New examples of maximal curves with low genus

Bartoli, Daniele; Giulietti, Massimo; Kawakita, Motoko; Montanucci, Maria

Published in:
Finite Fields and Their Applications

Link to article, DOI:
10.1016/j.ffa.2020.101744

Publication date:
2020

Document Version
Peer reviewed version

Citation (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
NEW EXAMPLES OF MAXIMAL CURVES WITH LOW GENUS

DANIELE BARTOLI, MASSIMO GIULIETTI, MOTOKO KAWAKITA, AND MARIA MONTANUCCI

Abstract. Explicit equations for algebraic curves with genus 4, 5, and 10 that are either maximal or minimal over the finite field with $p^2$ elements are obtained for infinitely many $p$’s. The key tool is the investigation of their Jacobian decomposition. Lists of small $p$’s for which maximality holds are provided. In some cases we also describe the automorphism group of the curve.

1. Introduction

Throughout the paper, by curve we mean a projective, non-singular, geometrically irreducible algebraic curve defined over a finite field $\mathbb{F}_{q^2}$ of order $q^2$. A curve $\mathcal{X}$ with genus $g = g(\mathcal{X})$ is called $\mathbb{F}_{q^2}$-maximal if the number of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound, that is,

$$|\mathcal{X}(\mathbb{F}_{q^2})| = q^2 + 1 + 2qg.$$ 

Apart from being mathematical objects with intrinsic interest, maximal curves are often used for applications in Coding Theory, Cryptography, and Finite Geometry. For a survey on maximal curves we refer to [46, Chapter 10]. For a given $q$, the largest $g$ for which there exists an $\mathbb{F}_{q^2}$-maximal curve of genus $g$ is $q(q - 1)/2$ [49], and equality holds if and only if the curve is the Hermitian curve $\mathcal{H}_q$ with equation $X^{q+1} = X^q + X$ [69].

A complete solution of the classification problem for maximal curves seems to be out of reach and looking for new examples is still a very active line of research. A well-known construction method for maximal curves is based on a result of Kleiman [56], sometimes attributed to Serre (see [58]), stating that any non-singular curve which is $\mathbb{F}_{q^2}$-covered by an $\mathbb{F}_{q^2}$-maximal curve is also $\mathbb{F}_{q^2}$-maximal. Concrete examples of $\mathbb{F}_{q^2}$-maximal curves which are Galois-covered by $\mathcal{H}_q$ can be found e.g. in [11,52,59,63]. For a long time the problem of establishing whether all $\mathbb{F}_{q^2}$-maximal curves were covered by $\mathcal{H}_q$ remained open; see e.g. [87]. The problem was solved in [35], where examples of $\mathbb{F}_{q^2}$-maximal curves, with $q = p^{3h} > 8$, $p$ a prime, non-covered by $\mathcal{H}_q$ were constructed. Applying Kleiman-Serre covering result to these curves and to their generalizations [30], [7] and [71] provided further examples of maximal curves; see [18,15,22,38,39]. Other recent constructions can be found in [72,78,81].

The aim of this paper is to provide new examples of $\mathbb{F}_{p^2}$-maximal curves with low genus. We remark that an $\mathbb{F}_{p^2}$-maximal curve is also $\mathbb{F}_{p^2h}$-maximal for every positive odd integer $h$. By a criterion going back to Tate [76, Theorem 2(d)] and explicitly pointed out by Lachaud [58, Proposition 5], a curve defined over $\mathbb{F}_p$ with genus $g$ is $\mathbb{F}_{p^2}$-maximal if and only if its Jacobian is $\mathbb{F}_{p^2}$-isogenous to the $g$-th power of an $\mathbb{F}_{p^2}$-maximal elliptic curve. Here, such a criterion is applied to plane curves whose
Jacobian decomposition was originally studied in the zero characteristic case. In this direction, our main achievements are Theorem 2.4, Remark 2.5, Theorem 3.14, and Theorem 3.15. These results rely on a theorem by Kani and Rosen, which provides a decomposition of the Jacobian of a curve under some conditions on its automorphism group.

**Theorem 1.1.** [41, Theorem B] For a curve $X$, let $G \leq \text{Aut}_{\mathbb{F}_q}(X)$ be a finite group such that $G = H_1 \cup \cdots \cup H_m$, where the subgroups $H_i$ satisfy $H_i \cap H_j = \{1\}$ if $i \neq j$. Then we have the following $\mathbb{F}_q$-isogeny relation

$$J_{X}^{g-1} \times J_{X/G}^{g} \simeq J_{X/H_1}^{h_1} \times \cdots \times J_{X/H_m}^{h_m},$$

where $g = |G|$, $h_i = |H_i|$, and, as usual, $J^r = J \times \cdots \times J$ ($r$ times).

**Corollary 1.2.** [41, Example 1] With the same notation as in Theorem 1.1, if $G$ is the direct product of two cyclic groups of order 2, say $G = \{1, \alpha_1, \alpha_2, \alpha_3\}$, then

$$J_X \times J_{X/G} \simeq J_X/\langle \alpha_1 \rangle \times J_X/\langle \alpha_2 \rangle \times J_X/\langle \alpha_3 \rangle.$$

Theorem 1.1 has already been used e.g. in [2, 10, 47, 48, 51–54, 66] to describe examples of curves with many points with respect to their genus, including maximal curves. For some curves investigated in this work, Theorem 1.1 gives a decomposition of their Jacobian into elliptic curves. In order to establish whether these factors are isogeneous or not, we will use modular polynomials of low degrees, for which we refer to [12] and the web database [13].

The full $\mathbb{F}_{p^2}$-automorphism group $G$ is an invariant of great relevance for an $\mathbb{F}_{p^2}$-maximal curve $X$. In fact, by Kleiman-Serre covering result, for each subgroup $H$ of $G$ the quotient curve $X/H$ is still $\mathbb{F}_{p^2}$-maximal. Therefore, automorphism groups of some of the curves under investigation are determined.

The paper is organized as follows. In Section 2 we study the curve $C$ with equation

$$\frac{4(x^2 - x + 1)^3}{27x^2(x-1)^2} + \frac{4(y^2 - y + 1)^3}{27y^2(y-1)^2} = 1.$$

In characteristic zero, $C$ is one of the two genus 4 curves with exactly 72 automorphisms and its Jacobian decomposes as the 4-th power of an elliptic curve; see [89]. We prove that such a curve is $\mathbb{F}_{p^2}$-maximal for infinitely many primes $p$; see Theorem 2.4 and Remark 2.5. We show that its full automorphism group is isomorphic to $(S_3 \times S_3) \rtimes C_2$, as it happens in characteristic zero; see Section 2.2.

In Section 3 we deal with a family of curves with genus 5, given by Equation 10. In characteristic zero, these curves were characterized by Shaska [70] as the genus 5 hyperelliptic curves with automorphism group isomorphic to the direct product of $A_4$ and a group of order 2; Paulhus later observed that their Jacobian decomposes in the product of three isogenous elliptic curves and a hyperelliptic curve of genus 2; see [67, Proposition 4]. The main result of the section is Theorem 3.14, which states that some curves in the family are either $\mathbb{F}_{p^2}$-maximal or $\mathbb{F}_{p^2}$-minimal (that is, attaining the Hasse-Weil lower bound) for infinitely many primes $p$. A list of $p$ for which specific curves of the family are $\mathbb{F}_{p^2}$-maximal is provided; see Theorem 3.15. In Section 4 we extend Shaska’s characterization result to the positive characteristic case; see Theorem 4.2.
Finally, in Section 5 we report some results on the Jacobian decomposition and the \( F_p^2 \)-maximality of other curves with genus 10.

2. A CURVE OF GENUS 4

In this section we study the plane curve \( \mathcal{C} \) of the affine equation

\[
\frac{4(X^2 - X + 1)^3}{27X^2(X - 1)^2} + \frac{4(Y^2 - Y + 1)^3}{27Y^2(Y - 1)^2} = 1
\]

over the finite fields \( F_p \), \( p > 7 \) prime.

2.1. \( F_p^2 \)-maximality of \( \mathcal{C} \). Let \( F = F_p^2(x, y) \) with \( (4(x^2 - x + 1)^3/(27x^2(x - 1)^2) + (4(y^2 - y + 1)^3)/(27y^2(y - 1)^2) = 1 \) be the function field of the curve \( \mathcal{C} \). Let \( \tau_1, \tau_2, \sigma \) be the order-2 automorphisms of \( F \) defined by \( \sigma(x, y) = (y, x) \), \( \tau_1(x, y) = (-x+1, y) \), \( \tau_2(x, y) = (x, -y+1) \). We consider the group \( G = \langle \tau_1, \tau_2, \sigma \rangle \). Such a group is elementary abelian of order 8 and can be written as

\[
G = \langle \tau_1 \rangle \cup \langle \tau_2 \rangle \cup \langle \sigma \rangle \cup \langle \sigma \tau_1 \rangle \cup \langle \sigma \tau_2 \rangle ,
\]

where \( \langle \sigma \tau_1 \rangle = \{ \text{id}, \sigma \tau_1, \tau_1 \tau_2, \sigma \tau_2 \} \) and \( |\langle \tau_1 \rangle| = |\langle \tau_2 \rangle| = |\langle \sigma \rangle| = |\langle \sigma \tau_1 \rangle| = 2 \).

**Proposition 2.1.** The Jacobian variety of both the quotient curves \( \mathcal{C}/\langle \tau_1 \rangle \) and \( \mathcal{C}/\langle \tau_2 \rangle \) is \( F_p \)-isogenous to twice the Jacobian variety of the elliptic curve with equation

\[
Y^2 = X^3 + \frac{9}{16}X^2 + \frac{3}{16}X + \frac{1}{64}.
\]

**Proof.** Note that \( \tau_1 \) fixes both \( y_1 = y \) and \( x_1 = x(-x+1) \). As \( \tau_1 \) is an involution, the function field of \( \mathcal{C}/\tau_1 \) over \( F_p \) is \( F_p \)-isomorphic to \( F_p(x_1, y_1) \). A straightforward computation gives

\[
4((-y_1+1)^3x_1^2(x_1-1)^2 + (x_1^2-x_1+1)^3y_1^2) - 27y_1^2x_1^2(x_1-1)^2 = 0.
\]

Consider the genus 2 hyperelliptic function field \( \overline{F}_p(u, v) \) with

\[
v^2 = 4u^6 - 12u^5 + 21u^4 - 22u^3 + 21u^2 - 12u + 4,
\]

and let \( \mathcal{G} : Y^2 = 4X^6 - 12X^5 + 21X^4 - 22X^3 + 21X^2 - 12X + 4 \) be the corresponding hyperelliptic curve of genus 2. Then \( \overline{F}_p(x_1, y_1) \cong \overline{F}_p(u, v) \) via the \( F_p \)-isomorphism \( \psi : \overline{F}_p(u, v) \to \overline{F}_p(\xi, \eta) \) defined by

\[
\psi(u, v) = \left( \frac{a_1(u, v)}{a_3(u, v)}, \frac{a_2(u, v)}{a_3(u, v)} \right),
\]

with
It is immediate to see that the quotient curve $G/\psi$ are elliptic. In fact, 

$$a_1(u, v) = \frac{1}{2}u^8 - \frac{3}{2}u^7 + \frac{21}{8}u^6 - \frac{1}{4}u^5v - \frac{13}{4}u^5 + \frac{3}{8}u^4v + \frac{17}{4}u^4$$

$$+ \frac{1}{8}u^3v - \frac{13}{4}u^3 + \frac{1}{8}u^2v + \frac{21}{8}u^2 + \frac{3}{8}uv - \frac{3}{2}u - \frac{1}{4}v + \frac{1}{2},$$

$$a_2(u, v) = u^6 - \frac{3}{2}u^5 + u^4 + \frac{1}{2}u^3v - \frac{1}{2}u^2v,$$

$$a_3(u, v) = u^6 - 2u^5 + 2u^4 - 2u^3 + u^2.$$ 

Hence $G \cong C/\langle \tau_1 \rangle$ and applying the same argument to $x_2 = x$, $y_2 = y(-y + 1)$, and $\tau_2$, we see that $G \cong C/\langle \tau_2 \rangle$ as well.

Now we investigate the Jacobian decomposition of the hyperelliptic curve $G$. We apply Corollary 1.2 to $G$ and the automorphism group of order 4 generated by the involutions

$$\psi_1(u, v) = (u, -v), \quad \psi_2(u, v) = (-u + 1, v).$$

It is immediate to see that the quotient curve $G/\langle \psi_1 \rangle$ is rational, whereas both $G/\langle \psi_2 \rangle$ and $G/\langle \psi_1\psi_2 \rangle$ are elliptic. In fact, $\psi_2$ fixes $u_1 = -u^2 + u$ and $v_1 = v$, and

$$v_1^2 = -4u_1^3 + 9u_1^2 - 12u_1 + 4$$

holds; also, $\psi_1\psi_2$ fixes $u_2 = u_1$ and $v_2 = v(2u - 1)$ and

$$v_2^2 = (-4u_2^3 + 9u_2^2 - 12u_2 + 4)(-4u_2 + 1).$$

The function fields of the curves $G/\langle \psi_2 \rangle$ and $G/\langle \psi_1\psi_2 \rangle$ are $\mathbb{F}_p$-isomorphic to $\mathbb{F}_p(C_1) = \mathbb{F}_p(x', y')$ and $\mathbb{F}_p(C_2) = \mathbb{F}_p(x'', y'')$ with

$$(y')^2 = (x')^3 + \frac{9}{16}(x')^2 + \frac{3}{16}x' + \frac{1}{64}$$

and

$$(y'')^2 = (x'')^3 + \frac{11}{12}(x'')^2 + \frac{1}{9}x'' + \frac{1}{81},$$

respectively, where

$$x' = -\frac{1}{4}u_1, \quad y' = \frac{1}{16}v_1, \quad x'' = \frac{1/6u_2 - 1/24}{-(u_2)^2 + 1/2u_2 - 1/16}, \quad y'' = \frac{1/36v_2}{-(u_2)^2 + 1/2u_2 - 1/16}. $$

The two elliptic curves $C_1$ and $C_2$ are isogenous via the isogeny defined over their function field by $\theta(x'', y'') = (\theta_1(x'', y''), \theta_2(x'', y''))$ where

$$\theta_1 = \frac{1/4(x'')^3 - 1/9x''}{(x'' + 2/9)^2},$$

$$\theta_2 = \frac{1/8(x'')^3y'' + 1/12(x'')^2y'' + 1/18(x'')y'' - 1/81y''}{(x'' + 2/9)^3}.$$ 

By Corollary 1.2 the claim follows.
Proposition 2.2. The Jacobian varieties of both the quotient curves $C/\langle \sigma \rangle$ and $C/\langle \sigma \tau \rangle$ are $\mathbb{F}_p$-isogenous to the Jacobian variety of the elliptic curve of equation

$$Y^2 = X^3 + \frac{9}{16} X^2 + \frac{3}{16} X + \frac{1}{64}.$$ 

Proof. First note that the curves $C/\langle \sigma \rangle$ and $C/\langle \sigma \tau \rangle$ are $\mathbb{F}_p$-isomorphic since the subgroups $\langle \sigma \rangle$ and $\langle \sigma \tau \rangle$ are conjugated in the $\mathbb{F}_p$-automorphism group of $C$. Indeed $\gamma(x,y) = (x, -y + 1)$ is an automorphism of $F$. Therefore, we are going to deal only with the curve $C/\langle \sigma \rangle$.

Both $x_2 = x + y$ and $y_2 = xy$ are fixed by $\sigma$. Then $\mathbb{F}_p(x_2, y_2) \cong \mathbb{F}_p(C/\langle \sigma \rangle)$. Also,

$$4x_2^3y_2^3 + 4x_2^4 - 8x_2^3y_2^3 - 12x_2^3y_2 - 8x_2^3 + 4x_2^2y_2^2 + 8x_2y_2^2 + 21x_2y_2 + 8y_2^2$$
$$+ 4x_2^2 + 12x_2y_2 + 14x_2y_2^2 + 12x_2y_2 - 8y_2^3 - 19y_2^2 - 19y_2 - 8y_2 = 0.$$ 

As $\sigma$ fixes exactly 6 points of $C$, by the Riemann-Hurwitz formula the genus of $C/\langle \sigma \rangle$ is 1.

An isogeny $\varphi$ between $C/\langle \sigma \rangle$ (with homogeneous coordinates $X_1$, $Y_1$ and $Z_1$) and the elliptic curve

$$Y^2Z = X^3 + \frac{9}{16} X^2Z + \frac{3}{16} XZ^2 + \frac{1}{64} Z^3$$

can be constructed as follows. Consider the map $\varphi_1$ given by

$$\varphi_1(X_2) = 2^7 \cdot 7^4 X_2^2 Y_2 Z_2 - 2^4 \cdot 3 \cdot 7^4 X_2^2 Y_2^2 Z_2 - 2^4 \cdot 7^4 X_2 Y_2 Z_2 + 2^5 \cdot 7^4 Y_2 Z_2 + 2^3 \cdot 7^4 X_2^2 Y_2 Z_2^2 - 2^3 \cdot 7^5 X_2 Y_2^2 Z_2^2$$
$$+ 2^3 \cdot 7^4 X_2 Y_2 Z_2^3 + 2^3 \cdot 5 \cdot 7^4 Y_2^2 Z_2^3 + 2^6 \cdot 7^4 \cdot X_2 Y_2^2 Z_2^3 - 2^4 \cdot 7^6 Y_2^2 Z_2^3 - 2^3 \cdot 3 \cdot 7^4 X_2 Y_2 Z_2^2 + 2^5 \cdot 7^5 Y_2^2 Z_2^2$$
$$+ 2^3 \cdot 7^4 X_2 Y_2 Z_2^3 + 2^4 \cdot 7^3 X_2^2 Y_2 Z_2^3 - 2 \cdot 7^4 \cdot 19 X_2 Y_2 Z_2^3 + 2 \cdot 7^4 \cdot 97 Y_2^2 Z_2^3 + 2^5 \cdot 7^4 X_2^2 Y_2 Z_2^3 - 2^3 \cdot 7^5 X_2 Y_2^2 Z_2^3$$
$$- 2^3 \cdot 3 \cdot 7^4 X_2^2 Y_2 Z_2^3 + 2 \cdot 2^3 \cdot 17 Y_2 Z_2^3 + 2^3 \cdot 7^4 X_2 Y_2 Z_2^3 + 2^3 \cdot 7^5 Y_2 Z_2^3 - 2^4 \cdot 7^4 X_2 Y_2 Z_2^3$$
$$+ 2^3 \cdot 3 \cdot 7^3 Y_2 Z_2^3,$$

$$\varphi_1(Y_2) = -2^7 \cdot 7^6 X_2 Y_2^2 + 2^8 \cdot 7^6 X_2 Y_2^3 - 2^7 \cdot 7^6 X_2 Y_2^4 - 2^6 \cdot 3 \cdot 7^6 X_2 Y_2^5 - 2^6 \cdot 3 \cdot 7^6 Y_2^2 Z_2 - 2^5 \cdot 7^6 \cdot 11 X_2 Y_2 Z_2^2 + 2^5 \cdot 7^6 \cdot 29 X_2 Y_2 Z_2^2$$
$$- 2^5 \cdot 7^6 \cdot 11 X_2 Y_2 Z_2^2 - 2^5 \cdot 7^6 \cdot 11 X_2 Y_2 Z_2^2 - 2^5 \cdot 7^6 \cdot 127 Y_2 Z_2^2 + 2^6 \cdot 3 \cdot 7^6 X_2^2 Y_2 Z_2^2 - 2^6 \cdot 7^6 \cdot X_2^2 Y_2 Z_2^2$$
$$- 2^5 \cdot 3 \cdot 7^6 Y_2 Z_2^2 - 2^5 \cdot 5 \cdot 7^5 \cdot 13 Y_2 Z_2^2 - 2^3 \cdot 7^6 \cdot 11 X_2 Y_2 Z_2^2 + 2^3 \cdot 7^6 \cdot X_2 Y_2 Z_2^2$$
$$- 2^5 \cdot 3 \cdot 7^5 \cdot 13 Y_2 Z_2^2 + 2^6 \cdot 3 \cdot 7^6 X_2 Y_2 Z_2^2 - 2^5 \cdot 3 \cdot 7^6 X_2 Y_2 Z_2^2 + 2^4 \cdot 3 \cdot 7^6 X_2 Y_2 Z_2^2$$
$$+ 2^5 \cdot 3 \cdot 7^5 \cdot 13 Y_2 Z_2^2 + 2^3 \cdot 7^5 \cdot 13 Y_2 Z_2^2 + 2^7 \cdot 7^5 \cdot 41 Y_2 Z_2^2$$
$$- 2^6 \cdot 7^5 \cdot 13 Y_2 Z_2^2,$$

$$\varphi_1(Z_2) = Y_2^2 Z_2^2 - 3/2 Y_2^2 Z_2^2 + 15/4 Y_2^2 Z_2^2 + 1/4 Y_2^2 Z_2^2 + 15/4 Y_2^2 Z_2^2 - 3/2 Y_2^2 Z_2^2 + Y_2 Z_2^2.$$ 

Then define

$$\varphi(X_2 : Y_2 : 1) = (1/(2^6 7^4) \varphi_1(X_2) : 1/(2^6 7^4) \varphi_1(Y_2) - 1/(2^6 7^4) \varphi_1(X_2) + 3^2/(2^7 7) : 1).$$

By direct checking with MAGMA $\varphi$ is an isogeny between the two elliptic curves over the field of rationals. Clearly this map provides an isogeny over $\mathbb{F}_p$ for every $p$ such that no coefficients of $\varphi_1$ vanish. It has been checked with MAGMA that also for these special values of $p$ the two elliptic curves are $\mathbb{F}_p$-isogenous. □
Proposition 2.3. The Jacobian variety of the curve \(C/\langle \tau_1 \tau_2 \rangle\) is \(\mathbb{F}_p\)-isogenous to twice the Jacobian variety of the elliptic curve of equation

\[
Y^2 = X^3 + \frac{9}{16}X^2 + \frac{3}{16}X + \frac{1}{64}.
\]

Proof. Note that

\[
x_3 = x(-x + 1) + y(-y + 1), \quad y_3 = \frac{x}{y} + \frac{-x + 1}{-y + 1}
\]

are both fixed by the involution \(\tau_1 \tau_2\). They satisfy \(L(u, v) = 0\), where

\[
L(x_3, y_3) := 16x_3^6y_3^4 - 40x_3^5y_3^4 - 32x_3^5y_3^4 - 32x_3^4y_5^2 + 32x_3^4y_3^6 - 80x_3^4y_3^5 + 185x_3^4y_3^4 + 80x_3^3y_3^3 + 128x_3^2y_3^3 \\
-32x_3^2y_3 + 16x_3^4 - 40x_3^3y_3^2 - 124x_3^3y_3 - 24x_3^2y_3^2 - 482x_3^2y_3^2 - 518x_3y_3^2 - 112x_3^2y_3 - 104x_3^3 \\
+ 16x_3^3y_3^2 - 48x_3y_3^5 + 1212x_3^2y_3^5 - 352x_3^2y_3^5 + 1184x_3^2y_3^5 - 916x_3y_3^5 + 2193x_3y_3^5 + 318x_3^2y_3^5 \\
+ 425x_3 - 32x_3y_3^2 - 48x_3y_3^5 - 296x_3y_3^5 - 304x_3y_3^5 - 1076x_3y_3^5 + 524x_3y_3^5 - 1312x_3y_3 \\
- 832x_3 + 32x_3y_3^2 - 64y_3^5 + 308y_3^5 - 488y_3^5 + 100y_3^5 - 1024x_3 + 1024.
\]

To show that \(\mathbb{F}_p(x_3, y_3)\) with \(L(x_3, y_3) = 0\) is the function field of \(C/\langle \tau_1 \tau_2 \rangle\) it is sufficient to note that \(\mathbb{F}_p(x_3, y_3)\) has genus 2. Indeed, from the Hurwitz genus formula and Theorem 1.2 applied with respect to \(G\), \(C/\langle \sigma_1 \rangle\) has genus 1 and since \(\tau_1 \tau_2 \in \langle \sigma_1 \rangle\),

\[
g(C/\langle \sigma_1 \rangle) < g(C/\langle \tau_1 \tau_2 \rangle) \leq 2.
\]

Also, \(\mathbb{F}_p(x_3, y_3)\) is \(\mathbb{F}_p\)-isomorphic to \(\mathbb{F}_p(u', v')\), with

\[
v'^2 + (u'^2 + u')v' = -u'^6 - 3u'^5 - u'^4 - 7u'^3 - u'^2 - 3u' - 1,
\]

via the isomorphism \(\phi(x_3, y_3) = \left(\frac{b_1(x_3, y_3)}{b_3(x_3, y_3)}, \frac{b_2(x_3, y_3)}{b_3(x_3, y_3)}\right)\) given by

\[
b_1(x_3, y_3) = -2x_3^4 + x_3^3 - 2x_3^2, \\
b_2(x_3, y_3) = \frac{2x_3^5 - 3x_3^4 + x_3^3 - 2x_3^2y_3 - 3x_3^2 - x_3y_3 - y_3 - 1}{2}, \\
b_3(x_3, y_3) = x_3^5 + 2x_3^4 + x_3.
\]

Now, \(\mathbb{F}_p(u', v')\) is \(\mathbb{F}_p\)-isomorphic to \(\mathbb{F}_p(u'', v'')\), with

\[
(v'')^2 = -4(u'')^6 - 12(u'')^5 - 3(u'')^4 - 26(u'')^3 - 3(u'')^2 - 12(u'') - 4,
\]

via the isomorphism \(\theta(u', v') = \left(\frac{c_1(u', v')}{c_3(u', v')}, \frac{c_2(u', v')}{c_3(u', v')}\right)\)

\[
c_1(u', v') = u'^2, \\
c_2(u', v') = u'^2 + u' + 2v', \\
c_3(u', v') = u'^3.
\]
Consider the involutory automorphisms of the hyperelliptic function field \( \mathbb{F}_p(u'', v'') \) given by
\[
\psi_1(u'', v'') = (1/u'', v''/(u'')^3) \quad \psi_2(u'', v'') = (u'', -v'').
\]
The fixed fields of \( \mathbb{F}_p(u'', v'') \) with respect to \( \psi_1, \psi_2, \psi_1\psi_2 \) are
\[
\mathbb{F}_p(s, t_1), \mathbb{F}_p(u''), \mathbb{F}_p(s, t_2),
\]
respectively, where \( s = u'' + 1/u'' \), \( t_1 = v'' + v''/(u'')^3 \), \( t_2 = v'' - v''/(u'')^3 \) and
\[
t^2_1 - 4s^6 - 12s^5 + 21s^4 + 26s^3 - 51s^2 + 24s - 4 = 0,
\]
\[
-t^2_2 - 4s^6 - 12s^5 + 21s^4 + 42s^3 - 3s^2 - 12s + 4 = 0.
\]
Consider the function fields \( \mathbb{F}_p(s', t'_1), \mathbb{F}_p(s'', t'_1) \) with
\[
(t'_1)^2 = (s')^3 - 9517824s' + 11448262656
\]
and
\[
(t'_2)^2 = (s'')^3 - 4541184(s'') + 493881753.
\]
The function field \( \mathbb{F}_p(s, t_1) \) is isomorphic to \( \mathbb{F}_p(s', t'_1) \) via the isomorphism
\[
\theta'(s, t_1) = (d_1(s, t_1)/d_3(s, t_1), d_2(s, t_1)/d_3(s, t_1))
\]
where
\[
d_1(s, t_1) = 2304s^5 + 9216u^4 - 2880s^3 + 11522t_1 - 17856s^2 + 2880st_1 + 11520s + 720t_1 - 2304,
\]
\[
d_2(s, t_1) = 248832s^5 + 995328s^4 + 552963t_1 - 311040s^3 + 207360s^2t_1 - 1928448s^2 + 103680st_1 + 27648t_1^2 + 1244160s - 55296t_1 - 248832,
\]
\[
d_3(s, t_1) = t_1.
\]
The function field \( \mathbb{F}_p(s, t_2) \) is isomorphic to \( \mathbb{F}_p(s'', t'_2) \) via the isomorphism
\[
\theta''(s, t_2) = (d'_1(s, t_2)/d'_3(s, t_2), d'_2(s, t_2)/d'_3(s, t_2))
\]
where
\[
d'_1(s, t_2) = 36864s^5t_2 + 184320s^4t_2 + 175104s^3t_2 - 36864s^2t_2 - 4176t_2^3 - 46080st_2 + 18432t_2,
\]
\[
d'_2(s, t_2) = 84934656s^5 - 442368s^3t_2^2 + 424673280s^4 - 2654208s^2t_2^2 + 403439616s^3 - 5640192st_2^2 - 84934656s^2 - 10506240t_2^2 - 106168320s + 42467328,
\]
\[
d'_3(s, t_2) = t_2^3.
The two elliptic curves $\mathcal{E}_1 : Y^2 = X^3 - 9517824X + 11448262656$ and $\mathcal{E}_2 : Y^2 = X^3 - 4541184X + 493881753$ are isogenous to $Y^2 = X^3 + 9/16X^2 + 3/16X + 1/64$ via the $\mathbb{F}_p$-isogenies

$$(X : Y) \mapsto \left( \frac{f_1(X)}{f_2(X)} : \frac{g(X,Y)}{f_3(X)} \right),$$

where

$f_1(X) = -1/20736X^3 - 1/16X^2 + 837X - 1123632,$

$f_2(X) = X^2 - 2592X + 1679616,$

$g(X,Y) = -\xi/2985984X^3Y + \xi/768X^2Y - 75\xi/16XY + 8073\xi Y,$

$f_3(X) = -X^3 + 3888X^2 - 5038848X + 2176782336;$$$

with $\xi^2 = -1$ for $\mathcal{E}_1,$ and

$f_1(X) = 1/20736X^3 - 11/48X^2 - 213X + 720720,$

$f_2(X) = X^2 - 864X + 186624,$

$g(X,Y) = 1/2985984X^3Y - 1/2304X^2Y + 137/48XY - 9371Y,$

$f_3(X) = X^3 - 1296X^2 + 559872X - 80621568;$

for $\mathcal{E}_2.$ From Corollary 1.2 applied to $\mathbb{F}_p(u'', v'')$ with respect to $\langle \psi_1, \psi_2 \rangle \cong C_2 \times C_2$ the claim follows.

**Theorem 2.4.** Let $p > 7$ be a prime. Then the $\mathbb{F}_p$-rational curve $C$ is $\mathbb{F}_{p^2}$-maximal if and only if the elliptic curve

$$C : Y^2 = X^3 + 9/16X^2 + 3/16X + 1/64$$

is $\mathbb{F}_{p^2}$-maximal. In particular, $C$ is $\mathbb{F}_{p^2}$-maximal for infinitely many primes.

**Proof.** We apply Theorem 1.1 to the curve $C$ and the group $G = \langle \tau_1, \tau_2, \sigma \rangle.$ Such a group can be written as

$$G = \langle \tau_1 \rangle \cup \langle \tau_2 \rangle \cup \langle \sigma \rangle \cup \langle \sigma \tau_1 \rangle \cup \langle \sigma \tau_2 \rangle;$$

see Equation (2). In this case, $m = 5,$ $h_1 = h_2 = h_3 = h_5 = 2,$ $h_4 = 4$ and

$$J_C^3 \times J_C^4 \simeq J_{C/G}(\tau_1) \times J_{C/\langle \tau_2 \rangle} \times J_{C/\langle \sigma \rangle} \times J_{C/\langle \sigma \tau_1 \rangle} \times J_{C/\langle \sigma \tau_2 \rangle}.$$ 

By the Hurwitz genus formula applied to $G,$ we deduce that $C/G$ is rational. In fact, the number of places of $C$ fixed by elements of $G$ exceeds 6. By Propositions 2.1 and 2.2 the Jacobians of $C/\langle \tau_1 \rangle,$ $C/\langle \tau_2 \rangle,$ $C/\langle \sigma \rangle$ and $C/\langle \sigma \tau_1 \rangle$ are $\mathbb{F}_p$-isogenous to a power of the Jacobian of $\mathcal{E}.$ Hence Equation (7) reads

$$J_C \simeq J_C^3 \times J_{C/\langle \sigma \tau_1 \rangle}.$$ 

To prove the first claim, note that the $\mathbb{F}_{p^2}$-maximality of $C$ implies the $\mathbb{F}_{p^2}$-maximality of $\mathcal{E}$ since $\mathcal{E}$ is $\mathbb{F}_{p^2}$-covered by $C.$ Assume now that $\mathcal{E}$ is $\mathbb{F}_{p^2}$-maximal. By Proposition 2.3 the Jacobian of the curve $C/\langle \tau_1 \tau_2 \rangle$ is $\mathbb{F}_{p^2}$-isogenous to a power of $J_C,$ and hence $C/\langle \tau_1 \tau_2 \rangle$ is an $\mathbb{F}_{p^2}$-maximal curve. But $C/\langle \sigma \tau_1 \rangle$ is $\mathbb{F}_{p^2}$-covered by $C/\langle \tau_1 \tau_2 \rangle,$ therefore $C/\langle \sigma \tau_1 \rangle$ is $\mathbb{F}_{p^2}$-maximal too, and so is $C$ by the Tate-Lachaud criterion mentioned in the introduction.
An elliptic curve over the complex field with integer coefficients, when it is viewed as a curve defined over \( \mathbb{F}_p \) with \( p \) a prime, is supersingular for infinitely many \( p \)'s; see [19]. Since a supersingular elliptic curve defined over \( \mathbb{F}_p \) is \( \mathbb{F}_{p^2} \)-maximal, the elliptic curve \( \mathcal{E} \) is \( \mathbb{F}_{p^2} \)-maximal for infinitely many \( p \)'s. This proves the second claim.

\[ \square \]

**Remark 2.5.** MAGMA code computations show that the list of primes up to 100000 for which the curve \( \mathcal{E} \), and therefore \( \mathcal{C} \), is \( \mathbb{F}_{p^2} \)-maximal is

\[
17, 71, 251, 647, 827, 1889, 3527, 3617, 4409, 6569, 11969, 12113, 12527, 12689, 13913, 22031, 23039, 23633, 26297, 28871, 31769, 35171, 35729, 48527, 60497, 60623, 61487, 82457, 93383, 93761.
\]

**Remark 2.6.** For \( p = 17 \) the curve \( \mathcal{C} \) is Galois covered by the Hermitian curve \( \mathcal{H}_{17} \) over \( \mathbb{F}_{17^2} \). In fact, let \( \mathcal{H}_{17} : Y^{18} = X^{17}Z + Z^{17}X \). Consider the automorphism group \( G \) of \( \mathcal{H}_{17} \) generated by \( \alpha_1, \alpha_2, \alpha_3 \) and \( \gamma \) where

\[
\alpha_1(X, Y, Z) = (-X, \lambda Y, Z), \quad \alpha_2(X, Y, Z) = (-\lambda cZ, Y, -\lambda/cX),
\]

\[
\alpha_3(X, Y, Z) = (cX, Y, -X/c), \quad \text{and} \quad \gamma(X, Y, Z) = (X, \mu Y, Z),
\]

with \( \mu^3 = 1 \), \( \lambda^2 = -1 \) and \( 2c^2 = \lambda + 1 \). Then \( G = \langle \alpha_1, \alpha_2, \alpha_3 \rangle \times \langle \gamma \rangle \cong \mathbb{Q}_8 \times C_3 \), where \( \mathbb{Q}_8 \) is the quaternion group of order 8. Using MAGMA we obtained a model for the quotient curve \( \mathcal{H}_{17}/G \) over \( \mathbb{F}_{17^2} \):

\[
\mathcal{H}_{17}/G : \begin{cases}
YZ + 16XW = 0, \\
X^3 + 4XY^2 + 16Z^2W + 9W^3 = 0.
\end{cases}
\]

An \( \mathbb{F}_{17^2} \)-rational isomorphism between \( \mathcal{C} \) : \((4(X^2 - XZ + Z^2)^3)(27Y^2(2Y - Z)^2) + (4Y^2 - YZ + Z^2)^3)(27X^2(X - Z)^2) = (27Y^2(Y - Z)^2)(27X^2(X - Z)^2)Z^2 \) and \( \mathcal{H}_{17}/G \) is given by \( \phi(X, Y, Z) = (\phi_1(X, Y, Z), \phi_2(X, Y, Z), \phi_3(X, Y, Z), \phi_4(X, Y, Z)) \) where

\[
\phi_1(X, Y, Z) = \begin{align*}
&w^{149}X^{5}Y^{6}Z + w^{159}X^{3}Y^{8}Z + w^{33}X^{5}Y^{5}Z^{2} + w^{28}X^{4}Y^{6}Z^{2} + w^{231}X^{3}Y^{7}Z^{2} + w^{89}X^{2}Y^{8}Z^{2} \\
&\quad + w^{141}X^{5}Y^{4}Z^{3} + w^{190}X^{4}Y^{5}Z^{3} + w^{78}X^{3}Y^{6}Z^{3} + w^{161}X^{2}Y^{7}Z^{3} + w^{93}X^{2}Y^{8}Z^{3} + w^{213}X^{5}Y^{3}Z^{4} + w^{135}X^{4}Y^{4}Z^{4} \\
&\quad + 2X^{3}Y^{5}Z^{4} + 4X^{2}Y^{6}Z^{4} + w^{165}X^{6}Y^{7}Z^{4} + w^{156}X^{6}Y^{8}Z^{4} + w^{177}X^{5}Y^{2}Z^{5} + w^{253}X^{4}Y^{3}Z^{5} + w^{119}X^{3}Y^{4}Z^{5} \\
&\quad + w^{91}X^{2}Y^{5}Z^{5} + w^{127}X^{2}Y^{6}Z^{5} + w^{228}X^{2}Y^{7}Z^{5} + w^{124}X^{2}Y^{8}Z^{5} + w^{281}X^{3}Y^{2}Z^{6} + X^{2}Y^{4}Z^{6} + w^{52}X^{2}Y^{5}Z^{6} \\
&\quad + 14Y^{6}Z^{6} + w^{209}X^{3}Y^{2}Z^{7} + w^{101}X^{2}Y^{3}Z^{7} + w^{64}X^{2}Y^{4}Z^{7} + w^{64}Y^{5}Z^{7} + w^{69}X^{3}Y^{8}Z + w^{194}X^{2}Y^{2}Z^{8} \\
&\quad + w^{221}X^{2}Y^{3}Z^{8} + w^{275}X^{2}Y^{4}Z^{8} + w^{177}X^{2}Y^{9}Z + w^{74}X^{2}Y^{8}Z^{9} + w^{97}X^{2}Y^{9}Z^{9} + 3X^{2}Z^{10} + w^{75}X^{2}Y^{10} \\
&\quad + w^{202}Y^{2}Z^{10} + w^{129}X^{2}Z^{11} + w^{12}Y^{2}Z^{11} \end{align*}
\]

\[
\phi_2(X, Y, Z) = \begin{align*}
&w^{105}X^{5}Y^{7} + w^{105}X^{3}Y^{9} + w^{195}X^{5}Y^{6}Z + w^{52}X^{4}Y^{7}Z + w^{33}X^{3}Y^{8}Z + 12X^{2}Y^{9}Z + w^{267}X^{5}Y^{5}Z^{2} \\
&\quad + w^{142}X^{4}Y^{6}Z^{2} + w^{94}X^{3}Y^{7}Z^{2} + 14X^{2}Y^{8}Z^{2} + w^{57}X^{4}Y^{9}Z^{2} + w^{51}X^{5}Y^{4}Z^{3} + w^{214}X^{4}Y^{5}Z^{3} + w^{132}X^{3}Y^{6}Z^{3} \\
&\quad + w^{76}X^{2}Y^{7}Z^{3} + w^{273}X^{2}Y^{8}Z^{3} + w^{231}X^{5}Y^{3}Z^{4} + w^{286}X^{4}Y^{4}Z^{4} + w^{38}X^{3}Y^{5}Z^{4} + w^{286}X^{2}Y^{6}Z^{4} + w^{128}X^{7}Y^{4}Z^{4} \\
&\quad + w^{285}X^{5}Y^{2}Z^{5} + w^{178}X^{4}Y^{3}Z^{5} + w^{8}X^{3}Y^{4}Z^{5} + w^{75}X^{2}Y^{5}Z^{5} + w^{207}X^{4}Y^{6}Z^{5} + w^{165}Y^{7}Z^{5} + w^{232}X^{4}Y^{2}Z^{6} \\
&\quad + w^{175}X^{3}Y^{3}Z^{6} + w^{187}X^{2}Y^{4}Z^{6} + w^{231}X^{5}Y^{5}Z^{6} + w^{255}Y^{6}Z^{6} + w^{212}X^{3}Y^{2}Z^{7} + w^{145}X^{2}Y^{3}Z^{7} + w^{179}X^{4}Y^{4}Z^{7} \\
&\quad + w^{39}Y^{5}Z^{7} + w^{123}X^{3}Y^{7}Z^{8} + w^{71}X^{2}Y^{2}Z^{8} + w^{151}X^{3}Y^{3}Z^{8} + w^{111}Y^{4}Z^{8} + w^{285}X^{3}Z^{9} + 2X^{2}Y^{9}Z^{9} \end{align*}
\]
It is easily seen that
and
\[ w^{27} X^5 Y^9 Z + w^{243} X^2 Y^2 Z^2 + w^{45} X^5 Y^4 Z^3 + w^{27} X^4 Y^5 Z^3 + w^{171} X^3 Y^6 Z^3 \]
\[ + w^{27} X^2 Y^7 Z^3 + w^{171} X Y^8 Z^3 + w^9 X^5 Y^3 Z^4 + w^{27} X^4 Y^4 Z^4 + w^{27} X^3 Y^5 Z^4 + w^{207} X^2 Y^6 Z^4 + w^{135} X Y^7 Z^4 \]
\[ + w^{207} X^5 Y^2 Z^5 + w^{279} X^4 Y^3 Z^5 + w^{27} X^3 Y^4 Z^5 + w^9 X^2 Y^5 Z^5 + w^9 X Y^6 Z^5 + w^{167} Y^7 Z^5 + w^{189} X Y^2 Z^6 \]
\[ + w^{171} X^3 Y^3 Z^6 + w^9 X^2 Y^4 Z^6 + w^{207} X Y^5 Z^6 + w^{257} Y^6 Z^6 + w^{225} X^3 Y^2 Z^7 + w^{207} X^2 Y^3 Z^7 \]
\[ + w^{207} X Y^4 Z^7 + w^{136} X^5 Y^7 + w^{135} X Y^3 Z^8 + w^{27} X^2 Y^2 Z^8 + w^9 X Y^3 Z^8 + w^{171} Y^4 Z^8 + w^{207} X^3 Z^9 + w^{45} X^2 Y Z^9 \]
\[ + w^{135} X Y^2 Z^9 + w^{257} Y^3 Z^9 + w^{117} X^2 Z^{10} + w^{171} X Y Z^{10} + w^{140} Y^2 Z^{10} + w^{243} X Z^{11} + 4Y Z^{11}, \]

and \( w \) is a primitive element of \( \mathbb{F}_{172} \). We are not able to tell whether \( C \) is Galois covered by the Hermitian curve for \( p > 17 \).

2.2. Automorphism group of \( C \). The aim of this section is to compute the full automorphism group of \( C \) when \( p \geq 5 \). First, we construct a subgroup \( H \) of automorphisms of \( C \), and then we will prove that when \( p \geq 5 \), \( H \) coincides with the full automorphism group of \( C \).

**Remark 2.7.** The full automorphism group of \( C \) contains a subgroup
\[ H = (\langle \alpha_1, \alpha_2 \rangle \times \langle \alpha_3, \alpha_4 \rangle) \times \langle \alpha_5 \rangle \cong (S_3 \times S_3) \rtimes C_2, \]
where
\[ \alpha_1 : (x, y) \mapsto \left( \frac{-1}{x-1}, y \right), \quad \alpha_2 : (x, y) \mapsto \left( \frac{1}{x}, y \right) \]
\[ \alpha_3 : (x, y) \mapsto \left( x, \frac{-1}{y-1} \right), \quad \alpha_4 : (x, y) \mapsto \left( x, \frac{1}{y} \right), \quad \alpha_5 : (x, y) \mapsto (y, x). \]
It is easily seen that
\[ \alpha_2^2 = \alpha_4^2 = \alpha_5^2 = \alpha_1^3 = \alpha_3^3 = 1 \]
and \( \alpha_2 \alpha_1 \alpha_2 = \alpha_2^2, \) \( \alpha_1 \alpha_3 \alpha_4 = \alpha_2^3 \) so that \( \langle \alpha_1, \alpha_2 \rangle \cong S_3 \) and \( \langle \alpha_3, \alpha_4 \rangle \cong S_3 \), and \( \alpha_5 \) interchanges \( \langle \alpha_1, \alpha_2 \rangle \) into \( \langle \alpha_3, \alpha_4 \rangle \) by conjugation.

**Lemma 2.8.** \( |\text{Aut}(C)| \in \{72, 144, 216\} \).
Proof. We first prove that the size of $Aut(C)$ is coprime with $p$. Assume on the contrary that $S$ is a Sylow $p$-subgroup of $Aut(C)$. Then by [65, Theorem 1],

$$|S| \leq \max \left\{ 4, \frac{4p}{(p-1)^2} \right\}.$$ 

For $p \geq 11$ this contradicts $|S| \geq p$. By direct checking with MAGMA, if either $p = 5$ or $p = 7$ then the curve $C$ is ordinary, that is, the $p$-rank $\gamma$ of $C$ equals its genus $g(C) = 4$. If $p = 7$, by [65, Theorem 1 (i)] we have $|S| \leq 3p/(p-2) \leq 21/5 < 7$, a contradiction. If $p = 5$ then $|S| = 5$. By [37, Theorem 1.3], $|Aut(C)|$ divides $2p(p-1) = 40$, a contradiction as $72 \nmid \ |Aut(C)|$ by Remark 2.7. This shows that $p$ does not divide $|Aut(C)|$. By [46, Theorem 11.108], $|Aut(C)| = 2^a3^b5^c7^d$ for some integers $a, b, c, d \geq 0$. Observe that $a \geq 3$ and $b \geq 2$ as $72 \nmid |Aut(C)|$. Hurwitz bound [46, Theorem 11.56] yields $|Aut(C)| \leq 84(g-1) = 252$, hence $|Aut(C)| \in \{72, 144, 216\}$. □

Next we prove that the cases $|Aut(C)| = 144$ and $|Aut(C)| = 216$ cannot actually occur.

**Theorem 2.9.** Let $p \geq 5$ and let $H$ be as in Remark 2.7. The full automorphism group $Aut(C)$ coincides with $H$. In particular, $Aut(C) \cong (S_3 \times S_3) \rtimes C_2$, where $C_2$ denotes a cyclic group of order 2 and $S_3$ is the symmetric group on 3 letters.

**Proof.**

- Suppose that $|Aut(C)| = 216$. Then $Aut(C)$ is one of the 177 groups of order 216 (up to isomorphism) and it contains a subgroup $G$ isomorphic to $(S_3 \times S_3) \rtimes C_2$. By direct checking with MAGMA, we have that $Aut(C) \cong SmallGroup(216, i)$ for some $i = 157, 158, 159$. We recall that from [46, Theorem 11.79] if $A$ is an abelian subgroup of $Aut(C)$, then $|A| \leq 4g + 4$. On the other hand, for each $i = 157, 158, 159$ the group $SmallGroup(216, i)$ has an abelian subgroup of order 27, a contradiction.

- Suppose that $|Aut(C)| = 144$. In particular, $Aut(C)$ is one of the 197 groups of order 144 (up to isomorphism) containing a subgroup isomorphic to $(S_3 \times S_3) \rtimes C_2$. By direct checking with MAGMA, $Aut(C) \cong SmallGroup(144, i)$ for some $i = 182, 186$. Since $SmallGroup(144, 186)$ contains an elementary abelian group of order 8 and $C$ has even genus, [36, Lemma 6.3] provides a contradiction. Hence, $Aut(C) \cong SmallGroup(144, 182)$. Therefore, $Aut(C)$ contains a unique Sylow 3-subgroup $S_3$, which is elementary abelian of order 9; also, the elements of order 3 are all conjugated in $Aut(C)$ whereas they split into 2 conjugacy classes in the subgroup $H \cong (S_3 \times S_3) \rtimes C_2$. Let $S$ denote the unique Sylow 3-subgroup of $Aut(C)$ and let $\tilde{g}$ be the genus of the quotient curve $C/S$. By the Hurwitz genus formula [46, Theorem 11.72] applied to $S$, either $\tilde{g} = 1$ or $\tilde{g} = 0$.

Assume that $\tilde{g} = 1$. Then from [46, Theorem 11.72],

$$6 = 2 \cdot a + 8 \cdot b,$$

for some $a \geq 0$ and $b \geq 0$ as $S$ contains just proper subgroups of order 3. Necessarily, $b = 0$ and $a = 3$. Geometrically, this shows that for 3 points, say $P_1, P_2,$ and $P_3$, the stabilizer $S_{P_i}$ has order 3. Since the 8 elements of order 3 in $S$ are all conjugated and therefore fix the same number $n$ of points, the only possibility is $n = 1$ and $S_{P_i} \neq S_{P_j}$ for every $i \neq j$ and $i, j = 1, 2, 3$. Note that $S$ acts transitively on the set $\{P_1, P_2, P_3\}$. Let $N$ be the normalizer of $S$ in $Aut(C)$. Then by direct checking with MAGMA, $N = S \rtimes M$, for some subgroup
$M$ of order 16. The group $M$ is isomorphic to a subgroup of automorphisms of the elliptic curve $C/S$, which fixes the point of $C/S$ corresponding to the orbit $\{P_1, P_2, P_3\}$. But this is impossible by [46, Theorem 11.94(ii)].

We are left with the case where $C/S$ is a rational curve. Note that $S$ cannot have fixed points on $C$ since it is not a cyclic group; see [46, Theorem 11.49]. By the Hurwitz genus formula we get that

$$6 = -2 \cdot 9 + 2a,$$

and hence $a = 12$ and each element of order 3 in $S$ has exactly 3 fixed points. For a subgroup $T$ of $S$ of order 3, by the Hurwitz genus formula applied to $T$, the quotient curve $C/T$ is elliptic. The normalizer $N_T$ of $T$ in $\text{Aut}(C)$ has order 36 and the factor group $N_T/T$ contains an elementary abelian subgroup $K$ of order 4. Clearly, $N_T$ acts on the set of 3 points fixed by $T$. Therefore $K$, viewed as an automorphism group of $C/T$, acts on the set of 3 points of $C/T$ corresponding to the fixed points of $T$. Necessarily $K$ fixes at least one of these 3 points. Since $K$ is not cyclic we have a contradiction by [46, Theorem 11.49].

This shows that the elements of order 3 cannot be all conjugated in $\text{Aut}(C)$ and hence that $\text{Aut}(C)$ cannot be isomorphic to $\text{SmallGroup}(144, 182)$.

By Lemma 2.8 $\text{Aut}(C)$ has order 72, and the claim follows by Remark 2.7.

**Remark 2.10.** Up to our knowledge, the unique known examples of $\mathbb{F}_{17^2}$-maximal curves of genus 4 were

$$y^{12} = x(x + 1)^{16}$$

and

$$x^6 + y^6 + 2x^3y^2 + 12xy + 14 = 0;$$

see [DS, SS]. We point out that the curve $C$ is not $\mathbb{F}_{17}$-isomorphic to either of them, since the automorphism group of the former is $((C_2 \times C_2) \rtimes (C_3 \times C_3)) \rtimes C_2 \not\cong \text{Aut}(C)$, whereas the order of the automorphism group of the latter is 12.

### 3. Curves of Genus 5

Let $q = p^h$ where $h \in \mathbb{N}$ and $p$ is an odd prime. Let $a \in \mathbb{F}_{q^2}$ be such that

$$a^2 + 108 \neq 0.$$

We consider the following family of algebraic curves

$$C_a : Y^2 = X^{12} - aX^{10} - 33X^8 + 2aX^6 - 33X^4 - aX^2 + 1. \tag{10}$$

Let $F_a = \overline{\mathbb{F}}_p(x, y)$ with $y^2 = x^{12} - ax^{10} - 33x^8 + 2ax^6 - 33x^4 - ax^2 + 1$ be the corresponding function field. Let $G = \langle \alpha_1, \alpha_2 \rangle$, where $\alpha_1, \alpha_2$ are the following involutory automorphisms of $F_a$:

$$\alpha_1 : (x, y) \to (x, -y),$$

$$\alpha_2 : (x, y) \to (-x, y).$$

**Lemma 3.1.** Let $q = p^h$ where $h \in \mathbb{N}$ and $p$ is an odd prime. Let $a \in \mathbb{F}_{q^2}$. Then the curve $C_a$ defined as in (10) has genus 5 and it is hyperelliptic.
Proof. To prove the statement it is sufficient to observe that, if \( f(X) = X^{12} - aX^{10} - 33X^8 + 2aX^6 - 33X^4 - aX^2 + 1 \) then \( f(X) \) has multiple roots if and only if \( a^2 + 108 = 0 \) since the resultant of \( f(X) \) and its derivative \( f'(X) \) is equal to \((a^2 + 108)^8\). Now the claim follows from \cite[Proposition 3.7.3 and Corollary 3.7.4]{74}. \( \square \)

A decomposition of the Jacobian \( J_a \) of \( C_a \) is obtained applying Theorem 3.1 with respect to the automorphism group \( G = \langle \alpha_1, \alpha_2 \rangle \).

**Remark 3.2.** Since \( \alpha_1 \) is the hyperelliptic involution of \( C_a \), the fixed fields \( \text{Fix}\,G \) and \( \text{Fix}\,(\alpha_1) \) are both rational, see \cite[Theorem 11.98]{46}. More precisely, it is easily seen that \( \text{Fix}\,(\alpha_1) = \mathbb{F}_p(x) \) and \( \text{Fix}\,G = \mathbb{F}_p(x^2) \).

To apply Theorem 3.1 we need to compute the fixed fields of \( \langle \alpha_2 \rangle \) and \( \langle \alpha_3 \rangle = \langle \alpha_1 \alpha_2 \rangle \).

**Lemma 3.3.** Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_q^\ast \) with \( a^2 + 108 \neq 0 \). Then \( \text{Fix}\,(\alpha_2) = \mathbb{F}_p(\eta, \theta) \) where \( \eta = y, \theta = x^2 \) and

\[
\eta^2 = \theta^6 - a\theta^5 - 33\theta^4 + 2a\theta^3 - 33\theta^2 - a\theta + 1.
\]

In particular \( \text{Fix}\,(\alpha_2) \) is a hyperelliptic curve of genus 2.

**Proof.** The first assertion follows from the fact that \( x^2 \) is fixed by \( \alpha_2 \).

The polynomial \( f_1(X) = X^6 - aX^5 - 33X^4 + 2aX^3 - 33X^2 - aX + 1 \) has no multiple roots by Lemma 3.1. From \cite[Proposition 3.7.3 and Corollary 3.7.4]{74}, \( \text{Fix}\,(\alpha_2) \) is hyperelliptic of genus 2. \( \square \)

**Lemma 3.4.** Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_q^\ast \) with \( a^2 + 108 \neq 0 \) and let \( \alpha_3 = \alpha_1\alpha_2 \) so that \( \alpha_3 : (x, y) \to (-x, -y) \). Then \( \text{Fix}\,(\alpha_3) = \mathbb{F}_p(\rho, \theta) \) where \( \rho = xy, \theta = x^2 \) and

\[
\rho^2 = \theta^7 - a\theta^6 - 33\theta^5 + 2a\theta^4 - 33\theta^3 - a\theta^2 + \theta.
\]

In particular \( \text{Fix}\,(\alpha_3) \) is a hyperelliptic curve of genus 3.

**Proof.** Since \( \alpha_3 \) fixes both \( \theta \) and \( \rho \), we have \( \mathbb{F}_p(\theta, \rho) \subseteq \text{Fix}\,(\alpha_3) \). As the degree of the function field extension \( \mathbb{F}_p(x, y) : \mathbb{F}_p(\theta, \rho) \) is clearly 2, we have that \( \text{Fix}\,(\alpha_3) = \mathbb{F}_p(\theta, \rho) \). By Equation (10),

\[
\rho^2 = y^2\theta = (x^{12} - ax^{10} - 33x^8 + 2ax^6 - 33x^4 - ax^2 + 1)\theta = \theta^7 - a\theta^6 - 33\theta^5 + 2a\theta^4 - 33\theta^3 - a\theta^2 + \theta.
\]

Consider the polynomial \( f_2(X) = X^7 - aX^6 - 33X^5 + 2aX^4 - 33X^3 - aX^2 + X \). Then \( f_2(X) \) has no multiple roots over \( \mathbb{F}_p \) since the resultant of \( f_2(X) \) and \( f_2'(X) \) is equal to \((a^2 + 108)^4 \neq 0 \). From \cite[Proposition 3.7.3 and Corollary 3.7.4]{74}, \( \text{Fix}\,(\alpha_3) \) is a hyperelliptic function field of genus 3. \( \square \)

At this point, we get a first decomposition of the Jacobian of \( C_a \) as a straightforward application of Corollary 3.2.

**Corollary 3.5.** Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_q^\ast \) with \( a^2 + 108 \neq 0 \). Then the Jacobian variety \( J_a \) of the curve \( C_a \) defined in (10) decomposes as

\[
J_a \sim J_{a,2} \times J_{a,3},
\]
where \( J_{a,2} \) is the Jacobian variety of the hyperelliptic curve of genus 2

\[
C_{a,2} : Y^2 = X^6 - aX^5 - 33X^4 + 2aX^3 - 33X^2 - aX + 1,
\]

while \( J_{a,3} \) is the Jacobian variety of the hyperelliptic curve of genus 3

\[
C_{a,3} : Y^2 = X^7 - aX^6 - 33X^5 + 2aX^4 - 33X^3 - aX^2 + X.
\]

Now, a decomposition of the Jacobian \( J_{a,2} \) of the curve \( C_{a,2} \) whose function field is defined by Equation (11), is obtained by applying Theorem 1.1 to the automorphism group \( G_2 = \langle \beta_1, \beta_2 \rangle \) with

\[
\beta_1 : (\theta, \eta) \mapsto (\theta, -\eta),
\]

\[
\beta_2 : (\theta, \eta) \mapsto (1/\theta, \eta/\theta^3).
\]

It is easily seen that \( \beta_1, \beta_2 \in Aut(C_{a,2}) \) and that \( G_2 = \langle \beta_1, \beta_2 \rangle \) is elementary abelian of order 4. Also, since \( \beta_1 \) is the hyperelliptic involution of \( C_{a,2} \) we know that both \( Fix\langle \beta_1 \rangle = \mathbb{F}_p(\theta) \) and \( FixG_2 = \mathbb{F}_p(\theta + 1/\theta) \) are rational. We will prove that \( J_{a,2} \) decomposes completely as a power of the Jacobian of a unique elliptic curve. First, we compute the fixed fields of \( \langle \beta_2 \rangle \) and \( \langle \beta_3 \rangle = \langle \beta_1 \beta_2 \rangle \).

**Lemma 3.6.** Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_q^2 \) with \( a^2 + 108 \neq 0 \). Then \( Fix\langle \beta_2 \rangle = \mathbb{F}_p(\tilde{x}, \tilde{y}) \) where

\[
\tilde{y}^2 = 4\tilde{x}^3 + (a + 6)\tilde{x}^2 + (a - 6)\tilde{x} - 4.
\]

In particular \( Fix\langle \beta_2 \rangle \) is elliptic.

**Proof.** Let

\[
\tilde{x} = -\frac{(\theta - 1)^2}{(\theta + 1)^2} \quad \text{and} \quad \tilde{y} = -\frac{\eta}{(\theta + 1)^3}.
\]

Note that both \( \tilde{x} \) and \( \tilde{y} \) are fixed by \( \beta_2 \); also, the field extension \( \mathbb{F}_p(\theta, \eta) : \mathbb{F}_p(\tilde{x}, \tilde{y}) \) has degree 2, whence \( Fix\langle \beta_2 \rangle = \mathbb{F}_p(\tilde{x}, \tilde{y}) \). By Equation (11) \( \tilde{y}^2 = \tilde{x}^3 + \frac{a+6}{4}\tilde{x}^2 + \frac{a-6}{4}\tilde{x} - 1 \). The polynomial \( X^3 + \frac{a+6}{4}X^2 + \frac{a-6}{4}X - 1 \) has no multiple roots since \( (a^2 + 108) \neq 0 \) and hence \( Fix\langle \beta_2 \rangle \) is elliptic. The claim follows considering the isomorphism \( (\tilde{x}, \tilde{y}) \mapsto (\tilde{x}, \tilde{y}/2) \). \( \square \)

**Lemma 3.7.** Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_q^2 \) with \( a^2 + 108 \neq 0 \). Let \( \beta_3 = \beta_1 \beta_2 \) so that \( \beta_3 : (\theta, \eta) \mapsto (1/\theta, -\eta/\theta^3) \). Then \( Fix\langle \beta_3 \rangle = \mathbb{F}_p(\overline{x}, \overline{y}) \) where

\[
\overline{y}^2 = 4\overline{x}^3 + (-a + 6)\overline{x}^2 + (-a - 6)\overline{x} - 4.
\]

In particular \( Fix\langle \beta_3 \rangle \) is elliptic.

**Proof.** Let

\[
\overline{x} = -\frac{(\theta + 1)^2}{(\theta - 1)^2} \quad \text{and} \quad \overline{y} = \frac{\eta}{(\theta - 1)^3}.
\]

Then the proof is analogous to that of Lemma 3.6. \( \square \)
Remark 3.8. Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_{q^2} \) with \( a^2 + 108 \neq 0 \). Then the quotient curves \( \mathcal{C}_{a,2}/\langle \beta_2 \rangle \) and \( \mathcal{C}_{a,2}/\langle \beta_3 \rangle \) are \( \mathbb{F}_{q^2} \)-isomorphic. The isomorphism between the two curves is given by

\[
\varphi : (\bar{x}, \bar{y}) \mapsto (-\bar{x} - 1, \xi \bar{y}),
\]

where \( \xi^2 = -1 \).

At this point the complete decomposition of \( J_{a,2} \) follows by applying Corollary 3.5 to \( G_2 \).

Corollary 3.9. Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_{q^2} \) with \( a^2 + 108 \neq 0 \). Then the Jacobian variety \( J_{a,2} \) of the curve \( \mathcal{C}_{a,2} \) defined in (14) decomposes as \( J_{a,2} \sim J_{E_1}^2 \) where \( J_{E_1} \) is the Jacobian variety of the elliptic curve

\[
E_1 : Y^2 = 4X^3 + (a + 6)X^2 + (a - 6)X - 4.
\]

Furthermore, the Jacobian variety \( J_a \) of the curve \( \mathcal{C}_a \) defined in (10) decomposes as

\[
J_a \sim J_{E_1}^2 \times J_{a,3},
\]

where \( J_{a,3} \) is as in Corollary 3.2.

We proceed now with the complete decomposition of the Jacobian \( J_{a,3} \) of the curve \( \mathcal{C}_{a,3} \), whose function field \( \overline{\mathbb{F}}_p(\rho, \theta) \) is defined in Equation (12), by applying Theorem 1.1 with respect to the automorphism group \( G_3 = \langle \gamma_1, \gamma_2 \rangle \), where

\[
\gamma_1 : (\theta, \rho) \mapsto (\theta, -\rho),
\]

\[
\gamma_2 : (\theta, \rho) \mapsto (1/\theta, \rho/\theta^4).
\]

It is easily seen that \( \gamma_1, \gamma_2 \in \text{Aut}(\mathcal{C}_{a,3}) \) and that \( G_3 = \langle \gamma_1, \gamma_2 \rangle \) is elementary abelian of order 4. Since \( \gamma_1 \) is the hyperelliptic involution of \( \mathcal{C}_{a,c} \), both \( \text{Fix}(\gamma_1) = \overline{\mathbb{F}}_p(\theta) \) and \( \text{Fix}G_3 \) are rational. We first show that \( J_{a,3} \) decomposes as a product of the Jacobians of an elliptic curve and of a curve of genus 2.

Lemma 3.10. Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_{q^2} \) with \( a^2 + 108 \neq 0 \). Then \( \text{Fix}(\gamma_2) = \overline{\mathbb{F}}_p(\delta, \nu) \) where

\[
\nu^2 = \delta^3 - a\delta^2 - 36\delta + 4a.
\]

In particular \( \text{Fix}(\gamma_2) \) is elliptic.

Proof. Let \( \delta = (\theta^2 + 1)/\theta = \theta + 1/\theta = \theta + \gamma_2(\theta) \) and \( \nu = -\rho/\theta^2 \). Then \( \delta \) and \( \rho \) are fixed by \( \gamma_2 \) since \( \gamma_2(\delta) = \gamma_2(\theta) + \gamma_2^2(\theta) = \gamma_2(\theta) + \theta \) and \( \gamma_2(\nu) = (-\rho/\theta^4) \cdot \theta^2 = -\rho/\theta^2 = \nu \). Also from (12),

\[
\nu^2 = \frac{\rho^2}{\theta^4} = \frac{\theta^7 - a\theta^6 - 33\theta^5 + 2a\theta^4 - 33\theta^3 - a\theta^2 + \theta}{\theta^4} = \frac{\theta^6 - a\theta^5 - 33\theta^4 + 2a\theta^3 - 33\theta^2 - a\theta + 1}{\theta^3},
\]

whereas

\[
\delta^3 - a\delta^2 - 36\delta + 4a = \frac{(\theta^2 + 1)^3 - a\theta(\theta^2 + 1)^2 - 36\theta^2(\theta^2 + 1) + 4a\theta^3}{\theta^3} = \frac{\theta^6 - a\theta^5 - 33\theta^4 + 2a\theta^3 - 33\theta^2 - a\theta + 1}{\theta^3}.
\]
Remark 3.11. Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_{q^2} \) with \( a^2 + 108 \neq 0 \). Then the elliptic curves \( E_1 : Y^2 = 4X^3 + (a + 6)X^2 + (a - 6)X - 4 \) and \( C_{a,3}/\langle \gamma_2 \rangle : Y^2 = X^3 - a^2X^2 - 36X + 4a \) are \( \mathbb{F}_{q^2} \)-isomorphic through the birational morphism \( \varphi : E_1 \rightarrow C_{a,3}/\langle \gamma_2 \rangle \) given by
\[
\varphi(X, Y) \mapsto (-4X - 2, 4\xi Y),
\]
where \( \xi^2 = -1 \).

Lemma 3.12. Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_{q^2} \) with \( a^2 + 108 \neq 0 \). Let \( \gamma_3 = \gamma_1\gamma_2 \) so that \( \gamma_3 : (\theta, \rho) \mapsto (1/\theta, -\rho/\theta^4) \). Then \( \text{Fix}(\gamma_3) = \mathbb{F}_p(\delta, \epsilon) \) where
\[
eq (\delta - 4)(\delta^3 - a\delta^2 - 36\delta + 4a).
\]
In particular, \( \text{Fix}(\gamma_3) \) is hyperelliptic of genus 2.

Proof. Let \( \delta = (\theta^2 + 1)/\theta = \theta + \theta = \theta + \gamma_3(\theta) \) and \( \epsilon = (\theta^2\rho - \rho)/\theta^3 \). Then \( \delta \) and \( \epsilon \) are fixed by \( \gamma_3 \) since \( \gamma_3(\delta) = \gamma_3(\theta) + \gamma_3^3(\theta) = \gamma_3(\theta) + \theta \) and \( \gamma_3(\epsilon) = (-\rho/\theta^6 + \rho/\theta^4) \cdot \theta^3 = (-\rho + \rho\theta^2)/\theta^3 = \epsilon \). Using Equation (12) one can easily check that \( \epsilon^2 = \delta^5 - a\delta^4 - 40\delta^3 + 8a\delta^2 + 144\delta - 16a \) holds. Arguing as in the previous proofs, we have that \( \mathbb{F}_p(\delta, \epsilon) \) coincides with \( \text{Fix}(\gamma_3) \) and it is hyperelliptic of genus 2.

The following corollary summarizes the results obtained in this section so far.

Corollary 3.13. Let \( q = p^h \) where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let \( a \in \mathbb{F}_{q^2} \) with \( a^2 + 108 \neq 0 \). Then the Jacobian variety \( J_{a,3} \) of the curve \( C_{a,3} \) defined in (13) decomposes as \( J_{a,3} \sim J_{a,3,2} \times J_{E_1} \) where \( J_{E_1} \) is the Jacobian variety of the elliptic curve
\[
E_1 : Y^2 = 4X^3 + (a + 6)X^2 + (a - 6)X - 4,
\]
and \( J_{a,3,2} \) is the Jacobian variety of the genus 2 curve
\[
C_{a,3,2} : Y^2 = X^3 - a^2X^2 - 40X^3 + 8aX^2 + 144X - 16a.
\]
Furthermore, the Jacobian variety \( J_a \) of the curve \( C_a \) defined in (10) decomposes as
\[
J_a \sim J_{a,3} \times J_{a,3,2}.
\]
In the rest of the section we investigate the curve \( C_{a,3,2} \), whose function field is \( \mathbb{F}_q(\delta, \epsilon) \), where Equation (21) holds.

For \( k \in \mathbb{F}_p^*, k \neq \pm 2 \) and \( k \neq \pm 6 \), let \( \lambda = \frac{12 - k^2}{2k} \) and \( a = \frac{\lambda^3 - 36\lambda}{\lambda^2 - 4} \). Then, by straightforward computation
\[
\epsilon^2 = (\delta^2 - 4)(\delta - \lambda),
\]
and
\[
\psi_1(\delta, \epsilon) = \left( \frac{\lambda\delta + 12}{\delta - \lambda}, \frac{(-1)^i\mu\epsilon}{(\delta - \lambda)^3} \right).
\]
\( i = 0, 1 \), where \( \mu^2 = (\lambda^2 + 12)^3 \), which is elementary abelian of order 4. Note that \( \mu \in \mathbb{F}_{p^2} \), since \( \lambda^2 + 12 = \left( \frac{k^2 + 12}{2k} \right)^2 \) is a square in \( \mathbb{F}_{p^2} \).

The functions
\[
\frac{(\delta - \lambda)(\lambda^2 + 12) + (-1)^i \mu}{(\delta - \lambda)^2(\lambda^2 + 12)} \cdot \epsilon, \quad \frac{\delta^2 + 12}{\delta - \lambda}
\]
are fixed by \( \psi_i \).

By direct computations, the quotient curves \( C_{a,3,2} = C_{a,3,2}/\langle \psi_i \rangle \) have equations
\[
\left( \frac{1}{4} k^4 - 10k^2 + 36 \right) \epsilon^2 = \left( \frac{1}{4} k^4 - 10k^2 + 36 \right) \delta^3 + \left( \frac{1}{2} k^5 - 36k^3 + 264k \right) \delta^2 + \left( -32k^4 + 640k^2 \right) \delta + 512k^3;
\]
\[
\left( \frac{1}{4} k^5 - 10k^3 + 36k \right) \epsilon^2 = \left( \frac{1}{4} k^5 - 10k^3 + 36k \right) \delta^3 + \left( -22k^4 + 432k^2 - 864 \right) \delta^2 + \left( 640k^3 - 4608k \right) \delta - 6144k^2.
\]

It turns out that the two elliptic curves are isogenous over \( \mathbb{F}_{p^2} \) via the isogeny \( \varphi : C_{a,3,2}^0 \rightarrow C_{a,3,2}^1 \) with
\[
\varphi : (\delta, \epsilon) \mapsto \left( \frac{a_3 \delta^3 + a_2 \delta^2 + a_1 \delta + a_0}{(\delta + c)^2}, \frac{\delta \epsilon (b_2 \delta^2 + b_1 \delta + b_0)}{(\delta + c)^3} \right),
\]
where
\[
a_0 = -\frac{1536k}{(k^2 - 36)^2}, \quad a_1 = -\frac{3072k}{(k^2 - 36)k}, \quad a_2 = \frac{32}{k}, \quad a_3 = \frac{4}{k^2},
\]
\[
b_0 = \frac{-2048}{k^3 - 36k}, \quad b_1 = \frac{1536k^2}{k^3 - 36}, \quad b_2 = \frac{8}{k^3}, \quad c = -\frac{64k}{k^2 - 36}.
\]

Now we need to investigate whether \( C_{a,3,2}^0 \) and \( E_1 \) are isogenous or not. To this end, we will consider the theory of modular polynomials, for which we refer to [12] and the web database [13]. We proceed by arguing as in [72] Section 1.

Let \( \Phi_\ell \in \mathbb{Z}[X,Y] \) be the classical modular polynomial of degree \( \ell \). It parametrizes pairs of \( \ell \)-isogenous elliptic curves in terms of their \( j \)-invariants. More precisely, over a field \( \mathbb{F} \) of characteristic not equal to \( \ell \), the modular equation \( \Phi_\ell(j_1, j_2) = 0 \) holds if and only if \( j_1 \) and \( j_2 \) are the \( j \)-invariants of elliptic curves defined over \( \mathbb{F} \) that are related by a cyclic isogeny of degree \( \ell \).

Here, \( \mathbb{F} \) is a finite field \( \mathbb{F}_{p^2} \). Let \( \overline{j}(k) \), and \( \tilde{j}(k) \) be the \( j \)-invariants of \( C_{a,3,2}^0 \) and \( E_1 \), respectively, both expressed as a function of \( k \). We have
\[
\overline{j}(k) = \frac{(k^2 + 12)^3(k^6 - 60k^4 + 1200k^2 + 192)^3}{64(k^2 - 36)^2(k^2 - 4)^6k^2}, \quad \tilde{j}(k) = \frac{4(k^2 + 12)^6}{(k^2 - 36)^2(k^2 - 4)^2k^2}.
\]
We consider the case $\ell = 3$. The class of elliptic curves 3-isogenous to $E_1$ can be determined by computing (if any) the roots of $\Phi_3(Y) = \Phi_3(j(E_1), Y) \in \mathbb{F}_{p^2}[Y]$ over $\mathbb{F}_{p^2}$. Hence we search for $\overline{k} \in \mathbb{F}_{p^2}$ with $\Phi_3(j_\overline{k}), j(\overline{k})) = 0$ satisfying Condition [9].

We are not able a priori to decide whether the 3-isogeny is between $E_1$ and $C_{a,3,2}^0$ or its twists. So, the condition $\Phi_3(j_\overline{k}), j(\overline{k})) = 0$ ensures the existence of a 3-isogeny over $\mathbb{F}_{p^2}$ between $C_{a,3,2}^0$ and $E_1$. Thus we look for explicit descriptions of such 3-isogenies and check if they are defined over $\mathbb{F}_{p^2}$.

- $\overline{k}^2 = 36/5$. In this case the 3-isogeny between $C_{a,3,2}^0$ and $E_1$ is $(x, y) \mapsto \left(\frac{\psi_x}{\theta_x}, \frac{\psi_y}{\theta_y}\right)$, where

\[
\begin{align*}
\psi_x &= -360x^3\overline{k} + 2160x^3 + 14688x^2\overline{k} - 36288x^2 - 138240x\overline{k} + 331776x + 368640\overline{k} - 1105920; \\
\psi_y &= y(103680x^2\overline{k} - 124416x^2 - 1105920x^2\overline{k} + 6635520x^3 + 17694720\overline{x}y\overline{k} - 21233664x^2 - 17694720x\overline{k} + 106168320); \\
\theta_x &= 360x^3\overline{k} - 1296x^3 - 10368x^2 - 69120x\overline{k} + 82944x + 92160\overline{k} - 552960; \\
\theta_y &= -6480x^6\overline{k} + 12960x^6 - 103680x^5\overline{k} - 103680x^4\overline{k} - 6842880x^4 - 15482880x^3\overline{k} - 53084160x^3 - 225607680x^2\overline{k} - 79626240x^2 - 2548039680x - 1415577600\overline{k}.
\end{align*}
\]

- $\overline{k}^2 = -4/7$. In this case the 3-isogeny between $C_{a,3,2}^0$ and $E_1$ is $(x, y) \mapsto \left(\frac{\psi_x}{\theta_x}, \frac{\psi_y}{\theta_y}\right)$, where

\[
\begin{align*}
\psi_x &= 9756997844651904x^3\overline{k} + 1773999608118528x^3 - 23671355742557452x^2\overline{k} - 88881615135103896x^2 - 149484312145104132x\overline{k} + 93592177008289512x + 108081789310424734\overline{k} + 80629249554918068; \\
\psi_y &= 5y(3457479429497341193236434568000000x^4\overline{k} - 101419365985886720682687432800000x^4 - 15545163634077077821994778380160000x^3\overline{k} - 2826393388014011494535960961200000x^2\overline{k} - 11740672498801891719005038164803520x^2\overline{k} + 352140700050447457907472923900067776x^2 + 89750287397469588933863745055844520x\overline{k} + 4311238594702381782253416046625966x + 8638419263233382597513730705421100\overline{k} - 65824077521259664661193935638615080)/6; \\
\theta_x &= -9756997844651904x^3\overline{k} + 14445425380393728x^3 + 117767323565720640x^2\overline{k} + 35210297348410752x^2 + 76832921522684208x\overline{k} - 181553980415546592x - 164874109067025579\overline{k} - 3465731030990490; \\
\theta_y &= 5y(3457479429497341193236434568000000x^4\overline{k} - 101419365985886720682687432800000x^4 - 15545163634077077821994778380160000x^3\overline{k} - 2826393388014011494535960961200000x^2\overline{k} - 11740672498801891719005038164803520x^2\overline{k} + 352140700050447457907472923900067776x^2 + 89750287397469588933863745055844520x\overline{k} + 4311238594702381782253416046625966x + 8638419263233382597513730705421100\overline{k} - 65824077521259664661193935638615080)/6; \\
\theta_y &= 1201227138933933626787155527680000x^6\overline{k} + 463631527307833929454942849284928000x^6 + 58558963160486989619604042762240000x^5\overline{k} - 111920992422190876567021530009600000x^5 - 753377091175625014779032387560320000x^4\overline{k} - 1715858976054022531489199696468464000x^4 - 45534196356564626596557476985787040000x^3\overline{k} + 1538861603635221234136102831680000x^3 + 30930629429571752624793406954480000x^2\overline{k} + 374348928145257960497936027483040000x^2 + 274459963096197145160822714714460000x\overline{k} - 190005879817255112438950576291080920000x - 855848892852162349927591124235841875\overline{k} - 45599538718475703951502910235251250.
\end{align*}
\]
NEW EXAMPLES OF MAXIMAL CURVES WITH LOW GENUS

\[ \overline{k}^2 = 24k + 36. \] In this case the 3-isogeny between \( C_{a,32}^0 \) and \( E_1 \) is \((x, y) \mapsto (A(x), cyA'(x))\),

\[
A(x) = \frac{ax^3 + ay^2}{x^2 + b_2x^2 + b_1x + b_0}, \quad c^2 - 1/3c - 1/9 = 0, \quad \text{and}
\]

\[
\overline{k}a_3 + 2/7\overline{k} + 6/7a_3 = 0
\]
\[
a_2^2 + 276/5a_2 + 17424/25 = 0
\]
\[
a_1^2 - 384a_1 + 36864/5 = 0
\]
\[
a_0^2 + 512a_0 + 65536/5 = 0
\]
\[
b_2^2 - 12b_2 - 1584/5 = 0
\]
\[
b_1^2 - 192b_1 + 36864/5 = 0
\]
\[
b_0^2 + 256b_0 + 65536/5 = 0.
\]

\[ \overline{k}^2 = -24k + 36. \] In this case the 3-isogeny between \( C_{a,32}^0 \) and \( E_1 \) is \((x, y) \mapsto (A(x), cyA'(x))\),

\[
A(x) = \frac{ax^3 + ay^2}{x^2 + b_2x^2 + b_1x + b_0}, \quad c^2 - 1/3c - 1/9 = 0, \quad \text{and}
\]

\[
\overline{k}a_3 - 2/5\overline{k} - 6/5a_3 = 0
\]
\[
a_2^2 - 132a_2 + 11376/5 = 0
\]
\[
a_1^2 - 768a_1 + 589824/5 = 0
\]
\[
a_0^2 - 1024a_0 + 1048576/5 = 0
\]
\[
b_2^2 + 48b_2 - 144 = 0.
\]

We summarize all the results about the curve \( C_a \) in the following theorem.

**Theorem 3.14.** Let \( q = p^h \), where \( h \in \mathbb{N} \) and \( p \) is an odd prime. Let

\[
a = \frac{-k^6 + 180k^4 - 2160k^2 + 1728}{2k^5 - 80k^3 + 288k} \in \mathbb{F}_{q^2}, \quad k \in \mathbb{F}_{q^2}, \quad a^2 + 108 \neq 0.
\]

If \( k^2 = 36/5, k^2 = -4/7, \) or \( k^2 = \pm 24k^2 + 36, \) then \( a \in \mathbb{F}_{p^2} \) and the Jacobian variety \( J_a \) of the curve \( C_a \) defined in (10) is \( \mathbb{F}_{p^2} \)-isogenous to the fifth power of the Jacobian variety \( J_{E_1} \) of the elliptic curve

\[
E_1 : Y^2 = 4X^3 + (a + 6)X^2 + (a - 6)X - 4.
\]

In particular, there exist infinitely many primes \( p \) such that \( C_a \) is either maximal or minimal over \( \mathbb{F}_{p^2} \).

**Proof.** We only need to prove that there exists a fixed elliptic curve \( E \) defined over \( \mathbb{Q} \) such that \( E_1 \) and \( E \) are \( \mathbb{F}_{p^2} \)-isogenous for any \( p \). This is clear since the \( j \)-invariant of \( E_1 \) is a rational number. \( \Box \)

Using the software MAGMA [9] we determined all the primes \( p \) less than 100000 such that one of the above conditions on \( \overline{k} \in \mathbb{F}_p \) is satisfied and \( E_1 \) is \( \mathbb{F}_{p^2} \)-maximal.

**Theorem 3.15.** For \( a \) and \( p \) as in Tables [1] [3] [4] [5] the curve \( C_a \) defined in (15) is \( \mathbb{F}_{p^2} \)-maximal.
Table 1. Values $a \in \mathbb{F}_p$ for which $C_{a,3}$ defined in (15) is $\mathbb{F}_p^2$-maximal ($k^2 = 36/5$)

<table>
<thead>
<tr>
<th>$p$</th>
<th>$a$</th>
<th>$p$</th>
<th>$a$</th>
<th>$p$</th>
<th>$a$</th>
<th>$p$</th>
<th>$a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>0</td>
<td>131</td>
<td>75</td>
<td>251</td>
<td>221</td>
<td>491</td>
<td>254</td>
</tr>
<tr>
<td>1439</td>
<td>984</td>
<td>3371</td>
<td>933</td>
<td>5639</td>
<td>4445</td>
<td>5879</td>
<td>1294</td>
</tr>
<tr>
<td>7079</td>
<td>6366</td>
<td>8039</td>
<td>4751</td>
<td>8291</td>
<td>5367</td>
<td>9839</td>
<td>7465</td>
</tr>
<tr>
<td>11171</td>
<td>5951</td>
<td>12119</td>
<td>4310</td>
<td>14879</td>
<td>2439</td>
<td>16931</td>
<td>14808</td>
</tr>
<tr>
<td>18839</td>
<td>17890</td>
<td>23039</td>
<td>5286</td>
<td>23159</td>
<td>16126</td>
<td>25919</td>
<td>24335</td>
</tr>
<tr>
<td>53411</td>
<td>49474</td>
<td>53639</td>
<td>10108</td>
<td>59051</td>
<td>25275</td>
<td>69371</td>
<td>51864</td>
</tr>
<tr>
<td>74891</td>
<td>48023</td>
<td>75239</td>
<td>47655</td>
<td>81119</td>
<td>7710</td>
<td>81359</td>
<td>48587</td>
</tr>
</tbody>
</table>

Table 2. Values $a \in \mathbb{F}_p$ for which $C_{a,3}$ defined in (15) is $\mathbb{F}_p^2$-maximal ($k^2 = -4/7$)

<table>
<thead>
<tr>
<th>$p$</th>
<th>$a$</th>
<th>$p$</th>
<th>$a$</th>
<th>$p$</th>
<th>$a$</th>
<th>$p$</th>
<th>$a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>0</td>
<td>23</td>
<td>0</td>
<td>71</td>
<td>45</td>
<td>263</td>
<td>185</td>
</tr>
<tr>
<td>1283</td>
<td>1276</td>
<td>1583</td>
<td>207</td>
<td>2039</td>
<td>1586</td>
<td>2087</td>
<td>752</td>
</tr>
<tr>
<td>2843</td>
<td>2158</td>
<td>7823</td>
<td>2710</td>
<td>9851</td>
<td>6895</td>
<td>10859</td>
<td>7298</td>
</tr>
<tr>
<td>15647</td>
<td>4803</td>
<td>18719</td>
<td>9865</td>
<td>23459</td>
<td>17387</td>
<td>25463</td>
<td>14115</td>
</tr>
<tr>
<td>27791</td>
<td>27198</td>
<td>29759</td>
<td>25238</td>
<td>31511</td>
<td>30573</td>
<td>32579</td>
<td>25335</td>
</tr>
<tr>
<td>34283</td>
<td>3491</td>
<td>35099</td>
<td>20799</td>
<td>37619</td>
<td>25640</td>
<td>54959</td>
<td>54405</td>
</tr>
<tr>
<td>61007</td>
<td>47142</td>
<td>61559</td>
<td>42225</td>
<td>67043</td>
<td>32831</td>
<td>71339</td>
<td>1126</td>
</tr>
<tr>
<td>89783</td>
<td>68842</td>
<td>95027</td>
<td>9806</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3. Values $a \in \mathbb{F}_p$ for which $C_{a,3}$ defined in (15) is $\mathbb{F}_p^2$-maximal ($k^2 = 24k + 36$)

<table>
<thead>
<tr>
<th>$p$</th>
<th>$a$</th>
<th>$p$</th>
<th>$a$</th>
<th>$p$</th>
<th>$a$</th>
<th>$p$</th>
<th>$a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>0</td>
<td>131</td>
<td>56</td>
<td>251</td>
<td>221</td>
<td>491</td>
<td>237</td>
</tr>
<tr>
<td>1439</td>
<td>455</td>
<td>3371</td>
<td>2438</td>
<td>5639</td>
<td>1194</td>
<td>5879</td>
<td>1294</td>
</tr>
<tr>
<td>7079</td>
<td>713</td>
<td>8039</td>
<td>3288</td>
<td>8291</td>
<td>2924</td>
<td>9839</td>
<td>7465</td>
</tr>
<tr>
<td>11171</td>
<td>5951</td>
<td>12119</td>
<td>4310</td>
<td>14879</td>
<td>12440</td>
<td>16931</td>
<td>2123</td>
</tr>
<tr>
<td>18839</td>
<td>17890</td>
<td>23039</td>
<td>5286</td>
<td>23159</td>
<td>7033</td>
<td>25919</td>
<td>24335</td>
</tr>
<tr>
<td>53411</td>
<td>3937</td>
<td>53639</td>
<td>10108</td>
<td>59051</td>
<td>33776</td>
<td>69371</td>
<td>51864</td>
</tr>
<tr>
<td>74891</td>
<td>48023</td>
<td>75239</td>
<td>27584</td>
<td>81119</td>
<td>7710</td>
<td>81359</td>
<td>48587</td>
</tr>
</tbody>
</table>

4. A characterization in terms of automorphism groups

In this section we extend to the positive characteristic case a characterization of curves with equation (10) in terms of their automorphism group, provided by Shaska in [70]. Let $q = p^h$ where $h \in \mathbb{N}$ and $p$ is an odd prime. Let $a \in \mathbb{F}_{q^2}$ with $a^2 + 108 \neq 0$. Denote by $\overline{\mathbb{F}}_p$ the algebraic closure of $\mathbb{F}_{q^2}$. We consider the family of algebraic curves $C_a$ as described in (10).
We know that \( g(C_a) = 5 \), \( C_a \) is hyperelliptic and that the hyperelliptic involution is
\[
\alpha_1 : (X, Y) \mapsto (X, -Y).
\]

Our first aim is to show that \( \text{Aut}(C_a) \) admits a subgroup \( H \) with \( H \cong A_4 \times C_2 \cong \text{SmallGroup}(24, 13) \) where \( A_4 \) denotes the alternating group in 4 letters. Then we prove that if \( \mathcal{X}_5 \) is an hyperelliptic curve of genus 5 admitting an automorphism group isomorphic to \( H \) then \( \mathcal{X} \) is \( \mathbb{F}_p \)-birationally equivalent to a curve \( C_a \) in (10).

Let \( i \in \mathbb{F}_q^2 \) with \( i^2 = -1 \). Consider the following map
\[
\beta : (X, Y) \mapsto \left( \frac{X - i}{X + i}, \frac{8iY}{(X + i)^6} \right).
\]

It is easily seen that \( \beta \in \text{Aut}(C_a) \). Also, \( \beta \) has order 3. Involutory automorphisms of \( C_a \) are described as follows:

\[
\alpha_2 : (X, Y) \mapsto (-X, Y) \quad \text{and} \quad \alpha_3 : (X, Y) \mapsto \left( \frac{1}{X^6}, \frac{Y}{X} \right).
\]

The group generated by \( \alpha_1, \alpha_2, \) and \( \alpha_3 \) is an elementary abelian group of order 8.

To show that \( H_1 = \langle \alpha_2, \beta \rangle \cong A_4 \) and that \( \alpha_1 \not\in H_1 \), we first observe that
\[
\beta^{-1} \alpha_2 \beta = \alpha_3.
\]

Then \( \beta \) normalizes the elementary abelian group of order 4 generated by \( \alpha_2 \) and \( \alpha_3 \). This implies that \( H_1 \cong (C_2 \times C_2) \rtimes C_3 \cong A_4 \). Also, \( \alpha_1 \not\in \langle \alpha_2, \alpha_3 \rangle \) yields \( \alpha_1 \not\in H_1 \). This proves that \( \text{Aut}(C_a) \) contains a subgroup \( H = \langle H_1, \alpha_1 \rangle = H_1 \times \langle \alpha_1 \rangle \cong A_4 \times C_2 \cong \text{SmallGroup}(24, 13) \).

Assume now that, for an odd prime \( p \), \( \mathcal{X}_5 \) is a hyperelliptic curve of genus 5 defined over a finite field of characteristic \( p \) admitting an automorphism group \( H \cong A_4 \times C_2 \). Our aim is to prove that \( \mathcal{X}_5 \) is \( \mathbb{F}_p \)-birationally equivalent to a curve belonging to the family in (10).

The curve \( \mathcal{X}_5 \) admits an affine model
\[
\mathcal{X}_5 : Y^2 = F(X) = \prod_{i=1}^{12} (X - \gamma_i),
\]
where the points \( P_i = (\gamma_i, 0), i = 1, \ldots, 12 \), are the Weierstrass points of \( \mathcal{X}_5 \); see [74, Proposition 6.2.3] and [46, Theorem 11.98]. Let \( \mathbb{F}_p(x, y) \) be the function field of \( \mathcal{X}_5 \). The hyperelliptic involution

\begin{table}
\begin{tabular}{|c|c|c|c|c|c|c|c|c|c|c|}
\hline
\( p \) & \( a \) & \( p \) & \( a \) & \( p \) & \( a \) & \( p \) & \( a \) & \( p \) & \( a \) \\
\hline
11 & 0 & 131 & 56 & 251 & 30 & 491 & 237 & 599 & 24 \\
1439 & 455 & 3371 & 933 & 5639 & 4445 & 5879 & 4585 & 6971 & 4842 \\
7079 & 6366 & 8039 & 3288 & 8291 & 2924 & 9839 & 2374 & 10799 & 1835 \\
11171 & 5220 & 12119 & 4310 & 14879 & 2439 & 16931 & 14808 & 17159 & 12471 \\
18839 & 17890 & 23039 & 5286 & 23159 & 16126 & 25919 & 1584 & 50291 & 5355 \\
53411 & 3937 & 53639 & 10108 & 59051 & 33776 & 69371 & 17507 & 74771 & 11482 \\
74891 & 48023 & 75239 & 27584 & 81119 & 73409 & 81359 & 32772 & & \\
\hline
\end{tabular}
\end{table}

Table 4. Values \( a \in \mathbb{F}_p \) for which \( C_{a,3} \) defined in (15) is \( \mathbb{F}_p^2 \)-maximal \((k^2 = -24k + 36)\).
\( \alpha_1 \in H \) is \( \alpha_1 : (X,Y) \mapsto (X,-Y) \) and its fixed field is \( \mathbb{F}_p(x) \). The fixed points of \( \alpha_1 \) on \( \mathcal{X}_5 \) are exactly \( P_i, i = 1, \ldots, 12 \).

Let \( \overline{H} = H/\langle \alpha_1 \rangle \cong \mathbb{A}_4 \leq \text{PGL}(2, \mathbb{F}_p) \). From \cite[Theorem 1]{[1]} (see also \cite[Theorem A.8]{[2]}), any subgroup of \( \text{PGL}(2, \mathbb{F}_p) \) which is isomorphic to \( \mathbb{A}_4 \) is conjugated to \( \overline{H} \) in \( \text{PGL}(2, \mathbb{F}_p) \). This means that up to conjugation we can assume that \( \overline{H} \), seen as an automorphism group of the rational function field \( \mathbb{F}_p(x) \), is generated by the following maps

\[
\theta_1 : x \mapsto -x, \quad \text{and} \quad \theta_2 : x \mapsto \frac{x-i}{x+i},
\]

where \( i^2 = -1 \).

**Lemma 4.1.** The subgroup \( H_1 \) of \( H \) with \( H_1 \cong \mathbb{A}_4 \) acts sharply transitively on the set of Weierstrass points of \( \mathcal{X}_5 \).

**Proof.** Since \( H_1 \) is an automorphism group of \( \mathcal{X}_5 \), it acts on the set \( W \) of its Weierstrass points. Since the stabilizer in \( Aut(\mathcal{X}_5) \) of a point \( P \in W \) is cyclic from \cite[Lemma 11.44]{[2]} and clearly contains \( \alpha_1 \) we deduce that the 3 involutions in \( H_1 \) fix no points on \( W \). Suppose that \( H_1 \) does not act transitively on \( W \). Then the stabilizer \( H_{1,P} \) of \( P \) has order 3. A nontrivial element \( \delta \in H_{1,P} \) fixes at least three points of \( W \), since the number of fixed points must be congruent to 0 modulo 3. Consider the element \( \overline{\delta} \) induced by \( \delta \) on \( Aut(\mathcal{X}_5/\langle \alpha_1 \rangle) \). Each point \( \overline{P} \) lying under a fixed point of \( \delta \) in \( W \) is fixed by \( \overline{\delta} \). On the other hand, by \cite[Theorem 11.14 (d)]{[2]}, \( \overline{\delta} \) fixes exactly 2 points on \( \mathcal{X}_5/\langle \alpha_1 \rangle \), a contradiction. \( \Box \)

**Theorem 4.2.** Let \( p \) be an odd prime and let \( \overline{\mathbb{F}}_p \) be the algebraic closure of \( \mathbb{F}_p \). Let \( \mathcal{X}_5 : Y^2 = F(X) \) be an hyperelliptic curve of genus 5 defined over \( \overline{\mathbb{F}}_p \) and let \( \alpha_1 \) denote its hyperelliptic involution. If \( \mathcal{X}_5 \) admits an automorphism group \( H \cong \mathbb{A}_4 \times C_2 \) with \( \overline{H} = H/\langle \alpha_1 \rangle \cong \mathbb{A}_4 \) then \( \mathcal{X}_5 \) is \( \mathbb{F}_p \)-birationally equivalent to a curve \( \mathcal{C}_a \) given in \cite{[10]}. If in addition \( \mathcal{X}_5 \) is defined over a finite field \( \mathbb{F}_q \) with \( q \equiv 1 \pmod{4} \) and admits at least an \( \mathbb{F}_q \)-rational Weierstrass point \( P = (t,0) \), then \( \mathcal{X}_5 \) is \( \mathbb{F}_q \)-birationally equivalent to \( \mathcal{C}_a \).

**Proof.** Without loss of generality assume that \( \text{deg}(F(x)) = 12 \). Lemma 4.1 shows that the roots of \( F(X) \) form an orbit under the action of an automorphism group of \( \overline{\mathbb{F}}_p(x) \) isomorphic to \( \mathbb{A}_4 \), namely \( \overline{H} = H/\langle \alpha_1 \rangle \). Then there is an automorphism \( \gamma \) of \( \overline{\mathbb{F}}_p(x) \) such that

\[
\gamma \overline{H} \gamma^{-1} = \langle \theta_1, \theta_2 \rangle.
\]

Hence \( \gamma \) maps the roots of \( F(X) \) to an orbit \( \Omega \) under the action of \( \langle \theta_1, \theta_2 \rangle \). If \( t \) is a point in \( \Omega \), then \( \Omega \) consists of

\[
t, \quad \theta_1(t) = -t, \quad \theta_2(t) = \frac{t-i}{t+i}, \quad \theta_2(t) = \frac{t+1}{t-1}, \quad \theta_1 \theta_2(t) = \frac{-t-i}{t+i}, \quad \theta_2 \theta_1(t) = \frac{t+i}{t-i}, \quad \theta_1 \theta_2 \theta_1(t) = \frac{-t+i}{t-i}, \quad \theta_2 \theta_1 \theta_2(t) = \frac{t-i}{t+i}, \quad \theta_1 \theta_2 \theta_1 \theta_2(t) = \frac{-t+i}{t-i}.
\]

\[
\theta_2 \theta_1 \theta_2 \theta_1(t) = \frac{-t-1}{t+1}, \quad \theta_1 \theta_2 \theta_1 \theta_2(t) = \frac{i t+1}{t-1}, \quad \theta_1 \theta_2 \theta_1 \theta_2(t) = \frac{i t-1}{t+1}, \quad \theta_2 \theta_1 \theta_2 \theta_1(t) = \frac{-1}{t}, \quad \theta_1 \theta_2 \theta_1 \theta_2 \theta_1 \theta_2(t) = \frac{1}{t}.
\]
Label these values with $z_1, \ldots, z_{12}$. Then $G(X) := \prod_{i=1}^{12} (X - z_i)$ coincides with

$$X^{12} + \frac{-t^{12} + 33t^8 + 33t^4 - 1}{t^{10} - 2t^6 + t^2} x^{10} - 33X^8 + 2 \frac{t^{12} - 33t^8 - 33t^4 + 1}{t^{10} - 2t^6 + t^2} X^6 - 33X^4 + \frac{-t^{12} + 33t^8 + 33t^4 - 1}{t^{10} - 2t^6 + t^2} X^2 + 1,$$

Since the roots of $F(X)$ are mapped to the roots of $G(X)$ by an automorphism of $\mathbb{F}_p(x)$, the curve $\mathcal{X}_5$ is birationally equivalent to that of equation $Y^2 = G(X)$, which clearly belongs to the family described in [10] for

$$a = \frac{t^{12} - 33t^8 - 33t^4 + 1}{t^{10} - 2t^6 + t^2} = \frac{t^{12} - 33t^8 - 33t^4 + 1}{t^2(t^4 - 1)^2}.$$

Note that if $q \equiv 1 \pmod{4}$ then the group $H$ is defined over $\mathbb{F}_q$ and $\overline{H}$ is conjugated to $\langle \theta_1, \theta_2 \rangle$ in $\text{PGL}(2, q)$; see [16] Theorem A.8. This implies that if the curve $\mathcal{X}_5$ admits a Weierstrass point $(t, 0)$ which is $\mathbb{F}_q$-rational then $\mathcal{X}_5$ is isomorphic over $\mathbb{F}_q$ to a curve of type $C_a$ in [10].

5. OTHER EXAMPLES OF MAXIMAL CURVES

In this section we investigate other examples of maximal curves.

**Definition 5.1.** Let $p$ be an odd prime and $b \in \mathbb{F}_p$. We denote by $U_{p,b}$ the curve of the affine equation

$$(25) \quad x^6 + y^6 + 1 + bx^2y^2 = 0.$$

**Proposition 5.2.** Let $p \geq 5$, then $U_{p,b}$ has genus $10$ and $\text{Jac}(U_{p,b}) \cong_{\mathbb{F}_p^2} E_1^3 \times E_2^3 \times E_3^3 \times E_4^3$, where

$$E_1 : y^2 = x^3 + 3(b + 6)x^2 + 3(b + 3)(b + 12)x + 27(b + 3)^2,$$
$$E_2 : y^2 = x^3 - 3^3b^2x^2 + 2^33^3b(b^3 + 27)x - 3^32^4(b^3 + 27)^2,$$
$$E_3 : y^2 = x^3 + 2bx^2 + b^2x - 2^2,$$
$$E_4 : y^2 = x^3 - 48b^2x^2 + 768b(b^3 + 27)x - 4096(b^3 + 27)^2.$$

**Proof.** By [51] Proposition 10], $\text{Jac}(U_{p,b}) \cong_{\mathbb{F}_p^2} H_1^3 \times H_2 \times \text{Jac}(H_3)^3$, where

$$H_1 : y^2 = (-(b - 3)x + 3)(1 - 3x(1 - x)),$$
$$H_2 : x^3 + y^3 + 1 + bxy = 0,$$
$$H_3 : y^2 = -(x^3 + bx^2 + 4)(x^3 + 1).$$

By [16] Page 27], for $G_a : y^2 = (x^3 + ax^2 - 4)(-16x^3 + 16)$, $a \in \mathbb{F}_p$, we have that $\text{Jac}(G_a) \cong_{\mathbb{F}_p^2} E'_3 \times E'_4$, where

$$E'_3 : y^2 = x^3 - a/2 + a^2/16 - 1/16,$$
$$E'_4 : y^2 = 16(a^3 - 27)x^3 - 48a^2x^2 + 48ax - 16.$$
This shows that $\text{Jac}(H_3) \cong_{\mathbb{F}_p^2} E_3 \times E_4$. Finally, it turns out that $H_1$ is birational to $E_1$, $H_2$ is birational to $E_2$. Then the claim follows. □

**Proposition 5.3.** The curve $U_{p,b}$ in (25) is $\mathbb{F}_{p^2}$-maximal when

$$(p, b) \in \{(89, 58), (101, 96), (131, 100), (191, 116), (227, 69), (239, 94), (251, 3)\}.$$

**Proof.** Direct computations done using the package MAGMA [9] for $p \leq 251$. □

**ACKNOWLEDGMENTS**

The research of D. Bartoli and M. Giulietti was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). D. Bartoli was supported by Università degli Studi di Perugia - Fondo ricerca di base Esercizio 2015 - Project: Codici Correttori di Errori. M. Giulietti was supported by Università degli Studi di Perugia - Fondo ricerca di base Esercizio 2015 - Project: Geometrie di Galois, Curve Algebriche su campi finiti e loro Applicazioni. M. Kawakita was partially supported by JSPS Grant-in-Aid for Scientific Research (C) 17K05344.

**REFERENCES**


NEW EXAMPLES OF MAXIMAL CURVES WITH LOW GENUS


NEW EXAMPLES OF MAXIMAL CURVES WITH LOW GENUS


Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, via Vanvitelli 1, 06123 Perugia, Italy
E-mail address: daniele.bartoli@unipg.it

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, via Vanvitelli 1, 06123 Perugia, Italy
E-mail address: massimo.giulietti@unipg.it

Division of Mathematics, Shiga University of Medical Science, Seta Tsukinowa-cho, Otsu City, Shiga, 520-2192 Japan
E-mail address: kawakita@belle.shiga-med.ac.jp

Department of Applied Mathematics and Computer Science, Technical University of Denmark, Asmussens All, 2800 Kgs. Lyngby, Denmark
E-mail address: marimo@dtu.dk