$\mathbb{F}_{p^2}$-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, $q = p^t$ with p prime. It is sometimes attribute 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 $t \equiv 0 \pmod 3$. In this paper, we show that if an $\mathbb{F}$-maximal curve $\mathcal{X}$ of genus $g \geq 2$, $q = p$, 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 $q = p = 71$ 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

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

Ihara [30] proved that if $\mathcal{X}$ is $\mathbb{F}$-maximal of genus g then $g \leq q(q-1)/2$. Also, equality holds if and only if $\mathcal{X}$ is $\mathbb{F}$-isomorphic to the Hermitian curve, namely the plane curve $\mathcal{H}_{q+1}$: $y^{q+1} = x^q + x$; see Rück and Stichtenoth [42]. For surveys on maximal curves we refer the readers to [13–17, 19, 42, 45, 50, 51].

Maximal curves have also been investigated for their applications in Coding theory. In fact, Algebraic-Geometric codes constructed from maximal curves have the largest possible minimum distances with the respect to other parameters since they have the maximum number of rational points compared with their genus; see [26,38,39,43,44,48,53–55]. Also, many examples of maximal curves have large automorphism groups and codes constructed from them inherit a large number of symmetries and therefore can have good performance in encoding [27] and decoding [31].

In general it is quite difficult to prove the maximality of a given curve $\mathcal{X}$. A well-known approach is based on a result of Kleiman [33], sometimes attributed to Serre (see [35]),

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

stating that any non-singular curve which is $\mathbb{F}$-covered by an $\mathbb{F}$-maximal curve is also $\mathbb{F}$-maximal. Concrete examples of $\mathbb{F}$-maximal curves which all are Galois-covered by $\mathcal{H}_{q+1}$ can be found e.g. in [6, 20, 36, 40].

For a long time it has been conjectured that all $\mathbb{F}$-maximal curves are covered by a Hermitian curve; see e.g. [52]. This conjecture was disproved by Giulietti and Korchmáros [23, 46], who exhibited an example of $\mathbb{F}$-maximal curve $\mathcal{C}$, with $q = p^{3h} > 8$, p is a prime, non-covered by the Hermitian curve. The curve $\mathcal{C}$ has a large automorphism group whose size exceeds the classical Hurwitz bound $84(g(\mathcal{C}) - 1)$.

Up to now the Giulietti-Korchmáros curve and some of its quotients are the only known examples of $\mathbb{F}$-maximal curves which are not covered by the Hermitian curve; see [24, 46]. It is somehow natural to ask whether there exist other curves with this feature, also when $q \neq p^{3h}$ for any $h \geq 1$. A generalization of Giulietti-Korchmáros curve, often called the Garcia-Güneri-Stichtenoth (GGS) curve or the generalized GK curve, was introduced in [18].

In this paper we deal with the case $q = p$. Our main result is summarized in Theorem 1.1. We show that an $\mathbb{F}_{p^2}$-maximal curve with a large automorphism group and not Galois-covered by the Hermitian curve $\mathcal{H}_{p+1}$ cannot exist. This emphasizes once more the importance of the Giulietti-Korchmáros curve among the class of maximal curves.

Theorem 1.1. *Let p be a prime and $\mathbb{F} = \mathbb{F}_{p^2}$ the finite field 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 $\mathrm{Aut}(\mathcal{X})$ does not satisfy the classical Hurwitz bound; i.e., $|\mathrm{Aut}(\mathcal{X})| > 84(g-1)$, then $\mathcal{X}$ is Galois-covered by the Hermitian curve $\mathcal{H}_{p+1} : y^{p+1} = x^p + x$ over $\mathbb{F}$.*

The bound $Aut(\mathcal{X}) > 84(g-1)$ in Theorem 1.1 is sharp. As we show in Theorem 4.4 the so-called *Fricke-Macbeath* curve over $\mathbb{F}_{71^2}$ is $\mathbb{F}$-maximal and not covered by $\mathcal{H}_{71}$. Such a curve is named after Robert Fricke who first studied it as Riemann surface in the early 1899; see [12]. Since the size of its automorphism group is exactly $84(g-1)$, this shows that the bound in Theorem 1.1 is sharp and it cannot be further improved in general.

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 $q = p^t$ 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 a characterization of $\mathcal{H}_m$ involving automorphisms of curves. This characterization is due to Garcia and Tafazolian, see [21, Thm. 5.2] and [47, 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.*

Lemma 2.2. *The curve $\mathcal{H}_m$ above is Galois-covered over $\mathbb{F}$ 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 $g = g(\mathcal{H}_m) = (m-1)(q-1)/2$.*

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 Σ' is the fixed field of G on 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 [29, 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 $P \in \mathcal{X}$. We recall that an *orbit* (resp. a *stabilizer*) of P in G 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 of G on $\mathcal{X}$ when $|G| > 84(g(\mathcal{X})-1)$; see [29, Thm 11.56, Thm. 11.126].

Theorem 2.3. *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 G has at most three short orbits on $\mathcal{X}$ as follows*:

(1) *Exactly three short orbits*: *one non-tame and two tame. Each point in each tame short orbit 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 non-tame tame and one 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 $q(q-1)/2$*;
   - *$p = 2$, $q_0 = 2^s$, $q = 2q_0^2$ 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 an $\mathbb{F}$-maximal curve $\mathcal{X}$ fixes exactly one $\mathbb{F}$-rational point of $\mathcal{X}$.

Lemma 2.4. ([25, 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 $\mathbb{F}$.*

Corollary 2.5. *Let p denote the characteristic of the finite field $\mathbb{F} = \mathbb{F}_{q^2}$ where $q = p^t$ and let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve with $g = g(\mathcal{X}) \geq 2$ such that $p \mid |\mathrm{Aut}(\mathcal{X})|$. If H is a p-subgroup of $\mathrm{Aut}(\mathcal{X})$, then H fixes exactly one point $P \in \mathcal{X}(\mathbb{F})$ and acts semiregularly on the set of the remaining $\mathbb{F}$-rational points of $\mathcal{X}$. In particular, if $p \nmid g$, then every p-element in $\mathrm{Aut}(\mathcal{X})$ has order at most equal to q.*

Proof. Assume first that H is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$. Then from Lemma 2.4, H acts on the set $\mathcal{X}(\mathbb{F})$ of $\mathbb{F}$-rational points of $\mathcal{X}$. Since $|\mathcal{X}(\mathbb{F})| \equiv 1 \pmod p$, S must fix at least a point $P \in \mathcal{X}(\mathbb{F})$. Also, $\mathcal{X}$ has zero p-rank and hence the claim follows from [29, Lemma 11.129]. Now assume that H is an arbitrary p-subgroup of $\mathrm{Aut}(\mathcal{X})$. Since H is contained in at least a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$ and the properties of fixing a point $P \in \mathcal{X}$ and being semiregular are preserved by subgroups the claim follows for H as well. □

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 2.6. *Let p be a prime and $\mathbb{F}$ a field of order p^2. Let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve of genus g such that there exists $G \leq \mathrm{Aut}(\mathcal{X})$ with $p \mid |G|$. 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 2.5, H has exactly one fixed point P which is thus $\mathbb{F}$-rational. Clearly H acts semiregularly on $\mathcal{X}(\mathbb{F}) \setminus \{P\}$ and so $|H| \mid (p^2 + 2gp)$. From the Riemann-Hurwitz formula $2g - 2 = p(2a_2 - 2) + (a_1 + 2)(p - 1)$, so that

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

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 [42], 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

$$2g - 2 = p^2(2g(\mathcal{X}/S) - 2) + (a_4 + 2)(p^2 - 1) + a_3 p(p-1)\,,$$

for some non-negative integers a_3, a_4. 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 [29, Lemma 11.75 (v)]. Thus,

$$p(p-1) > 2g = 2g(\mathcal{X}/S)p^2 + a_4(p^2-1) + a_3 p(p-1)\,.$$

By direct checking, since a_4, a_3 and $g(\mathcal{X}/S)$ are non-negative, this implies that $g(\mathcal{X}/S) = a_4 = a_3 = 0$ and hence $g = 0$, a contradiction. □

In the following lemma the known results on $\mathbb{F}$-maximal curves of high genus are collected; see [13, 15, 30, 34, 42].

Lemma 2.7. *Let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve of genus $g = g(\mathcal{X})$, where $\mathbb{F} = \mathbb{F}_{q^2}$.*

(1) *$g \leq g_2 := \lfloor (q^2 - q + 4)/6 \rfloor$, or $g = g_1 := \lfloor (q-1)^2/4 \rfloor$, or $g = g_0 := q(q-1)/2$;*
(2) *$g = g_0$ if and only if $\mathcal{X}$ is $\mathbb{F}$-isomorphic to $\mathcal{H}_{q+1}$;*
(3) *$g = g_1$ if and only if $\mathcal{X}$ is $\mathbb{F}$-isomorphic to $\mathcal{H}_{(q+1)/2}$ (resp. $y^{q+1} = x^{q/2} + \ldots + x$) if q is odd (resp. q even). In particular, in this case $\mathcal{X}$ is a cyclic quotient of the Hermitian curve $\mathcal{H}_{q+1}$ of order 2.*

Corollary 2.8. *Let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve of genus g with $\mathbb{F} = \mathbb{F}_{p^2}$, $p \geq 7$ a prime. Let a_1 and a_2 be as in Lemma 2.6 and suppose that one of the following conditions holds*:

(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 Lemma 2.7. 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 Lemma 2.7. □

3. Proof of Theorem 1.1

Throughout this section, let $\mathcal{X}$ be an $\mathbb{F}$-maximal curve of genus g, where $\mathbb{F} = \mathbb{F}_{p^2}$ with p a prime. To prove Theorem 1.1, we first analyze the case in which $p \leq 5$.

3.1. **Case: $p \leq 5$.** Here we do not need the hypothesis $|\mathrm{Aut}(\mathcal{X})| > 84(g-1)$. For $p = 2$ and $p = 3$ the result is trivial by Lemma 2.7. For $p = 5$ we use the complete classification, up to isomorphism, of $\mathbb{F}_{25}$-maximal curves given in [10].

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

Proof. From [10, Thm. 11], $g(\mathcal{X}) \in \{0, 1, 2, 3, 4, 10\}$ where

(1) $g = 10$ if and only if $\mathcal{X} \cong \mathcal{H}_6 : y^6 = x^5 + x$ over $\mathbb{F}_{25}$;
(2) $g = 4$ if and only if $\mathcal{X} \cong \mathcal{H}_3 : y^3 = x^5 + x$ over $\mathbb{F}_{25}$;
(3) $g = 3$ if and only if $\mathcal{X} \cong \mathcal{C} : y^6 = x^5 + 2x^4 + 3x^3 + 4x^2 + 3xy^3$ over $\mathbb{F}_{25}$,
(4) $g = 2$ if and only if $\mathcal{X} \cong \mathcal{H}_2 : y^2 = x^5 + x$ over $\mathbb{F}_{25}$,
(5) $g(\mathcal{X}) = 1$ if and only if $\mathcal{X} \cong \mathcal{D} : y^2 + x^3 + 1 = 0$ over $\mathbb{F}_{25}$.

The cases (2) and (4) are Galois covered by $\mathcal{H}_6$ by Lemma 2.2. The elliptic curve given in (5) is Galois covered by $\mathcal{H}_6$ as this curve can also be described by the Fermat equation $y^6 + x^6 + 1 = 0$. Then $\mathcal{D} = \mathcal{H}_6/G$, where

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

Finally, to prove that $\mathcal{C}$ is also Galois covered by $\mathcal{H}_6$, since there is an unique, up to isomorphism, $\mathbb{F}_{25}$-maximal curve of genus 3 which is Galois covered by $\mathcal{H}_6$ [6, Thm. 5.6], it is sufficient to construct a quotient curve of $\mathcal{H}_6$ of genus 3. This follows considering the plane curve

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

From [6, Prop. 2.1], the curve $\mathcal{Z}$ equals $\mathcal{H}_6/H$ where $H \leq \mathrm{Aut}(\mathcal{H}_6)$ is a subgroup of order 3 of a Singer group of order 21. □

3.2. **Case $p \geq 7$.** Here we assume that $\mathcal{X}$ is an $\mathbb{F}_{p^2}$-maximal curve of genus $g \geq 2$ such that $|\mathrm{Aut}(\mathcal{X})| > 84(g-1)$ so that one of the cases listed in Theorem 2.3 is satisfied. Let us start by showing that cases (1) and (2) in that result cannot occur.

Lemma 3.2. *There is no $\mathbb{F}_{p^2}$-maximal curve $\mathcal{X}$ whose full automorphism group $\mathrm{Aut}(\mathcal{X})$ satisfies any of the following property:*

(1) *It admits exactly one non-tame short orbit O_1 and two tame short orbits O_2 and O_3.*
(2) *It admits exactly two non-tame short orbits O_1 and O_2.*

Proof. (1) By Theorem 2.3 $\mathcal{X}$ is not isomorphic to $\mathcal{H}_{p+1}$, as the Hermitian curve is a particular subcase of Theorem 2.3(4). In particular, from Lemma 2.6 $p \mid |\mathrm{Aut}(\mathcal{X})|$ but $p^2 \nmid |\mathrm{Aut}(\mathcal{X})|$. Let H be a p-Sylow subgroup of $\mathrm{Aut}(\mathcal{X})$. From Corollary 2.5 H fixes exactly one $\mathbb{F}_{p^2}$-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

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

Indeed the points in O_1 contribute to the Riemann-Hurwitz formula as follows. First, from the Orbit-Stabilizer Theorem $|\mathrm{Aut}(\mathcal{X})|/(1+np)$ is the order of the stabilizer $\mathrm{Aut}(\mathcal{X})_P$ of every point $P \in O_1$. Since p divides $|\mathrm{Aut}(\mathcal{X})_P|$ for all $P \in O_1$ but p^2 does not, every higher ramification group at P is either trivial or of order p. Hence a_1+1 counts the number of non-trivial ramification groups, including the first one which is a conjugate of H in $\mathrm{Aut}(\mathcal{X})$. We now assume that $n>0$. From Lemma 2.7 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)

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

Since this implies that $2a_2p = p$, we have a contradiction.

(2) From Corollary 2.5 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. □

Now we deal with cases (3) and (4) of Theorem 2.3.

Lemma 3.3. *Let $\mathcal{X}$ be an $\mathbb{F}_{p^2}$-maximal curve and assume that $\mathrm{Aut}(\mathcal{X})$ satisfies any of the following properties*:

(1) *It has exactly one non-tame short orbit O_1;*
(2) *It 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. We can clearly assume that $\mathcal{X}$ is not isomorphic to $\mathcal{H}_{p+1}$, so that from Lemma 2.6 a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$ has order p and Lemma 2.6 can be used to write the genus of $\mathcal{X}$. 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 $n \geq 0$.

(1) From [29, 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. Since $p^2+2g+1 = |\mathcal{X}(\mathbb{F}_{p^2})| = |O_1| + t|\mathrm{Aut}(\mathcal{X})|$ and $|O_1|$ divides $|\mathrm{Aut}(\mathcal{X})|$ from the Orbit-Stabilizer Theorem, $|O_1|$ divides p^2+2g+1.

This implies three possible cases: either $|O_1| = (p+1)^2$ (a) or $|O_1| = 1$ (b) or $|O_1| = p+1$ (c).

(a) holds. Here from Lemma 2.7, $p(p-1)-2 > 2g-2 \geq (p+1)^2$, a contradiction.

(b) holds. Here 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 $a_2 > 0$.

(c) holds. 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 2.8.

(2) **Case 1:** $\mathcal{X}(\mathbb{F}_{p^2}) = O_1 \cup O_2$. From the Riemann-Hurwitz formula

$$2g-2 = |\mathrm{Aut}(\mathcal{X})|(-2) + (1+np)\Big[(a_1+1)(p-1) + \frac{|\mathrm{Aut}(\mathcal{X})|}{1+np} - 1\Big]$$
$$+(p^2+1+2gp-1-np)\Big(\frac{|\mathrm{Aut}(\mathcal{X})|}{p^2+1+2gp-1-np} - 1\Big) \quad \text{and hence}\,,$$
$$2g-2 = (1+np)[(a_1+1)(p-1)-1] - (p^2+(2g-n)p)\,.$$

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 $P \in O_1$ 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 [29, 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 [29, (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

$$a_2 \geq \frac{a_1p^2+p^2-a_1p-4p-1}{4p} \geq \frac{p^2-4p-1}{4p}\,, \quad \text{while } g \geq \frac{p(p^2-4p-1)}{4p} > g_3\,.$$

If $p \geq 11$ this gives a contradiction from [13]. 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 [11, 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

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

Then $2a_2p - p = -|O_2|$, a contradiction since $a_2 > 0$.

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 2.8. If O_2 is contained in $\mathcal{X}(\mathbb{F}_{p^2})$, $p^2+1+2gp-(p+1)-|O_2|$ 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

$$2g - 2 = -2|\mathrm{Aut}(\mathcal{X})|$$
$$+(1 + np)\Big(\frac{|\mathrm{Aut}(\mathcal{X})|}{1 + np} - 1 + (a_1 + 1)(p - 1)\Big) + |O_2|\Big(\frac{|\mathrm{Aut}(\mathcal{X})|}{|O_2|} - 1\Big) \quad \text{and hence}\,,$$
$$|O_2| = p[-2a_2 - n + 1 + n(a_1 + 1)(p - 1)]\,.$$

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 $p^2+1+2gp-1-np = p(p+2g-n)$, we have that $p+2g-n = p(1 + a_1 + 2a_2) - a_1 - n$. 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 $n \neq 1$.

□

Thereferore the proof of Theorem 1.1 follows from Theorem 2.2 and Lemmas 3.2, 3.3.

We end this section with the following natural question.

Question 3.4. Is Theorem 1.1 true in general for $\mathbb{F}_{p^{2n}}$-maximal curves where $n \geq 2$? For example, is it true that every $\mathbb{F}_{p^4}$-maximal curve having a large automorphism group is Galois-covered by the Hermitian curve? The answers to these questions seem to be more involved and arguing as we did in Section 3 would give a larger number of exceptions to be considered.

4. On the hypothesis concerning the classical Hurwitz's bound

Let p be a prime and $\mathbb{F}$ be the finite field of order p^2. In view of Theorem 1.1, a natural question arises:

Is any $\mathbb{F}$-maximal curve $\mathcal{X}$ of genus $g = g(\mathcal{X})$ Galois-covered by $\mathcal{H}_{p+1}$ also when the classical Hurwitz's bound

$$|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1) \tag{4.1}$$

holds true?

As a matter of fact, it is not difficult to find examples of such curves which are then not $\mathbb{F}$-isomorphic to $\mathcal{H}_m : y^m = x^p + x$ with $m \mid (p+1)$.

Example 4.1. 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 [20, Ex. 6.4, Case 1].

Even if the previous example is given by a Galois subcover of the Hermitian curve, our aim now is to show that the bound $|\mathrm{Aut}(\mathcal{X})| > 84(g-1)$ in Theorem 1.1 is sharp, that is, there exists an $\mathbb{F}_{p^2}$-maximal curve $\mathcal{X}$ of genus $g \geq 2$ with $|\mathrm{Aut}(\mathcal{X})| = 84(g-1)$ such that $\mathcal{X}$ is not Galois-covered by the Hermitian curve $\mathcal{H}_{p+1}$ over $\mathbb{F}_{p^2}$.

In fact, we present an $\mathbb{F}_{71^2}$-maximal curve of genus 7 such that (4.1) holds which is not $\mathbb{F}_{71^2}$-Galois covered by $\mathcal{H}_{72}$. The starting point is the plane equation over the complex field

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

which defines the unique compact Riemann surface $\mathcal{F}$ of genus 7 such that $\mathrm{Aut}(\mathcal{F}) \cong PSL(2,8)$ (so that equality in (4.1) holds true); see Fricke [12], Macbeath [37], Edge [7], Hidalgo [28]. The curve $\mathcal{F}$ is referred nowadays as the *Fricke-Macbeath curve*. This curve was considered over finite fields by Top and Verschoor [49]. In particular, we have the following.

Proposition 4.2. *Let p be a prime, $p \equiv \pm 1 \pmod{14}$, and $\mathbb{F} = \mathbb{F}_{p^2}$. Then the Fricke-Macbeath curve $\mathcal{F}$ above is $\mathbb{F}$-maximal if and only if the elliptic curve $\mathcal{E} : y^2 - (x^3 + x^2 - 114x - 127) = 0$ is so.*

Proof. From [49, 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 4.3. By direct checking with MAGMA, the curve $\mathcal{F}$ is $\mathbb{F}_{p^2}$-maximal for $p \in \{71, 251, 503, 2591\}$ and $\mathrm{Aut}(\mathcal{X}) \cong PSL(2,8)$. Moreover, 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 [8].

The main result of this section is the following.

Theorem 4.4. *The Fricke-Macbeath curve $\mathcal{F}$ above is $\mathbb{F}_{71^2}$-maximal of genus 7 with $\mathrm{Aut}(\mathcal{F}) \cong PSL(2,8)$ but it is not a Galois subcover of $\mathcal{H}_{72}$. In particular, the bound $|\mathrm{Aut}(\mathcal{X})| > 84(g-1)$ in Theorem 1.1 is sharp.*

Proof. We only need to show the assertion on the covering. The proof is long and very technical. 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,

$$\frac{|\mathcal{H}_{72}(\mathbb{F}_{71^2})|}{|\mathcal{F}(\mathbb{F}_{71^2})|} \leq |G| \leq \frac{2g(\mathcal{H}_{72})-2}{2g(\mathcal{F})-2},$$

which yields $60 \leq |G| \leq 414$, as $2g(\mathcal{H}_{72})-2 = 4968$ and $2g(\mathcal{F})-2 = 12$. Since $|G|$ divides $|PGU(3,71)|$, we have to deal with 47 cases, namely

$$\begin{aligned} |G| \in \{&60, 63, 64, 70, 71, 72, 80, 81, 84, 90, 96, 105, 108, 112, 120, 126, \\ &128, 135, 140, 142, 144, 160, 162, 168, 180, 189, 192, 210, 213, 216, 224, \\ &240, 243, 252, 270, 280, 284, 288, 315, 320, 324, 336, 355, 360, 378, 384, 405\}. \end{aligned} \tag{4.2}$$

The different divisor Δ has degree

$$\deg(\Delta) = \sum_{\sigma \in G \setminus \{id\}} i(\sigma) = (2g(\mathcal{H}_{72})-2) - |G|(2g(\mathcal{F})-2) = 4968 - 12|G|. \tag{4.3}$$

We recall that $i(\sigma) = \sum_{P \in \mathcal{H}_p} v_P(\sigma(t)-t)$, where t is a local parameter at P, see [44, Theorem 3.8.7]. For the computation of $i(\sigma)$ we refer to the notation used in [41, Lemma 2.2] and the complete classification given in [41, Thm. 2.7]. In particular the possible values for $i(\sigma)$ are $0, 1, 2, 3, 72, 73$.

Case 1: 71 **divides** $|G|$**.**

$|G| = 71$**.** From (4.3), $\deg(\Delta) = 4116$ but from [41, Thm. 2.7] only Cases 8 and 9 can occur so that 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 (4.3), $\deg(\Delta) = 3264$. Assume that G is dihedral. From [41, Thm. 2.7], since elements satisfy either Case 1 or Case 5, either $\deg(\Delta) = 70 \cdot 2 + 71 \cdot 72$ or $70 \cdot 73 + 71$, a contradiction. Similarly, 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 (4.3), $\deg(\Delta) = 2412$ and G is cyclic. From [41, Lemma 2.2], if $\sigma \in G$ is tame then σ is of type (A) and hence $i(\sigma) = p + 1 = 72$. From [41, 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 [41, 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 (4.3), 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 (4.3) if and only if $\alpha = 2$. Thus from the Riemann-Hurwitz formula $g(\mathcal{H}_{72}/G) = 7 = g(\mathcal{F})$. Geometrically, the elements of C_{71} have exactly one fixed point $P \in \mathcal{H}_{72}$ while the elements of C_5 fix exactly the $\mathbb{F}_{71^2}$-rational vertexes of a triangle $T = \{P, Q, R\}$, where $Q \in \mathcal{H}_{72}$ and $R \notin \mathcal{H}_{72}$. 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 $\mathcal{H}_{72}/G$ are not isomorphic.

This shows that if $\mathcal{H}_{72}/G \cong \mathcal{F}$, then G must be tame.

Case 2: 71 does not divide $|G|$. 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 cases a numerical contradiction to (4.3) is obtained using [41, Thm. 2.7]. Here we underline again that, considering subgroups G of $PGU(3, 71)$ with $|G|$ satisfying one of the cases classified in (4.2), quotient curves $\mathcal{H}_{72}/G$ of $\mathcal{H}_{72}$ 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 analysis of the list of quotient curves $\mathcal{H}_{72}/G$ where $|G|$ satisfies (4.2) and $g(\mathcal{H}_{72}/G) = 7$.

$|G| = 72$ 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 [41, Lemma 2.2]. In both cases we can assume up to conjugation that $\mathcal{H}_{72}$ is given by the Fermat equation $\mathcal{H}_{72} : x^{72} + y^{72} + z^{72} = 0$ 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 the orders $o(a)$ and $o(b)$ of a and b in $\mathbb{F}_{71^2}^*$ divide $p + 1 = 72$. Since $\mathcal{H}_{72}/G$ 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 $\mathcal{H}_{72}/G$ 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 $\mathrm{Aut}(\mathcal{H}_{72}/G)$ inherits a cyclic group of order n where $n \mid 72$ and $m \geq 9$. This conflicts with $\mathrm{Aut}(\mathcal{H}_{72}/G)$ 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 [41, Lemma 2.2], we can assume that up to conjugation $\mathcal{H}_{72}$ 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 [29, Page 644 case 8]. Consider the automorphism α of $\mathcal{H}_{72}$ 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 $\langle \alpha \rangle / G \cong C_{28} < \mathrm{Aut}(\mathcal{H}_{72}/G)$. Since $PSL(2,8)$ has no cyclic subgroups of order 28, the curves $\mathcal{H}$ and $\mathcal{H}_{72}/G$ 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 [41, Lemma 2.2]. The center of α is given by the fixed common point $P \notin \mathcal{H}_{72}$ 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 $\mathcal{H}_{72}/G$ 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 $\mathcal{H}_{72}/G$ 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 $\mathcal{H}_{72}/G$ are not isomorphic.

$|G| = 315$ **and** $G \cong SmallGroup(315, 2)$**.** As $\mathcal{H}_{72}/G$ 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 $\mathcal{H}_{72}/G$ 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 $\mathcal{H}_{72}/G$ inherits a cyclic automorphisms group of order at least 16.

In the following we only list the cases for which $|G| \leq 72$ and a numerical contradiction to the Riemann-Hurwitz formula is obtained. The cases $|G| > 72$ can be found in [2, pp. 23–46].

$|G| = 60$**.** 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 [41, 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 $G_i \cong SmallGroup(63, i)$ 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 [41, 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 [41, 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 $G \cong SmallGroup(70, k)$ for $k = 1, \ldots, 4$. Since $70 = p - 1$, by [41, 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 $G \cong SmallGroup(70, 1)$ then $i = 5$, if $G \cong SmallGroup(70, 2)$ then $i = 7$, if $G \cong SmallGroup(70, 3)$ then $i = 35$, and if $G \cong SmallGroup(70, 4)$ then $i = 1$. Since in all cases $i \neq 57$ this case cannot occur.

$|G| = 72$**.** In this case $G \cong SmallGroup(72, a)$ 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 [41, 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 $G \cong SmallGroup(72, 1)$. Since G has a unique involution, which is a homology, G fixes an $\mathbb{F}_{71^2}$-rational point P with $P \notin \mathcal{H}_{72}$. 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 $\mathcal{H}_{72}$. 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 $\mathcal{H}_{72}$, $G \leq C_{72} \times C_{72} = Stab_{PGU(3,71)}(T)$ and G is abelian, a contradiction. Thus γ is a homology. From [40, 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 $\mathcal{H}_{72}$ 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 $P_1,\dots,P_7$ which are $\mathbb{F}_{71^2}$-rational but not in $\mathcal{H}_{72}$. 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 $\mathcal{H}_{72}$ 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.

This finishes the proof of Theorem 4.4. □

Question 4.5. From Theorem 4.4 the Fricke-Macbeath curve $\mathcal{F}$ is an $\mathbb{F}_{71^2}$-maximal curve which is not a Galois subcover of the Hermitian curve $\mathcal{H}_{72}$ over $\mathbb{F}_{71^2}$. It is still an open problem to determine whether $\mathcal{F}$ is covered by $\mathcal{H}_{72}$ or not. A positive answer would provide with 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, $\mathcal{F}$ would be the first known example of an $\mathbb{F}_{p^2}$-maximal curve which is not covered by the Hermitian curve over a field of order p^{2h} with $h \not\equiv 0 \pmod 3$.

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; he also was partially supported by CNPq-Brazil (grant 310623/2017-0). This research was partially supported by Ministry for Education, University and Research of Italy (MIUR) (Project PRIN 2012 *Geometrie di Galois e strutture di incidenza*-Prot. N. 2012XZE22K_005) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA-INdAM).

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] Bartoli, D., Montanucci, M., Torres, F.: $\mathbb{F}_{p^2}$-maximal curves with many automorphisms are Galois-covered by the Hermitian curve, arXiv: 1708.03933v1.

[3] Bartoli, D., Montanucci, M., Zini, G.: Multi point AG codes on the GK maximal curve, *Des. Codes Cryptogr.*, **86**(1), (2018) 161–177.

[4] Bartoli, D., Montanucci, M., Zini, G.: AG codes and AG quantum codes from the GGS curve, *Des. Codes Cryptogr.*, (2017) DOI:10.1007/s10623-017-0450-5.

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

[6] Cossidente, A., Korchmáros, G., Torres, F.: Curves of large genus covered by the Hermitian curve, *Comm. Algebra*, **28**(10), (2000) 4707–4728.

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

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

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

[10] Fanali, S., Giulietti, M.: On maximal curves with Frobenius dimension 3, *Des. Codes Cryptogr.* **53**(3), (2009) 165–174.

[11] Fanali, S., Giulietti, M., Platoni, I.: On maximal curves over finite fields of small order, *Adv. Math. Commun.* **6**(1), (2012) 107–120.

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

[13] Fuhrmann, R., Garcia, A., Torres, F.: On maximal curves, *J. Number Theory*, **67**(1), (1997) 29–51.

[14] Fuhrmann, R., Torres, F.: On Weierstrass points and optimal curves, *Rend. Circ. Mat. Palermo Suppl.* **51** (Recent Progress in Geometry, E. Ballico, G. Korchmáros Eds.) (1998), 25–46.

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

[16] Garcia, A: Curves over finite fields attaining the Hasse-Weil upper bound, *European Congress of Mathematics*, Vol. II (Barcelona, 2000), Progr. Math. **202**, Birkhäuser, Basel 2001, 199–205.

[17] Garcia, A: On curves with many rational points over finite fields, *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, Springer, Berlin, 2002, 152–163.

[18] Garcia, A., Güneri, C., Stichtenoth, H.: A generalization of the Giulietti-Korchmáros maximal curve, *Advances in Geometry* **10**(3), (2010) 427–434.

[19] Garcia, A., Stichtenoth, H.: Algebraic function fields over finite fields with many rational places, *IEEE Trans. Inform. Theory* **41**, (1995) 1548-1563.

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

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

[22] Giulietti, M., Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Curves covered by the Hermitian curve, *Finite Fields Appl.* **12**(4), (2006) 539–564.

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

[24] Giulietti, M., Quoos, L., Zini, G.: Maximal curves from subcovers of the GK-curve, *J. Pure Appl. Algebra* **220**, (2016) 3372–3383.

[25] Gunby, B., Smith, A., Yuan, A.: Irreducible canonical representations in positive characteristic, *Res. Number Theory* **1**, (2015), Art. 3, 25 pp.
[26] Hansen, J.P.: Codes on the Klein quartic, ideals and decoding. IEEE Trans. Inf. Theory **33**(6), (1987), 923–925.
[27] Heegard, C., Little, J., Saints, K.: Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes. *IEEE Trans. Inf. Theory* **41**, (1995) 1752–1761.
[28] Hidalgo, R.A.: Edmonds maps on the Fricke-Macbeath curve, *Ars Math. Contemp.* **8**, (2015) 275–289.
[29] Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: *Algebraic Curves over a Finite Field*. Princeton Series in Applied Mathematics, Princeton (2008).
[30] Ihara, Y.: Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo* **28**, (1981) 721–724.
[31] Joyner, D.: An error-correcting codes package, *SIGSAM Commun. Comput. Algebra* **39**(2), (2005) 65–68.
[32] Klein, F.: Über die Transformation siebenter Ordnung der elliptischen Functionen, *Math. Ann.* **14**, (1989) 428–471.
[33] Kleiman, S.L.: Algebraic cycles and the Weil conjectures. In: Dix esposés sur la cohomologie des schémas, pp. 359–386. North-Holland, Amsterdam, 1968.
[34] Korchmáros, G.; Torres, F.: On the genus of a maximal curve, *Math. Ann.* **323**(3), (2002) 589–608.
[35] 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.
[36] Ma, L., Xing, C.: On subfields of the Hermitian function fields involving the involution automorphism, arXiv:1707.07314.
[37] Macbeath, A.: On a curve of genus 7, *Proc. Lond. Math. Soc. (3)* **15**, (1965), 527-542.
[38] Matthews, G.L.: Codes from the Suzuki function field, *IEEE Trans. Inf. Theory* **50**(12), (2004) 3298–3302.
[39] Matthews, G.L.: Weierstrass semigroups and codes from a quotient of the Hermitian curve, *Des. Codes Cryptogr.* **37**, (2005) 473–492.
[40] Montanucci, M., Zini, G.: On the spectrum of genera of quotients of the Hermitian curve, *Comm. Algebra*, DOI 10.1080/00927872.2018.1455100, (2018).
[41] Montanucci, M., Zini, G.: Some Ree and Suzuki curves are not Galois covered by the Hermitian curve, *Finite Fields Appl.* **48**, (2017), 175-195.
[42] Rück, H.G., Stichtenoth, H.: A characterization of Hermitian function fields over finite fields, *J. Reine. Angew. Math.* **457**, (1994) 185–188.
[43] Stichtenoth, H.: A note on Hermitian codes over $GF(q^2)$, *IEEE Trans. Inf. Theory* **34**(5), (1988) 1345–1348.
[44] Stichtenoth, H.: Algebraic function fields and codes. In:Graduate Texts inMathematics, vol. 254. Springer, Berlin (2009).
[45] Stichtenoth, H., Xing, C.P.: The genus of maximal function fields, *Manuscripta Math.* **86**, (1995) 217–224.
[46] Tafazolian, 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.
[47] Tafazolian, S., Torres, F.: A note on certain maximal curves, *Comm. Algebra* **45**(2), (2017) 764–773.
[48] Tiersma, H.J.: Remarks on codes from Hermitian curves, *IEEE Trans. Inf. Theory* **33**(4), (1987) 605–609.
[49] Top, J., Verschoor, C.: Counting points on the Fricke-Macbeath curve over finite fields, *J. Th. des Nombres Bordeaux*, to appear, (2016).

[50] van der Geer, G.: Curves over finite fields and codes, *European Congress of Mathematics*, Vol. II (Barcelona, 2000), Progr. Math. **202**, Birkhäuser, Basel, 2001, 225–238.
[51] van der Geer, G.: Coding theory and algebraic curves over finite fields: a survey and questions, *Applications of Algebraic Geometry to Coding Theory, Physics and Computation*, NATO Sci. Ser. II Math. Phys. Chem. **36**, Kluwer, Dordrecht, 2001, 139-159.
[52] van Der Geer, G.: Counting curves over finite fields, *Finite Fields Appl.* **32**, (2015) 207–232.
[53] Xing, C.P., Chen, H.: Improvements on parameters of one-point AG codes from Hermitian curves, *IEEE Trans. Inf. Theory* **48**(2), (2002) 535–537.
[54] Xing, C.P., Ling S.: A class of linear codes with good parameters from algebraic curves, *IEEE Trans. Inf. Theory* **46**(4), (2000) 1527–1532.
[55] Yang, K., Kumar, P.V.: On the true minimum distance of Hermitian codes. In: Coding Theory and Algebraic Geometry. Lecture Notes in Mathematics, vol. 1518, pp. 99–107. Springer, Berlin (1992).

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, via Vanvitelli 1, 06123 Perugia, Italy

Email 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

Email address: maria.montanucci@unibas.it

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

Email address: ftorres@ime.unicamp.br