$\mathbb{F}_{p^2}$-MAXIMAL CURVES WITH MANY AUTOMORPHISMS ARE GALOIS-COVERED BY THE HERMITIAN CURVE

DANIELE BARTOLI, MARIA MONTANUCCI, AND FERNANDO TORRES

ABSTRACT. Let $\mathbb{F}$ be the finite field of order q^2, $q = p^h$ with p prime. It is commonly atribute to J.P. Serre the fact that any curve $\mathbb{F}$-covered by the Hermitian curve $\mathcal{H}_{q+1}$: $y^{q+1} = x^q + x$ is also $\mathbb{F}$-maximal. Nevertheless, the converse is not true as the Giulietti-Korchmáros example shows provided that $q > 8$ and $h \equiv 0 \pmod 3$. In this paper, we show that if an $\mathbb{F}$-maximal curve $\mathcal{X}$ of genus $g \geq 2$ where $q = p$ is such that $|\mathrm{Aut}(\mathcal{X})| > 84(g-1)$ then $\mathcal{X}$ is Galois-covered by $\mathcal{H}_{p+1}$. Also, we show that the hypothesis on the order of $\mathrm{Aut}(\mathcal{X})$ is sharp, since there exists an $\mathbb{F}$-maximal curve $\mathcal{X}$ for $q = 71$ of genus $g = 7$ with $|\mathrm{Aut}(\mathcal{X})| = 84(7-1)$ which is not Galois-covered by the Hermitian curve $\mathcal{H}_{72}$.

1. Introduction

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

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

A basic obstruction here is given by the well-known Ihara's bound $g \leq q(q-1)/2$ (see [20]); by Rück and Stichtenoth [30] this bound is sharp as equality holds if and only if $\mathcal{X}$ is isomorphic to the Hermitian curve over $\mathbb{F}$, namely the plane curve $\mathcal{H}_{q+1} : y^{q+1} = x^q + 1$. Further examples of maximal curves arise from $\mathbb{F}$-subcovers of $\mathbb{F}$-maximal curves, which is a result commonly attributed to J.P. Serre (see [23]). Concrete examples which all are dominated by $\mathcal{H}_{q+1}$ can be found e.g. in [13, 4, 28, 25].

However, not every maximal curve arises in this way as the Giulietti-Korchmáros curve (currently referred as the GK-curve) shows [16] (see also [33]). Any of these examples occurs whenever $q = p^{3h} > 8$, where p a prime. In this paper we investigate the existence of similar examples for $q = p$. Our main result is the following.

Theorem 1.1. *Let p be a prime and $\mathbb{F} = \mathbb{F}_{p^2}$ the finite fields of order p^2. Let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve with genus $g = g(\mathcal{X}) \geq 2$, and $\mathrm{Aut}(\mathcal{X})$ the $\mathbb{F}$-automorphism group of $\mathcal{X}$. If*

2010 Math. Subj. Class.: Primary 11G; Secondary 14G.
Keywords: Finite field, maximal curve, Hermitian curve, Galois-covering.

$|\mathrm{Aut}(\mathcal{X})| > 84(g-1)$ *then* $\mathcal{X}$ *is Galois-covered by the Hermitian curve* $\mathcal{H}_{p+1} : y^{p+1} = x^p + x$ *over* $\mathbb{F}$.

Furthermore we show that the bound on the size of $\mathrm{Aut}(\mathcal{X})$ in the main theorem is sharp. In fact, the following remark is considered in Section 6.

Remark 1.2. The hypothesis $|\mathrm{Aut}(\mathcal{X})| > 84(g-1)$ in the main theorem is necessary. In fact, let $\mathbb{F} = \mathbb{F}_{71^2}$ and let $\mathcal{F}$ be the *Fricke-Macbeath curve* which by definition is the non-singular model over $\mathbb{F}$ of the plane curve

$$1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0\,.$$

We will see that $\mathcal{F}$ is an $\mathbb{F}$-maximal curve with $g = g(\mathcal{F}) = 7$ and $\mathrm{Aut}(\mathcal{F}) = PSL(2,8)$; thus $|\mathrm{Aut}(\mathcal{F})| = 504 = 84(7-1)$ but $\mathcal{F}$ is not Galois-covered by the Hermitian curve $\mathcal{H}_{72}$.

2. Preliminary results

Let $\mathcal{X}$ be a curve defined over the finite field $\mathbb{F} = \mathbb{F}_{q^2}$ of order q^2 with $q = p^h$ a power of a prime p. Let $\mathrm{Aut}(\mathcal{X})$ be the $\mathbb{F}$-automorphism group of $\mathcal{X}$. For $m \geq 1$ a divisor of $q+1$, we let $\mathcal{H}_m$ denote the non-singular model of the plane curve

$$y^m = x^q + x\,.$$

Notice that $\mathcal{H}_{q+1}$ is the aforementioned Hermitian curve. We start by recalling two characterizations of $\mathcal{H}_m$; the first one, involving automorphisms of curves, is due to Garcia and Tafazolian [14, Thm. 5.2] (see also [34, Thm, 4.1]).

Theorem 2.1. *Let* $\mathcal{X}$ *be an* $\mathbb{F}$*-maximal curve. Suppose that there exists an abelian subgroup* H *of* $\mathrm{Aut}(\mathcal{X})$ *whose order equals* q *such that the quotient curve* $\mathcal{X}/H$ *is rational. Then there exists a divisor* m *of* $q+1$ *such that* $\mathcal{X}$ *is* $\mathbb{F}$*-isomorphic to the curve* $\mathcal{H}_m$ *above.*

The second characterization of $\mathcal{H}_m$ that we shall point out here is given in terms of the Weierstrass semigroup at certain $\mathbb{F}$-rational point of $\mathcal{H}_m$ (e.g. the unique point $P_\infty \in \mathcal{H}_m$ over $x = \infty$); see Garcia et al. [11, Thm. 5.2].

Theorem 2.2. *Let* $\mathcal{X}$ *be an* $\mathbb{F}$*-maximal curve. Suppose that there is a non-gap* m *at a point* $P \in \mathcal{X}(\mathbb{F})$ *such that* m *is a divisor of* $q+1$*. Then* $\mathcal{X}$ *is* $\mathbb{F}$*-isomorphic to* $\mathcal{H}_m$.

Lemma 2.3. *The curve* $\mathcal{H}_m$ *above is Galois-covered by the Hermitian curve* $\mathcal{H}_{q+1}$*. Also,* $\mathrm{Aut}(\mathcal{H}_m)$ *contains a cyclic subgroup* C_m *of order* m *such that* $\mathrm{Aut}(\mathcal{H}_m)/C_m \cong PGL(2,q)$ *and hence* $|\mathrm{Aut}(\mathcal{H}_m)| > 84(g-1)$*, where* $g = g(\mathcal{H}_m)$.

Proof. Let Σ and Σ' be the corresponding $\mathbb{F}$-function fields of $\mathcal{H}_{q+1}$ and $\mathcal{H}_m$ respectively. Clearly Σ' is $\mathbb{F}$-covered by Σ, because of the morphism $\varphi : (x,y) \mapsto (x, y^{(q+1)/m})$; also, $[\Sigma : \Sigma'] = (q+1)/m$. Consider the $\mathbb{F}$-automorphism group G of Σ given by

$$G = \{\varphi_\lambda : (x,y) \mapsto (x, \lambda y) \mid \lambda^{(q+1)/m} = 1\}\,,$$

which is of order $(q+1)/m$. Then the quotient function field Σ/G equals Σ', as the functions x and $y^{(q+1)/m}$ are fixed by G and $|G| = [\Sigma : \Sigma']$. The claim on the structure of $\mathrm{Aut}(\mathcal{H}_m)$ follows from [19, Thm. 12.11]. □

Let $\mathcal{X}$ be a curve over $\mathbb{F}$ of genus $g = g(\mathcal{X})$, G a subgroup of $\mathrm{Aut}(\mathcal{X})$ and $P \in \mathcal{X}$; recall that an *orbit under* G (resp. a *stabilizer in* G) of P is the set $G(P) := \{\tau(P) : \tau \in G\}$ (resp. $G_P := \{\tau \in G : \tau(P) = P\}$). The orbit $G(P)$ is either *short* or *long* provided that $|G_P| > 1$ or not. A short orbit $G(P)$ is either *tame* or *non-tame* according to $p \nmid |G_P|$ or not, where p is the characteristic of $\mathbb{F}$.

The following theorem gives the exact structure of the short orbits under G for which the classical Hurwitz bound $|G| \leq 84(g(\mathcal{X}) - 1)$ does not hold; see [19, Thm 11.56] and [19, Thm 11.126].

Theorem 2.4. *Let $\mathcal{X}$ be curve over $\mathbb{F}$ of genus $g \geq 2$ and let $G \leq \mathrm{Aut}(\mathcal{X})$ with $|G| > 84(g-1)$. Then the quotient curve $\mathcal{X}/G$ is rational and there are at most three short orbits under G as follows*:

1. *Exactly three short orbits, two tame and one non-tame. Each point in the tame short orbits has stabilizer in G of order 2;*
2. *Exactly two short orbits, both non-tame;*
3. *Only one short orbit which is non-tame;*
4. *Exactly two short orbits, one tame and one non-tame. In this case $|G| < 8g^3$, with the following exceptions*:
   - *$p = 2$ and $\mathcal{X}$ is isomorphic to the hyperelliptic curve $y^2 + y = x^{2^k+1}$ with genus 2^{k-1};*
   - *$p > 2$ and $\mathcal{X}$ is isomorphic to the Roquette curve $y^2 = x^q - x$ with genus $(q-1)/2$;*
   - *$p \geq 2$ and $\mathcal{X}$ is isomorphic to the Hermitian curve $y^{q+1} = x^q + x$ with genus $(q^2 - q)/2$;*
   - *$p = 2$, $q_0 = 2^s$, $q = 2q_0^2$ and $\mathcal{X}$ is isomorphic to the Suzuki curve $y^q + y = x^{q_0}(x^q + x)$ with genus $q_0(q-1)$.*

The following lemma will be used to ensure that a Sylow p-subgroup of a non-tame automorphism group of a $\mathbb{F}$-maximal curve $\mathcal{X}$ fixes exactly an $\mathbb{F}_{p^2}$-rational point of $\mathcal{X}$.

Lemma 2.5. ([17, Prop. 3.8, Thm. 3.10]) *Let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve of genus $g \geq 2$. Then the automorphism group $\mathrm{Aut}(\mathcal{X})$ fixes the set $\mathcal{X}(\mathbb{F})$ of $\mathbb{F}$-rational points. Also, automorphisms of $\mathcal{X}$ over the algebraic closure of $\mathbb{F}$ are always defined over $\mathbb{F}$.*

The following result follows as a corollary of the previous lemma.

Corollary 2.6. *For $q = p^h$, let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve with $g(\mathcal{X}) \geq 2$ such that $p \mid |\mathrm{Aut}(\mathcal{X})|$, and let S be a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$. Then S fixes exactly one point*

$P \in \mathcal{X}(\mathbb{F})$ and acts semiregularly on the set of the remaining $\mathbb{F}$-rational points of $\mathcal{X}$. In particular, if $p \nmid g$, every $\sigma \in S$ has order at most equal to q.

Proof. From Lemma 2.5, S acts on the set $\mathcal{X}(\mathbb{F})$ of $\mathbb{F}$-rational points of $\mathcal{X}$. Since $|\mathcal{X}(\mathbb{F}_{p^2})| \equiv 1 \mod p$, S must fix at least a point $P \in \mathcal{X}(\mathbb{F}_{q^2})$. Also, $\mathcal{X}$ has zero p-rank and hence the claim follows from [19, Lemma 11.129]. □

The following lemma provides a characterization of the Hermitian curve $\mathcal{H}_{p+1}$ in terms of the order of a Sylow p-subgroup of its full automorphism group.

Lemma 2.7. *Let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve of genus $g > 0$ with $\mathbb{F}$ of order p^2, where p is a prime. Suppose that there exists $G \leq \mathrm{Aut}(\mathcal{X})$ such that $p \mid |G|$. Then we can write*

$$g = \frac{a_1(p-1)}{2} + a_2 p \,, \tag{2.1}$$

where a_1 is a non-negative integer such that ${G_P}^{(a_1+1)}$ is the last non-trivial ramification group at a point $P \in \mathcal{X}$ and $a_2 = g(\mathcal{X}/H)$, where H is a subgroup of G of order p. Also, $p^2 \nmid |G|$ unless $\mathcal{X}$ is $\mathbb{F}$-isomorphic to the Hermitian curve $\mathcal{H}_{p+1}$.

Proof. Let $H \leq G$ with $|H| = p$. From Corollary 2.6, H has exactly one fixed point P which is $\mathbb{F}$-rational. Clearly H acts semiregularly on $\mathcal{X}(\mathbb{F}) \setminus \{P\}$ and so $|H| \mid (p^2 + 2gp)$. From the Riemann-Hurwitz formula

$$2g - 2 = p(2a_2 - 2) + (a_1 + 2)(p - 1) \,,$$

and hence

$$g = \frac{p(2a_2 - 2) + (a_1 + 2)(p-1) + 2}{2} = \frac{a_1(p-1)}{2} + a_2 p \,.$$

If $\mathcal{X} \cong \mathcal{H}_{p+1}$, there is nothing to prove; thus we assume that $\mathcal{X} \ncong \mathcal{H}_{p+1}$. From [30], this implies that $p^2 + 2gp < p^2 + p^2(p-1) = p^3$, as $2g < p(p-1)$. Thus, if S is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$ containing H, either $|S| = p^2$ or $S = H$. Assume that $|S| = p^2$. From the Riemann-Hurwitz formula

$$2g - 2 = p^2(2g(\mathcal{X}/S) - 2) + (a_1 + 2)(p^2 - 1) + a_3 p(p-1) \,,$$

for some non-negative integer a_3. In fact, if $i, j \geq 1$ are such that $G_P^{(i+1)} \neq G_p^{(i)}$ and $G_P^{(j+1)} \neq G_p^{(j)}$ then $i - j \equiv 0 \mod p$; see [19, Lemma 11.75 (v)]. Thus,

$$p(p-1) > 2g = 2g(\mathcal{X}/S)p^2 + a_1(p^2 - 1) + a_3 p(p-1) \,.$$

By direct checking, since a_1, a_3 and $g(\mathcal{X}/S)$ are non-negative, this implies that $g(\mathcal{X}/S) = a_1 = a_3 = 0$ and hence $g = 0$, a contradiction. □

In the following Lemma the known results on $\mathbb{F}_{q^2}$-maximal curves of high genus are collected; see [20, 30, 11, 12, 24],

Lemma 2.8. *Let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve of genus g, where $\mathbb{F} = \mathbb{F}_{q^2}$.*

(1) *$g \leq q(q-1)/2$. If the equality holds, then $\mathcal{X}$ is $\mathbb{F}_{q^2}$-isomorphic to the Hermitian curve $\mathcal{H}_{q+1}$;*
(2) *$g \leq (q-1)^2/4$ if $g < q(q-1)/2$;*
(3) *If q is odd and $g = (q-1)^2/4$, then $\mathcal{X}$ is $\mathbb{F}_{q^2}$-isomorphic to $\mathcal{X}_{(q+1)/2} : y^{(q+1)/2} = x^q + x$. If q is even and $g = q(q-2)/4$, then $\mathcal{X}$ is $\mathbb{F}$-isomorphic to the non-singular model of $y^{q+1} = x^{q/2} + \ldots + x$. Also, $\mathcal{X}$ is a cyclic quotient of the Hermitian curve $\mathcal{H}_{q+1}$ of order 2;*
(4) *If $g < \lfloor (q-1)^2/4 \rfloor$, then $g \leq \lfloor (q^2-q+4)/6 \rfloor$.*

The following result can be obtained as an application of Lemma 2.8.

Corollary 2.9. *Let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve with $\mathbb{F} = \mathbb{F}_{p^2}$, $p \geq 7$ a prime. Write $g = g(\mathcal{X})$ using the notation of Lemma 2.7. Suppose that one of the following conditions holds for g:*

(1) *$a_1 > \lfloor (p^2-p+4)/3(p-1) \rfloor$,*
(2) *$a_2 > \lfloor (p^2-p+4)/6p \rfloor$,*
(3) *$a_1 + a_2 \geq (p-1)/2$ but $a_2 \leq \lfloor (p^2-p+4)/6p \rfloor$.*

Then $\mathcal{X}$ is Galois-covered by the Hermitian curve $\mathcal{H}_{p+1}$.

Proof. If (1) or (2) holds then $g > \lfloor (p^2-p+4)/6 \rfloor$, and the claim follows from (3) and (4) of Lemma 2.8. Assume that $a_1 + a_2 \geq (p-1)/2$ but $a_2 \leq \lfloor (p^2-p+4)/6p \rfloor$. Then $a_1 \geq \lceil (p-1)/2 - (p^2-p+4)/6p \rceil = \lceil (2p^2-2p+4)/6p \rceil = (p-1)/3$. Hence, $g \geq (p-3)(p-1)/6 + p > (p^2-p+4)/6$, and the claim follows again from (3) and (4) of Lemma 2.8. □

3. Proof of Theorem 1.1

3.1. **$\mathbb{F}_{p^2}$-maximal curves with $p \leq 5$.** We prove that for $p \leq 5$ *every* $\mathbb{F}_{p^2}$-maximal curve is Galois-covered by the Hermitian curve $\mathcal{H}_{p+1}$ over $\mathbb{F}_{p^2}$. For $p = 2$ and $p = 3$ the result is trivial by Lemma 2.8), while for $p = 5$ it can be obtained as a direct application of the complete classification, up to isomorphism, of $\mathbb{F}_{25}$-maximal curves in [8].

Lemma 3.1. *Let $\mathcal{X}$ be an $\mathbb{F}_{25}$-maximal curve. Then $\mathcal{X}$ is Galois-covered by the Hermitian curve $\mathcal{H}_6$.*

Proof. Denote by $\mathbf{M}(5) := \{g \mid \text{there exists an } \mathbb{F}_{25} - \text{maximal curve of genus } g\}$. From [8, Thm. 11], [11, Thm. 3.1] and [36, Thm. 1], $\mathbf{M}(5) = \{0,1,2,3,4,10\}$ where

(1) $g(\mathcal{X}) = 10$ if and only if $\mathcal{X} \cong \mathcal{H}_5 : y^6 = x^5 + x$ over $\mathbb{F}_{25}$,
(2) $g(\mathcal{X}) = 4$ if and only if $\mathcal{X} \cong \mathcal{Y}_4 : y^3 = x^5 + x$ over $\mathbb{F}_{25}$,
(3) $g(\mathcal{X}) = 3$ if and only if $\mathcal{X} \cong \mathcal{Y}_3 : y^6 = x^5 + 2x^4 + 3x^3 + 4x^2 + 3xy^3$ over $\mathbb{F}_{25}$,
(4) $g(\mathcal{X}) = 2$ if and only if $\mathcal{X} \cong \mathcal{Y}_2 : y^2 = x^5 + x$ over $\mathbb{F}_{25}$,

(5) $g(\mathcal{X})=1$ if and only if $\mathcal{X}\cong\mathcal{Y}_1 : x^3+y^3+1=0$ over $\mathbb{F}_{25}$.

The curves given in (2) and (4) are covered by the Hermitian curve $\mathcal{H}_6 : y^6=x^5+x$, because of the morphisms $(x,y)\mapsto(x,y^{6/n})$ with $n=2,3$ respectively. The covers $\mathcal{H}_6|\mathcal{Y}_4$ and $\mathcal{H}_6|\mathcal{Y}_2$ are Galois, and the Galois groups are given by

$$G_4=\langle\alpha\rangle,\quad \text{where}\quad \alpha(x,y)=(x,\lambda y),\quad \text{with}\quad \lambda^2=1\,,$$

$$G_2=\langle\beta\rangle,\quad \text{where}\quad \beta(x,y)=(x,\gamma y),\quad \text{with}\quad \gamma^3=1,$$

respectively. Also the curve given in (5) is Galois covered by the Hermitian curve $\mathcal{H}_6$. To show this, take $\mathcal{H}_6$ in its Fermat plane model $\mathcal{H}_6 : x^6+y^6+1=0$, and consider its automorphisms group

$$G=\{\alpha_{a,b}(x,y)=(ax,by)\mid a^2=b^2=1\}\cong\mathbb{Z}_2\times\mathbb{Z}_2\,.$$

By direct checking $\mathcal{Y}_1$ is fixed by G and since $[\mathcal{H}_5:\mathcal{Y}_1]=4=|G|$, we have that $\mathcal{Y}_1=\mathcal{H}_6/G$. To prove that $\mathcal{Y}_3$ is Galois-covered by $\mathcal{H}_6$, since $\mathcal{Y}_3$ is the unique $\mathbb{F}_{25}$-maximal curve of genus 3 up to isomorphism over $\mathbb{F}_{25}$, it is sufficient to construct a quotient curve of $\mathcal{H}_6$ of genus 3. The claim follows considering the plane curve

$$\mathcal{Z}:\quad x^5+y+2x^2y^2+xy^5=0\,.$$

From [4, Prop. 2.1], the curve $\mathcal{Z}$ equals $\mathcal{H}_6/H$ where $H\le \mathrm{Aut}(\mathcal{H}_6)$ is a subgroup of order 3 of a Singer group of order 21. □

3.2. **$\mathbb{F}_{p^2}$-maximal curves with $p\ge 7$.** We will show that every $\mathbb{F}_{p^2}$-maximal curve $\mathcal{X}$ is Galois-covered by the Hermitian curve $\mathcal{H}_{p+1}$ whenever one of the following short-orbits structures under $\mathrm{Aut}(\mathcal{X})$ holds true,

- exactly three short orbits, two tame and one non-tame; each point in the tame short orbits has stabilizer in $\mathrm{Aut}(\mathcal{X})$ of order 2,
- exactly two short orbits, both non-tame,
- only one short orbit which is non-tame,
- exactly two short orbits, one tame and one non-tame,

In this way the proof of Theorem 1.1 follows from Theorem 2.4. In particular, our aim is to prove that the assumption on the short-orbits structure of $\mathrm{Aut}(\mathcal{X})$ implies the existence of a subgroup S of $\mathrm{Aut}(\mathcal{X})$ with $|S|=p$ such that the quotient curve $\mathcal{X}/S$ is rational. Therefore Theorem 1.1 follows from Theorem 2.2 and Lemma 2.3. By Lemma 2.3 we have the following corollary.

Corollary 3.2. *Let p be a prime and $\mathbb{F}=\mathbb{F}_{p^2}$. Let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve with $g=g(\mathcal{X})\ge 2$, and $\mathrm{Aut}(\mathcal{X})$ the $\mathbb{F}$-automorphism group of $\mathcal{X}$. Then $|\mathrm{Aut}(\mathcal{X})|>84(g-1)$ if and only if $\mathcal{X}$ is $\mathbb{F}$-isomorphic to the plane curve $\mathcal{H}_m : y^m=x^p+x$ for some divisor m of $p+1$.*

We note that Corollary 3.2 appears to be an improvement of [17, Thm. 3.16], where the authors show that if $\mathcal{X}$ is an $\mathbb{F}_{p^2}$-maximal curve with $g = g(\mathcal{X}) \geq 2$, and $|\mathrm{Aut}(\mathcal{X})| > \max\{84(g-1), g^2\}$ then $\mathcal{X}$ is isomorphic to $\mathcal{X}_m : y^m = x^p - x$ for some divisor m of $p+1$. Since the curve $\mathcal{X}_m$ is not $\mathbb{F}_{p^2}$-maximal for every divisor m of $p+1$ their result represents a necessary condition.

We now proceed with a case-by-case analysis on the short-orbits structures listed above.

Lemma 3.3. *An $\mathbb{F}_{p^2}-$maximal curve $\mathcal{X}$ whose full automorphism group admits exactly one non-tame short orbit O_1 and two tame short orbits O_2 and O_3 does not exist.*

Proof. Since from Theorem 2.4 $\mathrm{Aut}(\mathcal{H}_{p+1})$ has just two short orbits, we have that $\mathcal{X}$ is not isomorphic to $\mathcal{H}_{p+1}$. In particular, from Lemma 2.7 $p \mid |\mathrm{Aut}(\mathcal{X})|$ but $p^2 \nmid |\mathrm{Aut}(\mathcal{X})|$. Let H be a p-Sylow subgroup of $\mathrm{Aut}(\mathcal{X})$. From Corollary 2.6 H fixes exactly an $\mathbb{F}_{p^2}$-rational point $P \in O_1$ and acts semiregularly in $O_1 \setminus \{P\}$. Thus we have that $|O_1| = 1 + np$ for some $n \geq 0$. From the Riemann-Hurwitz formula

$$2g-2 = |\mathrm{Aut}(\mathcal{X})|(2 \cdot 0 - 2) + (1+np)[(|\mathrm{Aut}(\mathcal{X})|/(1+np) - 1)$$
$$+(a_1+1)(p-1)] + \frac{|\mathrm{Aut}(\mathcal{X})|}{2}[(2-1)+(2-1)],$$

and hence

$$2g - 2 = (1+np)(a_1 p + p - a_1 - 2)\,. \tag{3.1}$$

We now assume that $n > 0$. From Lemma 2.8 we have that $2g < p(p-1)$ as $\mathcal{X}$ is not isomorphic to $\mathcal{H}_{p+1}$. Thus, by direct checking, Equality (3.1) yields $n = 1$ and $a_1 = 0$. In this case $2p(p-1) - 2 > 2g - 2 = (p+1)(p-2) = 2p(p-1) - 2$, a contradiction. This yields that $n = 0$ and $\mathrm{Aut}(\mathcal{X})$ fixes a point $P \in \mathcal{X}$. From (3.1) and (2.1)

$$a_1(p-1) + 2a_2 p - 2 = 2g - 2 = a_1(p-1) + (p-2)\,.$$

Since this implies that $2a_2 p = p$, we have a contradiction. □

Lemma 3.4. *An $\mathbb{F}_{p^2}-$maximal curve whose full automorphism group admits exactly two non-tame short orbits O_1 and O_2 does not exist.*

Proof. From Corollary 2.6 we know that the fixed points of the Sylow p-subgroups of $\mathrm{Aut}(\mathcal{X})$ lie on $\mathcal{X}(\mathbb{F}_{p^2})$, and hence O_1 and O_2 are contained in $\mathcal{X}(\mathbb{F}_{p^2})$. Also, as before, the size of each non-tame short orbit of $\mathrm{Aut}(\mathcal{X})$ is congruent to 1 modulo p.

The size of the set $\mathcal{X}(\mathbb{F}_{p^2}) \setminus O_1$ is congruent to $0 \pmod p$. As also $O_2 \subsetneq \mathcal{X}(\mathbb{F}_{p^2})$ has length congruent to $1 \pmod p$ and $|\mathrm{Aut}(\mathcal{X})| \equiv 0 \pmod p$ we have a contradiction. □

Lemma 3.5. *Let $\mathcal{X}$ be an $\mathbb{F}_{p^2}-$maximal curve and assume that* $\mathrm{Aut}(\mathcal{X})$ *has exactly one non-tame short orbit O_1. Then $\mathcal{X}$ is Galois-covered by $\mathcal{H}_{p+1}$.*

Proof. We can assume that for every Sylow p-subgroup H of $\mathrm{Aut}(\mathcal{X})$, the quotient curve $\mathcal{X}/H$ is not rational; otherwise, the claim follows from Theorem 2.1. In particular, this implies that $a_2>0$ in (2.1). As before, write $|O_1|=1+np$ for $n\geq 0$. From [19, Lemma 11.111] we have that $|O_1|$ divides $2g-2$. Since the unique short orbit of $\mathrm{Aut}(\mathcal{X})$ must be contained in $\mathcal{X}(\mathbb{F}_{p^2})$ then either $\mathcal{X}(\mathbb{F}_{p^2})=O_1$ or $\mathcal{X}(\mathbb{F}_{p^2})=O_1\cup(\bigcup_{i=1}^t\tilde{O}_i)$ where $|\tilde{O}_i|=|\mathrm{Aut}(\mathcal{X})|$ for $t\geq 1$. Clearly the first case is not possible as $p^2+1+2gp>2g-2$. Assume that $\mathcal{X}(\mathbb{F}_{p^2})=O_1\cup(\bigcup_{i=1}^t\tilde{O}_i)$ where $|\tilde{O}_i|=|\mathrm{Aut}(\mathcal{X})|$ for $t\geq 1$. This case can occur only if $|O_1|$ is a divisor of $p^2+1+2gp$ and $2g-2$, that is, only if $|O_1|$ is a divisor of $(p+1)^2$ which is congruent to 1 modulo p. This implies that either $|O_1|=(p+1)^2$ or $|O_1|=p+1$ or $|O_1|=1$.

- If $|O_1|=(p+1)^2$ then from Lemma 2.8 we have that $p(p-1)-2>2g-2\geq(p+1)^2$, a contradiction.
- If $|O_1|=1$, then from the Riemann-Hurwitz formula
$$2g-2=|\mathrm{Aut}(\mathcal{X})|(-2)+[|\mathrm{Aut}(\mathcal{X})|-1+(a_1+1)(p-1)]\,,$$
and hence from (2.1)
$$2a_2p-p=-|\mathrm{Aut}(\mathcal{X})|\,,$$
a contradiction to $a_2>0$.
- Assume that $|O_1|=(p+1)$. Since $\mathrm{Aut}(\mathcal{X})$ has no other short orbits, we have that $(p+1)\mid p^2+1+2gp-(p+1)$ and hence $(p+1)\mid(a_1+1)(p-1)+2a_2p$. By direct computation this implies that $(p+1)\mid 2a_1+2a_2+2$. In particular $a_1+a_2\geq\frac{p-1}{2}$, while $1\leq a_2\leq\frac{p^2-p+4}{6p}$. The claim now follows from Lemma 2.9.

□

Lemma 3.6. *Let $\mathcal{X}$ be an $\mathbb{F}_{p^2}$-maximal curve whose full automorphism group admits exactly one non-tame short orbit O_1 and one tame short orbit O_2. Then $\mathcal{X}$ is Galois-covered by $\mathcal{H}_{p+1}$.*

Proof. As before, we can assume that for every Sylow p-subgroup H of $\mathrm{Aut}(\mathcal{X})$ the quotient curve $\mathcal{X}/H$ is not rational, otherwise the claim follows from Theorem 2.1. In particular, this implies that $a_2>0$ in (2.1). Assume that $|O_1|=1+np$ for $n\geq 0$.

Case 1: $\mathcal{X}(\mathbb{F}_{p^2})=O_1\cup O_2$.

From the Riemann-Hurwitz formula
$$2g-2=|\mathrm{Aut}(\mathcal{X})|(-2)+(1+np)\Big[(a_1+1)(p-1)+\frac{|\mathrm{Aut}(\mathcal{X})|}{1+np}-1\Big]$$
$$+(p^2+1+2gp-1-np)\Big(\frac{|\mathrm{Aut}(\mathcal{X})|}{p^2+1+2gp-1-np}-1\Big)\,,$$
and hence
$$2g-2=(1+np)[(a_1+1)(p-1)-1]-(p^2+(2g-n)p)\,.$$
Using (2.1) this reduces to
$$2a_2(p+1)=(a_1+1)(n-1)(p-1)\,.$$

Since $a_2>0$ and $(p-1,p+1)=2$, we have that $a_2\geq (p-1)/4$ and hence $g\geq p(p-1)/2$. The claim now follows.

Case 2: $\mathcal{X}(\mathbb{F}_{p^2})=O_1$.

For $P\in O_2$ let $|\mathrm{Aut}(\mathcal{X})_P|=hp$, where $(h,p)=1$. Then $h\leq 4a_2+2$, as h is the order of a cyclic group in $\mathcal{X}/H$, where H is a p-group of order p; see [19, Thm. 11.60]. Let $Q\in O_2$. From the Riemann-Hurwitz formula

$$2g-2=-2ph|O_1|+|O_1|((hp-1)+(a_1+1)(p-1))+|O_2|(|\mathrm{Aut}(\mathcal{X})|/|O_2|-1)\,;$$

or equivalently

$$|\mathrm{Aut}(\mathcal{X})|=2(g-1)\frac{|\mathrm{Aut}(\mathcal{X})_P|\cdot|\mathrm{Aut}(\mathcal{X})_Q|}{N}\,,$$

where $N=|\mathrm{Aut}(\mathcal{X})_Q|(-1+(a_1+1)(p-1))-|\mathrm{Aut}(\mathcal{X})_P|\geq 1$; see [19, (11.67) and (11.68)]. This yields $-1/|\mathrm{Aut}(\mathcal{X})_Q|\geq -(-1+(a_1+1)(p-1))/(hp+1)$ and hence

$$\frac{2g-2}{ph|O_1|}=-\frac{1}{|\mathrm{Aut}(\mathcal{X})_Q|}+\frac{(a_1+1)(p-1)-1}{hp}\geq\frac{(a_1+1)(p-1)-1}{hp(hp+1)}\,.$$

Thus,

$$\frac{1}{hp^2}\geq\frac{2g-2}{2hgp^2}\geq\frac{2g-2}{ph|O_1|}\geq\frac{(a_1+1)(p-1)-1}{hp(hp+1)}\,.$$

From the last inequalities, using $h\leq 4a_2+2$, we get that $(4a_2+2)p+1\geq hp+1\geq a_1p^2+p^2-a_1p-2p)$ and hence

$$a_2\geq\frac{a_1p^2+p^2-a_1p-4p-1}{4p}\geq\frac{p^2-4p-1}{4p}\,,$$

while

$$g\geq\frac{p(p^2-4p-1)}{4p}>g_3\,.$$

If $p\geq 11$ this gives a contradiction from [11]. If $p=7$, then g is not bigger than g_3 if and only if $a_1=0$. But since we are assuming that $a_2\geq 1$, then $g\geq 7=g_3$. The claim now follows from [9, Thm. 5].

Case 3: $\mathcal{X}(\mathbb{F}_{p^2})$ contains O_1 and at least a long orbit of $\mathrm{Aut}(\mathcal{X})$.

A case-by-case analysis is considered according to $n=0$, $n=1$ or $n>1$.

Assume that $n=0$**.** In this case $O_1=\{P\}$ and $\mathrm{Aut}(\mathcal{X})_P=\mathrm{Aut}(\mathcal{X})$. From the Riemann-Hurwitz formula

$$2g-2=-2|\mathrm{Aut}(\mathcal{X})|+(a_1+1)(p-1)+|\mathrm{Aut}(\mathcal{X})|-1+|O_2|(|\mathrm{Aut}(\mathcal{X})|/|O_2|-1)\,.$$

Since this implies that

$$2a_2p-p=-|O_2|\,,$$

we have a contradiction to $a_2>0$.

Assume that $n = 1$**.** From the Riemann-Hurwitz formula

$$2g-2 = -2|\mathrm{Aut}(\mathcal{X})|+(p+1)(|\mathrm{Aut}(\mathcal{X})|/(p+1)-1+(a_1+1)(p-1))+|O_2|(|\mathrm{Aut}(\mathcal{X})|/|O_2|-1)\,,$$

and hence from (2.1)

$$|O_2| = p(a_1+1)(p-1) - 2a_2p\,.$$

The length $|O_2|$ must divide $p^2 + 2gp - p$.

If O_2 is not contained in $\mathbb{F}_{p^2}$ then also $(p+1) \mid p^2 + 1 + 2gp - (p+1)$ and hence $(p+1) \mid (a_1+1)(p-1)+2a_2p$ and it divides $|\mathrm{Aut}(\mathcal{X})|$. By direct computation this implies that $(p+1) \mid 2a_1 + 2a_2 + 2$. In particular $a_1 + a_2 \geq \frac{p-1}{2}$ and so the claim follows from Lemma 2.9.

If O_2 is contained in $\mathcal{X}(\mathbb{F}_{p^2})$ then $p^2+1+2gp-(p+1)-|O_2|$ must be positive and $|O_2|$ divides $p^2+1+2gp-(p+1)-|O_2| = 2a_2p(p+1)$. Also, $|O_2/p| = (a_1+1)(p-1)-2a_2$ divides $p+2g-1 = (a_1+1)(p-1)+2a_2p-1 = |O_2|/p+2a_2+2a_2p-1$. This implies that $|O_2|/p$ divides both $2a_2(p+1)-1$ and $2a_2p(p+1)$ and hence $|O_2| = p$. In particular $(a_1+1)(p-1)-2a_2 = 1$ and $a_2 \geq (p-2)/2$. Since this implies that $g \geq p(p-2)/2$ the claim follows.

Assume that $n > 1$**.** From the Riemann-Hurwitz formula

$$2g-2 = -2|\mathrm{Aut}(\mathcal{X})|$$
$$+(1+np)\Big(\frac{|\mathrm{Aut}(\mathcal{X})|}{1+np} - 1 + (a_1+1)(p-1)\Big) + |O_2|\Big(\frac{|\mathrm{Aut}(\mathcal{X})|}{|O_2|} - 1\Big)\,,$$

and hence

$$|O_2| = p[-2a_2 - n + 1 + n(a_1+1)(p-1)]\,.$$

Since $|O_2|$ is a divisor of $p(p+2g-n)$ we have that $|O_2| \leq (p^2-np)/2 + gp$ and

$$\frac{p^2-p+4}{6} \geq g_3 \geq g \geq \frac{(1+np)(-1+(a_1+1)(p-1))}{p+2} - \frac{p^2-np}{2(p+2)} + \frac{2}{p+2}\,,$$

which implies

$$n \leq \Big\lfloor \frac{p^3+4p^2-4p+8-6a_1(p-1)}{6p^2-9p+6a_1p^2-6a_1p} \Big\rfloor\,. \tag{3.2}$$

In particular we get that $a_1 < p/6$ and $n < (p+6)/6$.

Assume that O_2 is not contained in $\mathcal{X}(\mathbb{F}_{p^2})$. As $1+np$ divides $p^2+1+2gp-1-np = p(p+2g-n)$ and hence $p+2g-n = p(1+a_1+2a_2)-a_1-n$, write $p(1+a_1+2a_2)-a_1-n = \alpha(1+np)$. Then $\alpha \equiv -a_1 - n \pmod p$ and since $a_1 < p/6$, $n < (p+6)/6$ and $\alpha \leq p$, we get $\alpha = p - a_1 - n$. Thus,

$$p(1+a_1+2a_2) - a_1 - n = (p-a_1-n)(1+np)\,,$$

and hence

$$\frac{p}{2} = \frac{p}{6} + \frac{2p}{6} \geq a_1 + 2a_2 = n(p-a_1-n) \geq \frac{2p}{2} = p\,,$$

a contradiction.

Thus, we can assume that O_1 and O_2 are both contained in $\mathcal{X}(\mathbb{F}_{p^2})$.

Since $1+np$ divides $p^2-np+2gp-|O_2|$, we have in particular that $1+np$ divides $p+(1-n)a_1(p-1)+2a_2(p+1)+n$ and hence

$$n \leq 1+\frac{2a_2(p+1)}{(p-1)(a_1+1)}\,. \tag{3.3}$$

Write $k(1+np)=p+(1-n)a_1(p-1)+2a_2(p+1)+n$. Thus $k \equiv (n-1)a_1+2a_2+n \pmod p$ and $k \leq p$ as $p+(1-n)a_1(p-1)+2a_2(p+1)+n < p+\frac{p}{3}(p+1)+\frac{p+6}{6} = (2p^2+9p+6)/6 < p(1+2p) \leq p(1+np)$. We observe that from $a_2 \leq p/6$ and (3.3),

$$\begin{aligned}(n-1)a_1+2a_2+n &\leq \frac{2a_2(p+1)a_1}{(p-1)(a_1+1)}+2a_2+1+\frac{2a_2(p+1)}{(p-1)(a_1+1)}\\ &\leq \frac{2a_2(p+1)}{(p-1)}+2a_2+1 \leq \frac{2a_2(2p)}{p-1}+1 < p+1\,,\end{aligned}$$

and hence $k=(n-1)a_1+2a_2+n$ with

$$((n-1)a_1+2a_2+n)(1+np) = p+(1-n)a_1(p-1)+2a_2(p+1)+n\,.$$

Thus $(n-1)((n+1)(a_1+1)+2a_2)=0$, which is impossible for $(n+1)(a_1+1)+2a_2 \geq 5$ and $n \neq 1$. □

At this point, a natural question arises: is any $\mathbb{F}_{p^2}$-maximal curve $\mathcal{X}$ of genus g Galois-covered by $\mathcal{H}_{p+1}$ also when $|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1)$? The hypothesis $|\mathrm{Aut}(\mathcal{X})| > 84(g-1)$, more precisely the structure of the short orbits given by Theorem 2.4, is necessary to obtain that $\mathcal{X} \cong \mathcal{H}_m$ for some m. Nevertheless is not difficult to find examples of $\mathbb{F}_{p^2}$-maximal curves $\mathcal{X}$ of genus g and $|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1)$ which are Galois-covered by $\mathcal{H}_{p+1}$.

Example 3.7. The curve $\mathcal{X}$ given by the affine model over $\mathbb{F}=\mathbb{F}_{49}$

$$y^8 = x^4 - x^2\,,$$

is $\mathbb{F}$-maximal with $g=g(\mathcal{X})=5$ [1, Ex. 4.5.]. For $m \mid 8$, we have that $g(\mathcal{H}_m)=6(m-1)/2$. Thus, $\mathcal{X} \ncong \mathcal{H}_m$ for any $m \mid 8$. By direct checking using MAGMA (computational algebra system), $|\mathrm{Aut}(\mathcal{X})| = 192 < 336 = 84(g(\mathcal{X})-1)$. However we observe that $\mathcal{X}$ is Galois-Covered by $\mathcal{H}_8$ from [13, Ex. 6.4, Case 1].

4. Further results

Let $\mathcal{X}$ be an $\mathbb{F}_{p^2}$-maximal curve of genus g. Note that if $\mathrm{Aut}(\mathcal{X})$ has a short-orbits structure of type (1)-(4) in Theorem 2.4 and $|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1)$ then $\mathcal{X}$ is Galois-covered by $\mathcal{H}_{p+1}$, since the key point in the proof of Theorem 1.1 is the short-orbits structure. Therefore, in this section we deal with curves $\mathcal{X}$ such that $|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1)$ and having short-orbits structure not of type (1)-(4).

Lemma 4.1. *Let $p \geq 7$. Assume that $\mathcal{X}$ is $\mathbb{F}_{p^2}$-maximal of genus $g \geq 2$ and $40(g-1) < |\mathrm{Aut}(\mathcal{X})| \leq 84(g-1)$. Then $\mathcal{X}$ is Galois-covered by $\mathcal{H}_{p+1}$ unless* $\mathrm{Aut}(\mathcal{X})$ *has exactly* 3 *tame short orbits O_i for $i = 1, 2, 3$, $\mathcal{X}/\mathrm{Aut}(\mathcal{X})$ is rational and one of the following cases occurs.*

(1) $|O_1| = |\mathrm{Aut}(\mathcal{X})|/2$, $|O_2| = |\mathrm{Aut}(\mathcal{X})|/3$, $|O_3| = |\mathrm{Aut}(\mathcal{X})|/7$ *and* $p \geq 11$. *In each case*, $\mathrm{Aut}(\mathcal{X})$ *is a Hurwitz group*; *i.e.* $|\mathrm{Aut}(\mathcal{X})| = 84(g-1)$,
(2) $|O_1| = |\mathrm{Aut}(\mathcal{X})|/2$, $|O_2| = |\mathrm{Aut}(\mathcal{X})|/3$ *and* $|O_3| = |\mathrm{Aut}(\mathcal{X})|/8$. *In each case* $|\mathrm{Aut}(\mathcal{X})| = 48(g-1)$.

Proof. From the Riemann-Hurwitz formula

$$2g-2 = |\mathrm{Aut}(\mathcal{X})|(2g'-2+d')\,, \tag{4.1}$$

where $d'_P = d_p/|\mathrm{Aut}(\mathcal{X})_P|$ and $d' = \sum_P d'_P$. Here the summation is only over a set of representatives of places in $\mathcal{X}$, exactly one from each short orbit of $\mathrm{Aut}(\mathcal{X})$. So, it is necessary to investigate the possibilities for $|\mathrm{Aut}(\mathcal{X})|$ according to the number r of short orbits of $\mathrm{Aut}(\mathcal{X})$ on $\mathcal{X}$. From the Hilbert different formula, see [19, Thm. 11.70], $d_P \geq e_P - 1$, with equality holding if and only if e_P is prime to p. Therefore, if $d_P > 0$, then $d'_P \geq 1/2$. Also, if $d > 0$, then $d' \geq 1/2$. If $g' \geq 2$ then $|\mathrm{Aut}(\mathcal{X})| \leq g-1$, a contradiction. For $g' = 1$, it follows that $d' > 0$ since $g \geq 2$, and hence $|\mathrm{Aut}(\mathcal{X})| \leq 4(g-1)$, a contradiction. Thus $g' = 0$. Then

$$2g-2 = |\mathrm{Aut}(\mathcal{X})|(d'-2)\,.$$

In particular, $d' > 2$. Therefore G has some, say $r \geq 1$, short orbits on $\mathcal{X}$. Take representatives $Q_1, \ldots, Q_r$ from each short orbit and let $d'_i = d'_{Q_i}$ for $i = 1, \ldots, r$. Without loss of generality it may be assumed that $d'_i \leq d'_j$ for $i \leq j$.

- If $r \geq 5$ then $d' \geq 5/2$, and hence $|G| \leq 4(g-1)$.
- If $r = 4$ then $d' > 2$ and $d'_i > 1/2$ for at least one place P. As $d'_i > 1/2$ implies $d' \geq 2/3$, so $d' - 2 \geq 1/6$, whence $|\mathrm{Aut}(\mathcal{X})| \leq 12(g-1)$.
- If $r = 3$ then again use $d' > 2$. If $d'_1 = 2/3$ then $d'_3 \geq 3/4$ and hence $|\mathrm{Aut}(\mathcal{X})| \leq 24(g-1)$. If $d'_1 = 1/2$ and $d'_2 \geq 3/4$ then $|\mathrm{Aut}(\mathcal{X})| \leq 40(g-1)$. Thus, assume that $d'_1 = 1/2$ and $d'_2 = 2/3$. From (4.1) $6/7 \leq d'_3 \leq 53/60$, and hence either $d'_3 = 6/7$ or $d'_3 = 7/8$. Now one of the cases (1) and (2) occurs.
- If $r = 2$ then $d' = d'_1 + d'_2 > 2$. This can only occur when either d'_1 or d'_2 or both are greater than 1. Hence, one of cases (2) and (4) of Theorem 2.4 occurs.
- If $r = 1$ then $d' = d'_1 > 2$, and case (3) of Theorem 2.4 occurs.

□

Remark 4.2. The $\mathbb{F}_{49}$-maximal curve $\mathcal{X}$ of genus $g = 5$ given in Example 3.7 satisfies case (2) of the previous lemma, as $|\mathrm{Aut}(\mathcal{X})| = 192 = 48(5-1)$.

It is not difficult to find an example of an $\mathbb{F}_{p^2}$-maximal curve with $|\mathrm{Aut}(\mathcal{X})| = 84(g-1)$ satisfying case (1) of the previous lemma. According to the proof of Lemma 4.1, if $|\mathrm{Aut}(\mathcal{X})| = 84(g-1)$ then for the short orbits structure of $\mathrm{Aut}(\mathcal{X})$ either one of the cases listed in Theorem 2.4 or case (1) of Lemma 4.1 occurs. Since $|\mathrm{Aut}(\mathcal{X})|$ is coprime with p the cases listed in Theorem 2.4 cannot occur as $\mathrm{Aut}(\mathcal{X})$ cannot have non-tame short orbits. This is exactly what happens in the following example.

Example 4.3. The curve $\mathcal{X}_3$ defined by the plane equation

$$\mathcal{X}_3 : \quad x^3y + y^3z + z^3x = 0$$

is $\mathbb{F}_{13^2}$-maximal curves of genus $g = 3$ since it is in fact Galois-covered by the Hermitian curve $\mathcal{H}_{14}$, see [19, Lemma 10.76]. Its full automorphism group has order $168 = 84(3-1)$. Finally we observe that $\mathcal{X}_3$ is not isomorphic to any $\mathcal{H}_m$, $m \mid 14$ because $g(\mathcal{H}_m) = (m-1)6 \neq 3$.

5. $\mathcal{X}$ is classical and $\mathrm{Aut}(\mathcal{X})$ is a Hurwitz group

Throughout this section, let p be a prime, $\mathcal{X}$ a classical $\mathbb{F}_{p^2}$-maximal curve of genus g with $|\mathrm{Aut}(\mathcal{X})| = 84(g-1)$; in particular, the generic canonical order sequence is $0, 1, \ldots, g-1$. Classical maximal curves were studied in [15]. Recall that for $P_0 \in \mathcal{X}$ the linear system $\mathcal{D} = |(p+1)|P_0$ is an $\mathbb{F}$-invariant of $\mathcal{X}$ whose dimension $n+1 \geq 2$ is the so-called *Frobenius-dimension* of $\mathcal{X}$. We have that $g = p - n$ [11, Prop. 1.8(i)] and thus $g < p$.

From Theorem 1.1, since we are interested in $\mathbb{F}_{p^2}$-maximal curves which are not Galois-covered by the Hermitan curve, we can assume that case (1) of Lemma 4.1 occurs. Therefore, $\mathrm{Aut}(\mathcal{X}) = \langle x, y \mid x^2 = y^3 = (xy)^7 = 1 \rangle$ is tame and $p \geq 11$. Denote by O_i the short orbits under $\mathrm{Aut}(\mathcal{X})$ for $i = 1, 2, 3$ where $|O_1| = |\mathrm{Aut}(\mathcal{X})|/2$, $|O_2| = |\mathrm{Aut}(\mathcal{X})|/3$, $|O_3| = |\mathrm{Aut}(\mathcal{X})|/7$.

Next we extend the main ideas of Magaard and Völklein [27] to positive characteristic. Our main tool to find Weierstrass points is the following lemma which is a generalization in positive characteristic of a result of Schoeneberg [31]; this result is quite useful in the Theory of Riemann surfaces.

Lemma 5.1. *Let $\mathcal{X}$ be a classical curve and let $\alpha \in \mathrm{Aut}(\mathcal{X})$. If $o(\alpha) = n$ is a prime number with $(n, p) = 1$ and α has more than four fixed points on $\mathcal{X}$, then every fixed point of α is a Weierstrass point of $\mathcal{X}$.*

Proof. Let $P \in \mathcal{X}$ be a fixed point of α, and let $P' \in \mathcal{X}/\langle\alpha\rangle$ with $P|P'$. From the Weierstrass Gap Theorem [19, Thm. 6.89] there exists $z \in \mathbb{F}(\mathcal{X}/\langle\alpha\rangle)$ such that $(z)_\infty = m'P'$, with $m' \leq g' + 1$ and $g' = g(\mathcal{X}/\langle\alpha\rangle)$. Thus, $ord_P(z) = nm' \leq (g'+1)n$. On the other hand from [19, Thm. 11.72] applied to the subgroup $\langle\alpha\rangle$, together with the hypothesis that the number of the fixed points $\rho(\alpha)$ of α on $\mathcal{X}$ is bigger than 4 we have that

$$2g-2 \geq n(2g'-2)+(n-1)\rho(\alpha) > n(2g'-2)+4(n-1)\,.$$

This shows that $g+1 > n(g'+1)$. Hence $ord_P(z) < g+1$. Since $\mathcal{X}$ has a classical gap sequence at a general point, P is a Weierstrass point. □

The following remark is a group theoretical translation of Lemma 5.1.

Remark 5.2. Let $P \in \mathcal{X}$. Since $\mathrm{Aut}(\mathcal{X})$ satisfies case (1) of Lemma 4.1, $\mathrm{Aut}(\mathcal{X})_P$ is tame and cyclic. Let $1 \neq \tau \in \mathrm{Aut}(\mathcal{X})_P$. The number of fixed points of τ on the $\mathrm{Aut}(\mathcal{X})$-orbit of P is

$$[N_{\mathrm{Aut}(\mathcal{X})}(\langle\tau\rangle) : (N_{\mathrm{Aut}(\mathcal{X})}(\langle\tau\rangle) \cap \mathrm{Aut}(\mathcal{X})_P)]\,.$$

If this expression is ≥ 5, then P is a Weierstrass point by Lemma 5.1.

Proof. Since $\mathrm{Aut}(\mathcal{X})$ satisfies case (1) of Lemma 4.1, the non-trivial stabilizers of a point of $\mathcal{X}$ are of order 2, 3 and 7. Let $P, Q \in \mathcal{X}$ be distinct points lying on the same short orbit O_i of $\mathrm{Aut}(\mathcal{X})$ for some $i = 1,2,3$. Let $\langle\tau_1\rangle = \mathrm{Aut}(\mathcal{X})_P$ and $\langle\tau_2\rangle = \mathrm{Aut}(\mathcal{X})_Q$. Then $|\mathrm{Aut}(\mathcal{X})_P \cap \mathrm{Aut}(\mathcal{X})_Q| = 1$ as $|\mathrm{Aut}(\mathcal{X})_P| = |\mathrm{Aut}(\mathcal{X})_Q|$ is prime and $P \neq Q$. This shows that distinct elements having the same order in $\{2,3,7\}$ fix distinct points on $\mathcal{X}$ and, since the stabilizers of points lying on the same short orbit are conjugated, they fix the same number of places on $\mathcal{X}$. Let $r \in \{2,3,7\}$ and $\tau \in \mathrm{Aut}(\mathcal{X})$ with $o(\tau) = r$. Denote by O_i the short orbit of $\mathrm{Aut}(\mathcal{X})$ containing the fixed places of τ and let $\tau(P) = P$. From Sylow Theorems the number of Sylow r-subgroups of $\mathrm{Aut}(\mathcal{X})$ equals the length of the conjugacy class in $\mathrm{Aut}(\mathcal{X})$ of τ and hence the index $[\mathrm{Aut}(\mathcal{X}) : N_{\mathrm{Aut}(\mathcal{X})}(\langle\tau\rangle)]$. Denote by k the number of fixed points of τ. We can write $|O_i| = k[\mathrm{Aut}(\mathcal{X}) : N_{\mathrm{Aut}(\mathcal{X})}(\langle\tau\rangle)]$ as subgroups of order r have the same number but distinct fixed places on O_i. Hence from the Orbit Stabilizer Theorem

$$k = \frac{|O_i| \cdot |N_{\mathrm{Aut}(\mathcal{X})}(\langle\tau\rangle)|}{|\mathrm{Aut}(\mathcal{X})|} = \frac{|N_{\mathrm{Aut}(\mathcal{X})}(\langle\tau\rangle)|}{r} = [N_{\mathrm{Aut}(\mathcal{X})}(\langle\tau\rangle) : (N_{\mathrm{Aut}(\mathcal{X})}(\langle\tau\rangle) \cap \mathrm{Aut}(\mathcal{X})_P)]\,.$$

□

Let $K_{\mathcal{X}}$ be a canonical divisor of the curve $\mathcal{X}$. Consider the Riemann-Roch space

$$\mathcal{L}(K_{\mathcal{X}}) = \{f \in \mathbb{F}(\mathcal{X}) \setminus \{0\} \mid (f) + K_{\mathcal{X}} \geq 0\} \cup \{0\}\,,$$

where (f) is the divisor of the function $f \neq 0$ on $\mathcal{X}$. This vector space has dimension g and, given a point P on $\mathcal{X}$, we can find a basis for $\mathcal{L}(K_{\mathcal{X}})$, say $\{h_0, ..., h_{g-1}\}$, such that

$$0 = \mathrm{ord}_P((h_0) + K_{\mathcal{X}}) < \ldots < \mathrm{ord}_P((h_{g-1}) + K_{\mathcal{X}}) \leq 2g-2\,.$$

We will call such a basis a *basis at* P. Let $n_i = \mathrm{ord}_P((h_i) + K_{\mathcal{X}}) + 1$ for $i = 0, ..., g-1$. Then the n_i are called the *gaps* of P. If P is a general point then we know that $n_i = i$ for every $i = 0, \ldots, g-1$, that is a point P is not a Weierstrass point if and only if $n_i = i+1$ for all i.

The (Weierstrass) weight of a point P is $wt(P) := \sum_i (n_i - i)$, thus, P is a Weierstrass point if and only if $wt(P) \neq 0$. Since for a classical curve $\sum_{P \in \mathcal{X}} wt(P) = g(g-1)(g+1)$ and $\mathrm{Aut}(\mathcal{X})$ preserves the weights of Weierstrass points,

$$g(g-1)(g+1) = \sum_j w_j n_j \,, \tag{5.1}$$

where n_j is the length of the $\mathrm{Aut}(\mathcal{X})$-orbit in which the representative Weierstrass point P_j of weight w_j lies. Since $\mathrm{Aut}(\mathcal{X})$ satisfies case (1) of Lemma 4.1 we have that $n_j \in \{84(g-1), 42(g-1), 28(g-1), 12(g-1)\}$ for every j and

$$g(g+1) = \frac{\sum_j w_j n_j}{(g-1)} \,. \tag{5.2}$$

Lemma 5.3. *Let $\mathcal{X}$ be a classical and $\mathbb{F}_{p^2}$-maximal curve of genus g with $p \geq 11$. Assume that $\mathrm{Aut}(\mathcal{X})$ is a Hurwitz automorphism group.*

- *If O_1 does not consist of Weierstrass points of $\mathcal{X}$ then either*
  (1) $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,7)$ *and* $g = 3$ *or*
  (2) $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,8)$ *and* $g = 7$.
- *If O_2 does not consist of Weierstrass points of $\mathcal{X}$ then either*
  (1) $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,7)$ *and* $g = 3$ *or*
  (2) $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,13)$ *and* $g = 14$ *or*
  (3) $\mathrm{Aut}(\mathcal{X}) \cong AGL(3,2)$ *and* $g = 17$.
- *In particular, if* $\mathrm{Aut}(\mathcal{X})$ *acts transitively on the set of the Weierstrass points of* $\mathcal{X}$ *then either* $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,7)$ *and* $g = 3$, *or* $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,8)$ *and* $g = 7$ *or (possibly)* $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,13)$ *and* $g = 14$.

Proof. If O_1 does not consist of Weierstrass points of $\mathcal{X}$, then (5.2) reads

$$g(g+1) = \frac{84k(g-1) + 28j_2k_2(g-1) + 12j_3k_3(g-1)}{(g-1)} = 84k + 28j_2k_3 + 12j_3k_3 \,,$$

where $j_i \in \{0,1\}$ for $i = 2,3$. Thus, $4 \mid g(g+1)$ and hence $4 \nmid (g-1)$. Let P_2 be a Sylow 2-subgroup of $\mathrm{Aut}(\mathcal{X})$. Since $|\mathrm{Aut}(\mathcal{X})| = 84(g-1)$ and $4 \nmid (g-1)$ we get that $|P_2| \leq 8$. From [27, Lemma 2.5] and Remark 5.2 the claim follows. Analogously, if O_2 does not consist of Weierstrass points of $\mathcal{X}$ then (5.2) reads

$$g(g+1) = \frac{84k(g-1) + 42j_1k_1(g-1) + 12j_3k_3(g-1)}{(g-1)} = 84k + 42j_1k_1 + 12j_3k_3 \,,$$

where $j_i \in \{0,1\}$ for $i = 1,3$. Thus, $3 \mid g(g+1)$ and hence $3 \nmid (g-1)$. Let P_3 be a Sylow 3-subgroup of $\mathrm{Aut}(\mathcal{X})$. Since $|\mathrm{Aut}(\mathcal{X})| = 84(g-1)$ and $3 \nmid (g-1)$ we get that $|P_2| = 3$. Now the claim follows from [27, Lemma 2.5] and Remark 5.2. Assume that $\mathrm{Aut}(\mathcal{X})$ acts transitively on the set of Weierstrass points. If $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,7)$ we have that the sizes of the orbits of $\mathrm{Aut}(\mathcal{X})$ are $24, 56, 84$ and 168 and (5.1) reads,

$$24 = g(g-1)(g+1) = \sum_j w_j n_j = 24\sigma_1 + 56\sigma_2 + 84\sigma_3 + 168\sigma_4.$$

The only solution is $\sigma_1 = 1$, $\sigma_2 = \sigma_3 = \sigma_4 = 0$, and hence $\mathrm{Aut}(\mathcal{X})$ is transitive on the set of its 24 Weierstrass points and they have weight equal to 1. If $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,8)$ then the sizes of the orbits of $\mathrm{Aut}(\mathcal{X})$ are $72, 168, 252$, and 504. Thus (5.1) reads

$$336 = g(g-1)(g+1) = \sum_j w_j n_j = 72\sigma_1 + 168\sigma_2 + 252\sigma_3 + 504\sigma_4\,.$$

The only solution is $\sigma_2 = 2$ and $\sigma_1 = \sigma_3 = \sigma_4 = 0$. This proves that $PSL(2,8)$ acts transitively on the set of its 168 Weierstrass points and they have weight equal to 2. Let $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,13)$. Then the sizes of the orbits of $\mathrm{Aut}(\mathcal{X})$ are $156, 364, 546$, and 1092. Thus (5.1) reads,

$$2730 = g(g-1)(g+1) = \sum_j w_j n_j = 156\sigma_1 + 364\sigma_2 + 546\sigma_3 + 1092\sigma_4.$$

The possible solutions are

$$(\sigma_1,\sigma_2,\sigma_3,\sigma_4) \in \{(0,0,5,0),(0,0,1,2),(0,0,3,1),(0,3,3,0),$$
$$(0,6,1,0),(7,0,3,0),(14,0,1,0),(0,3,1,1),(7,0,1,1),(7,3,1,0)\}\,.$$

In the first case $PSL(2,13)$ acts transitively on the Weierstrass points which are all of weight 5, but if one of the next six cases occurs then there are two orbits of Weierstrass points, while if one of the remaining three cases occurs then there are 3 orbits of Weierstrass points. Therefore, $\mathrm{Aut}(\mathcal{X})$ acts transitively on the set of Weierstrass points of $\mathcal{X}$ if and only if case $(0,0,5,0)$ occurs. By direct checking, using MAGMA and Remark 5.2, the number of fixed places of an element of order 2 is 6, so by Lemma 5.1 they are Weierstrass points. In this case we cannot prove whether $\mathrm{Aut}(\mathcal{X})$ acts transitively or not, this justifies the fact that this case possibly occurs. We assume that $\mathrm{Aut}(\mathcal{X})$ is not isomorphic to $PSL(2,r)$ for $r = 7, 8, 13$. In this case O_1 consists of Weierstrass points. If $\mathrm{Aut}(\mathcal{X})$ is not isomorphic to $AGL(3,2)$ then O_2 consists of Weierstrass points and so $\mathrm{Aut}(\mathcal{X})$ is not transitive on the set of Weierstrass points. It only remains to consider the case $\mathrm{Aut}(\mathcal{X}) = AGL(3,2)$. Since $g = 17$, the left hand side of the orbit equation (5.2) is not divisible by 7. It follows that $n_j = 12(g-1)$ has to occur on the right side with non-zero coefficient, i.e., O_3 consists of Weierstrass points as well as O_2. □

Theorem 5.4. *Let $\mathcal{X}$ be a classical and $\mathbb{F}_{p^2}$-maximal curve of genus g with $p \geq 11$. Assume that $\mathrm{Aut}(\mathcal{X})$ is a Hurwitz automorphism group. If O_1 and O_2 do not consist of Weierstrass points of $\mathcal{X}$ then $\mathrm{Aut}(\mathcal{X}) = PSL(2,7)$, $g = 3$ and $\mathcal{X}$ is isomorphic to the Klein quartic $\mathcal{X}_3 :\ x^3y+y^3z+z^3x = 0$. In particular, $\mathcal{X}$ is Galois-covered by the Hermitian curve $\mathcal{H}_{p+1}$ where $p \equiv 6 \mod 7$.*

Proof. From Lemma 5.3 $\mathrm{Aut}(\mathcal{X})$ is isomorphic to $PSL(2,7)$ and $g=3$. As $p>2g+1=7$, $\mathcal{X}$ is not hyperelliptic from [3, Lemma 3.2]. From [3, Thm. 3.5], $\mathcal{X}$ is isomorphic to $\mathcal{X}_3$, as it is the unique non-hyperelliptic superspecial curve of genus 3 admitting $PSL(2,7)$ as an automorphism group. We conclude that $\mathcal{X}$ is Galois-covered by $\mathcal{H}_{p+1}$ by [19, Lemma 10.76] and [19, Thm. 10.78]. □

Remark 5.5. From the proof of Theorem 5.4 follows that if $\mathcal{X}$ is an $\mathbb{F}_{p^2}$-maximal curve with $g(\mathcal{X})=3$ and $\mathrm{Aut}(\mathcal{X})\cong PSL(2,7)$ then $\mathcal{X}$ is isomorphic to the Klein quartic $\mathcal{X}_3$ because the proof does not depend on the fact that O_1 and O_2 do not consist of Weierstrass points of $\mathcal{X}$.

The Klein quartic $\mathcal{X}_3$ above is the unique known example of curve admitting a Hurwitz group as a full automorphism group in positive characteristic. According to Lemma 5.3, if O_1 does not consist of Weierstrass points, then the next possible smallest Hurwitz group is $PSL(2,8)$, occurring for a curve of genus 7. In zero characteristic there exists such a curve, namely the so called *Fricke-Macbeath curve*; see [26]. Before constructing a Fricke-Macbeath curve in positive characteristic, which will give the desired example showing that the bound stated in Theorem 1.1 is sharp, we describe necessary conditions for a Hurwitz curve of genus 7 admitting $PSL(2,8)$ to exist.

Lemma 5.6. *Let $\mathcal{X}$ be a classical and $\mathbb{F}_{p^2}$-maximal curve of genus g with $p\geq 11$. Assume that $\mathrm{Aut}(\mathcal{X})$ is a Hurwitz automorphism group. If O_1 does not consist of Weierstrass points of $\mathcal{X}$, then $\mathcal{X}$ is isomorphic to the Klein quartic $\mathcal{X}_3: x^3y+y^3z+z^3x=0$ unless $\mathrm{Aut}(\mathcal{X})\cong PSL(2,8)$, $O_1,O_2,O_3\subseteq\mathcal{X}(\mathbb{F}_{p^2})$, $g=7$ and $p\equiv\pm1 \mod 14$. Also, O_2 is the set of Weierstrass points of $\mathcal{X}$ and $p\equiv-1 \mod 3$.*

Proof. According to Lemma 5.3 and Theorem 5.4, we can suppose that $\mathrm{Aut}(\mathcal{X})\cong PSL(2,8)$ and $g=7$. Let $n+1$ the Frobenius dimension of $\mathcal{X}$. Thus, $7=g=p-n$ as $\mathcal{X}$ is classical. From the proof of Lemma 5.3, O_2 is the set of Weierstrass points of $\mathcal{X}$. Suppose that $O_2\not\subseteq\mathcal{X}(\mathbb{F}_{p^2})$. From [15, Remark 4.1] $p=n^2+n-1$ since $g\geq 2$. Hence $7=p-n=n^2-1$, a contradiction. This shows that $O_2\subseteq\mathcal{X}(\mathbb{F}_{p^2})$. Since $\mathcal{X}$ is $\mathbb{F}_{p^2}$-maximal and $\mathrm{Aut}(\mathcal{X})$ acts on $\mathcal{X}(\mathbb{F}_{p^2})$ with at most three short orbits, we can write

$$p^2+1+14p=k_1(72)+168+k_2(252)+k(504)\,,$$

where $(k_1,k_2)\in\{(0,0),(0,1),(1,0),(1,1)\}$ and $k\geq 0$. If either $(k_1,k_2)=(0,0)$ or $(k_1,k_2)=(0,1)$ then $p^2-167=14(36k-p)$ or $p^2-419=14(36k-p)$ respectively. In both cases we get $p^2+1\equiv 0 \mod 7$, which is impossible. Thus $(k_1,k_2)\in\{(1,0),(1,1)\}$ and hence $O_3\subseteq\mathcal{X}(\mathbb{F}_{p^2})$. Assume that $(k_1,k_2)=(1,0)$. Then $p^2+14p+1=240+k(504)$. Suppose that $O_1\not\subseteq\mathcal{X}(\mathbb{F}_{p^4})$. Then $k\geq 1$, $|\mathrm{Aut}(\mathcal{X})|=504$ divides $p^4-14p^2-p^2-14p$ and since it divides also $p^2+14p-239$ we get that 504 divides $420p-3360=4(105p-840)$ because of the equality $p^3-14p-p-14=(p-14)(p^2+14p-239)+420p-3360$. Since $|105p-840|$ is odd we get a contradiction. Thus $O_1\subseteq\mathcal{X}(\mathbb{F}_{p^4})$. But since $\mathrm{Aut}(\mathcal{X})$ is defined over $\mathbb{F}_{p^2}$ the image of O_1 with respect to the Frobenius map Φ_{p^2} is another short orbit of $\mathrm{Aut}(\mathcal{X})$ having the same length of O_1, a contradiction. Thus we can assume that $(k_1, k_2) = (1, 1)$ and $p^2 + 1 + 14p = 492 + k(504)$. By direct checking $k \geq 1$ and hence 504 divides $p^2 + 14p - 491$. Then $\mathrm{Aut}(\mathcal{X})$ has only long orbits outside $\mathcal{X}(\mathbb{F}_{p^2})$ and from [17, Proposition 3.13], $504 = |\mathrm{Aut}(\mathcal{X})|$ divides $672(p + 1)$. Hence $p \equiv -1 \mod 3$. □

Remark 5.7. By direct checking, the smallest prime number p for which we do not have contradictions to the necessary numerical conditions described in the proof of Lemma 5.6 for an $\mathbb{F}_{p^2}$-maximal curve of genus 7 admitting a Hurwitz automorphism group to exist is $p = 71$.

6. On the Fricke-Macbeath curve over finite fields

It is well-known that an algebraic curve of genus $g > 1$ over $\mathbb{C}$ has at most $84(g - 1)$ automorphisms. A curve attaining this bound is called a Hurwitz curve. In this case the corresponding Riemann surface can be described as the standard action of a normal subgroup of finite index in the triangle group $G_{2,3,7}$ on the complex upper half plane; see Shimura's and Elkies' papers [32] and [7] for details. The already worked out Klein quartic with equation $\mathcal{X}_3 : x^3y + y^3z + z^3x = 0$, named after Felix Klein who studied it in 1879 in his paper [22], is the unique Hurwitz curve up to isomorphisms for $g = 3$. The next example occurs for $g = 7$ and was introduced as a Riemann surface by Robert Fricke in 1899 [10]. Explicit equations realizing Fricke's example as an algebraic curve were presented in 1965 by A. M. Macbeath [26]. Again, up to isomorphisms over $\mathbb{C}$, this curve is the unique Hurwitz curve of genus 7; here and elsewhere it is called the *Fricke-Macbeath curve*. Edge [5] derived the equations first presented by Macbeath by starting from the property that they need to define a curve in $\mathbb{P}^6$ having a given subgroup of order 504 in $PGL_7(\mathbb{C})$ as automorphism group. Rubén Hidalgo [18] presented a plane model for the Fricke-Macbeath curve over $\mathbb{Q}$ attributed to Bradley Brock, namely

$$\mathcal{F} : \quad 1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0\,.$$

In [35] a criterion to count the points of the Fricke-Macbeath curve over finite fields is provided. We will use such a method combined with Lemma 5.6 to construct $\mathbb{F}_{p^2}$-maximal Fricke-Macbeath curves. The $\mathbb{F}_{71^2}$-maximal Fricke-Macbeath curve provides an example showing that the bound stated in Theorem 1.1, that is $|\mathrm{Aut}(\mathcal{X})| > 84(g - 1)$, is sharp. According to Lemma 5.6 we focus on the case $p \equiv \pm 1 \pmod{14}$.

Proposition 6.1. *Let* $p \equiv \pm 1 \pmod{14}$. *Then the Fricke-Macbeath curve* $\mathcal{F} : 1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0$ *is* $\mathbb{F}_{p^2}$*-maximal if and only if the elliptic curve* $\mathcal{E} : y^2 - (x^3 + x^2 - 114x - 127) = 0$ *is* $\mathbb{F}_{p^2}$*-maximal.*

Proof. From [35, Thm. 2.6], since $p \equiv \pm 1 \pmod 7$, the number of $\mathbb{F}_{p^2}$-rational points of $\mathcal{F}$ satisfies $|\mathcal{F}(\mathbb{F}_{p^2})| = 7|\mathcal{E}(\mathbb{F}_{p^2})| - 6p^2 - 6$. Thus $|\mathcal{F}(\mathbb{F}_{p^2})| = p^2 + 1 + 14p$ if and only if $|\mathcal{E}(\mathbb{F}_{p^2})| = p^2 + 2p + 1$ that is if and only if $\mathcal{E}$ is $\mathbb{F}_{p^2}$-maximal. □

Remark 6.2. By direct checking with MAGMA, $\mathcal{F}$ is $\mathbb{F}_{p^2}$-maximal for $p \in \{71, 251, 503, 2591\}$ and $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,8)$. Clearly, since the $\mathbb{F}_{p^2}$-maximality of $\mathcal{F}$ is equivalent to an elliptic curve to be supersingular there exist infinitely many values of p for $\mathcal{F}$ to be $\mathbb{F}_{p^2}$-maximal, see [6].

We now show that the $\mathbb{F}_{71^2}$-maximal Fricke-Macbeath curve gives an example of an $\mathbb{F}_{p^2}$-maximal curve which is not Galois-covered by the Hermitian curve $\mathcal{H}_{p+1}$. The proof is long and very technical.

Theorem 6.3. *The $\mathbb{F}_{71^2}$-maximal Fricke-Macbeath curve $\mathcal{F}: 1+7xy+21x^2y^2+35x^3y^3+28x^4y^4+2x^7+2y^7=0$ has genus $g=7$ and $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,8)$. Also, $\mathcal{F}$ is not a Galois subcover of $\mathcal{H}_{72}$.*

Proof. Assume by contradiction that $\mathcal{F} \cong \mathcal{H}_{72}/G$ for some $G \leq PGU(3,71)$. The order of $PGU(3,71)$ is equal to $2^7 \cdot 3^5 \cdot 5 \cdot 7 \cdot 71 \cdot 1657$. From the Riemann-Hurwitz formula,

$$\frac{\mathcal{H}_{71}(\mathbb{F}_{71^2})}{\mathcal{F}(\mathbb{F}_{71^2})} \leq |G| \leq \frac{2g(\mathcal{H}_{71})-2}{2g(\mathcal{F})-2},$$

which yields $60 \leq |G| \leq 414$, as $2g(\mathcal{H}_{71})-2 = 4968$ and $2g(\mathcal{F})-2=12$. Since $|G|$ divides $|PGU(3,71)|$,

$$|G| \in \{60,63,64,70,71,72,80,81,84,90,96,105,108,112,120,126,\\ 128,135,140,142,144,160,162,168,180,189,192,210,213,216,224,\\ 240,243,252,270,280,284,288,315,320,324,336,355,360,378,384,405\}. \tag{6.1}$$

The different divisor Δ has degree

$$\deg(\Delta) = \sum_{\sigma \in G\setminus\{id\}} i(\sigma) = (2g(\mathcal{H}_{71})-2) - |G|(2g(\mathcal{F})-2) = 4968 - 12|G|. \tag{6.2}$$

For the computation of $i(\sigma)$ we refer to the notation used in [29, Lemma 2.2] and the complete classification given in [29, Thm. 2.7].

Case 1: 71 divides $|G|$

- $|G|=71$. From (6.2), $\deg(\Delta)=4116$ but from [29, Thm. 2.7] either $\deg(\Delta)=70\cdot 2$ or $\deg(\Delta)=70\cdot(73)$, a contradiction.
- $|G|=142$. In this case either G is dihedral or cyclic. From (6.2), $\deg(\Delta)=3264$. Assume that G is dihedral. From [29, Thm. 2.7] either $\deg(\Delta)=70\cdot 2+71\cdot 72$ or $70\cdot 73+71$, a contradiction. If G is cyclic then either $\deg(\Delta)=70\cdot 2+72+1\cdot 70$ or $\deg(\Delta)=70\cdot 73+72+1\cdot 70$, which are impossible.
- $|G|=213$. From (6.2), $\deg(\Delta)=2412$ and G is cyclic. From [29, Lemma 2.2], if $\sigma \in G$ is tame then σ is of type (A) and hence $i(\sigma)=p+1=72$. From [29, Thm. 2.7] either $\deg(\Delta)=70\cdot 2+2\cdot 72+140\cdot 1$ or $\deg(\Delta)=70\cdot 73+2\cdot 72+140\cdot 1$, a contradiction.

- $|G| = 284$. There are 4 groups of order 284 up to isomorphism. We will refer to such groups keeping the standard GAP notation as $G \cong SmallGroup(284, i)$ for $i = 1, 2, 3, 4$. From [29, Thm. 2.7], if $G \cong SmallGroup(284, 1)$ then $\deg(\Delta) = 70 \cdot 1 + 142 \cdot \alpha + 70 \cdot \beta + 72$, where $\alpha \in \{0, 72\}$ and $\beta \in \{2, 73\}$. If $G \cong SmallGroup(284, 2)$ then $\deg(\Delta) = 140 \cdot 1 + 70 \cdot 1 + 2 \cdot \alpha + 70 \cdot \beta + 72$, where $\alpha \in \{0, 72\}$ and $\beta \in \{2, 73\}$. If $G \cong SmallGroup(284, 3)$ then $\deg(\Delta) = 70 \cdot 1 + 70 \cdot \beta + 143 \cdot 72$, where $\beta \in \{2, 73\}$. If $G \cong SmallGroup(284, 2)$, then $\deg(\Delta) = 210 \cdot 1 + 70 \cdot \beta + 3 \cdot 72$, where $\beta \in \{2, 73\}$. In all these cases, by direct checking $\deg(\Delta)$ does not satisfies (6.2), contraddicition.
- $|G| = 355$. There are 2 groups of order 355 up to isomorphism, namely $G \cong C_{71} \rtimes C_5$ or $G \cong C_{355}$, where C_n denotes a cyclic group of order n. In the former case $\deg(\Delta) = 70 \cdot \alpha + 284 \cdot 2$, where $\alpha \in \{2, 73\}$. By direct checking $\deg(\Delta)$ satisfies (6.2) if and only if $\alpha = 2$. Thus from the Riemann-Hurwitz formula $g(\mathcal{H}_{71}/G) = 7 = g(\mathcal{F})$. Geometrically, the elements of C_{71} have exactly one fixed point $P \in \mathcal{H}_{71}$ while the elements of C_5 fix exactly the $\mathbb{F}_{71^2}$-rational vertexes of a triangle $T = \{P, Q, R\}$, where $Q \in \mathcal{H}_{71}$ and $R \notin \mathcal{H}_{71}$. Let $H \cong C_{71^2-1} < PGU(3, 71)$ fixing T point-wise. Clearly $C_5 < C_{71^2-1}$ and since H normalizes C_{71} $\tilde{H} = \langle C_{71}, H\rangle = C_{71} \rtimes H$. Since $PSL(2, 8)$ contains no subgroups of order $|\tilde{H}/G|$ the curves $\mathcal{F}$ and $\mathcal{H}_{71}/G$ are not isomorphic.

This shows that if $\mathcal{H}_{71}/G \cong \mathcal{F}$ then G must be tame.

Case 2: 71 does not divide $|G|$

When G is tame we proceed with a case-by-case analysis according to $|G|$ and the possible group theoretical structure of G up to isomorphisms. In most of the obtained cases a numerical contradiction to (6.2) is obtained using [29, Thm. 2.7]. Here we underline again that, considering subgroups G of $PGU(3, 71)$ with $|G|$ satisfying one of the cases classified in (6.1), quotient curves $\mathcal{H}_{71}/G$ of $\mathcal{H}_{71}$ of genus 7 can be obtained. However, in each of these cases there exists at least a subgroup of $N_{PGU(3,71)}(G)/G$ which is not isomorphic to any subgroup of $PSL(2, 8)$. The following is the complete list of quotient curves $\mathcal{H}_{71}/G$ where $|G|$ satisfies (6.1) and $g(\mathcal{H}_{71}/G) = 7$.

- $|G| = 72$ and $G \cong C_{72}$. In this case $C_{71} = \langle\alpha\rangle$ where α is either of type (A) or of type (B1) from [29, Lemma 2.2]. In both cases we can assume up to conjugation that $\mathcal{H}_{71}$ is given by the Fermat equation $\mathcal{H}_{71} : x^{72} + y^{72} + z^{72} = 0$ and α admits a diagonal matrix representation of type

$$\alpha = [a, b, 1] = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where $o(a)$ and $o(b)$ divide $p + 1 = 72$. Since $\mathcal{H}_{71}/G$ inherits at least a cyclic diagonal group of order 72 of type $[\gamma, 1, 1]$, $[1, \gamma, 1]$ or $[1, 1, \gamma]$ for some γ of order

72, we conclude that $\mathcal{H}_{71}/G$ is not isomorphic to $\mathcal{F}$, as $PSL(2,8)$ does not contains abelian groups of order 72.

- $|G| = 72$ and $G \cong SmallGroup(72,\ell)$ where $\ell \in \{9,18,36\}$. Arguing as in the previous case, we observe that $\mathrm{Aut}(\mathcal{H}_{71}/G)$ inherits a cyclic group of order n where $n \mid 72$ and $m \geq 9$. This conflicts with $\mathrm{Aut}(\mathcal{H}_{71}/G)$ to be isomorphic to $PSL(2,8)$.
- $|G| = 180$ and $G \cong SmallGroup(180,4)$, that is $G = \langle \sigma \rangle \cong C_{(71^2-1)/28}$. Since σ is of type (B2) of [29, Lemma 2.2], we can assume that up to conjugation $\mathcal{H}_{71}$ has equation $x^{71}z + xz^{71} = y^{72}$ and σ fixes the vertexes of the fundamental triangle $T = \{(1:0:0),(0:1:0),(0:0:1)\}$. Thus, σ is given by a matrix representation
$$\sigma = \begin{pmatrix} a^{72} & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
where $a \in \mathbb{F}_{71^2}$ with $o(a) = o(\sigma) = 180$; see [19, Page 644 case 8]. Consider the automorphism α of $\mathcal{H}_{71}$ given by
$$\begin{pmatrix} \xi^{72} & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
where $o(\xi) = 71^2 - 1$. Thus, $G < \langle \alpha \rangle \cong C_{71^2-1}$, and hence $\langle \alpha \rangle / G \cong C_{28} < \mathrm{Aut}(\mathcal{H}_{71}/G)$. Since $PSL(2,8)$ has no cyclic subgroups of order 28, the curves $\mathcal{H}$ and $\mathcal{H}_{71}/G$ are not isomorphic.
- $|G| = 240$ and $G \cong C_5 \rtimes C_{48}$. The center $Z(G)$ is cyclic of order 24. Geometrically, $Z(G) = \langle \alpha \rangle$ where α is of type (A) in [29, Lemma 2.2]. The center of α is given by the fixed common point $P \notin \mathcal{H}_{71}$ of C_5 and C_{48}. By direct checking, using again a matrix representation for C_{48} as in the previous case, we observe that the entire $C_{71^2-1} < PGU(3,71)$ containing C_{48} normalizes C_5 as well. This yields the quotient curve $\mathcal{H}_{71}/G$ to admit a cyclic group of automorphisms of order greater than 9, a contradiction.
- $|G| = 240$ and $G \cong C_{240}$. Arguing as in the case $|G| = 180$ we observe that $\mathcal{H}_{71}/G$ admits a cyclic automorphisms group of order $(71^2-1)/240 = 21$. Since $PSL(2,8)$ has no cyclic subgroups of order 21, the curves $\mathcal{F}$ and $\mathcal{H}_{71}/G$ are not isomorphic.
- $|G| = 315$ and $G \cong SmallGroup(315,2)$. As $\mathcal{H}_{71}/G$ admits at least a cyclic automorphisms group of order $(71^2-1)/315$, the claim follows.
- $|G| = 336$ and $G \cong SmallGroup(336,6)$. In this case a contradiction is obtained observing that the quotient curve $\mathcal{H}_{71}/G$ inherits a cyclic automorphisms group of order at least 15.
- $|G| = 324$ and $G \cong SmallGroup(324,81)$. In this case a contradiction is obtained observing that the quotient curve $\mathcal{H}_{71}/G$ inherits a cyclic automorphisms group of order at least 16.

We now proceed with a case-by-case analysis for those cases for which a numerical contradiction to the Riemann-Hurwitz formula is obtained.

- $|G| = 60$. In this case $\deg(\Delta) = 4248 = 59 \cdot 72$. Since G contains exactly 59 non-trivial elements whose contribution to $\deg(\Delta)$ is at most 72, every non-trivial element of G is a homology and hence in particular $o(\sigma) \mid (q+1)$ for every $\sigma \in G \setminus \{id\}$; see [29, Thm. 2.7]. Since $5 \mid |G|$ and $5 \nmid (p+1)$, this case is not possible.
- $|G| = 63$. In this case $\deg(\Delta) = 4214$, and $G_i \cong \mathit{SmallGroup}(63, i)$ for $i = 1, \ldots, 4$. Also, $G_1 = \{12_{12}, 9_{42}, 7_6, 3_2, 1_1\}$, $G_2 = \{63_{36}, 21_{12}, 9_6, 7_6, 3_2\}$, $G_3 = \{21_{12}, 7_6, 3_{44}, 1_1\}$, $G_4 = \{21_{48}, 7_6, 3_8, 1_1\}$, where n_m means that there are m elements of order n in the group. By [29, Thm. 2.7] this gives $\deg(\Delta) \leq 3204$, $\deg(\Delta) \leq 684$, $\deg(\Delta) \leq 3204$, $\deg(\Delta) \leq 684$ respectively, a contradiction.
- $|G| = 64$. Since every $\sigma \in G$ is a 2-elements, by [29, Thm. 2.7] we have that $i(\sigma) \in \{0, 2, 72\}$. Hence we can write $\deg(\Delta) = 4200$ as $72 \cdot i + 2 \cdot j$ for some $0 \leq i + j \leq 63$. Such i and j do not exist and we have a contradiction.
- $|G| = 70$. Arguing as in the previous case, we can write $\deg(\Delta) = 4128 = 72 \cdot i + 2 \cdot j$ for some $0 \leq i + j \leq 69$. By direct computation with MAGMA, the unique possibility is $(i, j) = (57, 12)$ and $G \cong \mathit{SmallGroup}(70, k)$ for $k = 1, \ldots, 4$. Since $70 = p - 1$, by [29, Thm. 2.7] the elements $\sigma \in G$ such that $i(\sigma) = 72$ are those of order equal to 2. Thus i equals the number of involutions in G. If $G \cong \mathit{SmallGroup}(70, 1)$ then $i = 5$, if $G \cong \mathit{SmallGroup}(70, 2)$ then $i = 7$, if $G \cong \mathit{SmallGroup}(70, 3)$ then $i = 35$, and if $G \cong \mathit{SmallGroup}(70, 4)$ then $i = 1$. Since in all cases $i \neq 57$ this case cannot occur.
- $|G| = 72$. In this case $G \cong \mathit{SmallGroup}(72, a)$ for $a = 1, \ldots, 50$, and $\deg(\Delta) = 4104$ can be written as $72 \cdot i + 3 \cdot j$ for some $0 \leq i + j \leq 71$ by [29, Thm. 2.7]. By direct checking with MAGMA $(i, j) = (57, 0)$ thus G does not contains Singer subgroups. We consider the remaining cases according to the previous results obtained for groups of order 72. We discard those cases for which G contains more than 57 involutions, which implies $i > 57$.

  Assume that $G \cong \mathit{SmallGroup}(72, 1)$. Since G has a unique involution, which is a homology, G fixes an $\mathbb{F}_{71^2}$-rational point P with $P \notin \mathcal{H}_{71}$. This implies that G is contained in the maximal subgroup $\mathcal{M}_{71}$ of $PGU(3, 71)$ fixing a $\mathbb{F}_{71^2}$-rational point off $\mathcal{H}_{71}$. The center of G is cyclic of order 4 and it is generated by a homology. In fact assume by contradiction that $Z(G)$ is generated by an element γ of type (B1). The elements $\alpha \in G$ of odd order commute with γ and they fix a common point which is the center of the unique involution of G. Thus, α fixes the fixed points of γ. This implies that the entire group G fixes the fixed points of γ, and hence G fixes pointwise a self-polar triangle T with respect to the unitary polarity defined by $\mathcal{H}_{71}$, $G \leq C_{72} \times C_{72} = \mathit{Stab}_{PGU(3,71)}(T)$ and G is abelian, a contradiction. Thus γ is a homology. From [28, Page 6], $Z(\mathcal{M}_{71})$ is a cyclic group of order 71 which is generated by a homology of center P. This implies that every element $\beta \in G \setminus Z(G)$ such that $\langle \beta \rangle$ intersects non-trivially $Z(G)$ is of type (B1) since otherwise $\beta \in Z(\mathcal{M}_{71})$ and hence $\beta \in Z(G)$, a contradiction. Looking at the subgroups structure of G we get that G contains at most $72 - 2 - 36 = 34$ homologies, so this case cannot occur.

If $G \cong SmallGroup(72, i)$, $i = 3, 4, 5, 6, 8, 10, 11, 12, 13, 14, 16, 20, 27, 28, 30, 47,$ then arguing as above we get that G contains at most $35, 10, 45, 41, 47, 47, 35, 47, 9, 9, 47, 45, 17, 56, 47, 47$ homologies respectively, a contradiction.

If $G \cong SmallGroup(72, 7)$ or $G \cong SmallGroup(72, 17)$ then G normalizes three distinct subgroups of order 2, and hence fixes their centers. Then G fixes the vertexes of self-polar triangle T with respect to the unitary polarity defined by $\mathcal{H}_{71}$ but G is not abelian. Such a subgroup does not exist.

If $G \cong SmallGroup(72, 15)$ then two cases are distinguished depending on the unique element of $\alpha \in G$ of order 3 being a homology or not. By direct checking with MAGMA, if α is a homology then $\alpha \in Z(G)$. Since $Z(G)$ is trivial, this case cannot occur. Thus α is of type (B1): in this cases G contains at most $71 - 2 - 24$ homologies, a contradiction.

If $G \cong SmallGroup(72, 19)$. Since G normalizes 7 groups of order 2, we have that G has 7 fixed points $P_1, \ldots, P_7$ which are $\mathbb{F}_{71^2}$-rational but not in $\mathcal{H}_{71}$. This proves that in particular every element of G is a homology, a contradiction.

The cases $G \cong SmallGroup(72, 21)$ and $G \cong SmallGroup(72, 22)$ cannot occur as in this case the unique subgroup of G of order 3 must be central, a contradiction.

If $G \cong SmallGroup(72, \ell)$ with $\ell \in \{29, 32, 33, 34, 35, 37, 48, 49, 50\}$, then G fixes the vertexes of a self-polar triangle T with respect to the unitary polarity defined by $\mathcal{H}_{71}$ but G is not abelian, a contradiction.

The case $G \cong SmallGroup(72, \ell)$ with $\ell \in \{39, 40, 41\}$ cannot occur as a subgroups of $PGU(3, 71)$. In fact G contains a unique elementary abelian subgroup of order 9 which is made by 6 homologies and 2 elements of type (B1). Thus elements of order 3 cannot be all conjugate, a contradiction.

The cases $G \cong SmallGroup(72, \ell)$ with $\ell \in \{42, 43, 44\}$ cannot occur since at least one involution of G must be central, a contradiction. The cases $G \cong SmallGroup(72, 45)$ and $G \cong SmallGroup(72, 46)$ cannot occur since at least one element of order 3 in G must be central, a contradiction.

- $|G| = 80$. In this case we can write $\deg(\Delta) = 4008 = 72 \cdot i + 2 \cdot j$, for $0 \leq i + j \leq 79$. By direct checking with MAGMA the unique possibility is $(i, j) = (55, 24)$. From [29, Thm. 2.7], the elements σ of G for which $i(\sigma) = 72$ are those with $o(\sigma) \in \{2, 4, 8\}$. Forcing $G \cong SmallGroup(80, k)$ to have at least 55 elements of order in $\{2, 4, 8\}$, we get $k \in \{28, 29, 30, 31, 32, 33, 34, 50\}$. Denote by o_i the number of elements $\alpha \in G$ such that $o(\alpha) = i$. By direct checking with MAGMA we obtain that in each of these cases $o_2 + o_4 + o_8 = 63$ and hence $j = 79 - 63 = 16$, a contradiction.

- $|G| = 81$. In this case $\deg(\Delta) = 3996 = 72 \cdot i + 3 \cdot j$ for some $0 \le i + j \le 80$. By direct checking with MAGMA the unique possibility is $(i, j) = (55, 12)$. This proves that G must contain at least 12 elements of order 3, as the unique elements β in G with $i(\beta) = 3$ are those with $o(\beta) = 3$ from [29, Thm. 2.7]. We note that these elements cannot be contained in cyclic groups of order 9, as Singer groups of order 9 does not exists in $PGU(3, 71)$ because $9 \nmid (71^2 - 71 + 1)$. This yields $G \cong \mathit{SmallGroup}(81, k)$ with $k \in \{1, 2, 3, 4\}$. The case $G \cong \mathit{SmallGroup}(81, 1)$ cannot occur, as G is cyclic of order not a divisor of $71^2 - 71 + 1$ and hence G cannot contains Singer subgroups. Case $G \cong \mathit{SmallGroup}(81, 2)$ cannot occur, as from a composition of elements of type (B1) or homologies it is not possible to generate Singer subgroups. Case $G \cong \mathit{SmallGroup}(81, 3)$ cannot occur, as elements of order 9 split in 3 conjugacy classes giving rise to at least 18 elements of order 3 of type (B1). Hence $j \ne 12$. Case $G \cong \mathit{SmallGroup}(81, 4)$ cannot occur, since elements of order 3 generates a subgroup of G isomorphic to $C_3 \times C_3$ but Singer subgroups do not commute.
- $|G| = 84$. Since $84 \mid (71^2 - 1)$, by [29, Thm. 2.7] we have that $i(\sigma) \in \{0, 2, 3, 72\}$ for any $\sigma \in G$. Writing $\deg(\Delta) = 3960 = 71 \cdot i + 2 \cdot j + 3 \cdot k$ for $0 \le i + j + k \le 83$ we get that $(i, j, k) = (54, 3m, 2(12 - m))$ for some $m = 0, \ldots, 5$ or $(i, j, k) = (55, 0, 0)$. We note that $(i, j, k) = (55, 0, 0)$ cannot occur as G contains at least an element γ with $o(\gamma) = 7$ for which $i(\gamma) = 2$ from [29, Thm. 2.7]. This implies that $(i, j, k) = (54, 3m, 2(12 - m))$ for some $m = 0, \ldots, 5$ and hence G contains at least $54 + 14 = 68$ elements α such that $o(\alpha) \in \{2, 3, 4, 6, 12\}$. By direct checking with MAGMA, $G \cong \mathit{SmallGroup}(84, \ell)$ where $\ell \in \{1, 2, 7, 9, 11\}$. For all these cases a contradiction is obtained combining the value of the parameter k with the lengths of the conjugacy classes of elements of order 3.
- $|G| = 90$. We argue as in the previous cases. For $\sigma \in G$ we have $i(\sigma) \in \{0, 2, 3, 72\}$. We can write $\deg(\Delta) = 3008 = 72 \cdot i + 2 \cdot j + 3 \cdot k$, for $0 \le i + j + k \le 90$. Also, we observe that $j \le 4$ since G contains at least 4 elements of order 5. By direct computation with MAGMA we obtain that $(i, j, k) = (53, 3m, 2(12 - m))$ for some $m = 2, \ldots, 11$. Forcing $|\{\sigma \in G \mid o(\sigma) = 2, 3, 6, 9, 18\}| \ge 53$ we get $G \cong \mathit{SmallGroup}(90, \ell)$ where $\ell \in \{7, 9, 11\}$. Assume that $G \cong \mathit{SmallGroup}(90, 7)$. Hence $|\{\sigma \in G \mid o(\sigma) = 2, 3, 6, 9, 18\}| = 71$ and $j = 18 = 3 \cdot 6$. This yields $k = 2(12 - 6) = 12$ which is impossible, as there exists a unique conjugacy class of elements of order 3 whose length is not equal to 12. Assume that $G \cong \mathit{SmallGroup}(90, 9)$ or $G \cong \mathit{SmallGroup}(90, 11)$. Hence $|\{\sigma \in G \mid o(\sigma) = 2, 3, 6, 9, 18\}| = 59$ and $j = 30 = 3 \cdot 10$. This yields $k = 2(12 - 10) = 4$ which is impossible, as there exists a unique conjugacy class of elements of order 3 whose length is not equal to 4.

- $|G| = 96$. Here for $\sigma \in G$ we have $i(\sigma) \in \{0, 2, 3, 72\}$ and $\deg(\Delta) = 3816 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ for $0 \leq i+j+k \leq 95$. By direct computation with MAGMA $(i, j, k) = (52, 3m, 2(12-m))$ for some $m = 0, \ldots, 12$ or $(i, j, k) = (53, 0, 0)$. Forcing $\tau = |\{\sigma \in G \mid o(\sigma) = 2, 3, 4, 6, 8, 12, 24\}| \geq 52$ we have $G \cong \mathit{SmallGroup}(96, \ell)$ with $\ell \in \{3, 6, 7, \ldots, 17, 20, \ldots, 58, 61, \ldots, 231\}$. We note that elements of order 3 in G are all conjugated as $9 \nmid |G|$. This implies that if $k \neq 0$ then k is exactly the number o_3 of elements of order 3 in G. Assume that $G \cong \mathit{SmallGroup}(96, 3)$. Then $\tau = 95$ and hence $j = 0 = 3 \cdot 0$. This implies that $k = 2(12-0) = 24$, since the number of elements of order 3 in G is not equal to 24 we have a contradiction. Using the same argument we can exclude all the remaining cases for G. In fact if $\ell = 6, 7, 8$ then $\tau = 71$ and $k = 8 \neq o_3$, if $\ell = 9, \ldots, 58$ then $\tau = 95$ and $k = 24 \neq o_3$, if $\ell = 61, 62, 63$ then $\tau = 71$ and $k = 8 \neq o_3$, while if $\ell \geq 64$ then $\tau = 71$ and $k = 8 \neq o_3$.
- $|G| = 105$. We write $\deg(\Delta) = 3708 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ where $10 \leq i+j+k \leq 104$ as $j \geq 10$ because G admits at least 4 elements of order 5 and 6 elements of order 7. By direct checking with MAGMA either $(i, j, k) = (50, 3m, 2(18-m))$ for some $m = 4, \ldots, 18$ or $(i, j, k) = (51, 3m, 2(6-m))$ for some $m = 4, \ldots, 6$. Since the unique elements α in G for which $i(\alpha)$ can be equal to 72 are those of order 3 and their number is always less then 50, this case is not possible.
- $|G| = 108$. For $\sigma \in G$ we have $i(\sigma) \in \{0, 2, 3, 72\}$ and elements of order 27, 54 or 108 do not exist as these integers do not occur as element orders in $PGU(3, 71)$. We can write $\deg(\Delta) = 3672 = 72 \cdot i + 2 \cdot j + 3 \cdot k$, for $0 \leq i+j+k \leq 107$. By direct checking with MAGMA, $(i, j, k) = (49, 3m, 2(24-m))$ for some $m = 0, \ldots, 10$ or $(i, j, k) = (50, 3m, 2(12-m))$ for some $m = 0, \ldots, 12$ or $(i, j, k) = (51, 0, 0)$. All these conditions force $G \cong \mathit{SmallGroup}(108, \ell)$ with $\ell = 6, \ldots, 45$.

  If $G \cong \mathit{SmallGroup}(108, 6)$ then $j = 0$ and hence $k \in \{48, 24, 0\}$. Since G contains 8 elements of order 3 we get that $k = 0$ and $(i, j, k) = (51, 0, 0)$. Here G contains 36 elements of order 12 which are all conjugated. They are all of type (B1) because otherwise G contains at least $36 + 18 + 1 + 2 > 51$ homologies, a contradiction. The center $Z(G) \cong C_6$ is generated by a homology as it has to commute with 6 groups of order 12 which are of type (B1). Also, G contains a normal cyclic group of order 18 which contains the central involution $\omega \in Z(G)$. If such a normal subgroup is generated by a homology then it must be contained in $Z(G)$, a contradiction. The same holds for the elements of order 6 and 3 contained in this normal subgroup. Thus G contains at most $107 - 36 - 2 - 2 - 6 = 61$ homologies. Arguing in the same way for the other elements of order 18 contained in G we get that G contains at most $61 - 12 = 49 < 51$ homologies, a contradiction.

  The case $G \cong \mathit{SmallGroup}(108, 7)$ cannot occur as a subgroup of $PGU(3, 71)$. In fact $Z(G) \cong C_{18}$ and it is generated by homologies as it has to commute with the elements of order 36 which are of type (B2) from [29, Thm. 2.7]. Clearly, the elements of order 12 contained in cyclic groups of order 36 are homologies as they are powers of elements of type (B2). This implies that there exist at least 6 elements of order 12 which are contained in $Z(G)$, a contradiction.

Assume that $G \cong SmallGroup(108, 8)$. Thus, $j = 0$ and $k = 0$ since G contains exactly 26 elements of order 3 which are normalized by involutions. This yields $(i, j, k) = (52, 0, 0)$. Arguing as in the previous case, we get that elements of order 12 and 4, which are all conjugated, are of type (B1), as they contain a central involution not belonging to the center of G. Thus G contains at most $107 - 4 \cdot 9 - 9 \cdot 2$ homologies. On the other hand, there exists no cyclic subgroup of G of order 6 generated by homology, containing a central involution, and not contained in the center of G and therefore $i \neq 52$.

If either $G \cong SmallGroup(108, 9)$, $G \cong SmallGroup(108, 10)$ or $G \cong SmallGroup(108, 11)$ then a contradiction is obtained arguing as in the previous case.

Denote by o_i the number of elements having order equal to i in G. We can exclude all the cases for which $o_2 + o_3 + o_4 + o_6 + o_9 + o_{12} + o_{18} = 107$, $o_2 = 1$ and $o_6 > 2$. This allows us to consider just the cases $G \cong SmallGroup(108, \ell)$ with $\ell \in \{12, 14, 15, \ldots, 31, 36, \ldots, 45\}$.

Assume that $G \cong SmallGroup(108, 12)$. Then G fixes an $\mathbb{F}_{71^2}$-rational point P with $p \notin \mathcal{H}_{71}$ as G has a central involution. Since G contains elements of type (B2), $Z(G)$ must be cyclic and generated by a homology. Thus, this case cannot occur.

Assume that $G \cong SmallGroup(108, 14)$. Since $j = 36$ we get that $(i, j, k) = (50, 36, 0)$. The elements of order 12 contained in $Z(G)$ are homologies. The other elements of order 12, the non-central elements of order 6, and the elements of order 18 in G are of type (B1), as the cyclic groups that they generate have non-trivial intersection with $Z(G)$, a contradiction. This yields that G contains at most 71 homologies. To have $i = 50$ we need 21 homologies more, but this cannot happen as the lengths of the conjugacy classes of the remaining elements in G are all even.

Assume $G \cong SmallGroup(108, 15)$. Here $j = 0$ and either $k = 0$ and $i = 51$ or $k = 24$ and $i = 50$. The elements of order 12 in G are of type (B1), because otherwise G contains at least $36 + 18 + 1$ homologies, a contradiction. This yields G to have at most 71 homologies. Since $Z(G)$ commutes with all these elements of type (B1) it is generated by a homology. We note that the elements of order 6 are of type (B1) because they are obtained as a composition $\alpha\beta$ where α is an involution which is not central and β is a central element of order 3. This implies that G contains at most $71 - 18 = 53$ homologies. The right number of homologies cannot be obtained as the elements of order 4 must be all homologies but the elements of order 3 are divided into conjugacy classes of length 12.

Assume that $G \cong \mathit{SmallGroup}(108,16)$. In this case $j=0$ and since G contains just 6 elements of order 3 we get $k=0$ and $i=51$. Looking at the conjugacy classes of elements in G we observe that G contains 39 involution, which are then homologies, and that just the elements of order 3 or 9 can be homologies as well, otherwise a direct computation shows that $i>51$. The unique possibility is that the normal subgroup C_9 of G is generated by a homology which implies that G fixes a point P which is $\mathbb{F}_{71^2}$-rational but $P \notin \mathcal{H}_{71}$. By [28, Page 6] C_9 must be contained in $Z(G)=\{id\}$, contradiction.

Assume that $G \cong \mathit{SmallGroup}(108,17)$. Since $j=0$ we have that either $i=50$ or $i=51$. Denote by $T := \{\alpha \in G \mid o(\alpha) \neq 2, \textit{ and } \alpha \textit{ is a homology}\}$. Then we require that either $|T|=23$ or $|T|=24$. Looking at the lengths of the conjugacy classes of elements in G we observe that they are all even, and hence the case $|T|=23$ cannot occur. Since the elements of order 6 are divided into three conjugacy classes each of length 18, they are all of type (B1) since otherwise $|T|>20$ and G contains no conjugacy classes of length 4 or two conjugacy classes of length equal to 2. Thus, the homologies of T are all of order 3. The unique possibility is that the remaining 24 homologies of order 3 are divided into 3 distinct conjugacy classes, of length 12, 6 and 6 respectively. This group cannot occur as a subgroup of $PGU(3,71)$ as every subgroup of type $C_3 \times C_3$ of $PGU(3,71)$ contains exactly 6 homologies and 2 elements of type (B1), a contradiction.

Assume that $G \cong \mathit{SmallGroup}(108,18)$. Denoting T as before, we note that $|T|=48$ as the lengths of the conjugacy classes of elements in G are all even. Since by a direct analysis of the conjugacy classes in G, $|T| \leq 31$, we have a contradiction.

Assume that $G \cong \mathit{SmallGroup}(108,19)$. Since G fixes a points P which is $\mathbb{F}_{71^2}$-rational but $P \notin \mathcal{H}_{71}$ and $Z(G)$ is cyclic and generated by a homology, we get that every $\beta \in G$ such that $\beta \notin Z(G)$ and $|Z(G) \cap \langle \beta \rangle| > 1$ is of type (B1). This implies that $48 = |T| \leq 29$, a contradiction.

Assume that either $G \cong \mathit{SmallGroup}(108,20)$ or $G \cong \mathit{SmallGroup}(108,21)$. Here we need $|T|=48$. Since the length of the 3 conjugacy classes of elements of order 9 is 24, we have that at most one of these conjugacy classes is given by homologies. Elements of order 3 split into 4 conjugacy classes each of length 2. Since they give rise to a subgroup of G which is isomorphic to $C_3 \times C_3$ we get that 6 of them are homologies while 2 of them are of type (B1) and that they fix the vertexes of a self-polar triangle. Since G contains also homologies of order 2 lying on the sides of the same triangles, G must contain also 6 homologies of order 6, which are obtained as a composition $\alpha\beta$ of homologies having a common center and such that $o(\alpha)=2$, $o(\beta)=3$. The remaining 24 elements of order 9 cannot be homologies since otherwise G must contain a subgroup isomorphic to

C_{18} generated by a homology of order 9 and an involution. Since this implies that $|T| < 51$ we have a contradiction.

Assume that $G \cong SmallGroup(108, 22)$. Here $j = 0$ and either $k = 0$ with $|T| = 48$, or $k = 48$ with $i = 46$ or $k = 24$ with $i = 47$. The lengths of the conjugacy classes of elements of order which is not equal to 2 are all even. This shows that the last case cannot occur. The elements of order 3 generate 13 subgroups of type $C_3 \times C_3$ sharing the same normal subgroup of G of order 3 which is generated by a homology, as different groups of type $C_3 \times C_3$ fix different $\mathbb{F}_{71^2}$-points. Since G contains 26 elements of type (B1) and the lengths of the conjugacy classes of elements of order 3 are $(24, 24, 24, 6, 2)$, where the last class is given by two homologies, this case cannot occur.

Assume that $G \cong SmallGroup(108, 23)$. In this case $|T| = 32$ and $Z(G) \cong C_6$. Since G contains two normal subgroup isomorphic to C_6, we note that just the central one is generated by a homology. Arguing as in the previous cases, observing that if $\alpha \notin Z(G)$ and $\langle \alpha \rangle \cap Z(G)$ is not trivial then α is of type (B1), we get that $|T| < 51$, a contradiction.

Assume that $G \cong SmallGroup(108, 24)$. In this case $Z(G) \cong C_{18}$ is generated by a homology, $(i, j, k) = (51, 0, 0)$ and $|T| = 44$. If $\alpha \notin Z(G)$ and $\langle \alpha \rangle \cap Z(G)$ is not trivial then α is of type (B1). This yields $|T| < 51$, a contradiction.

The cases $G \cong SmallGroup(108, 25)$ and $G \cong SmallGroup(108, 26)$ cannot occur as subgroups of $PGU(3, 71)$. In fact, it is sufficient to observe that from the number and intersection structures of subgroups of type $C_3 \times C_3$ of G at least a subgroup C_3 must be generated by a homology having the same center and axis of the generator of $Z(G)$. Since this implies that $C_3 \subseteq Z(G)$ but $|Z(G)| = 2$, we have a contradiction.

The case $G \cong SmallGroup(108, 27)$ cannot occur as G contains 55 involutions implying that $|T| > 55$.

Assume that $G \cong SmallGroup(108, 28)$. This case can be discarded observing that G contains 4 subgroups isomorphic to $C_3 \times C_3$, and hence 8 elements of type (B1). The lengths of the conjugacy classes of elements of order 3 are $(6, 6, 6, 6, 2)$ where the last two elements are contained in $Z(G)$ and hence are homologies, a contradiction.

Assume that $G \cong SmallGroup(108, 29) = C_9 \times C_3 \times C_2 \times C_2$. Here G fixes the vertexes of a self-polar triangle and we need $|T| = 52$. Since by direct checking $|T| = 3 + (2 + 2 + 2) + (2 + 2 + 2) + (6 + 6 + 6) = 33$, this case cannot occur.

Assume that $G \cong SmallGroup(108, 30)$ or $G \cong SmallGroup(108, 31)$. Then G fixes the vertexes of a self-polar triangle but G is not abelian, a contradiction.

Assume that $G \cong SmallGroup(108, 36)$. Then $(i, j, k) = (51, 0, 0)$ and $|T| = 42$. Since having homologies of order 12 would imply that $|T| > 42$, we get that they are all of type (B1) and $Z(G)$ is generated by a homology of order 3. Since there exist subgroups of type $C_3 \times C_3$ not containing the central element of order 3 this case cannot occur.

Assume that $G \cong SmallGroup(108, 37)$. Since $(i, j, k) = (51, 0, 0)$ then the elements of order 6 are homologies and there are just two elements of order 3 are of type (B1). Since these two elements must be contained in a subgroup C_6 generated by a homology we have a contradiction.

Assume that $G \cong SmallGroup(108, 38)$. This case cannot occur as G contains too many elements of order 3 fixing the vertexes of the same self-polar triangle.

Assume that either $G \cong SmallGroup(108, 39)$ or $G \cong SmallGroup(108, 40)$. In this case $k = 0$ and $|T| = 12$. Since G contains 13 subgroups of type $C_3 \times C_3$, and hence more than 12 homologies, this case cannot occur.

Assume that $G \cong SmallGroup(108, 41)$. In this case $Z(G) \cong C_3 \times C_3$ and the three involutions of G are not central, a contradiction.

Assume that $G \cong SmallGroup(108, 42)$. This group cannot occur as a subgroup of $PGU(3, 71)$ as it fixes a point P which is $\mathbb{F}_{71^2}$-rational but $P \notin \mathcal{H}_{71}$, its center is isomorphic to $C_3 \times C_3 \times C_2$ and G contains too many elements of order 3 fixing the same self-polar triangle.

Assume that $G \cong SmallGroup(108, 43)$. This group cannot occur as a subgroup of $PGU(3, 71)$ as G cannot normalize 5 groups of order 3.

The case $G \cong SmallGroup(108, 44)$ cannot occur as G contains 55 involution and hence $|T| > 51$.

Assume that $G \cong SmallGroup(108, 45)$. Since G fixes the vertexes of a self-polar triangle but contains more than one subgroup isomorphic to $C_3 \times C_3$ this case cannot occur.

- $|G| = 112$. From [29, Thm. 2.7] for $\sigma \in G$ we have $i(\sigma) \in \{0, 2, 72\}$. By direct checking with MAGMA the pairs (i, j) with $\deg(\Delta) = 3624 = 72 \cdot i + 2 \cdot j$ and $0 \leq i + j \leq 111$, are $(i, j) = (49, 48)$ and $(i, j) = (50, 12)$. Since there are no groups of order 112 having at least 49 elements of order equal to 2, 4 and 8 and either 48 or 12 elements of order in $\{7, 14, 16, 28, 56, 112\}$, this case cannot occur.
- $|G| = 120$. We write $\deg(\Delta) = 3528 = 71 \cdot i + 2 \cdot j + 3 \cdot k$ where $4 \leq i + j + k \leq 119$ as G contains at least a subgroup of type C_5 and hence $j \geq 4$ from [29, Thm. 2.7]. By direct checking with MAGMA either $(i, j, k) = (47, 3m, 2(24 - m))$ for some $m = 2, \ldots, 24$ or $(i, j, k) = (48, 3m, 2(12 - m))$ for some $m = 2, \ldots, 12$. Denote as before o_i the number of elements in G or order i. Then from [29, Thm. 2.7], $j = 119 - (o_2 + o_3 + o_4 + o_6 + o_8 + o_{12} + o_{24})$. Forcing 3 to divide j we get that no groups of order 120 satisfies the condition, a contradiction.
- $|G| = 126$. We write $\deg(\Delta) = 3456 = 72 \cdot i + 2 \cdot j + 3 \cdot k$, for some $6 \leq i + j + k \leq 125$, as G contains at least 6 elements of order 7 which implies $j \geq 6$ from [29, Thm. 2.7]. By direct checking with MAGMA, either $(i, j, k) = (45, 3m, 2(36 - m))$ for some $m = 2, \ldots, 8$, or $(i, j, k) = (46, 3m, 2(24 - m)$ for some $m = 2, \ldots, 24$, or

$(i, j, k) = (47, 3m, 2(12 - m))$ for some $m = 2, \ldots, 12$. There are 16 groups of order 126 up to isomorphism, we will denote them as $SmallGroup(126, \ell)$, with $\ell = 1, \ldots, 16$. Table 1 summarizes the possible values m, i, and k corresponding to each $G \cong SmallGroup(126, \ell)$ in order to obtain a quotient curve $\mathcal{H}_{71}/G$ of genus 7, according to the number of elements of order in $\{7, 14, 21, 42, 63, 126\}$, that is, the value of j.

Table 1. $G \cong SmallGroup(126, \ell)$, values for i, k and m

ℓ	m	(i, k)
1	6	(45,69), (46,36), (47,12)
2	12	(46,24), (47,0)
4	18	(46,12)
5	18	(46,12)
7	6	(45,60), (46,36), (47,12)
8	12	(46,24),(47,0)
9	6	(45,60), (46,36),(47,12)
10	12	(46,24),(47,0)
11	18	(46,12)
13	18	(46,12)
15	18	(46,12)

If $G \cong SmallGroup(126, 1)$ then G contains just 2 elements of order 2, a contradiction.

If $G \cong SmallGroup(126, 2)$ then G contains 2 elements of order 2 and hence $k = 0$ and $(i, j, k) = (47, 36, 0)$. The elements of order 18 in G are of type (B1) because otherwise $i > 47$, and all the remaining elements are homologies. Every subgroup $C_9 = \langle \alpha \rangle$ in G is such that α^3 generates the unique subgroup of order 3 of G. Since there exists just one cyclic group of order 9 generated by a homology having a fixed center, we have a contradiction.

Assume that $G \cong SmallGroup(126, 4)$. This case can be excluded observing that G contains just 2 elements of order 3, but we need $k = 12$.

The case $G \cong SmallGroup(126, 5)$ cannot occur as G contains just 2 elements of order 3.

Assume that $G \cong SmallGroup(126, 7)$. Since G contains 44 elements of order 3, either $(i, k) = (46, 36)$ or $(i, k) = (47, 12)$. A contradiction is obtained observing that the lengths of the conjugacy classes of elements of order 3 are $(14, 14, 14, 2)$ and hence neither $k = 36$ nor $k = 12$ can be obtained.

Assume that $G \cong SmallGroup(126, 8)$. Since the lengths of the conjugacy classes of elements of order 3 are $(28, 14, 2)$ we get that $(i, k) = (47, 0)$. The elements of order 6 are all of type (B1) because otherwise $i > 47$ and all the remaining elements are homologies. All these elements normalize a group isomorphic to C_3

which is generated by a homology, hence they share a fixed point and commute. This implies that every $\alpha\beta$ with $o(\alpha) = 2$ and $o(\beta) = 3$ generates an element of order 6. Since there are just 42 elements of order 6 we have a contradiction.

Assume that $G \cong \mathit{SmallGroup}(126, 9)$. A contradiction is obtained as before looking at the lengths of the conjugacy classes of elements of order 3 with respect to the admissible values of k.

Assume that $G \cong \mathit{SmallGroup}(126, 10)$. Since G normalizes an involution, we get that G fixes a point P which is $\mathbb{F}_{71^2}$-rational but $P \notin \mathcal{H}_{71}$. Thus G cannot contain Singer subgroups and $(i, j, k) = (47, 36, 0)$. Since G contains a unique element of order 2, which is central, arguing as before, we get that every element of order 6 that does not generate $Z(G)$ is of type (B1) because otherwise it would be central itself. Thus $Z(G)$ is generated by a homology, the remaining elements of order 6 are of type (B1) and the remaining elements of G are all homologies. Also, G contains 7 elementary abelian group of type $C_3 \times C_3$ and hence at least 14 elements of type (B1) of order 3, a contradiction.

The cases $G \cong \mathit{SmallGroup}(126, 13)$ and $G \cong \mathit{SmallGroup}(126, 15)$ cannot occur as G contains just 6 and 8 elements of order 3 respectively.

- $|G| = 128$. We write $\deg(\Delta) = 3432 = 72 \cdot i + 2 \cdot j$ with $0 \leq i + j \leq 127$. By direct checking with MAGMA this implies that either $(i, j) = (46, 60)$ or $(i, j) = (47, 24)$. Denote by o_i the number of elements in G having order equal to i. Since a group of order 126 with $o_{16} + o_{32} + o_{64} + o_{128} = 60$ and $127 - (o_{16} + o_{32} + o_{64} + o_{128}) \geq 46$ or $o_{16} + o_{32} + o_{64} + o_{128} = 24$ and $127 - (o_{16} + o_{32} + o_{64} + o_{128}) \geq 47$ does not exist, we get a contradiction.
- $|G| = 135$. Writing $\deg(\Delta) = 3348 = 71 \cdot i + 2 \cdot j + 3 \cdot k$ for $4 \leq i + j + k \leq 134$, we get that either $(i, j, k) = (43, 3m, 2(42 - m))$ for some $m = 2, \ldots, 7$, or $(i, j, k) = (44, 3m, 2(30 - m))$ for some $m = 2, \ldots, 29$, or $(i, j, k) = (45, 3m, 2(17 - m))$ for some $m = 2, \ldots, 17$, or $(i, j, k) = (46, 3m, 2(6 - m))$ for some $m = 2, \ldots, 6$. Since by direct checking with MAGMA there are no groups of order 135 with $o_3 + o_9 \geq 43$ and 3 dividing $134 - (o_3 + o_9) = j$, this case cannot occur.
- $|G| = 140$. We write $\deg(\Delta) = 3228 = 72 \cdot i + 2 \cdot j$ for some $4 \leq i + j \leq 139$. This yields either $(i, j) = (43, 96)$ or $(i, j) = (44, 60)$ or $(i, j) = (45, 24)$. Since there are no groups of order 140 with $o_2 + o_4 \geq 43$ and $139 - (o_2 + o_4) \in \{96, 60, 24\}$, this case cannot occur.
- $|G| = 144$. We write $\deg(\Delta) = 3240 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ for some $0 \leq i + j + k \leq 143$. By direct checking with MAGMA we get that $(i, j, k) = (41, 3m, 2(48 - m))$ for some $m = 0, \ldots, 6$, or $(i, j, k) = (42, 3m, 2(36 - m))$ for some $m = 0, \ldots, 29$, or $(i, j, k) = (43, 3m, 2(24 - m))$ for some $m = 0, \ldots, 24$, or $(i, j, k) = (44, 3m, 2(12 - m))$ for some $m = 0, \ldots, 12$, or $(i, j, k) = (45, 0, 0)$.

Assume that $G \cong \mathit{SmallGroup}(144, 1)$. In this case G contains 72 elements of order 16 which are of type (B2) by [29, Thm. 2.7]. Thus $Z(G) \cong C_8$ is generated by a homology. Arguing as before, since G has just one involution which is central, we get that G contains at most $8+1$ homologies, a contradiction.

If $G \cong \mathit{SmallGroup}(144,2)$ then G is cyclic and hence it contains 71 homologies, a contradiction.

Assume that $G \cong \mathit{SmallGroup}(144,3)$. Since $j=0$ and the number of elements of order 3 is 2 we have $(i,j,k)=(45,0,0)$. This implies that the 96 elements of order 9, which are all conjugated, are of type (B1), and all the remaining elements but 2 are homologies. The non-trivial elements of a group of order 3 are of type (B1) and obtained as powers of a homology of order 6, a contradiction.

Assume that $G \cong \mathit{SmallGroup}(144,4)$. In this case $Z(G) \cong C_2$, $(i,j,k) = (45,0,0)$ and, arguing as before, homologies can occur only of odd order. Then $i<45$, a contradiction.

Assume that $G \cong \mathit{SmallGroup}(144,\ell)$ for $\ell \in \{5,\ldots,27,31,\ldots,50\}$. Every cyclic group that intersects non-trivially $Z(G) \cong C_8$ is generated by an element of type (B1), G contains less than 41 homologies, a contradiction.

Assume that $G \cong \mathit{SmallGroup}(144,\ell)$ with $\ell \in \{28,29,30,51\}$. Here $m=24$ and G contains exactly one involution. Thus, $(i,j,k)=(47,72,0)$. A contradiction is obtained observing that G has one involution and the remaining elements are divided into conjugacy classes of even length.

Assume that $G \cong \mathit{SmallGroup}(144,52)$. Since G contains 8 elements of order 3 and $j=0$ we get $(i,j,k)=(45,0,0)$. A contradiction is obtained observing that $Z(G) \cong C_4$ is generated by a homology, G fixes a point P which is $\mathbb{F}_{71^2}$-rational but $P \notin \mathcal{H}_{71}$ and $i \le 39$.

Arguing as in the previous case, all $G \cong \mathit{SmallGroup}(144,\ell)$ with $\ell \in \{53,54,\ldots,62\}$ can be excluded.

Assume that $G \cong \mathit{SmallGroup}(144,\ell)$ with $\ell \in \{63,\ldots,67,69,70,71,72,74,76,\ldots,79,84,86,90,92,\ldots,95,100,105,\ldots,108,134\}$. A contradiction is obtained observing that G fixes the vertexes of a self-polar triangle and G is not abelian, thus G cannot occur as a subgroup of $PGU(3,71)$.

Assume that $G \cong \mathit{SmallGroup}(144,68)$. In this case G contains 98 elements of order 3 divided into 4 conjugacy classes of lengths $(28,28,28,2)$. The conjugacy classes of length 2 cannot be given by elements of Singer subgroups, as 2 divides the order of their normalizers. We note that $k \in \{96,72,48,24\}$ or $k=0$. Since $96,72,48,24$ are not divisible by 28, we get $(i,j,k)=(45,0,0)$. G contains 16 elementary abelian groups of order 9: this gives rise to $16 \cdot 4$ homologies and so this case can be excluded.

If $G \cong \mathit{SmallGroup}(144,73)$ then G has a normal involution and hence it fixes a point $P \notin \mathcal{H}_{71}$ which is $\mathbb{F}_{71^2}$-rational. As before we can obtain a contradiction noting that each cyclic group which intersects $Z(G)$ non-trivially is generated by an element of type (B1). This forces $i<45$, a contradiction.

In $G \cong SmallGroup(144,75)$ then either G fixes the vertexes of a self-polar triangle without being abelian or $i < 45$, a contradiction.

Assume that $G \cong SmallGroup(144,\ell)$ with $\ell \in \{80,81,82,83,85,89,97,99,115,121,122,124,126,128,\ldots,133,1135,\ldots,140\}$. Since G normalizes an involution, it fixes a point $P \notin \mathcal{H}_{71}$ which is $\mathbb{F}_{71^2}$-rational, hence $(i,j,k) = (45,0,0)$. Every cyclic group intersecting non-trivially $Z(G)$ is generated by an element of type (B1). Thus $i < 4$, a contradiction.

Assume that $G \cong SmallGroup(144,87)$. In this case $(i,j,k) = (45,0,0)$, G contains 37 involutions and 6 homologies of order 3 which are contained in a subgroup isomorphic to $C_3 \times C_3$. Then the number of the remaining homologies is $45-37-6 = 2$. Since there are no conjugacy classes for the remaining elements of length 2 we get a contradiction.

If $G \cong SmallGroup(144,\ell)$ with $\ell \in \{88,96\}$ then G contains more than 45 involutions, a contradiction.

Assume that $G \cong SmallGroup(144,91)$. This group cannot occur as a subgroup of $PGU(3,71)$ as the number and the conjugacy class structures of elements of order 6 are not compatible with the ones of elements of order 3 and 2.

Assume that $G \cong SmallGroup(144,98)$. The center $Z(G)$ is cyclic of order 2, and hence as before the elements that generate a cyclic group containing $Z(G)$ are of type (B1). Since G contains an elementary abelian group of order 9 and 37 involutions then G contains at least $37+(2+2+2)$ homologies and we need to find two extra homologies. Since C_4 is not central it cannot be generated by a homology. We get a contradiction looking at the lengths of the conjugacy classes of the remaining elements.

If $G \cong SmallGroup(144,104)$ then G contains at least 3 homologies of order 2, 6 homologies of order 3 and 6 homologies which are contained in a subgroup of type $C_6 \times C_6$. We need to find other extra 30 homologies, but this number is not compatible with the lengths of the remaining conjugacy classes, as 4 does not divide 30.

Assume that $G \cong SmallGroup(144,123)$. To obtain the right homologies configuration we need 12 homologies of order 4 and 6 homologies of order 6. The center $Z(G)$ is cyclic of order 6 and it is generated by a homology. Therefore the other elements α of order 6 such that $\langle \alpha \rangle \cap Z(G)$ is an element of order 3 in $Z(G)$ cannot be homologies because they are not central. A contradiction.

Assume that $G \cong SmallGroup(144,125)$. In this case G contains 37 homologies of order 2. We need $45-37$ extra homologies, but this is not compatible with the lengths of the conjugacy classes of elements in G.

Assume that $G \cong SmallGroup(144,127)$. Other than the involution we need G to contain 26 homologies and hence every element of order 3 must be a homology.

Since they form an elementary abelian group $C_3 \times C_3$ which contains at least 2 elements of type (B1) we get a contradiction.

- $|G| = 160$. Writing $\deg(\Delta) = 3048 = 72 \cdot i + 2 \cdot j$ for $4 \leq i + j \leq 159$ we get that $(i, j) \in \{(39, 120), (40, 84), (41, 48), 42, 12)\}$. Since by direct checking with MAGMA there are no groups of order 160 with at least 39 elements of order in $\{2, 4, 8\}$ and such that 3 divides the number of elements of order in $\{5, 10, 16, 20, 32, 40, 80, 160\}$, we get a contradiction.
- $|G| = 162$. We first observe that G must not contain elements of order in $\{27, 54, 81, 162\}$, since such orders do not occur for elements in $PGU(3, 71)$; see [29, Lemma 2.2]. Writing $\deg(\Delta) = 3024 = 72 \cdot i + 3 \cdot j$ for $0 \leq i + j \leq 161$ we get that $(i, j) \in \{(37, 120), (38, 96), (39, 72), (40, 48), (41, 24), (42, 0)\}$. Since by direct checking with MAGMA there are no groups of order 162 with at least 37 elements of order in $\tau = \{2, 6, 9, 18\}$ and such that either there no elements of order not in τ, or their number is divisible by 24, we get a contradiction.
- $|G| = 168$. Writing $\deg(\Delta) = 2952 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ for $6 \leq i + j + k \leq 159$ we get that $(i, j, k) = (36, 3m, 2(60 - m))$ for some $m = 2, \ldots, 11$, or $(i, j, k) = (37, 3m, 2(48 - m))$ for some $m = 2, \ldots, 34$, or $(i, j, k) = (38, 3m, 2(36 - m))$ for some $m = 2, \ldots, 36$, or $(i, j, k) = (39, 3m, 2(24 - m))$ for some $m = 2, \ldots, 24$, or $(i, j, k) = (40, 3m, 2(12 - m))$ for some $m = 2, \ldots, 12$. By direct checking with MAGMA the condition that either $j = 0$ or $3 \mid j$ and $i \geq 39$ yields $G \cong \mathit{SmallGroup}(168, \ell)$ with $\ell \in \{1, 4, 5, 7, \ldots, 18, 23, \ldots, 28, 34, \ldots, 38, 42, 43, 46, \ldots, 51, 53, 54, 56\}$.

  The cases $G \cong \mathit{SmallGroup}(144, \ell)$ with $\ell \in \{1, 7, \ldots, 11, 23, 42, 43, 47, 49, 53\}$ can be excluded because $2 \mid |Z(G)|$, which implies that G fixes a point $P \notin \mathcal{H}_{71}$ which is $\mathbb{F}_{71^2}$-rational and hence that $k = 0$, a contradiction to the required values (i, j, k) for $\deg(\Delta)$.

  The cases $G \cong \mathit{SmallGroup}(144, \ell)$ with $\ell \in \{4, 5, 12, \ldots, 18, 24, \ldots, 28, 34, 37\}$ can be excluded using the fact that $2 \mid |Z(G)|$. Hence every element of even order generating a cyclic group containing an involution of the center cannot be an homology without being central. This yields G to contain a small number of homologies.

  The cases $G \cong \mathit{SmallGroup}(144, \ell)$ with $\ell \in \{35, 36, 38, 46, 50, 56\}$ can be excluded because the number of involutions contained in G is greater than the total number of homologies that G can have according to the desired value of $\deg(\Delta)$.

  The cases $G \cong \mathit{SmallGroup}(144, \ell)$ with $\ell \in \{48, 54\}$ can be excluded because G fixes the vertexes of a self-polar triangle but G is not abelian.
- $|G| = 180$. Writing $\deg(\Delta) = 2808 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ for $4 \leq i + j + k \leq 179$ we get that $(33, 6, 140)$, or $(i, j, k) = (34, 3m, 2(60 - m))$ for some $m = 2, \ldots, 25$, or $(i, j, k) = (35, 3m, 2(48 - m))$ for some $m = 2, \ldots, 48$, or $(i, j, k) = (36, 3m, 2(36 -$

m)) for some $m = 2,\dots,36$, or $(i,j,k) = (37, 3m, 2(24-m))$ for some $m = 2,\dots,24$, or $(i,j,k) = (38, 3m, 2(12-m))$ for some $m = 2,\dots,12$.

The cases $G \cong \mathit{SmallGroup}(180,\ell)$ with $\ell \in \{1,10,14,23\}$ can be excluded as $5 \mid |Z(G)|$ yields G to contain too many homologies.

The cases $G \cong \mathit{SmallGroup}(180,\ell)$ with $\ell \in \{2,3,5,9,15,16,17\}$ can be excluded since $2 \mid |Z(G)|$ and hence every element of even order generating a cyclic group containing an involution of the center cannot be an homology without being central. This forces G to contain a small number of homologies.

The cases $G \cong \mathit{SmallGroup}(180,\ell)$ with $\ell \in \{7,11,25,27,29,30,34,36\}$ can be excluded since G contains too many involutions and hence too many homologies.

The cases $G \cong \mathit{SmallGroup}(180,\ell)$ with $\ell \in \{6,8,13,18,20,28,31,32,33,35,37\}$ can be excluded as they cannot occur as subgroups of $PGU(3,71)$.

The cases $G \cong \mathit{SmallGroup}(180,\ell)$ with $\ell \in \{12,22\}$ can be excluded as G fixes the vertexes of a self-polar triangle and it is not abelian.

The cases $G \cong \mathit{SmallGroup}(180,\ell)$ with $\ell \in \{19,21,26\}$ can be excluded since the value of i is not compatible with the lengths of the conjugacy classes of elements in G.

The case $G \cong \mathit{SmallGroup}(180,23)$ can be excluded since G acts on the vertexes of a self-polar triangle but its order does not divide the order of the maximal subgroup of $PGU(3,71)$ fixing globally a self-polar triangle; see [19, Thm. A.10].

- $|G| = 189$. Writing $\deg(\Delta) = 2700 = 72\cdot i + 2\cdot j + 3\cdot k$ for $6 \le i+j+k \le 179$ we get that $(i,j,k) = (32, 3m, 2(66-m))$ for some $m = 2,\dots,24$, or $(i,j,k) = (33, 3m, 2(54-m))$ for some $m = 2,\dots,47$, or $(i,j,k) = (34, 3m, 2(42-m))$ for some $m = 2,\dots,42$, or $(i,j,k) = (35, 3m, 2(30-m))$ for some $m = 2,\dots,30$, or $(i,j,k) = (36, 3m, 2(18-m))$ for some $m = 2,\dots,18$, or $(i,j,k) = (37, 3m, 2(6-m))$ for some $m = 2,\dots,6$. Forcing G to contain no elements of order in $\{27,189\}$, as they do not occur as orders of elements in $PGU(3,71)$ and the numerical conditions above, we get $G \cong \mathit{SmallGroup}(189,\ell)$ with $\ell \in \{3,\dots,13\}$. We have that $k \ge 1$ and G normalizes a cyclic group of order 7, which is generated by an element of type (B2) by [29, Thm. 2.7]. Such a group fixes at least a point $P \notin \mathcal{H}_{71}$ which is $\mathbb{F}_{71^2}$-rational and this implies that G cannot contain Singer subgroups. Therefore all these cases can be excluded.
- $|G| = 192$. Writing $\deg(\Delta) = 2664 = 72\cdot i + 2\cdot j + 3\cdot k$ for $0 \le i+j+k \le 179$ we get that $(i,j,k) = (31, 3m, 2(72-m))$ for some $m = 0,\dots,16$, or $(i,j,k) = (32, 3m, 2(60-m))$ for some $m = 0,\dots,39$, or $(i,j,k) = (33, 3m, 2(48-m))$ for some $m = 0,\dots,48$, or $(i,j,k) = (34, 3m, 2(36-m))$ for some $m = 0,\dots,36$, or $(i,j,k) = (35, 3m, 2(24-m))$ for some $m = 0,\dots,24$, or $(i,j,k) = (36, 3m, 2(12-m))$ for some $m = 0,\dots,12$, or $(i,j,k) = (37,0,0)$. Denote by o_i the number of elements of order i in G. Forcing, as for the previous case, G to have no elements

of order in $\{64, 96, 192\}$ and $o_3 \geq 24$ for $m = 0$, $o_3 \geq 8$ for $m = 32$, $o_3 \geq 16$ for $m = 16$, we get that $G \cong SmallGroup(192, \ell)$ with

$$\ell \in \{3, 4, 57, 58, 78, 79, 80, 81, 180, 181, 182, 184, \ldots, 199, 201, \ldots, 204, 944,$$
$$955, 956, 992, 1000, 1001, 1002, 1008, 1009, 1020, \ldots, 1025, 1489, \ldots, 1495,$$
$$1505, \ldots, 1508, 1509, 1538, 1540, 1541\}.$$

The cases $G \cong SmallGroup(192, \ell)$ with $\ell \in \{57, 58, 78, 79, 80, 81, 186, 187, 203, 204\}$ can be excluded as G normalizes an involution and hence it cannot contain Singer subgroups, but $m \neq 0$.

in the remaining cases a contradiction is obtained observing that the elements of order 3 form a unique conjugacy class in G and that o_3 is not equal to any value which is admissible for k.

- $|G| = 210$. Writing $\deg(\Delta) = 2448 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ for $10 \leq i + j + k \leq 209$ we get that $(i, j, k) = (27, 3m, 2(84 - m))$ for some $m = 4, \ldots, 14$, or $(i, j, k) = (28, 3m, 2(72 - m))$ for some $m = 4, \ldots, 37$, or $(i, j, k) = (29, 3m, 2(68 - m))$ for some $m = 4, \ldots, 60$, or $(i, j, k) = (30, 3m, 2(48 - m))$ for some $m = 4, \ldots, 48$, or $(i, j, k) = (31, 3m, 2(36 - m))$ for some $m = 4, \ldots, 36$, or $(i, j, k) = (32, 3m, 2(24 - m))$ for some $m = 4, \ldots, 24$, or $(i, j, k) = (33, 3m, 2(12 - m))$ for some $m = 4, \ldots, 12$. By direct checking with MAGMA $G \cong SmallGroup(210, \ell)$ with $\ell \in \{5, 6, 8, 9, 10, 12\}$. All these cases can be excluded as G cannot contain a sufficient number of homologies with respect to $\deg(\Delta)$.
- $|G| = 216$. Writing $\deg(\Delta) = 2376 = 72 \cdot i + 3 \cdot k$ for $0 \leq i + k \leq 215$ we get that $(i, k) \in \{(26, 168), (27, 144), (28, 120), (29, 96), (30, 72), (31, 48), (32, 24), (33, 0)\}$. By direct checking with MAGMA, forcing G to contain no elements of order in $\{27, 54, 108, 216\}$, we get $G \cong SmallGroup(216, \ell)$ with $\ell \in \{12, \ldots, 20, 25, \ldots, 177\}$.

  Cases $G \cong SmallGroup(216, 12)$ and $G \cong SmallGroup(216, 13)$ cannot occur as G fixes the vertexes of a self-polar triangle and G is not abelian.

  Assume that $G \cong SmallGroup(216, 14)$. A contradiction can be obtained since $2 \mid |Z(G)|$ and hence every element of even order generating a cyclic group containing an involution of the center cannot be an homology without being central. This yields G to contain a small number of homologies.

  Cases $G \cong SmallGroup(216, 15)$ and $G \cong SmallGroup(216, 16)$ cannot occur as subgroups of $PGU(3, 71)$, since $Z(G)$ must contain at least a subgroup of order 3.

  Case $G \cong SmallGroup(216, 17)$ can be excluded as G contains $16 + 11$ homologies, a contradiction.

  Assume that $G \cong SmallGroup(216, 18)$. In this case G fixes the vertexes of a self-polar triangle T and it is abelian. This implies that G is contained is the stabilizer in $PGU(3, 71)$ of T which is abelian and isomorphic to $C_{72} \times C_{72}$. Suppose that G is such that $g(\mathcal{H}_{71}/G) = 7$. Then the quotient curve $\mathcal{H}_{71}/G$ would inherit the quotient group $C_{72} \times C_{72}/G$ which is abelian of order 24. Since $PSL(2, 8)$ does not contain abelian subgroup of order 216, the claim follows.

Assume that $G \cong \mathit{SmallGroup}(216, 19)$ or $G \cong \mathit{SmallGroup}(216, 20)$. Since G has a unique involution, as before, G cannot contain Singer subgroups and hence $i = 33$. Since G contains 4 distinct subgroups isomorphic to $C_3 \times C_3$, G contains 16 homologies of order 3. The center $Z(G)$ is generated by a homology of order 24. This proves that G contains at least 39 homologies, a contradiction.

Assume that $G \cong \mathit{SmallGroup}(216, 25)$. As in the previous cases $i = 33$, G fixes a point $P \notin \mathcal{H}_{71}$ which is $\mathbb{F}_{71^2}$-rational, and G contains no Singer subgroups. This group cannot occur as a subgroup of $PGU(3, 71)$ as it contains 4 groups isomorphic to $C_3 \times C_3$ sharing a fixed homology of order 3 having center at P. Since they generate 8 elements of order 3 and of type (B1), we have a contradiction to the conjugacy class structure of elements of order 3 in G.

The cases $G \cong \mathit{SmallGroup}(216, \ell)$ with $\ell \in \{26, 27, 30, \ldots, 86, 100, \ldots, 152\}$ cannot occur as a subgroup of $PGU(3, 71)$ as G has to contain at least a central element of order 3, while $3 \nmid |Z(G)|$.

The cases $G \cong \mathit{SmallGroup}(216, \ell)$ with $\ell \in \{28, 29\}$ can be excluded since G contains too many involutions with respect to the desired value of i.

Assume that $G \cong \mathit{SmallGroup}(216, 87)$. In this case G contains too many involution compared to the desired value for i.

The case $G \cong \mathit{SmallGroup}(216, 88)$ cannot occur as a subgroup of $PGU(3, 71)$ as G contains 4 elementary abelian groups of order 9, which generate exactly 8 elements of type (B1) and order 3. This fact is in contradiction with the structure of the conjugacy classes of elements of order 3 in G.

The cases $G \cong \mathit{SmallGroup}(216, \ell)$ with $\ell \in \{89, 90, 91, 98\}$ cannot occur as G must contain at least a central element of order 2.

If $G \cong \mathit{SmallGroup}(216, 92)$ then, looking at the structure of the elementary abelian subgroups of G, G contains at least $12 \cdot 4 + 2 + 18 + 3$ homologies, a contradiction.

The cases $G \cong \mathit{SmallGroup}(216, \ell)$ with $\ell \in \{93, 94, 96, 97, 99, 165\}$ can be excluded as G contains too many involution with respect to the desired value for i.

If $G \cong \mathit{SmallGroup}(216, 95)$ then G contains at least $13 \cdot 4 + 2 + 18 + 3$ homologies, a contradiction.

If $G \cong \mathit{SmallGroup}(216, \ell)$ with $\ell \in \{153, 154, 156, 157, 158, 159, 160, 161, 162, 163, 164, 166, 167\}$, then G contains too many homologies with respect to the desired value for i. This fact can be deduced looking at the number and the structure of subgroups isomorphic to $C_3 \times C_3$ and the number of involutions in G.

If $G \cong SmallGroup(216,\ell)$ with $\ell = 168,\dots,177$ then G contains an abelian subgroup of order 54, a contradiction to [19, Thm. 11.79] as $4g+4=32$.

If $G \cong SmallGroup(216,155)$ then either $(i,k)=(33,0)$ or $(i,k)=(32,24)$. In fact the lengths of the conjugacy classes C_1, C_2 and C_3 of elements of order 3 are $|C_1|=8$ are $|C_2|=1$, $|C_3|=4$ and $\sigma \in C_1$ cannot be such that $i(\sigma)=3$ since it is a power of an element of order 6. Assume that $(i,k)=(33,0)$. We note that the elements of order 3 generate 13 elementary abelian groups of order 9. Since $k=0$ each of them must contain exactly two elements of type (B1) and 6 elements of type (A). Since one elementary abelian group is given by 8 elements of order 3 which are all conjugated, this case cannot occur. Assume now that $(i,k)=(32,24)$. In particular the number of homologies which are not involutions must be equal to $32-9=23$. The elements of order 8 or 12, which are conjugated, cannot be homologies since their number is strictly greater than 23. If elements of order 6 or 4 are generated by homologies then G contains exactly either $18+2+9=29$ or $18+9=27$ homologies, a contradiction.

- $|G| = 224$. We write $\deg(\Delta) = 2280 = 72\cdot i + 2\cdot j$, for some $6 \le i+j \le 223$. By direct checking with MAGMA $(i,j) \in \{(27,168),(28,132),(29,96),(30,60),(31,24)\}$. Since for every $G \cong SmallGroup(224,\ell)$ with $\ell=1,\dots,197$ we have that $j=96$, we need $(i,j)=(29,96)$. Forcing G to contain at least 29 elements of order a divisor of 72, we have $G \cong SmallGroup(224,\ell)$ with

$$\ell \in \{8,\dots,11,13,14,16,19,\dots,26,28,30,31,36,\dots 43,63,\dots,67,71,\dots 74,$$
$$82,\dots,87,91,\dots,96,100,101,102,104,107,110,112,115,\dots,121,128,$$
$$129,130,131,137,\dots,141,143,146,147,174,181,187\}.$$

Assume that $G \cong SmallGroup(224,\ell)$ for some $\ell \in \{8,9,10,14,16,19,20,\dots,24,26,36,37,38,41,63,\dots,67,72,73,74,82,83\}$. Then G fixes the vertexes of a self-polar triangle T and G is not abelian, a contradiction.

If $G \cong SmallGroup(224,\ell)$ for $\ell \in \{11,13,25,28,30,31\}$ then G contains at least 33, 33, 17, 17, 15, 29 homologies, a contradiction.

If $G \cong SmallGroup(224,\ell)$ with $\ell \in \{39,40,42,43,143,146\}$ then G normalizes an element γ of type (B2). Denote by P,Q,R the fixed points of γ; then they are $\mathbb{F}_{71^2}$-rational and $P \notin \mathcal{H}_{71}$, $Q,R \in \mathcal{H}_{71}$. Thus, G fixes P and $G \le \mathcal{M}_{71} = Stab_{PGU(3,71)}(P)$. If $\alpha \in G$ is a homology then either $\alpha(Q)=Q$ and $\alpha(R)=R$ which implies $\alpha \in Z(\mathcal{M}_{71})$ (see [28, Page 6]), or $o(\alpha)=2$ and $\alpha(R)=Q$ as homologies act with long orbits outside their center. Since the number of involutions in G is not equal to 29 and $|Z(G)|=2$, we have a contradiction.

If $G \cong SmallGroup(224,71)$ then G contains too many involution, and hence too many homologies, with respect to $i=29$.

By direct checking with MAGMA, excluding the cases for which G fixes the vertexes of a self-polar triangle but G is not abelian, we just need to analyze $G \cong SmallGroup(224, \ell)$ with $\ell \in \{96, 101, 102, 104, 107, 110, 112, 137\}$.

If $G \cong SmallGroup(224, \ell)$ with $\ell \in \{96, 101, 102, 104, 137\}$ then G contains more than 29 involution and hence more than 29 homologies, a contradiction.

If $G \cong SmallGroup(224, 107)$, $G \cong SmallGroup(224, 110)$, $G \cong SmallGroup(224, 112)$ then G contains at least 23, 19, 15 homologies. The extra homologies cannot be found because of the lengths of the conjugacy classes of elements in G.

- $|G| = 240$. We write $\deg(\Delta) = 2088 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ where $4 \le i + j + k \le 239$. By direct checking with MAGMA, Table 2 gives the complete list of possibilities for the triple (i, j, k).

TABLE 2. Admissible values for (i, j, k)

i	j	k	m
20	3m	2(108-m)	m=2,3
21	3m	2(96-m)	m=2,...,26
22	3m	2(84-m)	m=2,...,49
23	3m	2(72-m)	m=2,...,72
24	3m	2(60-m)	m=2,...,60
25	3m	2(48-m)	m=2,...,48
26	3m	2(36-m)	m=2,...,36
27	3m	2(24-m)	m=2,...,24
28	3m	2(12-m)	m=2,...,12

Also, Table 3 gives the complete list of cases $G \cong SmallGroup(240, \ell)$ that have to be considered. For each case the required triple (i, j, k) is described.

TABLE 3. Required values for m, k and i for $G \cong SmallGroup(240, \ell)$

ℓ	m	k	i
$1, \ldots, 4$	72	0	23
32	64	16	23
89,...,91	16	16	27
92, ..., 94	32	8	26
105, ..., 110	32	8$= o_3$	26
189	16	16	27
190	32	8	26
191	64	16	23
194	32	8$= o_3$	26
197,198	32	8$= o_3$	26
204	64	16	27

If $G \cong SmallGroup(224,1)$ then G normalizes an element γ of type (B2). Denote by P,Q,R the fixed points of γ; then they are $\mathbb{F}_{71^2}$-rational and $P \notin \mathcal{H}_{71}$ but $Q,R \in \mathcal{H}_{71}$. Thus, G fixes P and $G \leq \mathcal{M}_{71} = Stab_{PGU(3,71)}(P)$ and if $\alpha \in G$ is a homology then either $\alpha(Q)=Q$ and $\alpha(R)=R$ which implies $\alpha \in Z(\mathcal{M}_{71})$ (see [28, Page 6]), or $o(\alpha)=2$ and $\alpha(R)=Q$ as homologies act with long orbits outside their center. This implies that G contains 39 homologies, a contradiction.

If $G \cong SmallGroup(240,3)$ then G contains just 7 homologies, a contradiction.

The cases $G \cong SmallGroup(240,\ell)$ where $\ell \in \{32,89,\ldots,94,191,204\}$ can be excluded as G must contain Singer subgroups but elements of order 3 form a unique conjugacy class in G with $o_3 \neq k$.

The cases $G \cong SmallGroup(240,\ell)$ where $\ell \in \{105,107,\ldots,110,189,190\}$ can be excluded as G must contain Singer subgroups but all elements of order 3 are normalized by at least one involution and hence they cannot be elements from Singer subgroups of $PGU(3,71)$.

The cases $G \cong SmallGroup(240,\ell)$ where $\ell \in \{106,194,197,198\}$ can be excluded as G contains too many involution compared to the desired value for i.

- $|G|=243$. We write $\deg(\Delta)=2052=72\cdot i+3\cdot j$ for $0 \leq i+j \leq 242$. Also, note that elements of order in $\{27,81,243\}$ cannot exist as they do not occur as element of $PGU(3,71)$, see [29, Lemma 2.2]. This yields $G \cong SmallGroup(243,\ell)$ with $\ell \in \{47,51,\ldots,67\}$. By direct checking with MAGMA $(i,j) \in \{(20,204),(21,180),(22,156),(23,132),(24,108),(25,84),(26,60),(27,36),(28,12)\}$ and hence G must contain Singer subgroups of order 3.

If $G \cong SmallGroup(243,47)$ then the elements of order 3 of G such that their contribution to $\deg(\Delta)$ is 3 are either 0 or 18, since 243 does not divide the order of the normalizer of a Singer subgroup of $PGU(3,71)$; see [19, Thm. A.10]. Since 18 is not an admissible value for k we have a contradiction.

If $G \cong SmallGroup(243,\ell)$ for $\ell \in \{51,52,53,54\}$ then, arguing as in the previous case, the normal subgroups of order 3 cannot be Singer subgroups as 243 does not divide the order of the normalizer of a Singer subgroup of $PGU(3,71)$. Since they generate an elementary abelian group of order 9, G contains 3 normal homologies of order 3, and hence G fixes the vertexes of a self-polar triangle. This proves that G cannot contain Singer subgroups, a contradiction.

Assume that $G \cong SmallGroup(243,\ell)$ where $\ell \in \{55,56,57,58,59,60,61,62,63,64,65,66\}$, then G contains a central subgroup of order 3 which is generated by a homology. In fact it is a power of more than 9 different elements of order 9 where at least two of them are of type (B1) and fix different self-polar triangles. Thus G fixes a point P off $\mathcal{H}_{71}$ which is $\mathbb{F}_{71^2}$-rational and hence $j=0$, a contradiction.

If $G \cong \mathit{SmallGroup}(243, 67)$ then G is an elementary abelian 3-group. As before G contains no Singer subgroups as all the elements of order 3 are normal in G and 243 does not divide the order of the normalizer of a Singer subgroup of $PGU(3, 71)$, a contradiction.

- $|G| = 252$. There exist 46 different structures for groups of order 252 up to isomorphism. We write $\deg(\Delta) = 1944 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ for some $6 \leq i + j + k \leq 251$. By direct checking with MAGMA Table 4 summarizes the possibilities for (i, j, k) with respect to $\deg(\Delta)$.

TABLE 4. Admissible values for (i, j, k)

i	j	k	m
18	3m	2(108-m)	m=2,...,17
19	3m	2(96-m)	m=2,...,40
20	3m	2(84-m)	m=2,...,63
21	3m	2(72-m)	m=2,...,72
22	3m	2(60-m)	m=2,...,60
23	3m	2(48-m)	m=2,...,48
24	3m	2(36-m)	m=2,...,36
25	3m	2(24-m)	m=2,...,24
26	3m	2(12-m)	m=2,...,12

All the cases $G \cong \mathit{SmallGroup}(252, \ell)$ with $\ell \in \{1, 2, 3, 4, 5, 7, 13, 14, 16, \ldots, 19, 22, 24, 43, 45\}$ can be excluded as G contains just one involution which is central. This implies that non-central elements of even order cannot be homologies. We get that the number of homologies in G is strictly less that 18, a contradiction.

If $G \cong \mathit{SmallGroup}(252, 6)$ then, denoting by φ the Euler totient function, G contains exactly $1 + 2 + 2 + 2 + \varphi(9) + \varphi(12) + \varphi(18) + \varphi(36) = 35$ homologies, a contradiction.

If $G \cong \mathit{SmallGroup}(252, 8)$ then, G contains too many involution with respect to the desired value of i, a contradiction.

If $G \cong \mathit{SmallGroup}(252, 9)$ then G fixes the vertexes of a self-polar triangle but G is not abelian, a contradiction.

All the cases $G \cong \mathit{SmallGroup}(252, \ell)$ with $\ell \in \{10, 11, 21, 23, 27, 29, 31, 32, 35, 38, 39, 40, 42\}$ can be excluded as G normalizes a cyclic subgroup of order 7 which is generated by an element of type (B2), by [29, Lemma 2.2]. Thus, if $\alpha \in G$ is a homology then either $\alpha \in Z(G)$ or $o(\alpha) = 2$. This proves that G cannot contain i homologies.

All the cases $G \cong \mathit{SmallGroup}(252, \ell)$ with $\ell \in \{12, 15, 25, 26, 30, 33, 34, 36, 37, 41, 46\}$ can be excluded as G contains too many homologies with respect to the desired value of i.

The case $G \cong SmallGroup(252,20)$ cannot occur as a subgroup of $PGU(3,71)$ as $Z(G)$ must be cyclic.

Assume that $G \cong SmallGroup(252,28)$. Then G fixes a point $P \notin \mathcal{H}_{71}$ which is $\mathbb{F}_{71^2}$-rational as G normalizes an involution. This implies that G cannot contain Singer subgroups and hence all the elements of order 3 are either of type (B1) or homologies. Since G contains 7 subgroups isomorphic to $C_3 \times C_3$, it contains at least 29 homologies of order 3. Also, G contains 15 involution, a contradiction.

The case $G \cong SmallGroup(252,44)$ cannot occur as a subgroup of $PGU(3,71)$ as at least an element of order 3 must be central but $3 \nmid |Z(G)|$.

- $|G| = 270$.There exist 30 structures for groups of order 252 up to isomorphism. We write $\deg(\Delta) = 1728 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ for some $4 \le i + j + k \le 269$. Forcing G to contain no elements of order in $\{27, 54, 135, 270\}$, we get $G \cong SmallGroup(270, \ell)$ with $\ell \ge 5$. By direct checking with MAGMA Table 5 summarizes the possibilities for (i, j, k) with respect to $\deg(\Delta)$.

Table 5. Admissible values for (i, j, k)

i	j	k	m
14	3m	2(120-m)	m=2,...,15
15	3m	2(108-m)	m=2,...,38
16	3m	2(96-m)	m=2,...,61
17	3m	2(84-m)	m=2,...,84
18	3m	2(72-m)	m=2,...,72
19	3m	2(60-m)	m=2,...,60
20	3m	2(48-m)	m=2,...,48
21	3m	2(36-m)	m=2,...,36
22	3m	2(24-m)	m=2,...,24
23	3m	2(12-m)	m=2,...,12

If $G \cong SmallGroup(270, \ell)$, $\ell = 5, 6, 7$ then G contains 31, 7, 7 homologies, a contradiction.

The cases $G \cong SmallGroup(270, \ell)$ with $\ell \in \{8, 9\}$ can be excluded as they do not occur as subgroups of $PGU(3, 71)$.

The cases $G \cong SmallGroup(270, \ell)$ with $\ell \in \{10, 11\}$ can be excluded as G normalizes a cyclic subgroup of order 5, which is generated by an element of type (B2), by [29, Thm. 2.7], and hence the unique homologies of G are either central or of order 2. Since i is not equal to the sum of the number of element of order 2 and the number of the remaining non-trivial elements of $Z(G)$, this case cannot occur.

The cases $G \cong SmallGroup(270, \ell)$ with $\ell \in \{12, 14, 15, 16, 18, 19, 27, 28, 29\}$ can be excluded as G contains too many involutions with respect to the desired number of homologies i. By direct checking all the remaining cases do not occur as subgroups of $PGU(3,71)$.

- $|G| = 280$. We write $\deg(\Delta) = 1608 = 72 \cdot i + 2 \cdot j$ for some $10 \leq i + j \leq 279$. By direct checking with MAGMA, $(i,j) \in T = \{(15,264),(16,228),(17,192),(18,156),(19,120),(20,84),(21,48),(22,12)\}$. Denote by o_i the number of elements of order i in G. Since there are no groups of order 280 with $(o_5+o_7+o_{10}+o_{14}+o_{20}+o_{28}+o_{35}+o_{40}+o_{56}+o_{70}+o_{140}+o_{280}) \in \{12,48,84,120,156,192,228,264\}$ and $(o_2+o_4+o_8) \geq i_j$ where i_j denotes the value of i corresponding to $j = (o_5+o_7+o_{10}+o_{14}+o_{20}+o_{28}+o_{35}+o_{40}+o_{56}+o_{70}+o_{140}+o_{280})$ in T, this case cannot occur.
- $|G| = 288$. As before we can exclude all $SmallGroup(288,\ell)$ with $\ell = 1,\ldots,1045$ containing elements of order in $\{32,96,288\}$. Writing $\deg(\Delta) = 1512 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ with $0 \leq i + j + k \leq 287$ we get that $i = 10,\ldots,21$. We observe that $G \cong SmallGroup(288,\ell)$ is such that $2 \mid |Z(G)|$ unless $\ell \in \{73,74,75,397,406,407,634,635,636\}$. If $2 \mid |Z(G)|$ then G cannot contain Singer subgroups as they cannot be centralized by involutions; see [19, Thm. A.10]. This implies that $k = 0$ and hence $(i,j) \in \{(14,258),(15,222),(17,150),(18,114),(19,78),(20,42),(21,6)\}$. Since there are no groups of order 288 with $(o_{16}+o_{48}+o_{144}) \in \{258,222,186,150,114,78,42,6\}$ all these cases cannot occur.

  Assume that $G \cong SmallGroup(288,\ell)$ with $\ell = 73,74,75$. These cases can be excluded as G does not contain sufficient elements of order 3.

  Assume that $G \cong SmallGroup(288,\ell)$ with $\ell \in \{397,406,407,634,635,636\}$. These cases can be excluded as the desired values for k are not compatible with the lengths of the conjugacy classes of elements of order 3 in G.
- $|G| = 315$. We can write $\deg(\Delta) = 1188 = 72 \cdot i + 2 \cdot j + 3 \cdot k$, where $10 \leq i+j+k \leq 314$. Denote by o_i the number of elements of order i in G. By [29, Thm. 2.7], $j = o_5 + p_{15} + o_{21} + o_{35} + o_{45} + o_{63} + o_{105} + o_{315}$, while $i \leq o_3 + o_9$ and $k \leq o_3$.

  If $G \cong SmallGroup(315,1)$ then $j = 270$ and hence to obtain the right value for $\deg(\Delta)$ either $(i,k) = (8,24)$ or $(i,k) = (9,0)$. Since G contains at least $6 \cdot 7 + 2 = 44$ homologies, and elements of order 9 must be homologies, we get a contradiction.

  Assume that $G \cong SmallGroup(315,3)$. Then $j = 270$ and hence either $(i,k) = (8,24)$ or $(i,k) = (9,0)$. Since G contains at least 42 homologies this case can be excluded.

  The case $G \cong SmallGroup(315,4)$ can be excluded as it does not occur as a subgroup of $PGU(3,71)$.
- $|G| = 320$. We note that G cannot contain elements of order in $\{32,64,160,320\}$ as they cannot be contained in $PGU(3,71)$. We write $\deg(\Delta) = 1128 = 72 \cdot i + 2 \cdot j$ where $4 \leq i+j \leq 319$. Then by direct checking $(i,j) \in$

$\{(7,312),(8,276),(9,240),(10,204),(11,168),(12,132),(13,96),(14,60),15,24)\}$. Since there are no groups of order 320 with $o_2+o_4+o_8 \geq 7$ and $j = 319-(o_2+o_4+o_8) \in \{312,276,240,204168,132,96,60,24\}$, these cases can be excluded.

- $|G| = 324$. We write $\deg(\Delta) = 1080 = 72 \cdot i + 3 \cdot k$ for $0 \leq i+k \leq 324$. Then

$$(i,k) \in \{(2,312),(3,288),(4,264),(5,240),(6216),(7,192),(8,168),(9,144),$$
$$(10,120),(11,96),(12,72),(13,48),(14,24),(15,0)\}.$$

Also, G cannot contain elements of order in $\{27,54,81,108,162,324\}$ as they cannot be contained in $PGU(3,71)$.

Assume that $G \cong SmallGroup(324,\ell)$ with $\ell \in \{8,19,23,25\}$. Then 2 divides $|Z(G)|$ and hence G cannot contain Singer subgroups. This case can be excluded as at least an element of order 3 must be contained in $Z(G)$ but $3 \nmid |Z(G)|$.

The cases $G \cong SmallGroup(324,\ell)$ with $\ell \in \{13,14,16,18,20,22,24\}$ can be excluded as they do not contain Singer subgroups, because $2 \mid |Z(G)|$ and, looking at the number and the intersections of subgroups isomorphic to $C_3 \times C_3$ we get that G contains a number of homologies different from i.

The cases $G \cong SmallGroup(324,\ell)$ with $\ell \in \{46,47,48,83,87,89,101\}$ cannot occur as G fixes the vertexes of a self-polar triangle but G is not abelian.

All the remaining cases $G \cong SmallGroup(324,\ell)$ with $\ell \in \{49,50,51,\ldots,176\}$ can be excluded as they do not contain Singer subgroups and looking at the number and the intersections of subgroups isomorphic to $C_3 \times C_3$ we get that G contains number of homologies different from i.

- $|G| = 336$. We write $\deg(\Delta) = 936 = 72\cdot i+2\cdot j+3\cdot k$ with $6 \leq i+j+k \leq 335$. By direct checking, every $G \cong SmallGroup(336,\ell)$ with $\ell = 1,\ldots,228$ and $\ell \neq 114$ has a unique subgroup of order 7, which is hence characteristic.

Case $G \cong SmallGroup(336,114)$ cannot occur as a subgroup of $PGU(3,71)$. Thus we can assume that G has a unique Sylow 7-subgroup, say S. Since a generator of S is of type (B2) from [29, Thm. 2.7], G fixes a point $P \notin \mathcal{H}_{71}$ which is $\mathbb{F}_{71^2}$-rational and G does not contain Singer subgroups. In all the remaining admissible cases we have that $(i,j) \in \{(9,144),(5,288)\}$. Assume that $j = 288$. Then $G \cong SmallGroup(336,\ell)$ with $\ell \in \{56,74,75,78,\ldots,83,86,88,89,106,\ldots,113,115117,168,\ldots,170,190,192,204\}$.

Assume that $G \cong SmallGroup(336,56)$. Then $Z(G) \cong C_7$ and hence every element of order 3 is a homology. Since this implies that $i > 5$ we have a contradiction.

A contradiction to $i = 5$ is obtained also for $G \cong SmallGroup(336,\ell)$ with $\ell \in \{74,75,78,80,86,88,109,110,111,112,113,115,117,168,170,204\}$.

If $G \cong SmallGroup(336,\ell)$ with $\ell \in \{79,81,82,83,89,106,107,108,169,192\}$ then G fixes the vertexes of a self-polar triangle and G is not abelian, a contradiction.

The case $G \cong SmallGroup(336, 190)$ cannot occur as a subgroup of $PGU(3, 71)$ as the involution obtained as a power of an element of order 14 must be central. Assume that $j = 144$. Then $G \cong SmallGroup(336, \ell)$ with $\ell \in \{38, 39, 40, 62, 72, 94, 104\}$. Since in all these cases the number of homologies of G is 3 while $i = 9$, we have a contradiction.

- $|G| = 360$. We write $\deg(\Delta) = 648 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ where $4 \leq i + j + k \leq 359$. Thus, $i \leq 8$. We note that for every $G \cong SmallGroup(360, \ell)$ with $\ell = 1, \ldots, 162$ and $\ell ne 51$, G has a unique Sylow 5-subgroup, which is generated by an element of type (B2) from [29, Thm. 2.7]. This implies, as before, that G fixes a point P off $\mathcal{H}_{71}$ and every element of order 3 or 9 is a homology. Denote by o_i the number of elements of order i in G. Since for every $\ell \neq 51$ we have that $o_2 + o_3 + o_9 \geq 9$, while $i \leq 8$ we have a contradiction.

  Thus, assume that $G \cong SmallGroup(336, 51)$. Since G contains 5 homologies which belong to $Z(G)$ whereas all the elements of even order dividing 72 are of type (B1), we have that G contains exactly $5 + 20 \cdot i_1 + 40 \cdot i_2$ for some i_1 and i_2, a contradiction.
- $|G| = 378$. We write $\deg(\Delta) = 432 = 72 \cdot i + 2 \cdot j + 3 \cdot k$, where $6 \leq i + j + k \leq 377$. Since $i \leq 5$, G must contain at most 5 involutions and it contains no elements of order in $\{27, 54, 189, 378\}$. These conditions yield $G \cong SmallGroup(378, \ell)$ with $\ell \in \{2, 6, 16, , 23, 24, 25, 26, 27, 28, 33, 44, 45, , 46, 48, 52, 54, 60\}$. All these cases can be excluded observing that G has a unique Sylow 7-subgroup, which implies that every element of order 3 or 9 is a homology. This yields $i > 5$, a contradiction.
- $|G| = 384$. As before, G contains no elements of order in $\{32, 64, 96, 128, 192, 384\}$ and we write $\deg(\Delta) = 360 = 72 \cdot i + 2 \cdot j + 3 \cdot k$ for $0 \leq i + j + k \leq 383$. By direct checking with MAGMA $i \leq 4$ and $G \cong SmallGroup(384, \ell)$ with $\ell \leq 20169$ has 3 involutions. Thus, G contains at most one extra homology. If G contains one extra homology then G contains at least 2 extra homology, since its order is at least equal to 3. Thus $i = 3$ and G contains no homology of order different from 2. When $o_2 eq 3$ a direct checking with MAGMA shows that $2 \mid |Z(G)|$, hence G normalizes an involution and G fixes a point $P \notin \mathcal{H}_{71}$ which is $\mathbb{F}_{71^2}$-rational. Also, G normalizes a group of type $C_2 \times C_2$ and acts on the vertexes of a self-polar triangle. This implies that every element of order 3 is an homology. Since G contains at least 2 elements of order 3 we have a contradiction.
- $|G| = 405$. Here G contains no elements of order in $\{81, 135, 405\}$ and we write $\deg(\Delta) = 108 = 72 \cdot i + 2 \cdot j + 3 \cdot k$, obtaining either $(i, j, k) = (0, 3m, 2(18 - m))$ for some $m = 2, \ldots, 54$, or $(i, j, k) = (1, 3m, 2(6 - m))$ for some $m = 2, \ldots, 6$. By direct checking with MAGMA if $G \cong SmallGroup(405, \ell)$ with $\ell \neq 15$ then G has a unique Sylow 5-subgroup. This implies that every element of order 3 is a homology and then $i \geq 2$, a contradiction. Thus we assume that $G \cong SmallGroup(405, 15)$.

In this case $j = o_5 + o_{15} + o_{27} + o_{45} = 324$. Since 324 is not an admissible value for j we have a contradiction.

□

Question 6.4. From Theorem 6.3 the Fricke-Macbeath curve $\mathcal{F}$ is not a Galois subcover of the Hermitian curve of $\mathcal{H}_{72}$ over $\mathbb{F}_{71^2}$. It is still an open problem to determine whether $\mathcal{F}$ is covered by $\mathcal{H}_{72}$ or not. We observe that if $\mathcal{F}$ is covered by $\mathcal{H}_{72}$ over $\mathbb{F}_{71^2}$, then $\mathcal{F}$ provides the first known example of a maximal curve which is covered but not Galois covered by the Hermitian curve over the finite field of maximality. Otherwise, $\mathcal{F}$ provides the first known example of an $\mathbb{F}_{p^2}$-maximal curve which is not covered by the Hermitian curve over the field of maximality.

Acknowledgement

The authors would like to thank Massimo Giulietti for numerous discussions on the topic which led to significant improvements. The third author would like to thank Università degli Studi di Perugia for the financial support received during his academic visit in January-February 2017.

References

[1] Arakelian, N., Tafazolian, S., Torres, F.: On the spectrum for the genera of maximal curves over small fields, *Adv. Math. Commun.*, to appear.

[2] Biggs, N. L., White, A. T.: Permutation groups and combinatorial structures, *London Mathematical Society Lecture Note Series*, **33**, Cambridge University Press, Cambridge-New York, (1979), 140 pp.

[3] Brock, B. W.: Superspecial curves of genera two and three, Thesis (Ph.D.) Princeton University, (1993), 69 pp.

[4] Cossidente, A., Korchmáros, G., Torres, F.: Curves of large genus covered by the Hermitian curve, *Comm. Algebra*, **28**, (2000), no. 10, 4707-4728.

[5] Edge, W. L.: A canonical curve of genus 7, *Proc. LMS(3)*, **17**, (1967), 207-225.

[6] Elkies, N. D.: The existence of infinitely many supersingular primes for every elliptic curve over $\mathcal{Q}$, *Invent. Math.*, **89**(3), (1987), 561-567.

[7] Elkies, N. D.: Shimura curve computations, in: 'Algorithmic number theory' (Portland, OR, 1998, J. P. Buhler, ed.), 1-47, *Lecture Notes in Comput. Sci.*, **1423**, Springer-Verlag, Berlin, 1998.

[8] Fanali, S., Giulietti, M.: On maximal curves with Frobenius dimension 3, *Des. Codes Cryptogr.*, **53**, (2009), no. 3, 165–174.

[9] Fanali, S., Giulietti, M., Platoni, I.: On maximal curves over finite fields of small order. *Adv. Math. Commun.*, **6**, (2012), no. 1, 107-120.

[10] Fricke, R.: Ueber eine einfache Gruppe von 504 Operationen, *Math. Ann.*, **52**, (1899), 321-339.

[11] Fuhrmann, R., Garcia, A., Torres, F.: On maximal curves, *J. Number Theory*, **67** (1997), no. 1, 29-51.

[12] Fuhrmann, R., Torres, F.: The genus of curves over finite fields with many rational points, *Manuscripta Math.*, **89**, (1996), 103-106.

[13] Garcia, A., Stichtenoth, H., Xing, C.P.: On subfields of the Hermitian function field, *Compositio Math.* **120** (2), (2000), 137-170.

[14] Garcia, A., Tafazolian, S.: Certain maximal curves and Cartier operators, *Acta Arith.*, **135**, (2008), 199-218.

[15] Garcia, A., Torres, F.: On maximal curves having classical Weierstrass gaps, Applications of curves over finite fields (Seattle, WA, 1997), 49-59, *Contemp. Math., 245, Amer. Math. Soc.*, Providence, RI, (1999).

[16] Giulietti, M., Korchmáros, G.: A new family of maximal curves over a finite field, *Math. Ann.*, vol. 343, pp. 229–245, 2009.

[17] Gunby, B., Smith, A., Yuan, A.: Irreducible canonical representations in positive characteristic, *Res. Number Theory* **1**, (2015), Art. 3, 25 pp.

[18] Hidalgo, R. A.: Edmonds maps on the Fricke-Macbeath curve, *Ars Math. Contemp.*, **8**, (2015), 275-289.

[19] Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: *Algebraic Curves over a Finite Field*. Princeton Series in Applied Mathematics, Princeton (2008).

[20] Ihara, Y.: Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo*, **28**, (1981), 721-724.

[21] Kantor, W. M., O'Nan, M. E., Seitz, G. M.: 2-transitive groups in which the stabilizer of two points is cyclic. *J. Algebra*, **21**, (1972), 17–50.

[22] Klein, F.: Ueber die Transformation siebenter Ordnung der elliptischen Functionen, *Math. Ann.*, **14**, (1989), 428-471.

[23] Lachaud, G.: Sommes d'Eisentein et nombre de points de certaines courbes algébriques sur les corps finis, *C.R. Acad. Sci. Paris*, **305**, (1987), 729-732.

[24] Korchmáros, G.; Torres, F.: On the genus of a maximal curve, *Math. Ann.*, **323**, (2002), no. 3, 589-608.

[25] Ma, L., Xing, C.: On subfields of the Hermitian function fields involving the involution automorphism, arXiv:1707.07314.

[26] Macbeath, A.: On a curve of genus 7, *Proceedings of the London Mathematical Society*, **15**, (1965), 527-542.

[27] Magaard, K., Völklein, H.: On Weierstrass points of Hurwitz curves, *J. Algebra*, **300**, (2006), no. 2, 647-654.

[28] Montanucci, M., Zini, G.: On the spectrum of genera of quotients of the Hermitian curve, arXiv:1703.10592.

[29] Montanucci, M., Zini, G.: Some Ree and Suzuki curves are not Galois covered by the Hermitian curve, *Finite Fields Appl.* to appear.

[30] Rück, H.G., Stichtenoth, H.: A characterization of Hermitian function fields over finite fields, *J. Reine. Angew. Math.*, **457**, (1994), 185-188.

[31] Schoeneberg, B.: Über die Weierstrass-Punkte in den Körpern der elliptischen Modulfunktionen, *Abh. Math. Sem. Univ. Hamburg*, **17**, (1951), 104-111.

[32] Shimura, G.: Construction of class fields and zeta functions of algebraic curves, *Ann. of Math.*, **85**, (1967), 58-159.

[33] Tafazoliam, S., Teherán-Herrera, A., Torres, F.: Further examples of maximal curves which cannot be covered by the Hermitian curve, *J. Pure Appl. Algebra*, **220**(3), (2016), 1122–1132.

[34] Tafazolian, S., Torres, F.: A note on certain maximal curves, *Comm. Algebra*, **45**, (2017), no. 2, 764-773.

[35] Top, J., Verschoor, C.: Counting points on the Fricke-Macbeath curve over finite fields, *J. Th. des Nombres Bordeaux*, to appear, (2016).

[36] Valentini, R. C.: Hyperelliptic curves with zero Hasse-Witt matrix, *Manuscripta Math.*, **86**, (1995), no. 2, 185-194.

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 Informatica ed Economia, Università degli Studi della Basilicata, Campus di Macchia Romana, viale dell'Ateneo Lucano 10, 85100 Potenza, Italy

E-mail address: maria.montanucci@unibas.it

IMECC/UNICAMP, R. Sérgio Buarque de Holanda 651, Cidade Universitária "Zeferino Vaz", 13083-859, Campinas, SP-Brazil

E-mail address: ftorres@ime.unicamp.br