \), we have that \( \Sigma/(\Sigma \cap M) \) is cyclic. Then either \( \Sigma/(\Sigma \cap M) = \{1\} \) or \( \Sigma/(\Sigma \cap M) = C_{q^2} \).

When \( r \) is an odd prime, the Sylow \( r \)-subgroups of \( \text{PSL}(2, d^k) \) are cyclic unless \( r = d \). Since \( q > p \), this implies that \( d = p \) and either \( d^k = q^2 \) or \( d^k = q^2/p \). In both cases, arguing as in the proof of Proposition 3.8, we have that any element of \( \text{Aut}(X_{L,L}) \) normalizing \( \Sigma \cap M \) normalizes the whole.
group Σ. Therefore from [7] Hauptsatz 8.27 $\text{Aut}(\chi_{L_1, L_2})$ contains a cyclic group of order $q^2 - 1$ or $q^2/p - 1$ normalizing Σ, a contradiction to Lemma 3.5.

(ii) $M := \text{PSL}(3, d^k) \leq \text{Aut}(\chi_{L_1, L_2}) \leq \text{PGL}(3, d^k)$. We have $[\text{PGL}(3, d^k) : \text{PSL}(3, d^k)] \in \{1, 3\}$ and $\text{PGL}(3, d^k)/\text{PGL}(3, d^k)$ is cyclic of order $k$. Hence $\Sigma/(\Sigma \cap M)$ is cyclic. Then either $\Sigma/(\Sigma \cap M) = \{1\}$ or $\Sigma/(\Sigma \cap M) = C_p$. If $d = p$ then a contradiction is obtained since a Sylow $d$-subgroup of $\text{PSL}(3, d^k)$ is not abelian. If either $\gcd(3, d^k - 1) = 1$, or $\gcd(3, d^k - 1) = 3$ and $p \neq 3$, then a contradiction follows from Lemma 2.1. Suppose that $\gcd(3, d^k - 1) = 3$ and $p = 3$. In this case a contradiction is obtained because the Sylow 3-subgroup of $M$ is not abelian (see [7] Satz 7.2), and hence cannot be contained in Σ.

(iii) $M := \text{PSU}(3, d^k) \leq \text{Aut}(\chi_{L_1, L_2}) \leq \text{PGU}(3, d^k)$. We have $[\text{PGL}(3, d^k) : \text{PSL}(3, d^k)] \in \{1, 3\}$ and $\text{PGL}(3, d^k)/\text{PGL}(3, d^k)$ is cyclic of order $k$. Hence $\Sigma/(\Sigma \cap M)$ is cyclic. Then either $\Sigma/(\Sigma \cap M) = \{1\}$ or $\Sigma/(\Sigma \cap M) = C_p$. If $d = p$ then a contradiction is obtained since a Sylow $d$-subgroup of $\text{PSL}(3, d^k)$ is not abelian. If either $\gcd(3, d^k + 1) = 1$, or $\gcd(3, d^k + 1) = 3$ and $p \neq 3$, then a contradiction follows from Lemma 2.1. Suppose that $\gcd(3, d^k + 1) = 3$ and $p = 3$. In this case a contradiction is obtained because the Sylow 3-subgroup of $M$ is not abelian (see [6] Theorem A.10 Case (iii)), and hence cannot be contained in Σ.

(iv) $\text{Aut}(\chi_{L_1, L_2}) = A_7$. Since $|A_7| = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, we have $q = 3 = p$, which is impossible.

(v) $\text{Aut}(\chi_{L_1, L_2}) = M_{11}$. Since $|M_{11}| = 2^4 \cdot 3^2 \cdot 5 \cdot 11$, we have $q = 3 = p$, which is impossible.

From Propositions 3.8 and 3.9 Theorem 1.2 follows.

3.2. Proof of Theorem 1.2.

In this section, $L_1 \neq L_2$ and we refer to Σ and Γ as defined in Theorem 1.2.

Lemma 3.10. The normalizer $N$ of $\Sigma$ in $\text{Aut}(\chi_{L_1, L_2})$ is $N = \Sigma \rtimes \Gamma$.

Proof. From Corollary 3.2 $\tilde{N} = N/\Sigma$ is a tame subgroup of $\text{PGL}(2, \mathbb{K})$ containing a cyclic group $\tilde{\Gamma}$ which is isomorphic to Γ. Arguing as in the proof of Lemma 3.5, $N$ has no involution other than $\theta^{(q-1)/2}$, because by direct checking $\xi : (x, y) \mapsto (y, x)$ is not in $\text{Aut}(\chi_{L_1, L_2})$. From [7] Hauptsatz 8.27, one of the following holds:

1. $\tilde{N}$ is isomorphic either to $A_4$ or $S_4$ or $A_5$.
2. $\tilde{N}$ is isomorphic to a cyclic group $C_d$.

Arguing as in the proof of Lemma 3.5 Case (1) is not possible because $\tilde{N}$ is tame and it contains only one involution. Therefore, case (2) occurs. From Lemma 3.3 $d = \tilde{q} - 1$ and the claim follows.

The proofs of the following results are analogous to the ones of Lemma 3.9, Proposition 3.8, and Proposition 3.9, and are omitted.

Lemma 3.11. If $\text{Aut}(\chi_{L_1, L_2})$ has a minimal normal subgroup $E_{d^k}$ which is an elementary abelian $d$-group, then $\text{Aut}(\chi_{L_1, L_2})$ admits an elementary abelian minimal normal subgroup $M$ which is a $p$-group.

Proposition 3.12. If $\text{Aut}(\chi_{L_1, L_2})$ admits an elementary abelian minimal normal subgroup, then $\text{Aut}(\chi_{L_1, L_2}) = \Sigma \rtimes \Gamma$.

Proposition 3.13. $\text{Aut}(\chi_{L_1, L_2})$ admits an elementary abelian minimal normal subgroup.

From Propositions 3.12 and 3.13 Theorem 1.2 follows.
4. Curves with automorphism group containing $E_{q^2}$

We need the following result on curves admitting $E_{q^2}$ as an automorphism group.

**Proposition 4.1.** For a curve $X$ defined over $\mathbb{K}$, assume that one of the following holds.

(A) $X$ has genus $g \leq (q - 1)^2$ and the automorphism group $\text{Aut}(X)$ has a subgroup $H = E_{q^2} \times (C_2 \times C_2)$.

(B) $X$ has genus $g = (q - 1)^2$ and the automorphism group $\text{Aut}(X)$ has a subgroup $H = E_{q^2}$.

Let $\{M_i\}_i$ be the set of subgroups of $E_{q^2}$ of order $q$. Then the following hold.

1. $X$ is an ordinary curve of genus $(q - 1)^2$;
2. Up to relabeling the indeces, the cover $X \mid X/M_i$ is unramified for each $i \neq 1, 2$;
3. $E_{q^2}$ has only two short orbits $\Omega_1$ and $\Omega_2$ on $X$, each of size $q$. The places of $\Omega_1$ share the same stabilizer $M_i$ for $i \in \{1, 2\}$, and $M_1 \neq M_2$. Moreover, $X/M_1$ and $X/M_2$ are rational.

**Proof.** Let $g$ and $\gamma$, $\bar{g}$ and $\bar{\gamma}$, be the genus and $p$-rank of $X$, $\bar{X} := X/E_{q^2}$ respectively. Also, denote by $k \in \mathbb{N}$ the number of short orbits of $E_{q^2}$ on $X$, by $\Omega_i (1 \leq i \leq k)$ the $i$-th short orbit of $E_{q^2}$, by $\ell_i \in \{p, p^2, \ldots, q^2/p\}$ the length of $\Omega_i$, and by $M_i$ the stabilizer of a given place $P_i \in \Omega_i$ in $E_{q^2}$, of size $q^2/\ell_i$. Note that $M_i$ coincides with the stabilizer in $E_{q^2}$ of any place in $\Omega_i$, because $E_{q^2}$ acts on the fixed places of its normal subgroup $M_i$.

(A) Case $g \leq (q - 1)^2$ and $H := E_{q^2} \times (C_2 \times C_2) \leq \text{Aut}(X)$.

If $\gamma = 0$, then every element of $E_{q^2}$ fixes exactly one place of $X$ from [6] Lemma 11.129]. Since $E_{q^2}$ is abelian all elements of $E_{q^2}$ have the same fixed place $P$, which is fixed also by $H$. Thus, $H/E_{q^2}$ is cyclic by [6] Theorem 11.49, a contradiction to $H/E_{q^2} \cong C_2 \times C_2$. If $\gamma = 1$ then $E_{q^2}$ is cyclic by Theorem 2.1 (IV), a contradiction. Hence $\gamma \geq 2$. The Deuring-Shafarevich formula 8 applied to $E_{q^2}$ yields

\[
\gamma - 1 = q^2(\bar{\gamma} - 1) + \sum_{i=1}^{k} (q^2 - \ell_i).
\]

If $k = 0$ then $\bar{\gamma} = (\gamma - 1)/q^2 + 1 > 1$, and hence $q^2 \leq \gamma - 1 \leq g - 1 \leq q^2 - 2q$, a contradiction. Therefore $\bar{\gamma} \leq 1$ and $k \geq 1$.

Assume that $\bar{\gamma} = 1$. The Riemann-Hurwitz formula together with $\bar{g} \geq \bar{\gamma}$ yields $\bar{g} = 1$. If $k \geq 2$ then $\gamma - 1 \geq 2(q^2 - q^2/p)$ by equation (10), a contradiction to $\gamma \leq g$. This yields $k = 1$. Since $C_2 \times C_2$ normalizes $E_{q^2}$ which has a unique short orbit $\Omega_1$, the induced group $C_2 \times C_2$ fixes one place of the elliptic curve $\bar{X}$. From [6] Theorem 11.94 (ii) and its proof, $C_2 \times C_2$ is cyclic, a contradiction.

Therefore $\bar{\gamma} = 0$. If $k \geq 3$ then equation (10) together with $g \geq \gamma$ yields a contradiction. If $k = 1$ then equation (11) reads $2 \geq \gamma = 1 - \ell_1$, a contradiction. Thus $k = 2$ and equation (11) reads

\[
\gamma = q^2 + 1 - (\ell_1 + \ell_2).
\]

We prove that $\bar{g} = 0$. From the Riemann-Hurwitz formula applied to $X \rightarrow \bar{X}$ we have that

\[
q^2 \bar{g} \leq \ell_1 + \ell_2 - 2q \leq 2q^2/p - 2q,
\]

which implies $\bar{g} = 0$. Since $C_2 \times C_2$ normalizes $E_{q^2}$, the induced group $\bar{C}_2 \times \bar{C}_2$ is a subgroup of $\text{PGL}(2, \mathbb{K})$ acting on the two places $\bar{P}_1$ and $\bar{P}_2$ lying under $\Omega_1$ and $\Omega_2$. From [7] Hauptsatz 8.27, $\bar{C}_2 \times \bar{C}_2$ switches $\bar{P}_1$ and $\bar{P}_2$ and hence $\ell_1 = \ell_2 = \ell$. Let $P \in \Omega_1$. From [6] Lemma 11.75 (v)] either $(E_{q^2})^{(2)}$ is trivial, or $(E_{q^2})^{(2)} = E_{q^2}$, or $1 < \left|\left(E_{q^2}\right)^{(2)}_P\right| = \cdots = \left|\left(E_{q^2}\right)^{(2)}_P\right| < q^2$. By direct checking with the Riemann-Hurwitz formula applied to $X \rightarrow \bar{X}$, the second and the third case are not possible; hence $(E_{q^2})^{(2)}_P$ is trivial for all $P$, which implies $\ell = q$. Now the Deuring-Shafarevich formula yields $\gamma = (q - 1)^2 \geq g$; hence, $\gamma = g = (q - 1)^2$ and the claim (1) follows. Since $M_i$, $i = 1, 2$, is the stabilizer in $E_{q^2}$ of any place in $\Omega_i$, we have that any other subgroup $M_j$ of order $q$ of $E_{q^2}$,
Theorem 4.2. \[13\), Proposition 2.2 and Corollary 2.3\). \(\ell\) an elementary abelian subgroup \(E\). Let \(Y\) be a curve of genus \(q - 1\) defined over \(K\) whose automorphism group \(\text{Aut}(Y)\) contains an elementary abelian subgroup \(E_q\) of order \(q\). Then one of the following holds.

\[q = 2(q^2 - 2q) \geq 2q(q_0 - 1) + 2q(q - 1).

Hence \(q_i = 0\) for \(i = 1, 2\) and equality holds in (11). This proves that \(M_i\) has no fixed place out of \(\Omega_i\), and so \(M_1 \neq M_2\).

(B) Case \(g = (q - 1)^2\) and \(H := E_{q^2} \leq \text{Aut}(\mathcal{X})\).

Suppose \(c = 0\). Then by [6, Lemma 11.129) every element of \(H\) fixes exactly one place, which is the same place \(P\) for all of them. The Riemann-Hurwitz formula \([6]\) applied to the cover \(\mathcal{X} \to \mathcal{X}/H\) yields \(\bar{g} = 0\), \(H_p^{(2)} \neq \{1\}\), and

\[\sum_{i=2}^{\infty} (|H_p^{(i)}| - 1) = 2(q - 1)^2.

From [6, Th. 11.78], \(\mathcal{X}/H_p^{(2)}\) is rational; hence, the Riemann-Hurwitz formula applied to \(\mathcal{X} \to \mathcal{X}/H_p^{(2)}\) yields

\[\sum_{i=2}^{\infty} (|H_p^{(i)}| - 1) = 2q^2 - 4q + 2|H_p^{(2)}|.

Equations (12) and (13) provide a contradiction to \(H_p^{(2)} \neq \{1\}\). Suppose \(c = 1\). Then \(H\) is cyclic by Theorem [2, IV], a contradiction.

Therefore \(c = 2\). As in Case (A), \(\bar{c} \leq 1\) and \(k \geq 1\); also, if \(\bar{c} = 1\), then \(k = 1\).

Suppose \(\bar{c} = 1\) and \(k = 1\). From \(\bar{g} \geq \gamma\) and the Deuring-Shafarevich formula applied to \(\mathcal{X} \to \bar{\mathcal{X}}\) we have \(\bar{g} = 1\) and \(\ell_1 \geq 2q\); hence, \(pq\) divides \(\ell_1\). The Riemann-Hurwitz formula applied to \(\mathcal{X} \to \bar{\mathcal{X}}\) reads

\[2(q - 1)^2 = q^2(2 \cdot 0 - 2) + \ell_1 \sum_{i=0}^{\bar{c}} (|H_p^{(i)}| - 1)

for any \(P\) in \(\Omega_1\). This implies that \(\ell_1\) divides \(q\), a contradiction to \(pq \mid \ell_1\).

Therefore \(\bar{c} = 0\). Arguing as in the proof of Proposition [4, we have \(k = 2\), \(\gamma = q^2 + 1 - (\ell_1 + \ell_2)\), and \(\bar{g} = 0\). From the Riemann-Hurwitz formula applied to \(\mathcal{X} \to \bar{\mathcal{X}}\),

\[2(\ell_1 + \ell_2) - 4q = \ell_1c_1 + \ell_2c_2 \geq 0,

where \(c_j := \sum_{i=2}^{\infty} (|H_p^{(i)}| - 1) \geq 0\) for \(j = 1, 2\). From Equation (14), the integers \(\ell_1\) and \(\ell_2\) cannot be multiple of \(pq\) at the same time. Hence \(\ell_1 \leq q\) or \(\ell_2 \leq q\); say \(\ell_1 \leq q\). We have \(|H_p^{(2)}| < q^2/\ell_1\) and \(|H_p^{(2)}| < q^2/\ell_2\); otherwise, Equation (14) would imply \(2(\ell_1 + \ell_2) - 4q \geq q^2 - \ell_1\) or \(2(\ell_1 + \ell_2) - 4q \geq q^2 - \ell_2\), which is impossible because \(\ell_1 \leq q\) and \(\ell_2 \leq q^2/p\). Therefore, for \(j = 1, 2\), \(c_j\) is a multiple of \(p\) (possibly zero) from [6, Lemma 11.75 (v)]. Suppose \(\ell_2 \geq pq\). As \(c_2 \neq 2\), Equation (14) implies that \(\ell_2\) divides \([4q + (c_1 - 2)\ell_1]\); hence, \(p\) divides \(2(2q/\ell_1 - 1)]\), a contradiction. Therefore, \(\ell_2 \leq q\). Thus, from Equation (14), \(\ell_1 = \ell_2 = q\). The rest of the claim follows as in Case (A).

\[\square\]

Theorem 4.2 provides a characterization which generalizes a result by van der Geer and van der Vlugt; see [13, Proposition 2.2 and Corollary 2.3].
The proof is divided in several steps.

Proof. We show that $\mathcal{Y}_L,a$ has genus $q − 1$ and Aut($\mathcal{Y}_L,a$) contains a subgroup $\text{Dih}(E_q) \times \langle \mu \rangle$. Let $\overline{\mathcal{Y}}_0$ and $\overline{\mathcal{Y}}_\infty$ be the zeros and pole of $x$ in $\mathbb{K}(x)$, respectively. Then $\mathbb{K}(\mathcal{Y})|\mathbb{K}(x)$ is a generalized Artin-Schreier extension [11, Proposition 3.7.10]) which ramifies exactly over the simple poles $\overline{\mathcal{Y}}_0$ and $\overline{\mathcal{Y}}_\infty$.

Let $\mathcal{Y} \rightarrow \mathbb{C}$ be a curve of genus $q$. Thus, the Deuring-Shafarevich formula applied to $\mathcal{Y} \rightarrow \mathbb{C}$ shows that $\mathcal{Y}$ is birationally equivalent over $\mathbb{K}$ to the curve $Z_{L,b}$ with affine equation

\[ L(y) = ax^3 + bx, \]

for some $a \in \mathbb{K}$ and $L(T) \in \mathbb{K}[T]$ a separable $p$-linearized polynomial of degree $q$. For the curve $Z_{L,b}$ the following properties hold:

(i) $Z_{L,b}$ has zero $p$-rank;

(ii) $\text{Aut}(Z_{L,b})$ contains a generalized dihedral subgroup $\text{Dih}(E_q) = E_q \rtimes \langle \nu \rangle$.

We show that $\mathcal{Y}_L,a$ is ordinary and hyperelliptic with hyperelliptic involution $\mu$.

(iii) The full automorphism group $\text{Aut}(\mathcal{Y}_L)$ of $\mathcal{Y}_L,a$ has order $4q$ and is a direct product $\text{Dih}(E_q) \times \langle \mu \rangle$.

We show that $\mathcal{Y}$ is birationally equivalent over $\mathbb{K}$ to the curve $Z_{L,b}$ with affine equation

\[ L(y) = ax^3 + bx, \]

for some $a \in \mathbb{K}$ and $L(T) \in \mathbb{K}[T]$ a separable $p$-linearized polynomial of degree $q$. For the curve $Z_{L,b}$ the following properties hold:

(i) $Z_{L,b}$ has zero $p$-rank;

(ii) $\text{Aut}(Z_{L,b})$ contains a generalized dihedral subgroup $\text{Dih}(E_q) = E_q \rtimes \langle \nu \rangle$ of order $4q$ of $\mathcal{Y}_L,a$.

We show that $\mathcal{Y}_L,a$ is birationally equivalent over $\mathbb{K}$ to the curve $Z_{L,b}$ with affine equation

\[ L(y) = ax^3 + bx, \]

for some $a \in \mathbb{K}$ and $L(T) \in \mathbb{K}[T]$ a separable $p$-linearized polynomial of degree $q$. For the curve $Z_{L,b}$ the following properties hold:

(i) $Z_{L,b}$ has zero $p$-rank;

(ii) $\text{Aut}(Z_{L,b})$ contains a generalized dihedral subgroup $\text{Dih}(E_q) = E_q \rtimes \langle \nu \rangle$ of order $4q$ of $\mathcal{Y}_L,a$.

We show that $\mathcal{Y}_L,a$ has genus $q − 1$ and Aut($\mathcal{Y}_L,a$) contains a subgroup $\text{Dih}(E_q) \times \langle \mu \rangle$.

Let $P_0$ and $P_\infty$ be the zero and pole of $x$ in $\mathbb{K}(x)$, respectively. Then $\mathbb{K}(\mathcal{Y})|\mathbb{K}(x)$ is a generalized Artin-Schreier extension [11, Proposition 3.7.10]) which ramifies exactly over the simple poles $P_0$ and $P_\infty$ of $ax + 1$. Hence, $g(\mathcal{Y}_L,a) = q − 1$. The maps

\[ E_q = \{ \tau_\alpha : (x,y) \mapsto (x, y + \alpha) \mid L(\alpha) = 0 \}, \quad \nu : (x,y) \mapsto (1/ax,y), \quad \mu : (x,y) \mapsto (1/ax,y), \]

generate an automorphism group $\text{Dih}(E_q) \times \langle \mu \rangle = (E_q \rtimes \langle \nu \rangle) \times \langle \mu \rangle$ of order $4q$ of $\mathcal{Y}_L,a$.

We show that $\mathcal{Y}_L,a$ is ordinary and hyperelliptic with hyperelliptic involution $\mu$, and that the Weierstrass places of $\mathcal{Y}_L,a$ are the 2q fixed places of $\mu$.

Let $P_0$ and $P_\infty$ the places of $\mathcal{Y}$ lying over $P_0$ and $P_\infty$. The group $E_q$ and the involution $\nu$ fix $P_0$ and $P_\infty$, while the involution $\mu$ interchanges $P_0$ and $P_\infty$. Let $\overline{\mathcal{Y}} = \mathcal{Y}/E_q$ and $\overline{\mathcal{Y}}' = \mathcal{Y}/\langle \mu \rangle$. The Riemann-Hurwitz formula applied to the cover $\mathcal{Y} \rightarrow \overline{\mathcal{Y}}$ shows that $\overline{\mathcal{Y}}$ is rational and $P_0, P_\infty$ are the unique fixed places of any element of $E_q$. Thus, the Deuring-Shafarevich formula applied to $\mathcal{Y} \rightarrow \overline{\mathcal{Y}}$ shows that $\mathcal{Y}$ has $p$-rank $q − 1$; hence, $\mathcal{Y}$ is ordinary. Let $P_1$ and $P_2$ be the distinct zeros of $ax^2 + 1$ in $\mathbb{K}(x)$, and $P_1^1, \ldots, P_1^p$ and $P_2^1, \ldots, P_2^p$ be the distinct places of $\mathcal{Y}$ lying over $P_1$ and $P_2$. By direct checking, $\mu$ fixes $P_1^1, \ldots, P_1^p, P_2^1, \ldots, P_2^p$. Then the Riemann-Hurwitz formula applied to $\mathcal{Y} \rightarrow \overline{\mathcal{Y}}'$ shows that $\mu$ has no other fixed places and $\overline{\mathcal{Y}}'$ is rational; hence, $\mathcal{Y}$ is hyperelliptic with hyperelliptic involution $\mu$. Since $2q > 4$, the 2q fixed places of $\mu$ are Weierstrass places of $\mathcal{Y}$ from [11, Theorem 11.112]. Moreover, $\mathcal{Y}$ has exactly $2q$ Weierstrass places from [6, Theorem 7.103].

We show that $\mathcal{Y}_L,a$ has genus $q − 1$ and admits an automorphism group $\text{Dih}(E_q)$.

The curve $Z_{L,b}$ admits the automorphism group $\text{Dih}(E_q) = E_q \rtimes \langle \nu \rangle$, where

\[ E_q = \{ \tau_\alpha : (x,y) \mapsto (x, y + \alpha) \mid M(\alpha) = 0 \}, \quad \nu : (x,y) \mapsto (1/ax,y). \]

From [6] Lemma 12.1 (i), $Z_{L,b}$ has zero $p$-rank.

Let $\mathcal{Y}$ be a curve of genus $q − 1$ admitting an automorphism group $E_q$ with $p$ fixed places. We show that, if $\lambda = 1$, then $p \neq 3$ and $\mathcal{Y}$ is birationally equivalent to some $Z_{M,b}$.

Let $\overline{\mathcal{Y}} = \mathcal{Y}/E_q$. The Riemann-Hurwitz formula applied to $\mathcal{Y} \rightarrow \overline{\mathcal{Y}}$ shows that $\overline{\mathcal{Y}}$ has genus zero and

\[ 2(q − 1) = \sum_{i=2}^{\infty}((E_q)^{(i)}|p − 1) + \sum_{i} t_idp, \]
where $\ell_i$ are the lengths of the short orbits $\Omega_i$ of $E_q$ other than $\{P\}$ and $P_i$ is a place of $\Omega_i$; hence, the second summation in Equation (18) is multiple of $p$. From [6] Lemma 11.75 (v), the first summation in (18) is the sum of a multiple of $p$ and $j(q-1)$, where $j$ is the largest integer such that $(E_q)^{(j+1)} = E_q$. Thus $j = 2$, $E_q = \ldots = (E_q)^{(3)}_{P}, (E_q)^{(4)}_{P} = \{1\}$, and $\{P\}$ is the unique short orbit of $E_q$. Let $x \in \mathbb{K}(\mathcal{Y})$ with $\mathbb{K}(\mathcal{Y}) = \mathbb{K}(x)$ and $P$ be the place of $\mathcal{Y}$ lying under $P$. Up to conjugation in $\text{Aut}(\mathcal{Y}) \cong \text{PGL}(2, \mathbb{K})$, $\bar{P}$ is the simple pole of $x$. Since $\mathbb{K}(\mathcal{Y})|\mathbb{K}(x)$ is a generalized Artin-Schreier extension ([11] Proposition 3.7.10), $\mathbb{K}(\mathcal{Y})$ is defined as $\mathbb{K}(x,y)$ by $M(y) = h(x)$, where $M(T) \in \mathbb{K}[T]$ is a separable $p$-linearized polynomial of degree $q$ and $h(x) \in \mathbb{K}(x)$. Since $P$ is the unique ramified place in $\mathbb{K}(x,y)|\mathbb{K}(x)$, Proposition 3.7.10 in [11] implies that $h(x)$ is a polynomial function in $\mathbb{K}[x]$ and, in order for the genus of $\mathcal{Y}$ to be $q - 1$, the valuation of $x$ at $P$ is $-3$ and coprime to $p$. Hence, $h(T) \in \mathbb{K}[T]$ has degree $3$ and $p \neq 3$. Up to a linear transformation in $x$, we can assume that $h(x)$ has the form $x^3 + bx + c$; up to a translation in $y$, we can then assume that $c = 0$.

- Let $\mathcal{Y}$ be a curve of genus $q - 1$ admitting an automorphism group $E_q$ with $\lambda$ fixed places. We show that, if $\lambda \neq 1$, then $\mathcal{Y}$ is birationally equivalent to some $\mathcal{Y}_{L,a}$.

  Let $\mathcal{Y} = \mathcal{Y}/E_q$ with genus $\bar{g}$. From the Riemann-Hurwitz formula applied to $\mathcal{Y} \to \mathcal{Y}$,

$$2q - 4 = q(2\bar{g} - 2) + 2\lambda(q - 1) + \sum_{i=1}^{\lambda} \sum_{j=2}^{\infty} |(E_q)^{(j)}_{Q_i}| - 1 + \sum_1^{\infty} \ell_i d_{P_i},$$

where $Q_1, \ldots, Q_\lambda$ are the fixed places of $E_q$, $\ell_i$ are the lengths of the short orbits of $E_q$ other than $\{Q_i\}$, and $P_i$ is a place of the $i$-th short orbit. Note that $\ell_i$ is a multiple of $p$. If $\lambda = 0$, then Equation (19) yields a contradiction modulo $p$. Then $\lambda \geq 2$. Hence, from Equation (19), $\bar{g} = 0$, $\lambda = 2$, and $E_q$ has no short orbits other than the two fixed places $P$ and $Q$. Let $x \in \mathbb{K}(\mathcal{Y})$ with $\mathbb{K}(\mathcal{Y})|\mathbb{K}(x)$ is a generalized Artin-Schreier extension ([11] Proposition 3.7.10), $\mathbb{K}(\mathcal{Y})$ is defined as $\mathbb{K}(x,y)$ by $L(y) = h(x)$, for some separable $p$-linearized polynomial $L(T) \in \mathbb{K}[T]$ of degree $q$. Also, from [11] Proposition 3.7.10, $P$ and $Q$ are the unique poles of $h(x)$, and they are simple poles. Up to conjugation in $\text{Aut}(\mathcal{Y}) \cong \text{PGL}(2, \mathbb{K})$, $\bar{P}$ and $\bar{Q}$ are the zero and the pole of $x$. Therefore, $h(x) = (x - r)(x - s)/x$ for some $r, s \in \mathbb{K}$. Up to formal replacement of $x$ and $y$ with $rsx$ and $y + \delta$, where $\delta \in \mathbb{K}$ satisfies $L(\delta) = -r - s$, the equation $L(y) = h(x)$ is the equation defining the curve $\mathcal{Y}_{L,r,s}$.

- Finally, we show that $\text{Aut}(\mathcal{Y}_{L,a})$ is the group $\text{Di}h(E_q) \times \langle \mu \rangle = (E_q \times \langle \nu \rangle) \times \langle \mu \rangle$ described in (17).

  Let $\mathcal{Y}' = \mathcal{Y}/\mu$. Then $\text{Aut}(\mathcal{Y}')$ contains the group $G' \cong \text{Aut}(\mathcal{Y})/\langle \mu \rangle$ induced by $\text{Aut}(\mathcal{Y})$, and in particular the subgroup $E_q' \times \langle \nu' \rangle \cong E_q \times \langle \nu \rangle$ induced by $E_q \times \langle \nu \rangle$. The group $E_q'$ is a Sylow $p$-subgroup of $G'$, because $E_q$ is a Sylow $p$-subgroup of $\text{Aut}(\mathcal{Y})$ from Theorem 2.1 (II). From [6] Theorem 11.98 and [7] Hauptsatz 8.27, either $G' \cong \text{PSL}(2,q)$, or $G' \cong \text{PGL}(2,q)$, or $G' = E_q \times C_m$, where $C_m$ is cyclic of order $m$ with $m \mid (q - 1)$.

  Assume that $G'$ contains a subgroup $E_q' \times C_m$ with $m \mid (q - 1)$. Up to conjugation, $E_q'$ is the group induced by $E_q$ as in (17). Let $C$ be a tame subgroup of $\text{Aut}(\mathcal{Y})$ inducing $C_m$. Since $C$ normalizes $E_q$, $C$ acts on the two places of $\mathcal{Y}$ fixed by $E_q$ and acts on the other orbits of $E_q$; since $C$ commutes with $\mu$, $C$ acts on the fixed places of $\mu$, which form two orbits of $E_q$. Thus, the group $\bar{C}$ is $C$-induced by $C$ on the rational curve $\mathcal{Y} = \mathcal{Y}/E_q$ acts on two couples of places. From [7] Satz 8.5, $\bar{C}$ has two fixed places and no other short orbits on $\mathcal{Y}$; hence, $C$ has order 2. This implies $m = 2$. For $q - 1 > 2$ the Lemma is then proved, because both $\text{PGL}(2,q)$ and $\text{PSL}(2,q)$ contain subgroups $E_q \times C_{q-1}$ of order $q(q - 1)$; see [7] Hauptsatz 8.27 and [12].

  Assume $q = 3$. The case $G' \cong \text{PSL}(2,3)$ is not possible, since $\text{PSL}(2,3)$ contains no subgroup $\text{Di}h(E_q)$. Suppose $G' \cong \text{PGL}(2,3)$. Let $\rho'$ be an element of $G'$ of $q$ order 4, and $\rho \in G$ an element of $q$ order 4 inducing $\rho'$. From [7] Sätze 8.2 and 8.4 and [12], $\rho'$ does not fix the place $P'$ of $\mathcal{Y}$ lying under the fixed places $P, Q$ of $E_q$. Hence, $P$ and $Q$ are in a long orbit of $\rho$. Therefore, $\rho'$ has a short orbit of length 2 on $\mathcal{Y}$. This is impossible, since from [7] Satz 8.5 (see also [12]) $\rho'$ has two
fixed places and no other short orbits on $\mathcal{Y}$. We conclude that $G' = E_{q}^{x} \times C_{m}^{2}$, and $m = 0$ follows as above. The Lemma is thus proved.

\[\square\]

**Proposition 4.3.** For a curve $X$ defined over $\mathbb{K}$, assume that one of the following hold.

(A) $X$ has genus $g \leq (q - 1)^{2}$ and $\text{Aut}(X)$ contains a subgroup $H = E_{q^{2}} \times (C_{2} \times C_{2})$;

(B) $X$ has genus $g = (q - 1)^{2}$ and $\text{Aut}(X)$ contains a subgroup $H = E_{q^{2}}$.

Then $E_{q^{2}}$ has a subgroup $T$ of order $q$ such that the quotient curve $X/T$ is birationally equivalent over $\mathbb{K}$ to the curve $\mathcal{Y}_{L,a}$ in [11], for some $a \in \mathbb{K}^{*}$ and $L(T) \in \mathbb{K}[T]$ a separable $p$-linearized polynomial of degree $q$.

**Proof.** From Proposition (4.1), $X$ is ordinary of genus $(q - 1)^{2}$ and $E_{q^{2}}$ admits a subgroup $T$ of order $q$ such that the cover $X \rightarrow X/T$ is unramified. From the Riemann-Hurwitz formula and the Deuring-Shafarevich formula applied to $X \rightarrow X/T$, the curve $X/T$ is ordinary of genus $q - 1$. Since $T$ is normal in $E_{q^{2}}$, $\text{Aut}(X/T)$ contains a subgroup $E_{q^{2}}/T \cong E_{q}$. From Theorem 4.2, $X/T$ is birationally equivalent over $\mathbb{K}$ to $\mathcal{Y}_{L,a}$ for some $a$ and $L$. \[\square\]

**Proposition 4.4.** Let $X$ be a curve admitting an automorphism group $E_{q^{2}}$ such that, for some $E_{q} \leq E_{q^{2}}$ the quotient curve $X/E_{q}$ has affine equation

$$L(y) = ax + \frac{1}{x},$$

for some $a \in \mathbb{K}^{*}$ and $L(T) \in \mathbb{K}[T]$ a separable $p$-linearized polynomial of degree $q$. Then the following hold:

(1) $\mathbb{K}(X/E_{q^{2}}) = \mathbb{K}(x)$.

(2) If $X$ is an ordinary curve with genus $(q - 1)^{2}$, then $E_{q^{2}}$ contains a subgroup $M$ of order $q$ different from $E_{q}$ such that the quotient curve $X/M$ has affine equation

$$\tilde{L}(z) = b + \frac{1}{x},$$

for some $z \in \mathbb{K}(X), b \in \mathbb{K}$, and $\tilde{L}(T) \in \mathbb{K}[T]$ a separable $p$-linearized polynomial of degree $q$.

**Proof.** Since $[\mathbb{K}(X) : \mathbb{K}(x)] = q^{2} = [\mathbb{K}(X) : \mathbb{K}(X/E_{q^{2}})]$, it is enough to prove that $\tau(x) = x$ for any $\tau \in E_{q^{2}} \setminus E_{q}$. Since $\tau$ and $E_{q}$ commute, $\tau$ induces an automorphism $\tau'$ of $\mathbb{K}(x,y)$. If $\tau'$ is trivial then $\tau(x) = x$ and (1) follows. Otherwise, $\tau'$ has order $p$. Clearly $E_{q^{2}}/E_{q} \cong E_{q}$, where $E_{q}$ is an elementary abelian subgroup of $\text{Aut}(\mathcal{Y}_{L})$ of order $q$. Arguing as in the proof of Theorem [11], $\text{Aut}(\mathcal{Y}_{L})$ has a unique elementary abelian group $F$ of order $q$, namely

$$F = \{\tau_{\alpha} : (x, y) \mapsto (x, y + \alpha) \mid L(\alpha) = 0\},$$

and hence $F = \bar{E}_{q}$. Hence $\tau(x) = x$ for every $\tau \in E_{q^{2}} \setminus E_{q}$ and (1) follows. From (1), $\mathbb{K}(X/E_{q^{2}}) = \mathbb{K}(x)$, that is, $X/E_{q^{2}} = \mathbb{P}^{1}(\mathbb{K})$. The curve $\mathcal{Y}_{L}$ is the quotient curve $X_{(L,L)}/H$, where

$$H = \{\tau_{\alpha,\alpha} : (x, y) \mapsto (x + \alpha, y + \alpha) \mid L(\alpha) = 0\}.$$ 

In fact it is sufficient to consider the functions $\eta, \theta \in \mathbb{K}(X_{(L,L)})$ with $\eta = L(y)$ and $\theta = x + y$. By direct checking $L(\theta) = \eta + 1/\eta$ and $\mathbb{K}(X_{(L,L)}/H) = \mathbb{K}(\eta, \theta)$. Since $X_{(L,L)}$ is an ordinary curve of genus $(q - 1)^{2}$ and the cover $X_{(L,L)} \rightarrow X_{(L,L)}/H$ is unramified, from the Deuring-Shafarevich formula and the Riemann-Hurwitz formula, we have that $\mathcal{Y}_{L}$ is an ordinary curve of genus $q' = q - 1$. The Deuring-Shafarevich formula applied to $E_{q}$ shows that the extension $\mathbb{K}(X)/\mathbb{K}(\mathcal{Y}_{L})$ is unramified. Let $P_{0}$ and $P_{\infty}$ be respectively the zero and pole of $x$ in $\mathbb{K}(x)$. Then $P_{0}$ and $P_{\infty}$ are totally ramified in the extension $\mathbb{K}(\mathcal{Y}_{L})|\mathbb{K}(x)$ and no other place of $\mathbb{P}^{1}(\mathbb{K})$ ramifies; see [11] Proposition 3.7.10. Therefore, both $P_{0}$ and $P_{\infty}$ split completely in $X$. Let $M$ be the stabilizer in $E_{q^{2}}$ of a place $P_{\infty}$ of $X$ lying over $P_{\infty}$. We show that $P_{\infty}$ is unramified in the extension $\mathbb{K}(X/M)|\mathbb{K}(x)$. Note that $|M| = q$, since $P_{\infty}$ splits in $q$ distinct places in $X$. Furthermore, since $E_{q^{2}}$ is
4.1. Proof of Theorems 1.3 and 1.4.

From the Deuring-Shafarevich formula applied to the extension $K(x) / K$, we have that $K(x)$ has only one place that ramifies in $K(X/M) / K(x)$, and this place must be $P_0$.

We prove that the quotient curve $X/M$ has affine equation

$$\hat{L}(z) = b + \frac{1}{x},$$

for some $z \in K(x)$, $b \in K$, and $\hat{L}(T) \in K[T]$ a separable $p$-linearized polynomial of degree $q$. Since $K(X/M) / K(x)$ is a generalized Artin-Schreier extension ([11, Proposition 3.7.10]), we have that $K(X/M) = K(x, y)$ where $\hat{L}(y) = f(x)/g(x)$ for some separable $p$-linearized polynomial $\hat{L}(T) \in K[T]$ of degree $q$ and $f(x)/g(x) \in K(x)$. Recall that $P_0$ is the unique pole of $f(x)/g(x)$, and it is a simple pole.

- Suppose that $\deg(f) > \deg(g)$. Then $f(x)/g(x)$ has a pole at $P_0$, a contradiction.
- Suppose that $\deg(f) = \deg(g) > 0$. Let $g(x) = x \cdot r(x)^p$ with $r(x) \in K[x]$, then $f(x) = (x + \alpha)s(x)^p$ with $\alpha \in K$ and $s(x) \in K[x]$. If $r(x)$ has a zero $\beta$ then by [11, Proposition 3.7.10] it is easily checked that $f(x)/g(x)$ has a corresponding pole of multiplicity at least $p-1$, a contradiction. Therefore, $g(x) = \beta x$ and $f(x) = x + \alpha, \alpha, \beta \in K$. Applying a linear transformation to $x$, the claim follows.
- Suppose that $\deg(f) < \deg(g)$ and $\deg(g) > 0$. Then, arguing as in the previous case, $f(x) = \alpha$ and $g(x) = \beta x$ with $\alpha, \beta \in K$. Applying a linear transformation to $x$, the claim follows.
- Suppose that $\deg(g) = 0$. This is impossible since $P_0$ is a pole of $f(x)/g(x)$.

\[ \square \]

4.1. Proof of Theorems 1.3 and 1.4.

We keep our notation introduced in the previous sections. From Proposition 4.3, $E_{q^2}$ contains a subgroup $T$ of order $q$ such that the quotient curve $X/T$ is the curve $Y_{L, a}$ with affine equation

$$L(y) = ax + \frac{1}{x},$$

for some $a \in K^*$ and $L(T) \in K[T]$ a separable $p$-linearized polynomial of degree $q$. Let $K(x, y)$ be the function field $K(X/T)$. From Proposition 4.1, the $p$-rank of $X$ is $\gamma = q = (q-1)^2$. Thus by Proposition 4.4 $K(X)$ has a subfield $K(x, z)$ defined by

$$\hat{L}_1(z) = b + \frac{1}{x},$$

for some $z \in K(X)$, $b \in K$, and $\hat{L}_1(T) \in K[T]$ a separable $p$-linearized polynomial of degree $q$. Hence, the compositum $K(x, y, z)$ of $K(x, y)$ and $K(x, z)$ is a subfield of $K(X)$ such that

$$L(y) = ax + \frac{1}{x},$$

Therefore, $K(x, y, z) = K(y, z)$ with

$$\{L(y) = ax + \frac{1}{x},
\hat{L}_1(z) = b + \frac{1}{x}\}$$

Therefore, $K(x, y, z) = K(y, z)$ with

$$\{L_1(z) = b + \frac{1}{x}\}$$

From Proposition 4.3, $K(x, z) = K(X)^M$ and $K(x, y) = K(X)^T$, where $M \neq T$ is an elementary abelian $p$-subgroup of $E_{q^2}$ of order $q$. Thus,

$$Gal(K(X) / K(y, z)) = Gal(K(X) / K(X/M)) \cap Gal(K(X) / K(X/T)) = M \cap T.$$
Since the cover $\mathcal{X} \to \mathcal{X}/T$ is unramified, we have $M \cap T = \{1\}$ and hence $K(\mathcal{X}) = K(y, z)$.

Remark 4.5. Every $p$-element of $\text{Aut}(\mathcal{X})$ is an element of $E_{q^2}$.

Proof. Let $\sigma$ be a $p$-element of $\text{Aut}(\mathcal{X})$. By Nakajima’s bound, Theorem 2.1 (I), $|\langle E_{q^2}, \sigma \rangle| \leq q^2 = |E_{q^2}|$. Therefore $\sigma \in E_{q^2}$.

Let $z' = z - \delta$, with $L_1(\delta) = b$. Then $K(y, z) = K(y, z')$ where

$$L_1(z')L(y) - L_1(z')^2 = a. \tag{22}$$

Up to a $\mathbb{F}$-scaling of $z'$ and $y$, we can assume that both $L_1$ and $L$ are monic. Let $Z$ be the plane curve with affine equation $L_1(Z')L(Y) - L_1(Z')^2 = a$. By Remark 4.5 and Proposition 4.1, $E_{q^2} = \{\tau_{\alpha, \beta} : (y, z') \mapsto (y + \alpha, z' + \beta) \mid L(\alpha) = L_1(\beta) = 0\} \leq \text{Aut}(Z)$ has exactly two short orbits $\Omega_1$ and $\Omega_2$, which have length $q$ and are centered at the points at infinity $P_1 = (1 : 0 : 0)$ and $P_2 = (1 : 0 : 0)$, respectively. The $q$ distinct tangent lines to $Z$ at $P_1$ have equation $\ell_i : Y - Z' = \epsilon_i, i = 1, \ldots, q$, and the intersection multiplicity at $P_1$ of $Z$ and $\ell_i$ is equal to the intersection multiplicity at $P_1$ of the curve $W : L(Y) - L_1(Z') = 0$ with the line $\ell_i$. Since $W$ has degree $q$, this implies that $W$ splits into linear factors $\ell_1, \ell_2, \ldots, \ell_q$. Therefore $L(Y) - L_1(Z') = L_2(Y - Z')$ for some separable $p$-linearized polynomial $L_2(T) \in \mathbb{F}[T]$ of degree $q$. Thus, Equation (22) is the equation (3) defining $\mathcal{X}_{(L_1, L_2)}$, up to the formal replacement of $y - z'$ with $Y$ and of $z'$ with $bX$, where $b^q = a$.

Let $\bar{q}$ be the largest power of $p$ such that $\text{Aut}(\mathcal{X})$ contains a cyclic subgroup $C$ of order $\bar{q} - 1$. Up to conjugation in $\text{Aut}(\mathcal{X})$, $C$ contains the group

$$\Gamma = \{(X, Y) \mapsto (X + \alpha, Y + \beta) \mid L_1(\alpha) = L_2(\beta) = 0\}.$$  

Then $\mathcal{X} \in S_{\bar{q}^{L_1}}$ from Theorems 1.1 and 1.2. Thus, Theorem 1.3 is proved.

If $L_1 \neq L_2$, then from Theorem 1.2, $\mathcal{X}_{(L_1, L_2)}$ does not admit any automorphism group $C_2 \times C_2$. Thus, also Theorem 1.4 is proved.

5. Acknowledgments

This research was supported by the Italian Ministry MIUR, Struttura Geometriche, Combinatoria e loro Applicazioni, PRIN 2012 prot. 2012XZE22K, and by GNSAGA of the Italian INdAM. The authors would like to thank Nazar Arakelian and Gábor Korchmáros for useful comments and suggestions.

References

[1] N. Arakelian and G. Korchmáros, A characterization of the Artin-Mumford curve, J. Number Theory, 154 (2015), 278-291.
[2] G. Cornelissen and F. Kato, Equivariant deformation of Mumford curves and of ordinary curves in positive characteristic, Duke Math. J., 166, (2003), 431-470.
[3] G. Cornelissen and F. Kato, Discontinuous groups in positive characteristic and automorphisms of Mumford curves, Math. Ann., 320, (2001), 55-85.
[4] G. Cornelissen and F. Kato, Mumford curves with maximal automorphism group, Proceedings of the American Mathematical Society, 132, (2004), 1937-1941.
[5] M. Giulietti and G. Korchmáros, Algebraic curves with many automorphisms, preprint (2016).
[6] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics, Princeton (2008).
[7] B. Huppert, Endliche Gruppen. 1, Grundlehren der Mathematischen wissenschaften 134, Springer, Berlin, 1967, xii+793 pp.
[8] G. Korchmáros and M. Montanucci, Ordinary algebraic curves with many automorphisms in positive characteristic, arXiv:1610.05252v2 2016.
[9] A. Kontogeorgis and V. Rotger, On abelian automorphism groups of Mumford curves, Bull. London Math. Soc. 40 (2008), 353-362.
[10] S. Nakajima, p-ranks and automorphism groups of algebraic curves, Trans. Amer. Math. Soc. 303 (1987), 595-607.
[11] H. Stichtenoth, Algebraic function fields and codes, 2nd edn. Graduate Texts in Mathematics 254, Springer, Berlin (2009).
Authors’ addresses:

Maria MONTANUCCI  
Dipartimento di Matematica, Informatica ed Economia  
Università degli Studi della Basilicata  
Contrada Macchia Romana  
85100 Potenza (Italy).  
E–mail: maria.montanucci@unibas.it

Giovanni ZINI  
Dipartimento di Matematica e Informatica  
Università degli Studi di Firenze  
Viale Morgagni  
50134 Firenze (Italy).  
E–mail: gzini@math.unifi.it

[12] R. Valentini and M. Madan, A Hauptsatz of L.E. Dickson and Artin-Schreier extensions, *Journal für die reine und angewandte Mathematik*, (1980), 156-177.

[13] G. van der Geer and M. van der Vlugt, Kloosterman sums and the $p$-torsion of certain Jacobians, *Math. Ann.* 290, Birkhäuser, Basel, (1991), 549-563.