

On maximal curves that are not quotients of the Hermitian curve

Massimo Giulietti, Maria Montanucci, and Giovanni Zini

November 18, 2015

For each prime power ℓ the plane curve \mathcal{X}_ℓ with equation $Y^{\ell^2-\ell+1} = X^{\ell^2} - X$ is maximal over \mathbb{F}_{ℓ^6} . Garcia and Stichtenoth in 2006 proved that \mathcal{X}_3 is not Galois covered by the Hermitian curve and raised the same question for \mathcal{X}_ℓ with $\ell > 3$; in this paper we show that \mathcal{X}_ℓ is not Galois covered by the Hermitian curve for any $\ell > 3$. Analogously, Duursma and Mak proved that the generalized GK curve \mathcal{C}_{ℓ^n} over $\mathbb{F}_{\ell^{2n}}$ is not a quotient of the Hermitian curve for $\ell > 2$ and $n \geq 5$, leaving the case $\ell = 2$ open; here we show that \mathcal{C}_{2^n} is not Galois covered by the Hermitian curve over $\mathbb{F}_{2^{2n}}$ for $n \geq 5$.

1 Introduction

Let \mathbb{F}_{q^2} be the finite field with q^2 elements, where q is a power of a prime p , and let \mathcal{X} be an \mathbb{F}_{q^2} -rational curve, that is a projective, absolutely irreducible, non-singular algebraic curve defined over \mathbb{F}_{q^2} . \mathcal{X} is called \mathbb{F}_{q^2} -maximal if the number $\mathcal{X}(\mathbb{F}_{q^2})$ of its \mathbb{F}_{q^2} -rational points attains the Hasse-Weil upper bound

$$q^2 + 1 + 2gq,$$

where g is the genus of \mathcal{X} . Maximal curves have interesting properties and have also been investigated for their applications in Coding Theory. Surveys on maximal curves are found in [8, 9, 10, 12, 31, 32] and [21, Chapt. 10].

The most important example of an \mathbb{F}_{q^2} -maximal curve is the Hermitian curve \mathcal{H}_q , defined as any \mathbb{F}_{q^2} -rational curve projectively equivalent to the plane curve with Fermat equation

$$X^{q+1} + Y^{q+1} + T^{q+1} = 0.$$

The norm-trace equation

$$Y^{q+1} = X^q T + X T^q$$

gives another model of \mathcal{H}_q , \mathbb{F}_{q^2} -equivalent to the Fermat model, see [14, Eq. (2.15)]. For fixed q , \mathcal{H}_q has the largest possible genus $g(\mathcal{H}_q) = q(q-1)/2$ that an \mathbb{F}_{q^2} -maximal curve can have. The automorphism group $\text{Aut}(\mathcal{H}_q)$ is isomorphic to $\text{PGU}(3, q)$, the group of projectivities of $\text{PG}(2, q^2)$ commuting with the unitary polarity associated with \mathcal{H}_q .

By a result commonly attributed to Serre, see [25, Prop. 6], any \mathbb{F}_{q^2} -rational curve which is \mathbb{F}_{q^2} -covered by an \mathbb{F}_{q^2} -maximal curve is also \mathbb{F}_{q^2} -maximal. In particular, \mathbb{F}_{q^2} -maximal curves are given by the Galois \mathbb{F}_{q^2} -subcovers of an \mathbb{F}_{q^2} -maximal curve \mathcal{X} , that is by the quotient curves \mathcal{X}/G over a finite \mathbb{F}_{q^2} -automorphism group $G \leq \text{Aut}(\mathcal{X})$.

Most of the known maximal curves are Galois subcovers of the Hermitian curve, many of which were studied in [3, 4, 14]. Garcia and Stichtenoth [13] discovered the first example of maximal curve not Galois covered by the Hermitian curve, namely the curve $Y^7 = X^9 - X$ maximal over \mathbb{F}_{3^6} . It is a special case of the curve \mathcal{X}_ℓ with equation

$$Y^{\ell^2-\ell+1} = X^{\ell^2} - X, \tag{1}$$

which is \mathbb{F}_{ℓ^6} -maximal for any $\ell \geq 2$. In [16], Giulietti and Korchmáros showed that the Galois covering of \mathcal{X}_ℓ given by

$$\begin{cases} Z^{\ell^2-\ell+1} = Y^{\ell^2} - Y \\ Y^{\ell+1} = X^\ell + X \end{cases}$$

is also \mathbb{F}_{ℓ^6} -maximal, for any prime power ℓ . Remarkably, it is not covered by \mathcal{H}_{ℓ^3} for any $\ell > 2$. This curve, nowadays referred to as the GK curve, was generalized in [11] by Garcia, Güneri, and Stichtenoth to the curve

$$\mathcal{C}_{\ell^n} : \begin{cases} Z^{\frac{\ell^n+1}{\ell+1}} = Y^{\ell^2} - Y \\ X^\ell + X = Y^{\ell+1} \end{cases},$$

which is $\mathbb{F}_{\ell^{2n}}$ -maximal for any prime power ℓ and $n \geq 3$ odd. For $\ell = 2$ and $n = 3$, \mathcal{C}_8 is Galois covered by \mathcal{H}_8 , see [16]. Duursma and Mak proved in [7] that, if $\ell \geq 3$, then \mathcal{C}_{ℓ^n} is not Galois covered by \mathcal{H}_{ℓ^n} . In Section 3, we show that the same holds in the remaining open cases.

Theorem 1.1. *For $\ell = 2$ and $n \geq 5$, \mathcal{C}_{2^n} is not a Galois subcover of the Hermitian curve \mathcal{H}_{ℓ^n} .*

Duursma and Mak [7, Thm. 1.2] showed that if \mathcal{C}_{2^n} is the quotient curve \mathcal{H}_{2^n}/G for G a subgroup of $\text{Aut}(\mathcal{H}_{2^n})$, then G has order $(2^n + 1)/3$ and acts semiregularly on \mathcal{H}_{2^n} . We investigate all subgroups G of $\text{Aut}(\mathcal{H}_{2^n})$ satisfying these conditions, relying also on classical results by Mitchell [29] and Hartley [20] (see Section 2) which provide a classification of the maximal subgroups of $\text{PSU}(3, q)$ in terms of their order and their action on \mathcal{H}_q . For any candidate subgroup G , we find another subgroup \bar{G} of $\text{Aut}(\mathcal{H}_{2^n})$ containing G as a normal subgroup, and such that \bar{G}/G has an action on \mathcal{H}_{2^n}/G not compatible with the action of any automorphism group of \mathcal{C}_{2^n} .

In Section 4 we consider the curve \mathcal{X}_ℓ with equation (1). In [13] it was shown that \mathcal{X}_3 is not a Galois subcover of \mathcal{H}_{3^6} by [13], while \mathcal{X}_2 is a quotient of \mathcal{H}_{2^6} , as noted in [15]. Garcia and Stichtenoth [13, Remark 4] raised the same question for any $\ell > 3$. The case where ℓ is a prime was settled by Mak [28]. Here we provide an answer for any prime power $\ell > 3$.

Theorem 1.2. *For $\ell > 3$, \mathcal{X}_ℓ is not a Galois subcover of the Hermitian curve \mathcal{H}_{ℓ^6} .*

In the proof of Theorem 1.2 we bound the possible degree of a Galois covering $\mathcal{H}_{\ell^6} \rightarrow \mathcal{X}_\ell$ by means of [7, Thm. 1.3], then we exclude the three possible values given by the bound. To this aim, we use again the classification results of Mitchell [29] and Hartley [20], other group-theoretic arguments, and the Riemann-Hurwitz formula (see [30, Chapt. 3]) applied to the Galois coverings $\mathcal{H}_{\ell^6} \rightarrow \mathcal{H}_{\ell^6}/G$.

2 Preliminary results

Theorem 2.1. (Mitchell [29], Hartley [20]) *Let $q = p^k$, $d = \gcd(q + 1, 3)$. The following is the list of maximal subgroups of $\text{PSU}(3, q)$ up to conjugacy:*

- i) *the stabilizer of a \mathbb{F}_{q^2} -rational point of \mathcal{H}_q , of order $q^3(q^2 - 1)/d$;*
 - ii) *the stabilizer of a \mathbb{F}_{q^2} -rational point off \mathcal{H}_q and its polar line (which is a $(q + 1)$ -secant to \mathcal{H}_q), of order $q(q - 1)(q + 1)^2/d$;*
 - iii) *the stabilizer of the self-polar triangle, or order $6(q + 1)^2/d$;*
 - iv) *the normalizer of a cyclic Singer group stabilizing a triangle in $\text{PG}(2, q^6) \setminus \text{PG}(2, q^2)$, of order $3(q^2 - q + 1)/d$;*
- for $p > 2$:

- v) $\text{PGL}(2, q)$ preserving a conic;
- vi) $\text{PSU}(3, p^m)$ with $m \mid k$ and k/m odd;
- vii) subgroups containing $\text{PSU}(3, 2^m)$ as a normal subgroup of index 3, when $m \mid k$, k/m is odd, and 3 divides both k/m and $q + 1$;
- viii) the Hessian groups of order 216 when $9 \mid (q + 1)$, and of order 72 and 36 when $3 \mid (q + 1)$;
- ix) $\text{PSL}(2, 7)$ when $p = 7$ or -7 is not a square in \mathbb{F}_q ;
- x) the alternating group \mathbf{A}_6 when either $p = 3$ and k is even, or 5 is a square in \mathbb{F}_q but \mathbb{F}_q contains no cube root of unity;
- xi) the symmetric group \mathbf{S}_6 when $p = 5$ and k is odd;
- xii) the alternating group \mathbf{A}_7 when $p = 5$ and k is odd;
for $p = 2$:
- xiii) $\text{PSU}(3, 2^m)$ with $m \mid k$ and k/m an odd prime;
- xiv) subgroups containing $\text{PSU}(3, 2^m)$ as a normal subgroup of index 3, when $k = 3m$ with m odd;
- xv) a group of order 36 when $k = 1$.

The previous theorem will be used for a case-analysis of the possible unitary groups G such that the quotient curve \mathcal{H}/G realizes the Galois covering.

While dealing with case *ii*), we will invoke a result by Dickson [6] which classifies all subgroups of the projective special linear group $\text{PSL}(2, q)$ acting on $\text{PG}(1, q)$. We remark that $\text{PSL}(2, q)$ has index $\gcd(q - 1, 2)$ in the group $\text{PGL}(2, q)$ of all projectivities of $\text{PG}(1, q)$. From Dickson's result the classification of subgroups of $\text{PGL}(2, q)$ is easily obtained.

Theorem 2.2. ([6, Chapt. XII, Par. 260]; see also [21, Thm. A.8]) *Let $q = p^k$, $d = \gcd(q - 1, 2)$. The following is the complete list of subgroups of $\text{PGL}(2, q)$ up to conjugacy:*

- i) the cyclic group of order h with $h \mid (q \pm 1)$;
- ii) the elementary abelian p -group of order p^f with $f \leq k$;
- iii) the dihedral group of order $2h$ with $h \mid (q \pm 1)$;
- iv) the alternating group \mathbf{A}_4 for $p > 2$, or $p = 2$ and k even;
- v) the symmetric group \mathbf{S}_4 for $16 \mid (q^2 - 1)$;
- vi) the alternating group \mathbf{A}_5 for $p = 5$ or $5 \mid (q^2 - 1)$;
- vii) the semidirect product of an elementary abelian p -group of order p^f by a cyclic group of order h , with $f \leq k$ and $h \mid (q - 1)$;
- viii) $\text{PSL}(2, p^f)$ for $f \mid k$;
- ix) $\text{PGL}(2, p^f)$ for $f \mid k$.

3 \mathcal{C}_{2^n} is not Galois-covered by \mathcal{H}_{2^n} , for any $n \geq 5$

The aim of this section is to prove Theorem 1.1. Throughout the section, let $n \geq 5$ be odd and $q = 2^n$. We rely on the following result by Duursma and Mak.

Lemma 3.1. ([7, Thm. 1.2]) *Let $n \geq 5$ odd. If $\mathcal{C}_{2^n} \cong \mathcal{H}_{2^n}/G$ for some $G \leq \text{Aut}(\mathcal{H}_{2^n})$, then G has order $(2^n + 1)/3$ and acts semiregularly on \mathcal{H}_{2^n} .*

By Lemma 3.1 only subgroups G of $\text{Aut}(\mathcal{H}_q)$ of order $(q + 1)/3$ acting semiregularly on \mathcal{H}_q need to be considered. We will also use the fact that the whole automorphism group of $\text{Aut}(\mathcal{C}_{2^n})$ fixes a point.

Theorem 3.2. ([17, Thm. 3.10],[18, Prop. 2.10]) *For $n \geq 5$, the group $\text{Aut}(\mathcal{C}_{2^n})$ has a unique fixed point P_∞ on \mathcal{C}_q , and P_∞ is \mathbb{F}_{q^2} -rational.*

Corollary 3.3. *Let $G \leq \text{Aut}(\mathcal{H}_q)$. If there exists $\bar{G} \leq \text{Aut}(\mathcal{H}_q)$ such that G is a proper normal subgroup of \bar{G} and \bar{G} acts semiregularly on \mathcal{H}_q , then $\bar{G}/G \leq \text{Aut}(\mathcal{H}_q/G)$ acts semiregularly on \mathcal{H}_q/G , hence $\mathcal{C}_{2^n} \not\cong \mathcal{H}_q/G$.*

The following well-known result about finite groups will be used (see for example [27, Ex. 16 Page 232]).

Lemma 3.4. *Let H be a finite group and K a subgroup of H such that the index $[H : K]$ is the smallest prime number dividing the order of H . Then K is normal in H .*

Proposition 3.5. *Suppose $G \leq \text{PSU}(3, q)$ and a maximal subgroup of $\text{PSU}(3, q)$ containing G satisfies case ii) in Theorem 2.1. Then $\mathcal{C}_{2^n} \not\cong \mathcal{H}_q/G$.*

Proof. Let ℓ be the $(q + 1)$ -secant to \mathcal{H}_q stabilized by G ; we show that G is isomorphic to a cyclic subgroup of $\text{PSL}(2, q^2)$.

$\text{PGU}(3, q)$ is transitive on the points of $\text{PG}(2, q^2) \setminus \mathcal{H}_q$ (see for example [22]), hence also on the $(q + 1)$ -secant lines; therefore we can assume that ℓ is the line at infinity $T = 0$. The action on ℓ of an element $g \in G$ is given by $(X, Y, 0) \mapsto A_g \cdot (X, Y, 0)$, where the matrix $A_g = (a_{ij})_{i=1,2,3}^{j=1,2,3}$ satisfies $a_{31} = a_{32} = 0$, and we can assume $a_{33} = 1$. By direct computation, it is easy to check that the application

$$\varphi : G \rightarrow \text{PGL}(2, q^2), \quad \varphi(g) : \begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} X \\ Y \end{pmatrix},$$

is a well-defined group homomorphism. Moreover, φ is injective, since no non-trivial element of G can fix the points of $\mathcal{H}_q \cap \ell$, by the semiregularity of G . Hence G is isomorphic to a subgroup of $\text{PGL}(2, q^2) \cong \text{PSL}(2, q^2)$. Since $|G|$ is odd, then Theorem 2.2 implies that G is cyclic.

Let $g \in G$ be an element of prime order $d > 3$; such a d exists, since it is easy to check that $2^n + 1$ is a power of 3 only when $n = 1$ or $n = 3$. If we denote by d^h the highest power of d dividing $(q + 1)/3$, then d^{2h} is the highest power of d dividing

$$|\text{PGU}(3, q)| = q^3(q^3 + 1)(q^2 - 1) = q^3(q + 1)^2(q - 1)(q^2 - q + 1).$$

Let \mathcal{H}_q have equation $X^{q+1} + Y^{q+1} + T^{q+1} = 0$, then

$$D = \left\{ (X, Y, T) \mapsto (\lambda X, \mu Y, T) \mid \lambda^{d^h} = \mu^{d^h} = 1 \right\}$$

is a Sylow d -subgroup of $\text{PGU}(3, q)$, and by Sylow's theorems we can assume up to conjugation that $g \in D$, so the fixed points of the subgroup $\langle g \rangle$ generated by g are the fundamental points

P_i , $i = 1, 2, 3$. Since G is abelian, then $\langle g \rangle$ is normal in G , hence G acts on the fixed points $T = \{P_1, P_2, P_3\}$ of $\langle g \rangle$. In fact, for all $k \in G$ and $\bar{g} \in \langle g \rangle$,

$$k(P_i) = k(\bar{g}(P_i)) = \tilde{g}(k(P_i))$$

for some $\tilde{g} \in \langle g \rangle$, that is, $k(P_i)$ is fixed by \tilde{g} , hence $k(P_i)$ is a fundamental point P_j .

As $|G|$ is odd, we have by the orbit stabilizer theorem that the orbits of any $k \in G$ on T have length 1 or 3. If k has a single orbit on T , then the matrix representing k is

$$k = \begin{pmatrix} 0 & 0 & \lambda \\ \mu & 0 & 0 \\ 0 & \rho & 0 \end{pmatrix} \quad \text{or} \quad k = \begin{pmatrix} 0 & \lambda & 0 \\ 0 & 0 & \mu \\ \rho & 0 & 0 \end{pmatrix}, \quad \text{in both cases} \quad k^3 = \begin{pmatrix} \lambda\mu\rho & 0 & 0 \\ 0 & \lambda\mu\rho & 0 \\ 0 & 0 & \lambda\mu\rho \end{pmatrix},$$

that is $k^3 = 1$, hence G cannot be generated by k . Therefore a generator α of G has the form

$$\alpha : (X, Y, T) \mapsto (\theta X, \eta Y, T),$$

with $\theta^{\frac{q+1}{3}} = \eta^{\frac{q+1}{3}} = 1$. If θ had order $m < (q+1)/3$, then α^m would fix the points of $\mathcal{H}_q \cap (Y = 0)$, against the semiregularity of G . Then θ is a primitive $(q+1)/3$ -th root of unity, and the same holds for η , so that

$$\alpha = \alpha_\theta : (X, Y, T) \mapsto (\theta X, \theta^i Y, T), \quad (2)$$

where θ is a primitive $(q+1)/3$ -th root of unity, and i is co-prime with $(q+1)/3$.

Let $\zeta \in \mathbb{F}_{q^2}$ satisfy $\zeta^3 = \theta$, and let \bar{G} be the group generated by α_ζ , as defined in (2). Any element of \bar{G} fixes only the fundamental points, hence \bar{G} is semiregular on \mathcal{H}_q ; moreover, G is normal in \bar{G} of index 3. Then Corollary 3.3 yields the thesis. \square

Proposition 3.6. *Suppose $G \leq \text{PSU}(3, q)$ and a maximal subgroup of $\text{PSU}(3, q)$ containing G satisfies case iii) in Theorem 2.1. Then $\mathcal{C}_{2^n} \not\cong \mathcal{H}_q/G$.*

Proof. Up to conjugation, the self-polar triangle stabilized by G is the fundamental triangle $T = \{P_1, P_2, P_3\}$. Let N be the subgroup of G stabilizing T pointwise. Then N is normal in G , since $g^{-1}ng(P_i) = g^{-1}n(g(P_i)) = g^{-1}(g(P_i)) = P_i$, where $n \in N$, $g \in G$. The group G/N acts faithfully on T , hence either $G = N$ or $[G : N] = 3$.

If $G = N$, then G fixes one fundamental point P_i , which is off \mathcal{H}_q , and the polar line of P_i passing through the other fundamental points; therefore Proposition 3.5 yields the thesis.

Now suppose $[G : N] = 3$. As in the proof of Proposition 3.5, N is isomorphic to a subgroup of $\text{PSL}(2, q^2)$; since $|N|$ is odd, we have by Theorem 2.2 that N is cyclic, say $N = \langle \alpha_\xi \rangle$, where ξ is a primitive $(q+1)/9$ -th root of unity and α_ξ is defined in (2). Let $h \in G \setminus N$. By arguing as for k in the proof of Proposition 3.5, we have that h has order 3. Moreover, G is the semidirect product $N \rtimes \langle h \rangle$, because $N \triangleleft G$, $N \cap \langle h \rangle = \emptyset$, and the orders of the subgroups imply $G = \langle h \rangle \cdot N$.

Let \bar{N} be the cyclic group $\langle \alpha_\theta \rangle$, with $\theta \in \mathbb{F}_{q^2}$ such that $\theta^3 = \xi$, and let \bar{G} be the group generated by \bar{N} and h . \bar{G} is the semidirect product $\bar{N} \rtimes \langle h \rangle$; in fact, \bar{N} is normal in \bar{G} by Lemma 3.4, $\bar{N} \cap \langle h \rangle = \emptyset$, and the orders of the subgroups imply $\bar{G} = \bar{N} \cdot \langle h \rangle$. We have that G is normal in \bar{G} , again by Lemma 3.4.

We want to count in two ways the size of the set

$$I = \{(\bar{g}, P) \mid \bar{g} \in \bar{G} \setminus \{id\}, P \in \mathcal{H}_q, \bar{g}(P) = P\}$$

The diagonal group \bar{N} is semiregular on \mathcal{H}_q , like $\bar{G} \cap \text{PSU}(3, q) = G$. Then we consider only elements of the form $\bar{n}h$ or $\bar{n}h^2$, with $\bar{n} \in \bar{N} \setminus N$. We have

$$\bar{n} = \begin{pmatrix} \rho & 0 & 0 \\ 0 & \rho^i & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 0 & \lambda & 0 \\ 0 & 0 & \mu \\ 1 & 0 & 0 \end{pmatrix}$$

where $\lambda^{q+1} = \mu^{q+1} = 1$, $\gcd(i, (q+1)/3) = 1$, $\rho = \theta^j$ with $0 \leq j < (q+1)/3$ (the argument is analogous in case h acts as the other possible 3-cycle on the fundamental points). Hence $\bar{n}h$ is

$$\bar{n}h = \begin{pmatrix} \rho & 0 & 0 \\ 0 & \rho^i & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & \lambda & 0 \\ 0 & 0 & \mu \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & A & 0 \\ 0 & 0 & B \\ 1 & 0 & 0 \end{pmatrix},$$

where $A^{q+1} = B^{q+1} = 1$, and $\det(\bar{n}h) = AB$ is not a cube in \mathbb{F}_{q^2} , since $\bar{n}h \notin \text{PSU}(3, q)$. The eigenvalues of $\bar{n}h$ are the zeros of $X^3 - AB \in \mathbb{F}_{q^2}[X]$. Since \mathbb{F}_{q^2} has characteristic 2, we get 3 distinct eigenvalues in a cubic extension of \mathbb{F}_{q^2} , namely z , zx , and $z(x+1)$, where $x^2 + x + 1 = 0$ and $z^3 = AB$. Then $\bar{n}h$ has exactly 3 fixed points, given by 3 independent eigenvectors:

$$Q_1 = \left(z, \frac{z^2}{A}, 1\right), \quad Q_2 = \left(zx, \frac{z^2x^2}{A}, 1\right), \quad Q_3 = \left(z(x+1), \frac{z^2(x+1)^2}{A}, 1\right).$$

Q_1 is a point of \mathcal{H}_q . In fact, since \mathcal{H}_q has equation $X^{q+1} + Y^{q+1} + T^{q+1} = 0$, then

$$z^{q+1} + \left(\frac{z^2}{A}\right)^{q+1} + 1 = z^{q+1} + z^{2(q+1)} + 1 = \frac{(z^{q+1})^3 - 1}{z^{q+1} - 1} = \frac{A^{q+1} - 1}{z^{q+1} - 1} = 0$$

as $z \notin \mathbb{F}_{q^2}$ implies $z^{q+1} \neq 1$. Similarly we get $Q_2 \in \mathcal{H}_q$, $Q_3 \in \mathcal{H}_q$.

Then each element $\bar{n}h$ or $\bar{n}h^2$ with $\bar{n} \in \bar{N} \setminus N$ has exactly 3 fixed points on \mathcal{H}_q , and

$$|I| = 2 \cdot (|\bar{N}| - |N|) \cdot 3 = 2 \cdot \left(\frac{q+1}{3} - \frac{q+1}{9}\right) \cdot 3 = 4 \cdot \frac{q+1}{3}. \quad (3)$$

The orbit \mathcal{O} under \bar{G} of a point $P \in \mathcal{H}_q$ contains the orbit of P under G , hence $|\mathcal{O}| \geq (q+1)/3$; by the orbit stabilizer theorem, the stabilizer \mathcal{S} of P under \bar{G} has size $|\mathcal{S}| \leq 3$, in particular $|\mathcal{S}| \in \{1, 3\}$ since $|\bar{G}|$ is odd. Then $|I| = 2m$, where m is the number of points of \mathcal{H}_q which are fixed by some non-trivial element of \bar{G} . By (3), we get

$$m = 2 \cdot \frac{q+1}{3},$$

that is, these m points form 2 distinct orbits under the action of G . Then the quotient group \bar{G}/G has 2 fixed points on \mathcal{H}_q/G and any other orbit of \bar{G}/G is long, with length 3.

By 3.2, one of the fixed points of \bar{G}/G is \mathbb{F}_{q^2} -rational, and the other one may or may not be \mathbb{F}_{q^2} -rational. Then the number of \mathbb{F}_{q^2} -rational points of \mathcal{H}_q/G is congruent to 1 or 2 mod 3.

On the other side, the \mathbb{F}_{q^2} -maximal curve \mathcal{C}_{2^n} has genus $g = (3q-4)/2$ and number of \mathbb{F}_{q^2} -rational points equal to

$$|\mathcal{C}_{2^n}(\mathbb{F}_{q^2})| = q^2 + 1 + 2qg = q^2 + 1 + 2q \cdot (3q-4)/2 = 4q^2 - 4q + 1,$$

see [11, Prop. 2.2]; then $|\mathcal{C}_{2^n}(\mathbb{F}_{q^2})| \equiv 0 \pmod{3}$, as $q \equiv 2 \pmod{3}$. Therefore, $\mathcal{H}_q/G \not\cong \mathcal{C}_{2^n}$. \square

Proposition 3.7. *Suppose $G \not\subseteq \text{PSU}(3, q)$ and a maximal subgroup of $\text{PSU}(3, q)$ containing $G \cap \text{PSU}(3, q)$ satisfies case ii) in Theorem 2.1. Then $\mathcal{C}_{2^n} \not\cong \mathcal{H}_q/G$.*

Proof. Let $G' = G \cap \text{PSU}(3, q)$. Since $\text{PSU}(3, q)$ has prime index 3 in $\text{PGU}(3, q)$, then $\text{PGU}(3, q) = G \cdot \text{PSU}(3, q)$, hence $[G : G'] = 3$, and G' is normal in G by Lemma 3.4.

Arguing as in the proof of Proposition 3.5, $G' = \langle \alpha_\xi \rangle$ is cyclic, where ξ is a primitive $(q+1)/9$ -th root of unity, α_ξ is defined in (2) and fixes the fundamental points, and G stabilizes the fundamental triangle T .

Suppose there exists $h \in G \setminus G'$ of order 3. Arguing as for k in Proposition 3.6, $G = G' \rtimes \langle h \rangle$. Let $\theta \in \mathbb{F}_{q^2}$ with $\theta^3 = \xi$, we define \bar{G}' as the cyclic group generated by α_θ (given in (2)), and \bar{G} as the group generated by \bar{G}' and h . Again, it is easily seen that $\bar{G} = \bar{G}' \rtimes \langle h \rangle$; moreover, G' is normal in \bar{G}' and G is normal in \bar{G} with indices $[\bar{G} : G] = [\bar{G}' : G'] = 3$. We can repeat the same argument as in the proof of Proposition 3.6 after replacing N with G' and \bar{N} with \bar{G}' ; in this way we obtain that $|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv 1, 2 \pmod{3}$, while $|C_{2^n}| \equiv 0 \pmod{3}$. This yields the thesis.

Now suppose there is no $h \in G \setminus G'$ of order 3. This fact implies that G is made of diagonal matrices, since G acts on T . Then, by Theorem 2.2, G is cyclic and $G = \langle \alpha_\theta \rangle$, where the notations are the same as above. We define the diagonal group $\bar{G} = \langle \alpha_\xi \rangle$, with $\zeta^3 = \theta$. G is normal in \bar{G} of index 3 and \bar{G} is semiregular on \mathcal{H}_q , hence Corollary 3.3 yields the thesis. \square

Proposition 3.8. *Suppose $G \not\leq \text{PSU}(3, q)$ and a maximal subgroup of $\text{PSU}(3, q)$ containing $G \cap \text{PSU}(3, q)$ satisfies case iii) in Theorem 2.1. Then $C_{2^n} \not\cong \mathcal{H}_q/G$.*

Proof. As above, $G' = G \cap \text{PSU}(3, q)$ is normal in G of index 3. By applying to G' the argument of Proposition 3.6, we get that either G' is cyclic and $G' = \langle \alpha_\xi \rangle$, or $G' = \langle \alpha_\eta \rangle \rtimes \langle h \rangle$, where η is a primitive $(q+1)/27$ -th root of unity and h is an element of order 3 acting as a 3-cycle on the fundamental triangle T .

Consider the case $G' = \langle \alpha_\xi \rangle$. Since G' is normal in G , then G acts on T . If G fixed T pointwise, then G would be made of diagonal matrices whose non-zero coefficients are cubes in \mathbb{F}_{q^2} being $(q+1)/3$ -th roots of unity, hence $G \leq \text{PSU}(3, q)$, against the hypothesis. Then, arguing as above, $G = G' \rtimes \langle h \rangle$, where $h \in G \setminus G'$ has order 3. Let $\theta \in \mathbb{F}_{q^2}$ with $\theta^3 = \xi$, and define $\bar{G} = \langle \alpha_\theta \rangle \rtimes \langle h \rangle$. Arguing as in Proposition 3.6, we obtain that $|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv 1, 2 \pmod{3}$, while $|C_{2^n}| \equiv 0 \pmod{3}$. This yields the thesis.

Now consider the case $G' = \langle \alpha_\eta \rangle \rtimes \langle h \rangle$. $\langle \alpha_\eta \rangle$ is the only subgroup of G' of order $(q+1)/27$, then $\langle \alpha_\eta \rangle$ is a characteristic subgroup of G' ; also, G' is normal in G . Therefore $\langle \alpha_\eta \rangle$ is normal in G , hence G acts on the fundamental points. Let G'' be the subgroup of G fixing T pointwise; G'' is normal in G of index 3, and $G = G'' \rtimes \langle h \rangle$. Being made of diagonal matrices, G'' is abelian, with a subgroup G' of index 3. By the primary decomposition of abelian groups, we have either $G'' = \langle \alpha_\xi \rangle$ with $\xi^3 = \eta$, or $G'' = \langle \alpha_\eta \rangle \times \langle h' \rangle$, with $h' \in G'' \setminus \langle \alpha_\eta \rangle$ a diagonal matrix of order 3. In the latter case, by $h'^3 = id$ we get that $\det(h')^3 = 1$ and then $\det(h')$ is a cube in \mathbb{F}_{q^2} , hence $h' \in G \cap \text{PSU}(3, q) = G'$; therefore $G' = G''$, against the fact that h is a 3-cycle on T .

Then $G'' = \langle \alpha_\xi \rangle$, and $G = \langle \alpha_\xi \rangle \rtimes \langle h \rangle$. Let $\bar{G} = \langle \alpha_\theta \rangle \rtimes \langle h \rangle$, where $\theta \in \mathbb{F}_{q^2}$ satisfies $\theta^3 = \xi$. We can repeat the same argument as in the proof of Proposition 3.6 after replacing N with $\langle \alpha_\xi \rangle$ and \bar{N} with $\langle \alpha_\theta \rangle$; in this way we obtain that $|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv 1, 2 \pmod{3}$, while $|C_{2^n}| \equiv 0 \pmod{3}$. \square

Lemma 3.9. *Suppose $G \leq \text{PSU}(3, q)$ and any maximal subgroup M of $\text{PSU}(3, q)$ containing G does not satisfy case ii) nor case iii) in Theorem 2.2. Then M satisfies only case xiv), i.e. $G \not\leq \text{PSU}(3, 2^m)$ and M contains $\text{PSU}(3, 2^m)$ as a normal subgroup of index 3, where $n = 3m$.*

Proof. We can exclude cases ii) and iii) by hypothesis, case i) by the semiregularity of G , and cases iv) and xv) because $|G|$ is not a divisor of their orders. Then the thesis follows if we exclude case xiii). To this end, we apply again Theorem 2.1 to $\text{PSU}(3, 2^m)$, where $n = p'm$ with $p' \geq 3$ an odd prime. Note that since $n \geq 5$ is odd, then either $p' \geq 5$, or $p' = 3$ and $m \geq 5$.

Case i). G fixes a point $P \in \mathcal{H}_{2^m}$. Then $P \notin \mathcal{H}_q$ by the semiregularity of G on \mathcal{H}_q , hence G satisfies case ii) in the list of maximal subgroups of $\text{PSU}(3, q)$, contradicting the hypothesis.

Case ii). By Lagrange's theorem, the order $(2^{p'm} + 1)/3$ of G divides $2^m(2^m - 1)(2^m + 1)^2/3$, hence $\sum_{i=0}^{p'-1} (-1)^i 2^{im}$ divides $(2^{2m} - 1)$, which is impossible for any odd $p' \geq 3$.

Case iii). Now $(2^{p'm} + 1)/3$ divides $2(2^m + 1)^2$, hence $\sum_{i=0}^{p'-1} (-1)^i 2^{im}$ divides $3(2^m + 1)$, which is impossible since $\sum_{i=0}^{p'-1} (-1)^i 2^{im} > 3(2^m + 1)$.

Case *iv*). Now $(2^{p'm} + 1)/3$ divides $(2^{2m} - 2^m + 1)$, which is impossible since $(2^{p'm} + 1)/3 > 2^{2m} - 2^m + 1$ for any $p' \geq 3$, $m \geq 3$.

Case *xiii*). G is contained in $\text{PSU}(3, 2^r)$ with $m/r = p'' \geq 3$ an odd prime, and $n/r = p'p'' \geq 9$. This is impossible since $|G|$ is greater than the order of any maximal subgroup of $\text{PSU}(3, 2^r)$.

Case *xiv*). G is contained in a group K containing $\text{PSU}(3, 2^r)$ as a normal subgroup of index 3, where $r = m/3$. If $H \neq \text{PSU}(3, 2^r)$ is a maximal subgroup of K , we have $H \cdot \text{PSU}(3, 2^r) = \text{PGU}(3, 2^r)$, hence $[H : H \cap \text{PSU}(3, 2^r)] = [\text{PGU}(3, 2^r) : \text{PSU}(3, 2^r)] = 3$. Therefore, $|H|/3$ divides the order of a maximal subgroup of $\text{PSU}(3, 2^r)$. Then we get a contradiction, since $|G|$ does not divide three times the order of any maximal subgroup of $\text{PSU}(3, 2^r)$.

Case *xv*). $|G|$ divides 36, and $m = 1$, which implies $p' \geq 5$. For $p' = 5$, we have $|G| = 11$ which does not divide 36; for $p' > 5$, we have that $|G|$ is greater than 36. \square

Proposition 3.10. *Suppose $G \leq \text{PSU}(3, q)$ and a maximal subgroup M of $\text{PSU}(3, q)$ containing G satisfies only case *xiv*) in Theorem 2.2. Then $\mathcal{C}_{2^n} \not\cong \mathcal{H}_q/G$.*

Proof. M contains $\text{PSU}(3, 2^m)$ as a normal subgroup of order 3, where $m = n/3$. Arguing as in case *xiv*) of Lemma 3.9, $|G|$ divides three times the order of a maximal subgroup of $\text{PSU}(3, 2^m)$. Then we multiply by 3 the orders of maximal subgroups of $\text{PSU}(3, q)$ as listed in Theorem 2.2.

Case *i*). The order $(2^{3m} + 1)/3$ of G divides $2^{3m}(2^{2m} - 1)$, hence $(2^{2m} - 2^m + 1)$ divides $3(2^m - 1)$, which is impossible since $m \geq 3$.

Case *ii*). $(2^{3m} + 1)/3$ divides $2^m(2^m + 1)^2(2^m - 1)$, which is impossible as above.

Case *iii*). $(2^{3m} + 1)/3$ divides $6(2^m + 1)^2$, hence $(2^{2m} - 2^m + 1)$ divides $9(2^m + 1)$, which is impossible for any $m \geq 3$.

Case *iv*). $(2^{3m} + 1)/3$ divides $3(2^{2m} - 2^m + 1)$, hence $(2^m + 1) \mid 9$, which implies $m = 3$.

Cases *xiii*) and *xiv*). $(2^{3m} + 1)/3$ divides either $3 \cdot |\text{PSU}(3, 2^r)|$ or $3 \cdot |\text{PGU}(3, 2^r)|$, where $m/r = p'' \geq 3$ is an odd prime. As in the proof of Lemma 3.9, this is impossible since $|G|$ exceeds three times the order of any subgroup of $\text{PGU}(3, 2^r)$.

Case *xv*). $(2^{3m} + 1)/3$ divides 36, which is impossible for any $m \geq 3$.

Therefore the only possibility is given in case *iv*) for $m = 3$. Then G has order 171, $G'' = G \cap \text{PSU}(3, 2^m)$ has order $|G|/3 = 57$, and G'' is contained in the normalizer N of a cyclic Singer group S , of order $|N| = (2^{2m} - 2^m + 1) = 57$, hence $G'' = N$. G'' acts on the three non-collinear points Q_1, Q_2, Q_3 fixed by S , whose coordinates are in a cubic extension of $\mathbb{F}_{2^{2m}}$, hence in $\mathbb{F}_{2^{2n}}$. By the semiregularity of G , we have $Q_i \notin \mathcal{H}_q$; then $\{Q_1, Q_2, Q_3\}$ is a self-polar triangle, and we get the thesis as in the proof of Proposition 3.8, after replacing q with 2^m and G' with G'' . \square

Theorem 3.11. *\mathcal{C}_{2^n} is not a Galois subcover of the Hermitian curve \mathcal{H}_q .*

Proof. Suppose $\mathcal{C}_{2^n} \cong \mathcal{H}_q/G$. By Propositions 3.5, 3.6, 3.10 and Lemma 3.9, we have that $G \not\leq \text{PSU}(3, q)$; then $G' = G \cap \text{PSU}(3, q)$ has index 3 in G . After replacing G with G' , we can repeat the proofs of Propositions 3.7 and 3.8, the proof of Lemma 3.9, and the first part of the proof of Proposition 3.10. In this way, the only possibility we have is that $n = 9$ and a maximal subgroup M of $\text{PSU}(3, 2^9)$ containing G' contains $\text{PSU}(3, 2^3)$ as a normal subgroup of index 3; moreover, $G'' = G' \cap \text{PSU}(3, 2^3)$ is contained in the normalizer N' of a cyclic Singer group, of order $|N'| = 57$.

If $G' \leq \text{PSU}(3, 2^3)$, then we repeat the argument of the proof of Proposition 3.10, after G with G' . In this way we get a contradiction.

If $G' \not\leq \text{PSU}(3, 2^3)$, then $G'' = G' \cap \text{PSU}(3, 2^3)$ has order $|G'|/3 = 19$. Since $|G'| = 57$, then by the third Sylow theorem G' is the only Sylow 19-subgroup of G , hence G'' is the cyclic Singer group normalized by $G' = N'$. Therefore G'' fixes a triangle with coordinates in the cubic extension $\mathbb{F}_{2^{18}}$ of \mathbb{F}_{2^6} , which is the fundamental triangle T up to conjugation in $\text{PGU}(3, 2^9)$. Hence G' acts on T , and Proposition 3.8 yields the thesis.

4 \mathcal{X}_q is not Galois-covered by \mathcal{H}_{q^3} , for any $q > 3$

The aim of this section is to prove Theorem 1.2. Throughout the section, let $q > 3$ be a power of a prime p .

By direct application of a result by Duursma and Mak, we have the following bound.

Proposition 4.1. ([7, Thm. 1.3]) *If there exists a Galois-covering $\mathcal{H}_{q^3} \rightarrow \mathcal{X}_q$, of degree d , then*

$$q^2 + q \leq d \leq q^2 + q + 2.$$

Therefore we have to exclude three possible values of d .

Proposition 4.2. *There is no Galois-covering $\mathcal{H}_{q^3} \rightarrow \mathcal{X}_q$ of degree $q^2 + q + 2$.*

Proof. If such a Galois-covering exists, then $q^2 + q + 2$ divides the order $q^9(q^9 + 1)(q^6 - 1)$ of $\text{PGU}(3, q^3)$, hence $q^2 + q + 2$ divides the remainder of the polynomial division, which is equal to $2128q - 1568$. Then the possible values for q are 1, 2, 3, or 10, but none of these is acceptable. \square

Now we consider the possible value $d = q^2 + q + 1$.

Lemma 4.3. *Let $G \leq \text{PGU}(3, q^3)$ with $|G| = q^2 + q + 1$. Then $G \leq \text{PSU}(3, q^3)$.*

Proof. If $\text{PGU}(3, q^3) = \text{PSU}(3, q^3)$ there is nothing to prove, hence we can assume that $\text{PSU}(3, q^3)$ has index 3 in $\text{PGU}(3, q^3)$. Then $\gcd(3, q^3 + 1) = 3$, or equivalently $\gcd(3, q + 1) = 3$, so that 3 does not divide $q^2 + q + 1 = |G|$. If $G \not\leq \text{PSU}(3, q^3)$, then $\text{PGU}(3, q^3) = G \cdot \text{PSU}(3, q^3)$ and G has a subgroup $G \cap \text{PSU}(3, q^3)$ of index $[\text{PGU}(3, q^3) : \text{PSU}(3, q^3)] = 3$, contradiction. \square

Proposition 4.4. *There is no Galois-covering $\mathcal{H}_{q^3} \rightarrow \mathcal{X}_q$ of degree $q^2 + q + 1$.*

Proof. Suppose such a Galois-covering exists, say $\mathcal{X}_q \cong \mathcal{H}_{q^3}/G$. Then $G \leq \text{PSU}(3, q^3)$ by Lemma 4.3, and we can apply Theorem 2.1.

Case i) Let \mathcal{H}_{q^3} have equation $Y^{q^3+1} = X^{q^3} + X$; up to conjugation, G fixes the ideal point P_∞ . The stabilizer S of P_∞ in $\text{PGU}(3, q^3)$ is the semidirect product $P \rtimes H$, where P is the unique Sylow p -subgroup of S of order q^9 , and H is a cyclic group of order $q^6 - 1$ generated by

$$\alpha_a : (X, Y, T) \mapsto (a^{q^3+1}X, aY, T),$$

where a is a primitive $(q^6 - 1)$ -th root of unity; H fixes two \mathbb{F}_{q^3} -rational points of \mathcal{H}_{q^3} and acts semiregularly on the other points (see [14, Section 4]). Since $P \triangleleft S$, $|P|$ and $|H|$ are coprime, and $|G|$ divides $|H|$, then $G \subset H$, and $G = \langle \alpha_b \rangle$, where $b = a^{(q^3+1)(q-1)}$. Now consider the group $\bar{G} = \langle \alpha_c \rangle \subset H$, where $c = a^{q-1}$; G is normal in \bar{G} with index $q^3 + 1$. The automorphism group \bar{G}/G has two fixed points on \mathcal{H}_{q^3+1}/G and all other orbits are long; then the number of \mathbb{F}_{q^6} -rational points of \mathcal{H}_{q^3+1}/G is congruent to 2 modulo $q^3 + 1$. On the other side, the \mathbb{F}_{q^6} -maximal curve \mathcal{X}_q has genus $(q-1)(q^3 - q)/2$, hence the number of \mathbb{F}_{q^6} -rational points of \mathcal{X}_q is $q^7 - q^5 + q^4 + 1 \equiv q^2 + 1 \pmod{q^3 + 1}$, contradiction.

Case ii) Let \mathcal{H}_{q^3} have the Fermat equation $X^{q^3+1} + X^{q^3+1} + 1 = 0$; up to conjugation, G fixes the affine point $(0, 0)$ and the line at infinity $\ell : T = 0$. The action of G on ℓ is faithful. In fact, if $g \in G$ fixes ℓ pointwise, then $g : (X, Y, T) \mapsto (X, Y, \lambda T)$ is a homology whose order divides $q^3 + 1$; on the other hand, the order of g divides $|G| = q^2 + q + 1$, hence g is the identity since q is even. Therefore, as in the proof of Proposition 3.5, G is isomorphic to a subgroup of $\text{PGL}(2, q^6)$. Since $|G|$ is odd and coprime with p , then by Theorem 2.2 G is cyclic. Moreover, since $|G|$ divides $q^6 - 1$, then G has two fixed points $P_1, P_2 \in \ell$ and acts semiregularly on $\ell \setminus \{P_1, P_2\}$ (see [23, Hauptsatz 8.27]). Since $|\ell \cap \mathcal{H}_{q^3+1}| \equiv 2 \pmod{q^2 + q + 1}$, this implies $P_1, P_2 \in \mathcal{H}_{q^3+1}$. Therefore we can repeat the argument of Case i) to get a contradiction.

Cases iii) and iv) The order of G does not divide the order of these maximal subgroups.

Cases v) G acts on the $q^6 + 1$ \mathbb{F}_{q^6} -rational points of a conic \mathcal{C} ; as in Case ii), $G = \langle g \rangle$ is isomorphic to a cyclic subgroup $\Gamma \leq \mathrm{PGL}(2, q^6)$ acting on a line ℓ with no short orbits but two fixed points. The action of G on \mathcal{C} is equivalent to the action of Γ on ℓ , see [33, Chapt. VIII, Thm. 15]; hence G has no short orbits on \mathcal{C} but two fixed points P_1, P_2 . If G has a fixed \mathbb{F}_{q^6} -point on \mathcal{H}_{q^3} , then argue as in Case i). Otherwise, $P_1, P_2 \notin \mathcal{H}_{q^3}$, and by [29, Par. 2], [20, Page 141], we have that G fixes a third point P_3 such that $T = \{P_1, P_2, P_3\}$ is a self-polar triangle. Let \mathcal{H}_{q^3} be given in the Fermat form, then up to conjugation T is the fundamental triangle and g has the form $g : (X, Y, T) \mapsto (\lambda X, \mu Y, T)$. Then the order of g divides $q^3 + 1$, contradicting $|G| = q^2 + q + 1$.

Cases viii) to xii) and Case xv) $|G|$ does not divide the order of these maximal subgroups.

Cases vi), vii), xiii), and xiv) Note that, if K is a group containing $\mathrm{PSU}(3, p^h)$ as a normal subgroup of index 3, then the orders of maximal subgroups of K are three times the orders of maximal subgroups of $\mathrm{PSU}(3, p^h)$. With this observation, by applying Theorem 2.1 to $\mathrm{PSU}(3, p^m)$, it is easily seen that $|G|$ does not divide the orders of maximal subgroups of $\mathrm{PSU}(3, p^m)$ nor three times these orders. \square

Lemma 4.5. *Let $G \leq \mathrm{PGU}(3, q^3)$ with $|G| = q(q + 1)$. Then the number of Sylow p -subgroups is either 1 or $q + 1$.*

Proof. Let Q_1, \dots, Q_n be the Sylow p -subgroups of G , and let $P_i \in \mathcal{H}_{q^3}$ be the unique rational point fixed by Q_i , $i = 1, \dots, n$. Assume $n > 1$; note that $n \leq q + 1$, as $Q_i \cap Q_j$ is trivial for $i \neq j$. Since G has no fixed points and Q_i is semiregular on $\mathcal{H}_{q^3} \setminus \{P_i\}$, then the length of the orbit \mathcal{O}_{P_1} of P_1 under G is at least $q + 1$; on the other side, the stabilizer of P_1 in G has length at least q , since it contains Q_1 . Therefore $|\mathcal{O}_{P_1}| = q + 1$ by the orbit-stabilizer theorem. If $P \in \mathcal{O}_{P_1}$, then the stabilizer of P in G has order q , hence $P = P_i$ for some $i \in \{2, \dots, n\}$. Therefore $\mathcal{O}_{P_1} = \{P_1, \dots, P_n\}$ and the thesis follows. \square

Proposition 4.6. *Let $G \leq \mathrm{PGU}(3, q^3)$ with $|G| = q(q + 1)$. If G has a unique Sylow p -subgroup Q , then $\mathcal{X}_q \not\cong \mathcal{H}_{q^3}/G$.*

Proof. Let \mathcal{H}_{q^3} be given in the norm-trace form $Y^{q^3+1} = X^{q^3} + X$. Since Q is normal in G , then G fixes the unique fixed point of Q on \mathcal{H}_{q^3} ; up to conjugation, this is the ideal point P_∞ . By Hall's theorem, we can assume that $G = Q \rtimes \langle \alpha_\lambda \rangle$, where

$$\alpha_\lambda : (X, Y, T) \mapsto (\lambda^{q^3+1} X, \lambda Y, T) = (X, \lambda Y, T),$$

with λ primitive $(q + 1)$ -th root of unity. Suppose $\mathcal{X}_q \cong \mathcal{H}_{q^3}/G$, in particular the genus of \mathcal{X}_q equals the genus of \mathcal{H}_{q^3}/G , which is given in [14, Thm. 4.4]. With the notations of [14, Section 4], this implies $v = 0$ and $q = p^w$, that is, the elements of Q have the form

$$\beta_c : (X, Y, T) \mapsto (X + cT, Y, T),$$

with $c^{q^3} + c = 0$. The set $\{c \in \mathbb{F}_{q^6} \mid \beta_c \in Q\}$ is an additive group, isomorphic to Q . Then $Q \cong \{c \in \mathbb{F}_{q^6} \mid L(c) = 0\}$, where $L \in \mathbb{F}_{q^6}[X]$ is a linearized polynomial of degree q dividing $X^{q^3} + X$, and there is a linearized polynomial $F \in \mathbb{F}_{q^6}[X]$ of degree q^2 such that $F(L(X)) = X^{q^3} + X$ (see [26, Theorems 3.62, 3.65]). Therefore the quotient curve \mathcal{H}_{q^3}/G has equation $Y^{q^2-q+1} = F(X)$.

The thesis follows, if we show that there cannot exist an \mathbb{F}_{q^6} -isomorphism $\varphi : \mathcal{C} \rightarrow \mathcal{X}_q$, where $\mathcal{X}_q : V^{q^2-q+1} = U^{q^2} - U$ and \mathcal{C} is a curve with equation $Y^{q^2-q+1} = F(X)$, with $F \in \mathbb{F}_{q^6}[X]$ a linearized divisor of $X^{q^3} + X$ of degree q^2 .

Suppose such a φ exists. By [21, Thm. 12.11], the ideal points $P_\infty \in \mathcal{X}_q$, $Q_\infty \in \mathcal{C}$ are the unique fixed points of the respective automorphism groups $\text{Aut}(\mathcal{X}_q)$, $\text{Aut}(\mathcal{C})$, hence $\varphi(Q_\infty) = P_\infty$. Moreover, the coordinate functions have pole divisors

$$\text{div}(u)_\infty = (q^2 - q + 1)P_\infty, \quad \text{div}(v)_\infty = q^2 P_\infty, \quad \text{div}(x)_\infty = (q^2 - q + 1)Q_\infty, \quad \text{div}(y)_\infty = q^2 Q_\infty,$$

and the Weierstrass semigroups at the ideal points are $H(P_\infty) = H(Q_\infty) = \langle q^2 - q + 1, q^2 \rangle$ (see [21, Lemmata 12.1, 12.2]). By Riemann-Roch theory (see [30, Chapt. 1]), it is easily seen that $\{1, x\}$ is a basis of the Riemann-Roch space $\mathcal{L}((q^2 - q + 1)P_\infty)$ associated to $(q^2 - q + 1)P_\infty$, and $\{1, x, y\}$ is a basis of $\mathcal{L}(q^2 P_\infty)$. Then there exist $a, b, c, d, e \in \mathbb{F}_{q^6}$, $a, d \neq 0$, such that $\varphi^*(u) = ax + b$ and $\varphi^*(v) = cx + dy + e$, where $\varphi^* : \mathbb{F}_{q^6}(\mathcal{X}_q) \rightarrow \mathbb{F}_{q^6}(\mathcal{C})$ is the pull-back of φ ; equivalently, $\varphi(X, Y, T) = (aX + b, cX + dY + e, T)$. Then the polynomial identity

$$(aX + b)^{q^2} - (aX + b) - (cX + dY + e)^{q^2 - q + 1} = k \left(F(X) - Y^{q^2 - q + 1} \right)$$

holds, for some $k \in \mathbb{F}_{q^6}$, $k \neq 0$. By direct calculation and comparison of the coefficients, we get the constraints $c = e = 0$, $b \in \mathbb{F}_{q^2}$, $k = d^{q^2 - q + 1}$, which imply

$$F(X) = k^{-1} a^{q^2} X^{q^2} - k^{-1} a X.$$

It is easily checked that the conventional p -associate of the linearized polynomial $F(X)$ is not a divisor of the conventional p -associate of $X^{q^3} + X$, hence $F(X)$ is not a divisor of $X^{q^3} + X$. \square

Lemma 4.7. *Let $G \leq \text{PGU}(3, q^3)$ with $|G| = q(q + 1)$. If G has $q + 1$ distinct Sylow p -subgroup Q_1, \dots, Q_{q+1} , then $G \cong (\mathbb{Z}_{p'})^s \rtimes Q_1$, where p' is a prime and $(p')^s = q + 1$.*

Proof. By Lemma 4.5, the points P_1, \dots, P_{q+1} fixed respectively by Q_1, \dots, Q_{q+1} constitute a single orbit \mathcal{O} under the action of G . By Burnside's Lemma, G is sharply 2-transitive on \mathcal{O} . Then, by [19, Thm. 20.7.1], G is isomorphic to the group of affine transformations of a near-field F ; moreover, G has a regular normal subgroup N , hence $G = N \rtimes Q_1$. The order f of F satisfies $q(q + 1) = (f - 1)f$, which implies $f = q + 1$. By this condition, F cannot be one of the seven exceptional near-fields listed in [34], hence F is a Dickson near-field, see [19, Thm. 20.7.2] for a description. In particular, N is isomorphic to the additive group $(\mathbb{Z}_{p'})^s$ of a finite field $\mathbb{F}_{(p')^s}$. \square

Proposition 4.8. *Let $G \leq \text{PGU}(3, q^3)$ with $|G| = q(q + 1)$. If G has $q + 1$ distinct Sylow p -subgroup Q_1, \dots, Q_{q+1} , then $\mathcal{X}_q \not\cong \mathcal{H}_{q^3}/G$.*

Proof. We use the notations of Lemma 4.7 and assume $\mathcal{X}_q \cong \mathcal{H}_{q^3}/G$.

Suppose q is odd. Then all involutions of $\text{PGU}(3, q^3)$ are conjugate, and they are homologies of $\text{PG}(2, q^6)$, see [24, Lemma 2.2]. Two homologies commute if and only if the center of each lies on the axis of the other (see for example [5, Thm. 5.32]), hence the maximum number of involutions commuting pairwise is 3, since their centers are three non-collinear points. Then $(p')^s = 4$ and $q = 3$, against the assumptions of this section.

Suppose q is even. Q_1 is isomorphic to the multiplicative group of F , hence it is a metacyclic group, see for example [2, Ex. 1.19]; moreover, Q_1 has exponent 2 or 4 by [24, Lemma 2.1]. Therefore $q \in \{2, 4, 8, 16\}$. The case $q = 2$ is excluded. If $q = 16$, then F is a Dickson near-field of prime order 17, hence F is a field, against the exponent 2 or 4 of Q_1 . Then $q = 4$ or $q = 8$.

We use the Riemann-Hurwitz formula [30, Thm. 3.4.13] on the covering $\mathcal{H}_{q^3} \rightarrow \mathcal{X}_q \cong \mathcal{H}_{q^3}/G$, in order to get a contradiction on the degree $\Delta = (2g(\mathcal{H}_{q^3}) - 2) - |G|(2g(\mathcal{X}_q) - 2)$ of the Different. By [30, Thm. 3.8.7]

$$\Delta = \sum_{\sigma \in G \setminus \{id\}} i(\sigma),$$

where the contributions $i(\sigma) \geq 0$ to Δ satisfy the following:

- If σ has order 2, then $i(\sigma) = q^3 + 2$; if σ has order 4, then $i(\sigma) = 2$ (see [30, Eq. (2.12)]).
- If σ is odd, then $i(\sigma)$ equals the number of fixed points of σ on \mathcal{H}_{q^3} , see [30, Cor. 3.5.5]; moreover, by [20, pp. 141-142], either σ has exactly 3 fixed points or σ is a homology. In the former case $i(\sigma) \leq 3$, in the latter $i(\sigma) = q^3 + 1$.

Let $q = 4$, hence $\Delta = 470$ and $G = \mathbb{Z}_5 \rtimes Q_1$. If $Q_1 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then G has 15 involutions, whose contributions to Δ sum up to $990 > \Delta$. Then $Q_1 \cong \mathbb{Z}_4$, and the contributions to Δ of the Q_i 's sum up to $5 \cdot 66 + 10 \cdot 2 = 350$. The non-trivial elements of \mathbb{Z}_5 are generators of \mathbb{Z}_5 , then either all of them are homologies or all of them fix 3 points. In the former case their contribution to Δ exceeds 120, in the latter their contribution is smaller than 120.

Let $q = 8$, hence $\Delta = 7758$ and $G = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes Q_1$. If Q_1 has more than one involution, then the involutions of G contribute to Δ of at least $18 \cdot 514 > \Delta$. Then Q_1 is the quaternion group, and the Q_i 's contribute to Δ of $9 \cdot 514 + 54 \cdot 2 = 4734$. The contribution to Δ of any non-trivial element of $\mathbb{Z}_3 \times \mathbb{Z}_3$ is either 513 or less than 4, hence they cannot sum up to $\Delta - 4734$. \square

By Lemma 4.5 and Propositions 4.6, 4.8, we have shown the following result.

Proposition 4.9. *There is no Galois-covering $\mathcal{H}_{q^3} \rightarrow \mathcal{X}_q$ of degree $q^2 + q$.*

Finally, Theorem 1.2 follows from Propositions 4.1, 4.2, 4.4, and 4.9.

References

- [1] Abdón, M., Bezerra, J., Quoos, L.: Further examples of maximal curves. J. Pure Appl. Algebra **213** (6), 1192–1196 (2009)
- [2] Cameron, P.J.: Permutation Groups. Cambridge University Press (1999)
- [3] Cossidente, A., Korchmáros, G., Torres, F.: On curves covered by the Hermitian curve. J. Algebra **216** (1), 56–76 (1999)
- [4] Cossidente, A., Korchmáros, G., Torres, F.: Curves of large genus covered by the Hermitian curve. Comm. Algebra **28** (10), 4707–4728 (2000)
- [5] Coxeter, H.S.M.: The Real Projective Plane, 3rd edn. Springer, New York (1993)
- [6] Dickson, L. E.: Linear groups with an exposition of the Galois field theory. Teubner, Leipzig (1902)
- [7] Duursma, I., Mak, K.-H.: On maximal curves which are not Galois subcovers of the Hermitian curve. Bull. Braz. Math. Soc. (N.S.) **43** (3), 453–465 (2012)
- [8] Fuhrmann, R., Torres, F.: On Weierstrass points and optimal curves. Rend. Circ. Mat. Palermo Suppl. 51 (Recent Progress in Geometry, Ballico E, Korchmáros G, (Eds.)), 25–46 (1998)
- [9] Garcia, A.: Curves over finite fields attaining the Hasse-Weil upper bound. In: European Congress of Mathematics, vol. II (Barcelona 2000), Progr. Math. 202, pp. 199–205. Birkhäuser, Basel (2001)
- [10] Garcia, A.: On curves with many rational points over finite fields. In: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, pp. 152–163. Springer, Berlin (2002)

- [11] Garcia, A., Güneri, C., Stichtenoth, H.: A generalization of the Giulietti-Korchmáros maximal curve. *Advances in Geometry* **10** (3), 427–434 (2010)
- [12] Garcia, A., Stichtenoth, H.: Algebraic function fields over finite fields with many rational places. *IEEE Trans. Inform. Theory* **41**, 1548–1563 (1995)
- [13] Garcia, A., Stichtenoth, H.: A maximal curve which is not a Galois subcover of the Hermitian curve. *Bull. Braz. Math. Soc. (N.S.)* **37** (1), 139–152 (2006)
- [14] Garcia, A., Stichtenoth, H., Xing, C.P.: On Subfields of the Hermitian Function Field. *Compositio Math.* **120**, 137–170 (2000)
- [15] Garcia, A., Torres, F.: On unramified coverings of maximal curves. In: *Proceedings of AGCT-10 2005, Sémin. Congr.* 21, 35–42 (2010)
- [16] Giulietti, M., Korchmáros, G.: A new family of maximal curves over a finite field. *Math. Ann.* **343** (1), 229–245 (2009)
- [17] Güneri, C., Özdemir, M., Stichtenoth, H.: The automorphism group of the generalized Giulietti-Korchmáros function field. *Advances in Geometry* **13** (2), 369–380 (2013)
- [18] Guralnick, R., Malmskog, B., Pries, R.: The automorphism of a family of maximal curves. *J. Algebra* **361**, 92–106 (2012)
- [19] Hall, M.: *The Theory of Groups*. Macmillan, New York (1959)
- [20] Hartley, R. W.: Determination of the ternary collineation group whose coefficients lie in the $GF(2^n)$. *Ann. of Math. Second Series* **27** (2), 140–158 (1925)
- [21] Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: *Algebraic Curves over a Finite Field*. Princeton Series in Applied Mathematics, Princeton (2008)
- [22] Hughes, D.R., Piper, F.C.: *Projective planes*. Graduate Text in Mathematics **6**. Springer, New York (1973)
- [23] Huppert, B.: *Endliche Gruppen I. Die Grundlehren der Mathematischen Wissenschaften* **134**. Springer, Berlin (1967)
- [24] Kantor, W.N., O’Nan M.E., Seitz, G.M.: 2-Transitive Groups in Which the Stabilizer of Two Points is Cyclic. *J. Algebra* **21**, 17–50 (1972)
- [25] Lachaud, G.: Sommes d’Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis. *C.R. Acad. Sci. Paris* 305, Série I, 729–732 (1987)
- [26] Lidl, R., Niederreiter, H.: *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge (1986)
- [27] Macdonald, I.D.: *The theory of groups*. Oxford University Press, Oxford (1968)
- [28] Mak, K.-H.: On congruence function fields with many rational points. PhD Thesis. Available at www.ideals.illinois.edu
- [29] Mitchell, H.H.: Determination of the ordinary and modular ternary linear groups. *Trans. Amer. Math. Soc.* **12** (2), 207–242 (1911)

- [30] Stichtenoth, H.: Algebraic function fields and codes, 2nd edn. Graduate Texts in Mathematics **254**. Springer, Berlin (2009)
- [31] van der Geer, G.: Curves over finite fields and codes. In: European Congress of Mathematics, vol. II (Barcelona 2000), Progr. Math. 202, pp. 225–238. Birkhäuser, Basel (2001)
- [32] van der Geer, G.: Coding theory and algebraic curves over finite fields: a survey and questions. In: Applications of Algebraic Geometry to Coding Theory, Physics and Computation, NATO Sci. Ser. II Math. Phys. Chem. 36, pp. 139–159. Kluwer, Dordrecht (2001)
- [33] Veblen, O., Young, J.W.: Projective Geometry. The Atheneum Press, Boston (1910)
- [34] Zassenhaus, H.: Über endliche Fastkörper. Abh. Math. Sem. Univ. Hamburg **11**, 132–145 (1936)