Finite Fields and Their Applications 41 (2016) 72–88

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On maximal curves that are not quotients of the Hermitian curve

Massimo Giulietti[a,*], Maria Montanucci[b], Giovanni Zini[c]

[a] Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli, 1, 06123 Perugia, Italy

[b] Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Viale dell'Ateneo Lucano, 10, 85100 Potenza, Italy

[c] Dipartimento di Matematica e Informatica "Ulisse Dini", Università degli Studi di Firenze, Viale Morgagni, 67/a, 50134 Firenze, Italy

A R T I C L E I N F O

Article history:
Received 30 November 2015
Received in revised form 22 May 2016
Accepted 23 May 2016
Available online 8 June 2016
Communicated by Anne Canteaut

MSC:
11G20

Keywords:
Hermitian curve
Unitary groups
Maximal curves

A B S T R A C T

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

* Corresponding author.
E-mail addresses: massimo.giulietti@unipg.it (M. Giulietti), maria.montanucci@unibas.it (M. Montanucci), gzini@math.unifi.it (G. Zini).

http://dx.doi.org/10.1016/j.ffa.2016.05.005
1071-5797/

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 [9–11,13,32,33] and [23, 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 [15, 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 $\mathrm{Aut}(\mathcal{H}_q)$ is isomorphic to $\mathrm{PGU}(3, q)$, the group of projectivities of $\mathrm{PG}(2, q^2)$ commuting with the unitary polarity associated with $\mathcal{H}_q$.

By a result commonly attributed to Serre, see [26, 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 $G \leq \mathrm{Aut}(\mathcal{X})$.

Most of the known maximal curves are Galois subcovers of the Hermitian curve, many of which were studied in [4,5,15]. Garcia and Stichtenoth [14] 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 $\mathcal{X}_\ell$ with equation

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

which is $\mathbb{F}_{\ell^6}$-maximal for any $\ell \geq 2$; see [1]. In [17], Giulietti and Korchmáros showed that the Galois covering of $\mathcal{X}_\ell$ given by

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

is also $\mathbb{F}_{\ell^6}$-maximal, for any prime power ℓ. Remarkably, it is not covered by $\mathcal{H}_{\ell^3}$ for any $\ell > 2$. This curve, nowadays referred to as the GK curve, was generalized in [12] 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 [17]. Duursma and Mak proved in [8] that, if $\ell \geq 3$, then $\mathcal{C}_{\ell^n}$ is not Galois covered by $\mathcal{H}_{\ell^n}$. 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 $\mathcal{H}_{\ell^n}$.*

Duursma and Mak [8, Thm. 1.2] showed that if $\mathcal{C}_{2^n}$ is the quotient curve $\mathcal{H}_{2^n}/G$ for G a subgroup of $\mathrm{Aut}(\mathcal{H}_{2^n})$, then G has order $(2^n+1)/3$ and acts semiregularly on $\mathcal{H}_{2^n}$. Remember that G is *semiregular* on $\mathcal{H}_{2^n}$ if the stabilizer of any $P \in \mathcal{H}_{2^n}$ under G is trivial; by the orbit-stabilizer theorem, this is equivalent to require that G has just long orbits on $\mathcal{H}_{2^n}$, i.e. each orbit has length $|G|$. We investigate all subgroups G of $\mathrm{Aut}(\mathcal{H}_{2^n})$ satisfying these conditions, relying also on classical results by Mitchell [30] and Hartley [22] (see Section 2) which provide a classification of the maximal subgroups of $\mathrm{PSU}(3, q)$ in terms of their order and their action on $\mathcal{H}_q$. For any candidate subgroup G, we find another subgroup $\bar{G}$ of $\mathrm{Aut}(\mathcal{H}_{2^n})$ 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 $\mathcal{X}_\ell$ with equation (1). In [14] it was shown that $\mathcal{X}_3$ is not a Galois subcover of $\mathcal{H}_{3^6}$, while $\mathcal{X}_2$ is a quotient of $\mathcal{H}_{2^6}$, as noted in [16]. Garcia and Stichtenoth [14, Remark 4] raised the same question for any $\ell > 3$. The case where ℓ is a prime was settled by Mak [29]. Here we provide an answer for any prime power $\ell > 3$.

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

In the proof of Theorem 1.2 we bound the possible degree of a Galois covering $\mathcal{H}_{\ell^6} \to \mathcal{X}_\ell$ by means of [8, 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 [30] and Hartley [22], other group-theoretic arguments, and the Riemann–Hurwitz formula (see [31, Chapt. 3]) applied to the Galois coverings $\mathcal{H}_{\ell^6} \to \mathcal{H}_{\ell^6}/G$.

2. Preliminary results

Theorem 2.1. (Mitchell [30], Hartley [22]) *Let $q = p^k$, $d = \gcd(q+1, 3)$. The following is the list of maximal subgroups of $\mathrm{PSU}(3, q)$ up to conjugacy:*

i) the stabilizer of an $\mathbb{F}_{q^2}$-rational point of $\mathcal{H}_q$, of order $q^3(q^2-1)/d$;
ii) the stabilizer of an $\mathbb{F}_{q^2}$-rational point not on $\mathcal{H}_q$ 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, of order $6(q+1)^2/d$;
iv) the normalizer of a cyclic Singer group stabilizing a triangle in $\mathrm{PG}(2,q^6)\setminus\mathrm{PG}(2,q^2)$, of order $3(q^2-q+1)/d$.

Further, for $p>2$:

v) $\mathrm{PGL}(2,q)$ preserving a conic;
vi) $\mathrm{PSU}(3,p^m)$ with $m \mid k$ and k/m odd;
vii) subgroups containing $\mathrm{PSU}(3,2^m)$ 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) $\mathrm{PSL}(2,7)$ 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.

Further, for $p=2$:

xiii) $\mathrm{PSU}(3,2^m)$ with $m \mid k$ and k/m an odd prime;
xiv) subgroups containing $\mathrm{PSU}(3,2^m)$ 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-by-case analysis of the possible unitary groups G such that the quotient curve $\mathcal{H}/G$ realizes a putative Galois covering.

While dealing with case *ii)*, we will invoke a result by Dickson [7] which classifies all subgroups of the projective special linear group $\mathrm{PSL}(2,q)$ acting on $\mathrm{PG}(1,q)$. We remark that $\mathrm{PSL}(2,q)$ has index $\gcd(q-1,2)$ in the group $\mathrm{PGL}(2,q)$ of all projectivities of $\mathrm{PG}(1,q)$. From Dickson's result the classification of subgroups of $\mathrm{PGL}(2,q)$ is easily obtained.

Theorem 2.2. ([7, Chapt. XII, Par. 260]; see also [23, Thm. A.8]) *Let $q=p^k$, $d=\gcd(q-1,2)$. The following is the complete list of subgroups of $\mathrm{PGL}(2,q)$ 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 $f \le k$;
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) $\mathrm{PSL}(2, p^f)$ *for* $f \mid k$*;*
ix) $\mathrm{PGL}(2, p^f)$ *for* $f \mid k$*.*

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

Throughout the section, $n \geq 5$ is an odd integer and $q = 2^n$. We rely on a result by Duursma and Mak.

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

Proof. The order of G is equal to the degree of the covering $\varphi : \mathcal{H}_{2^n} \to \mathcal{H}_{2^n}/G \cong \mathcal{C}_{2^n}$. Hence, by [8, Thm. 1.2], G has order $(2^n + 1)/3$. Also, by [8, Thm. 1.2], φ is unramified. Since $\mathcal{H}_{2^n}$ is non-singular, this means that there are exactly $|G|$ points of $\mathcal{H}_{2^n}$ lying over each point of $\mathcal{H}_{2^n}/G$. Therefore, each orbit of G is long and the thesis follows. □

By Lemma 3.1 only subgroups G of $\mathrm{Aut}(\mathcal{H}_q)$ 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 $\mathrm{Aut}(\mathcal{C}_{2^n})$ fixes a point.

Theorem 3.2. ([18, Thm. 3.10], [19, Prop. 2.10]) *For* $n \geq 5$*, the group* $\mathrm{Aut}(\mathcal{C}_{2^n})$ *has a unique fixed point* P_∞ *on* $\mathcal{C}_q$*, and* P_∞ *is* $\mathbb{F}_{q^2}$*-rational.*

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

Proof. The claim follows from Theorem 3.2, taking into account that $\bar{G}/G \leq \mathrm{Aut}(\mathcal{H}_q/G)$ acts semiregularly on $\mathcal{H}_q/G$. □

The following well-known result about finite groups will be used (see [28, 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. *Let* $G \leq \mathrm{PSU}(3, q)$*. If a maximal subgroup of* $\mathrm{PSU}(3, q)$ *containing* G *is of type 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 $\mathrm{PSL}(2,q^2)$. We can assume that ℓ is the line at infinity $T=0$; in fact, the group $\mathrm{PGU}(3,q)$ is transitive on the points of $\mathrm{PG}(2,q^2)\setminus\mathcal{H}_q$, and hence also on the $(q+1)$-secant lines. The action of an element $g\in G$ on ℓ 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 $a_{31}=a_{32}=0$; we set $a_{33}=1$. By direct computation, the map

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

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 $\mathrm{PGL}(2,q^2)$. Since $|G|$ is odd, 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

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

Let $\mathcal{H}_q: X^{q+1}+Y^{q+1}+T^{q+1}=0$; 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 $\mathrm{PGU}(3,q)$. By Sylow theorems we can assume, up to conjugation, that $g\in D$; therefore, the fixed points of the subgroup $\langle g\rangle$ generated by g are the fundamental points $P_1=(1,0,0)$, $P_2=(0,1,0)$, and $P_3=(0,0,1)$. Since G is abelian, $\langle g\rangle$ is normal in G; hence, G acts on $\mathcal{T}=\{P_1,P_2,P_3\}$. As $|G|$ is odd, we have by the orbit-stabilizer theorem that the orbits of any $h\in G$ on $\mathcal{T}$ have length 1 or 3. If h has a single orbit on $\mathcal{T}$, then h is either

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

that is h^3 is the identity element of G and clearly G cannot be generated by h. 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; hence

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

with θ a primitive $(q+1)/3$-th root of unity, and i coprime with $(q+1)/3$. Let $\zeta \in \mathbb{F}_{q^2}$ with $\zeta^3 = \theta$, and let $\bar{G}$ be the group generated by $\alpha_\zeta : (X, Y, T) \mapsto (\zeta X, \zeta^i Y, T)$. 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 the thesis follows from Corollary 3.3. □

Proposition 3.6. *Let $G \leq \mathrm{PSU}(3, q)$. If a maximal subgroup of $\mathrm{PSU}(3, q)$ containing G is of type iii) in Theorem 2.1, then $\mathcal{C}_{2^n} \not\cong \mathcal{H}_q/G$.*

Proof. Let $\mathcal{H}_q : X^{q+1} + Y^{q+1} + T^{q+1} = 0$. Up to conjugation, the self-polar triangle stabilized by G is the fundamental triangle $\mathcal{T} = \{P_1, P_2, P_3\}$, whose vertices are not points of $\mathcal{H}_q$. The elements of G stabilizing $\mathcal{T}$ pointwise form a normal subgroup N of G, and G/N acts faithfully on $\mathcal{T}$; hence, either $G = N$ or $[G : N] = 3$.

If $G = N$, then G fixes one fundamental point, say P_1, and its polar line P_2P_3; therefore, the thesis follows from Proposition 3.5.

If $[G : N] = 3$, then N is cyclic, by the same argument used in the proof of Proposition 3.5; say $N = \langle \alpha_\xi \rangle$, where ξ is a primitive $(q+1)/9$-th root of unity, $\alpha_\xi : (X, Y, T) \mapsto (\xi X, \xi^i Y, T)$, and i is coprime with $(q+1)/9$. Let $h \in G \setminus N$. By arguing as in the proof of Proposition 3.5, h has order 3. Moreover, G is the semidirect product $N \rtimes \langle h \rangle$; in fact, N is normal in G, N and $\langle h \rangle$ have trivial intersection, and $|G| = |N| \cdot |\langle h \rangle|$. Let $\bar{N}$ be the cyclic group generated by $\alpha_\theta : (X, Y, T) \mapsto (\theta X, \theta^i Y, T)$, where $\theta \in \mathbb{F}_{q^2}$ satisfies $\theta^3 = \xi$. Let $\bar{G}$ be the group generated by $\bar{N}$ and h. Then $\bar{G}$ is the semidirect product $\bar{N} \rtimes \langle h \rangle$.

We want to double count the size of the set

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

Since G and $\bar{N}$ are semiregular on $\mathcal{H}_q$, we consider only elements of the form $\bar{n}h$ or $\bar{n}h^2$, with $\bar{n} \in \bar{N} \setminus N$. Up to reordering of the fundamental points, we have

$$\bar{n} = \begin{pmatrix} \rho & 0 & 0 \\ 0 & \rho^i & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad h = \begin{pmatrix} 0 & \lambda & 0 \\ 0 & 0 & \mu \\ 1 & 0 & 0 \end{pmatrix}, \tag{2}$$

where $\lambda^{q+1} = \mu^{q+1} = 1$, $\gcd(i, (q+1)/3) = 1$, and $\rho = \theta^{3j+u}$ with $0 < j < (q+1)/3$ and $u \in \{1, 2\}$. Hence

$$\bar{n}h = \begin{pmatrix} \rho & 0 & 0 \\ 0 & \rho^i & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & \lambda & 0 \\ 0 & 0 & \mu \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & A & 0 \\ 0 & 0 & B \\ 1 & 0 & 0 \end{pmatrix}, \tag{3}$$

where $A^{q+1} = B^{q+1} = 1$, and $\det(\bar{n}h) = AB$ is not a cube in $\mathbb{F}_{q^2}$, since $\bar{n}h \notin \mathrm{PSU}(3, q)$. Then $\bar{n}h$ has three 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 $z^3 = AB$. Therefore, $\bar{n}h$ has exactly three fixed points, namely

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

it is easy to check that Q_1, Q_2, and Q_3 are points of $\mathcal{H}_q$. The same holds for $\bar{n}h^2$.

Therefore, any element $\bar{n}h$ or $\bar{n}h^2$ with $\bar{n} \in \bar{N} \setminus N$ has exactly three fixed points on $\mathcal{H}_q$; then

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

The orbit $\mathcal{O}$ of a point $P \in \mathcal{H}_q$ under $\bar{G}$ has size $|\mathcal{O}| \geq |G| = (q+1)/3$. Then 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. Hence, the number $|\mathcal{S}| - 1$ of pairs in I having P in the second coordinate is either zero or 2.

Therefore $|I| = 2m$, where m is the number of points of $\mathcal{H}_q$ fixed by some non-trivial element of $\bar{G}$. By (4), we get

$$m = 2 \cdot \frac{q+1}{3} = 2 \cdot |G|.$$

Hence, $\bar{G}/G$ has two fixed points $R_1, R_2 \in \mathcal{H}_q/G$ and acts semiregularly on $\mathcal{H}_q/G \setminus \{R_1, R_2\}$. By Theorem 3.2, either R_1 or R_2 is $\mathbb{F}_{q^2}$-rational. Then the number $|\mathcal{H}_q/G(\mathbb{F}_{q^2})|$ of $\mathbb{F}_{q^2}$-rational points of $\mathcal{H}_q/G$ satisfies

$$|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv |\{P \in \{R_1, R_2\} \mid P \text{ is } \mathbb{F}_{q^2}\text{-rational}\}| \pmod{|\bar{G}/G|},$$

that is, $|\mathcal{H}_q/G(\mathbb{F}_{q^2})|$ is congruent to 1 or 2 modulo 3.

On the other side, the number $|\mathcal{C}_{2^n}(\mathbb{F}_{q^2})|$ of $\mathbb{F}_{q^2}$-rational points of $\mathcal{C}_{2^n}$ equals

$$q^2 + 1 + 2q \cdot (3q-4)/2 = 4q^2 - 4q + 1,$$

see [12, 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. *Let $G \leq \mathrm{PGU}(3,q)$, $G \not\subseteq \mathrm{PSU}(3,q)$. If a maximal subgroup of $\mathrm{PSU}(3,q)$ containing $G \cap \mathrm{PSU}(3,q)$ is of type ii) in Theorem 2.1, then $\mathcal{C}_{2^n} \not\cong \mathcal{H}_q/G$.*

Proof. Let $G' = G \cap \mathrm{PSU}(3,q)$. Since $\mathrm{PSU}(3,q)$ has index 3 in $\mathrm{PGU}(3,q)$, $\mathrm{PGU}(3,q) = G \cdot \mathrm{PSU}(3,q)$ and $[G : G'] = 3$; hence, G' is normal in G by Lemma 3.4. Arguing as in the proof of Proposition 3.5, G' is cyclic; moreover, G' is generated by $\alpha_\xi : (X, Y, T) \mapsto (\xi X, \xi^i Y, T)$, where ξ is a primitive $(q+1)/9$-th root of unity and i is coprime with $(q+1)/9$. Then G stabilizes the fundamental triangle $\mathcal{T}$.

If there exists $h \in G \setminus G'$ of order 3, then $G = G' \rtimes \langle h \rangle$ by arguing as in the proof of Proposition 3.6. Let $\theta \in \mathbb{F}_{q^2}$ with $\theta^3 = \xi$, and define $\alpha_\theta : (X, Y, T) \mapsto (\theta X, \theta^i Y, T)$.

Let $\bar{G}'$ be the cyclic group generated by α_θ, and let $\bar{G}$ be the group generated by $\bar{G}'$ and h; then $\bar{G} = \bar{G}' \rtimes \langle h \rangle$. Moreover, $[\bar{G} : G] = [\bar{G}' : G'] = 3$; hence, by Lemma 3.4, G' is normal in $\bar{G}'$ and G is normal in $\bar{G}$. We can repeat the same argument used in the proof of Proposition 3.6, after replacing N with G' and $\bar{N}$ with $\bar{G}'$; then $|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv 1, 2 \pmod 3$, while $|\mathcal{C}_{2^n}| \equiv 0 \pmod 3$. This yields the thesis.

If there is no $h \in G \setminus G'$ of order 3, then G is made of diagonal matrices, since G acts on $\mathcal{T}$. By Theorem 2.2, G is cyclic; a generator of G has the form $\alpha_\theta : (X, Y, T) \mapsto (\theta X, \theta^j Y, T)$, with θ a primitive $(q+1)/3$-th root of unity and j coprime with $(q+1)/3$. Let $\bar{G}$ be the group generated by $\alpha_\zeta : (X, Y, T) \mapsto (\zeta X, \zeta^i Y, T)$, where $\zeta \in \mathbb{F}_{q^2}$ satisfies $\zeta^3 = \theta$. Then G is a normal subgroup of $\bar{G}$ of index 3, and $\bar{G}$ acts semiregularly on $\mathcal{H}_q$. Corollary 3.3 yields the thesis. $\square$

Proposition 3.8. *Let $G \leq \mathrm{PGU}(3, q)$, $G \not\subseteq \mathrm{PSU}(3, q)$. If a maximal subgroup of $\mathrm{PSU}(3, q)$ containing $G \cap \mathrm{PSU}(3, q)$ is of type iii) in Theorem 2.1, then $\mathcal{C}_{2^n} \not\cong \mathcal{H}_q/G$.*

Proof. As in the proof of Proposition 3.7, $G' = G \cap \mathrm{PSU}(3, q)$ is normal in G of index 3. Arguing as in the proof of Proposition 3.6, it can be shown that there are two possible cases for G': (A) G' is cyclic and generated by $\alpha_\xi : (X, Y, T) \mapsto (\xi X, \xi^i Y, T)$, with ξ a primitive $(q+1)/9$-th root of unity and i coprime with $(q+1)/9$; (B) $G' = \langle \alpha_\eta \rangle \rtimes \langle h \rangle$, where $\alpha_\eta : (X, Y, T) \mapsto (\eta X, \eta^i Y, T)$ with η a primitive $(q+1)/27$-th root of unity and i coprime with $(q+1)/27$, and h is an element of order 3 acting with a single orbit on the fundamental triangle $\mathcal{T}$, hence having the form (2).

(A) Since G' is normal in G, we have that G acts on $\mathcal{T}$. If G fixes $\mathcal{T}$ pointwise, then the elements of G are diagonal matrices whose diagonal coefficients are $(q+1)/3$-th roots of unity, hence cubes in $\mathbb{F}_{q^2}$; therefore $G \leq \mathrm{PSU}(3, q)$, against the hypothesis. Then $G = G' \rtimes \langle h \rangle$, where $h \in G \setminus G'$ has order 3. Let $\theta \in \mathbb{F}_{q^2}$ with $\theta^3 = \xi$, and let $\bar{G}$ be the group generated by $\alpha_\theta : (X, Y, T) \mapsto (\theta X, \theta^i Y, T)$ and h; then $\bar{G} = \langle \alpha_\theta \rangle \rtimes \langle h \rangle$. By arguing as in the proof of Proposition 3.6, we have that $|\mathcal{H}_q/G(\mathbb{F}_{q^2})| \equiv 1, 2 \pmod 3$, while $|\mathcal{C}_{2^n}| \equiv 0 \pmod 3$. This yields the thesis.

(B) Any element of $G' \setminus \langle \alpha_\eta \rangle$ has order 3; in fact, it is the product of a diagonal matrix with a matrix of the form (2). Thus every element of $G' \setminus \langle \alpha_\eta \rangle$ has the form (3), which has order 3. Therefore, $\langle \alpha_\eta \rangle$ is the only cyclic subgroup of order $(q+1)/27$ in G'; thus $\langle \alpha_\eta \rangle$ is characteristic in G', and hence normal in G. Therefore, G acts on the set of points which are fixed by $\langle \alpha_\eta \rangle$, i.e. the fundamental points. Let G'' be the subgroup of G fixing $\mathcal{T}$ pointwise. The group G'' is abelian, as it is made of diagonal matrices; moreover, G'' is normal in G of index 3, and $G = G'' \rtimes \langle h \rangle$. By the primary decomposition of abelian groups, either $G'' = \langle \alpha_\xi \rangle$ with $\xi^3 = \eta$ and $\alpha_\xi : (X, Y, T) \mapsto (\xi X, \xi^i Y, T)$, or $G'' = \langle \alpha_\eta \rangle \times \langle k \rangle$, where k has order 3. In the latter case $\det(k)^3 = 1$, as k^3 is the identity element; hence, $\det(k)$ is a cube in $\mathbb{F}_{q^2}$, and $k \in G \cap \mathrm{PSU}(3, q) = G'$. Therefore $G' = G''$, contradicting $h \in G' \setminus G''$.

Then $G'' = \langle \alpha_\xi \rangle$ and $G = \langle \alpha_\xi \rangle \rtimes \langle h \rangle$. Let $\bar{G} = \langle \alpha_\theta \rangle \rtimes \langle h \rangle$, with $\theta^3 = \xi$ and $\alpha_\theta : (X, Y, T) \mapsto (\theta X, \theta^i Y, T)$. We can argue as in the proof of Proposition 3.6, after replacing N with $\langle \alpha_\xi \rangle$ and $\bar{N}$ with $\langle \alpha_\theta \rangle$; we get that $|\mathcal{H}_q / G(\mathbb{F}_{q^2})| \equiv 1, 2 \pmod 3$, while $|\mathcal{C}_{2^n}(\mathbb{F}_{q^2})| \equiv 0 \pmod 3$. This yields the thesis. □

Lemma 3.9. *Let $G \le \mathrm{PSU}(3, q)$. If a maximal subgroup M of $\mathrm{PSU}(3, q)$ containing G is neither of type ii) nor of type iii) in Theorem 2.1, then M is of type xiv); that is, $G \not\subseteq \mathrm{PSU}(3, 2^{n/3})$ and M contains $\mathrm{PSU}(3, 2^{n/3})$ as a normal subgroup of index 3.*

Proof. With the notations of Theorem 2.1, we can exclude cases *ii*) and *iii*) by hypothesis, case *i*) by the semiregularity of G, and cases *iv*) and *xv*) since $|G|$ does not divide either $3(q^2 - q + 1)$ or 36. The thesis will follow if we exclude case *xiii*). Assume by contradiction that M is of type *xiii*); we apply Theorem 2.1 to $M = \mathrm{PSU}(3, 2^m)$, where $n = p'm$ with p' an odd prime. Note that, since $n \ge 5$ is odd, either $p' \ge 5$, or $p' = 3$ and $m \ge 3$.

Case *i*). G fixes an $\mathbb{F}_{2^{2m}}$-rational point $P \in \mathcal{H}_{2^m}$. Since $P \notin \mathcal{H}_q$ by the semiregularity of G, M is of type *ii*) in the list of maximal subgroups of $\mathrm{PSU}(3, q)$, against the hypothesis.

Case *ii*). The order $(2^{p'm} + 1)/3$ of G divides $2^m(2^m - 1)(2^m + 1)^2/3$, which is impossible.

Case *iii*). The order of G divides $2(2^m + 1)^2$, which is impossible.

Case *iv*). The order of G divides $2^{2m} - 2^m + 1$, which is impossible.

Case *xiii*). G is contained in $\mathrm{PSU}(3, 2^r)$, where m/r is an odd prime; hence $n/r \ge 9$. This is impossible, since the order of G is greater than the order of any maximal subgroup of $\mathrm{PSU}(3, 2^r)$.

Case *xiv*). G is contained in a group K containing $\mathrm{PSU}(3, 2^r)$ as a normal subgroup of index 3, where $r = m/3$. If H is a maximal subgroup of K and $H \neq \mathrm{PSU}(3, 2^r)$, then $H \cap \mathrm{PSU}(3, 2^r)$ has index 3 in H; therefore, $|H|/3$ divides the order of a maximal subgroup of $\mathrm{PSU}(3, 2^r)$. This yields a contradiction, since, by direct computation, the order of G does not divide three times the order of any maximal subgroup of $\mathrm{PSU}(3, 2^r)$.

Case *xv*). The order of G divides 36, which is impossible. □

Proposition 3.10. *Let $G \le \mathrm{PSU}(3, q)$. If a maximal subgroup M of $\mathrm{PSU}(3, q)$ containing G is of type xiv) in Theorem 2.1, then $\mathcal{C}_{2^n} \not\cong \mathcal{H}_q / G$.*

Proof. The subgroup M contains $\mathrm{PSU}(3, 2^m)$ as a normal subgroup of order 3, where $m = n/3 \ge 3$. As in the proof of Lemma 3.9, $|G|$ divides three times the order of a maximal subgroup of $\mathrm{PSU}(3, 2^m)$. We apply Theorem 2.1 to $\mathrm{PSU}(3, 2^m)$.

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

Case *ii*). The order of G divides $2^m(2^m + 1)^2(2^m - 1)$, which is impossible.

Case *iii*). The order of G divides $6(2^m + 1)^2$, which is impossible.

Case *iv*). The order of G divides $3(2^{2m} - 2^m + 1)$; this happens if and only if $m = 3$.

Cases *xiii*) and *xiv*). The order of G divides either $3 \cdot |PSU(3, 2^r)|$ or $3 \cdot |PGU(3, 2^r)|$, where m/r is an odd prime. This is impossible, since $|G|$ exceeds three times the order of any subgroup of $\mathrm{PGU}(3, 2^r)$.

Case *xv*). The order of G divides 36, which is impossible.

Therefore, we have to consider only case *iv*), with $m = 3$. In this case, G has order 171 and $G'' = G \cap \mathrm{PSU}(3, 2^m)$ has order $|G|/3 = 57$; moreover, G'' coincides with the normalizer in $\mathrm{PSU}(3, 2^m)$ of a cyclic Singer group S. The fixed points of S are three non-collinear points P_1, P_2, P_3 whose coordinate are in a cubic extension of $\mathbb{F}_{2^{2m}}$, hence in $\mathbb{F}_{2^{2n}}$. Since G is semiregular, we have that $P_i \notin \mathcal{H}_q$; therefore, $\mathcal{T} = \{P_1, P_2, P_3\}$ is a self-polar triangle with respect to $\mathcal{H}_q$. Since G acts on $\mathcal{T}$, the thesis follows 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 $\mathcal{C}_{2^n} \cong \mathcal{H}_q/G$. Then $G \nsubseteq \mathrm{PSU}(3, q)$, by Propositions 3.5, 3.6, 3.10 and Lemma 3.9. Hence, $G' = G \cap \mathrm{PSU}(3, q)$ 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. Then $n = 9$, and any maximal subgroup M of $\mathrm{PSU}(3, 2^9)$ containing G' contains also $\mathrm{PSU}(3, 2^3)$ as a normal subgroup of index 3. Moreover, $G'' = G' \cap \mathrm{PSU}(3, 2^3)$ is contained in the normalizer N' of a cyclic Singer group with $|N'| = 57$.

If $G' \leq \mathrm{PSU}(3, 2^3)$, then we argue as in the proof of Proposition 3.10, after replacing G with G'. In this way we get a contradiction.

If $G' \nsubseteq \mathrm{PSU}(3, 2^3)$, then $G'' = G' \cap \mathrm{PSU}(3, 2^3)$ has order $|G'|/3 = 19$. By Sylow theorems, G'' is the only Sylow 19-subgroup of G'; hence, G'' is a cyclic Singer group. Therefore G'' fixes a triangle $\mathcal{T}$ with coordinates in the cubic extension $\mathbb{F}_{2^{18}}$ of $\mathbb{F}_{2^6}$, and $\mathcal{T}$ is self-polar with respect to $\mathcal{H}_{2^9}$. Since G' acts on $\mathcal{T}$, the thesis follows from Proposition 3.8. $\square$

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

Throughout the section, let $q > 3$ be a power of a prime p. We rely on the following bound by Duursma and Mak.

Proposition 4.1. ([8, Thm. 1.3]) *If there exists a Galois-covering $\mathcal{H}_{q^3} \to \mathcal{X}_q$ 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 $\varphi : \mathcal{H}_{q^3} \to \mathcal{X}_q$ of degree $q^2 + q + 2$.*

Proof. If such φ existed, then q^2+q+2 would divide the order $q^9(q^9+1)(q^6-1)$ of $\mathrm{PGU}(3,q^3)$, hence q^2+q+2 would divide $2128q-1568$. But this is impossible for any prime power greater than 3. $\square$

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

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

Proof. If $\mathrm{PSU}(3,q^3) \neq \mathrm{PGU}(3,q^3)$, then $\mathrm{PSU}(3,q^3)$ has index 3 in $\mathrm{PGU}(3,q^3)$ and 3 divides q^3+1; hence, 3 does not divide $|G|$. Suppose $G \not\subseteq \mathrm{PSU}(3,q^3)$; then $\mathrm{PGU}(3,q^3) = G \cdot \mathrm{PSU}(3,q^3)$, and G has a subgroup $G \cap \mathrm{PSU}(3,q^3)$ of index 3, which is impossible. $\square$

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

Proof. Assume by contradiction that such φ exists. Then $\mathcal{X}_q \cong \mathcal{H}_{q^3}/G$, with $G \le \mathrm{PSU}(3,q^3)$ by Lemma 4.3 and Theorem 2.1 can be applied.

Case *i)*. Let $\mathcal{H}_{q^3} : Y^{q^3+1} = X^{q^3} + X$. Up to conjugation, G fixes the ideal point P_∞ of $\mathcal{H}_{q^3}$. By [15, Section 4], the stabilizer S of P_∞ in $\mathrm{PGU}(3,q^3)$ has order $q^9(q^6-1)$. The group S is the semidirect product $Q \rtimes H$, where Q is the unique Sylow p-subgroup of S, and H is a cyclic group 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; moreover, H fixes two $\mathbb{F}_{q^3}$-rational points $P_\infty, O \in \mathcal{H}_{q^3}$ and is semiregular on $\mathcal{H}_{q^3} \setminus \{P_\infty, O\}$. We have $G \subset H$, because Q is normal in S, $|Q|$ and $|H|$ are coprime, and $|G|$ divides $|H|$. In particular, G is generated by $\alpha_b : (X,Y,T) \mapsto (b^{q^3+1}X, bY, T)$, with $b = a^{(q^3+1)(q-1)}$. Let $\bar{G}$ be the group generated by $\alpha_c : (X,Y,T) \mapsto (c^{q^3+1}X, cY, T)$, with $c = a^{q-1}$; then G is normal in $\bar{G}$ of index q^3+1. The group $\bar{G}/G$ fixes two $\mathbb{F}_{q^6}$-rational points of $\mathcal{H}_{q^3}/G$ and acts semiregularly on the other points of $\mathcal{H}_{q^3}/G$. Therefore, the number of $\mathbb{F}_{q^6}$-rational points of $\mathcal{H}_{q^3}/G$ is congruent to 2 modulo q^3+1. On the other hand, the number of $\mathbb{F}_{q^6}$-rational points of $\mathcal{X}_q$ is $q^7-q^5+q^4+1$, which is congruent to q^2+1 modulo q^3+1.

Case *ii)*. Let $\mathcal{H}_{q^3} : X^{q^3+1} + Y^{q^3+1} + 1 = 0$. 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 is a homology of the form $g : (X,Y,T) \mapsto (X,Y,\lambda T)$, whose order divides q^3+1; since $|G|$ and q^3+1 are coprime, g is the identity element. Therefore, as in the proof of Proposition 3.5, G is isomorphic to a subgroup of $\mathrm{PGL}(2,q^6)$; by Theorem 2.2, G is cyclic. Moreover, since $|G|$ divides q^6-1, G has two fixed points $P_1, P_2 \in \ell$ and acts semiregularly on $\ell \setminus \{P_1,P_2\}$; see [24, Chapt. II, Thm. 8.3]. As $|\ell \cap \mathcal{H}_{q^3}|$ is congruent to 2 modulo $|G|$, we have that $P_1, P_2 \in \mathcal{H}_{q^3}$. Now the same argument used in case *i)* yields a contradiction.

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

Case *v)*. The group G acts on the q^6+1 $\mathbb{F}_{q^6}$-rational points of a conic $\mathcal{C}$ defined over $\mathbb{F}_{q^6}$. As in case *ii)*, G is isomorphic to a cyclic subgroup Γ of $\mathrm{PGL}(2,q^6)$ acting on a line ℓ with no short orbits apart from two fixed $\mathbb{F}_{q^6}$-rational points. The action of G on $\mathcal{C}$ is equivalent to the action of Γ on ℓ, see [34, Chapt. VIII, Thm. 15]; hence G has no short orbits on $\mathcal{C}$ apart from two fixed $\mathbb{F}_{q^6}$-rational points P_1, P_2. If G has a fixed $\mathbb{F}_{q^6}$-point on $\mathcal{H}_{q^3}$, then we get a contradiction by arguing as in case *i*). Otherwise, $P_1, P_2 \notin \mathcal{H}_{q^3}$; by [30, Par. 2] and [22, page 141], G fixes a third $\mathbb{F}_{q^6}$-rational point $P_3 \in \mathcal{H}_{q^3}$, and $\mathcal{T} = \{P_1, P_2, P_3\}$ is a self-polar triangle. Let $\mathcal{H}_{q^3} : X^{q^3+1} + Y^{q^3+1} + 1 = 0$; up to conjugation, $\mathcal{T}$ is the fundamental triangle and a generator of G has the form $g : (X, Y, T) \mapsto (\lambda X, \mu Y, T)$. Then the order $|G|$ of g divides $q^3 + 1$, which is impossible.

Cases *viii)* to *xii)*, and case *xv)*. The order of G does not divide the order of these maximal subgroups.

Cases *vi), vii), xiii)*, and *xiv)*. If K is a group containing $\mathrm{PSU}(3, 2^m)$ as a normal subgroup of index 3, then the order of any maximal subgroup of K divides three times the order of a maximal subgroup of $\mathrm{PSU}(3, 2^m)$. Hence, by applying Theorem 2.1 to $\mathrm{PSU}(3, p^m)$, it can be checked that $|G|$ does not divide either the order of any maximal subgroup of $\mathrm{PSU}(3, p^m)$, or the order of any maximal subgroup of K. $\square$

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

Proof. Let $Q_1, \ldots, Q_n$ be the Sylow p-subgroups of G. By [23, Thm. 12.25 (i), (ii)], for each $i = 1, \ldots, n$ there is a unique point $P_i \in \mathcal{H}_{q^3}$ fixed by Q_i, P_i is $\mathbb{F}_{q^6}$-rational, and $P_i \neq P_j$ for $i \neq j$. If $n > 1$, then G has no fixed points; hence, the length of the orbit $\mathcal{O}_{P_1}$ of P_1 under G is at least $q+1$, since Q_1 is semiregular on $\mathcal{H}_{q^3} \setminus \{P_1\}$. On the other hand, the stabilizer of P_1 in G has length at least q, as 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 $i \in \{2, \ldots, n\}$. Then $n = q + 1$. $\square$

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 $\mathcal{H}_{q^3} : Y^{q^3+1} = X^{q^3} + X$. Since Q is normal in G, we have that G fixes the unique fixed point of Q on $\mathcal{H}_{q^3}$, which can be assumed to be the ideal point P_∞. The stabilizer of P_∞ in $\mathrm{PGU}(3, q^3)$ is solvable; hence, by Hall's theorem [21, Theorems 2.1–2.4], we have that, up to conjugation, $G = Q \rtimes \langle \alpha_\lambda \rangle$, where $\alpha_\lambda : (X, Y, T) \mapsto (X, \lambda Y, T)$ and λ is a primitive $(q+1)$-th root of unity. The genus g of $\mathcal{H}_{q^3}/G$ is computed in [15, Thm. 4.4]. In the terminology of [15, Thm. 4.4], $g = g(\mathcal{X}_q)$ implies $q = p^w$, that is, the elements of Q are involutions of the form $\beta_\mu : (X, Y, T) \mapsto (X + \mu T, Y, T)$, with $\mu^{q^3} + \mu = 0$. Then there exists a p-linearized polynomial $L \in \mathbb{F}_{q^6}[X]$ of degree q dividing $X^{q^3} + X$, such that the set of roots of L coincides with $\{\mu \in \mathbb{F}_{q^6} \mid \beta_\mu \in Q\}$. By [27, Thm. 3.62], there is also a p-linearized polynomial $F \in \mathbb{F}_{q^6}[X]$ of degree q^2 dividing $X^{q^3} + X$, such that $F(L(X)) = X^{q^3} + X$. Then it is easy to see that the quotient curve $\mathcal{H}_{q^3}/G$ is $\mathbb{F}_{q^6}$-birationally equivalent to the plane curve $\mathcal{C}$ with equation $V^{q^2-q+1} = F(U)$.

Assume that there exists an $\mathbb{F}_{q^6}$-isomorphism $\psi : \mathcal{C} \to \mathcal{X}_q$. We will show that in this case $F(U)$ cannot be a divisor of $U^{q^3} + U$, which is a contradiction.

By [23, Thm. 12.11], the ideal points $R_\infty \in \mathcal{X}_q$ and $S_\infty \in \mathcal{C}$ are the unique fixed points of the automorphism groups $\mathrm{Aut}(\mathcal{X}_q)$ and $\mathrm{Aut}(\mathcal{C})$, respectively. Hence, $\psi(S_\infty) = R_\infty$. Also, the coordinate functions have pole divisors

$$div(x)_\infty = (q^2 - q + 1)R_\infty,\ div(y)_\infty = q^2 R_\infty,$$
$$div(u)_\infty = (q^2 - q + 1)S_\infty,\ div(v)_\infty = q^2 S_\infty,$$

and the Weierstrass semigroups at the ideal points are $H(R_\infty) = H(S_\infty) = \langle q^2 - q + 1, q^2\rangle$ (see [23, Lemmata 12.1, 12.2]). Then $\{1, u\}$ is a basis of the Riemann–Roch space $\mathcal{L}((q^2 - q + 1)R_\infty)$ and $\{1, u, v\}$ is a basis of $\mathcal{L}(q^2 R_\infty)$. Therefore, there exist constants $a, b, c, d, e \in \mathbb{F}_{q^6}$, $a, d \neq 0$, such that $\psi^*(x) = au + b$ and $\psi^*(y) = cu + dv + e$, where $\psi^* : \mathbb{F}_{q^6}(\mathcal{X}_q) \to \mathbb{F}_{q^6}(\mathcal{C})$ is the pull-back of ψ; equivalently, $\psi : (U, V, T) \mapsto (aU + b, cU + dV + e, T)$.

Then the polynomial identity

$$(aU + b)^{q^2} - (aU + b) - (cU + dV + e)^{q^2-q+1} = k\left(F(U) - V^{q^2-q+1}\right)$$

holds for some non-zero $k \in \overline{\mathbb{F}}_{q^6}$. By comparing the coefficients we get $c = e = 0$, $b \in \mathbb{F}_{q^2}$, and $k = d^{q^2-q+1}$; this implies

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

It is easily checked that the conventional p-associate of the p-linearized polynomial $F(X)$ is not a divisor of the conventional p-associate of $U^{q^3} + U$, hence $F(U)$ is not a divisor of $U^{q^3} + U$ by [27, Thm. 3.62]. □

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

Proof. By the proof of Lemma 4.5, the points $P_1, \ldots, P_{q+1}$, fixed by $Q_1, \ldots, Q_{q+1}$, respectively, form a single orbit $\mathcal{O}$ under the action of G. By Burnside's Lemma [2, Chapt. VIII, Par. 118], G is sharply 2-transitive on $\mathcal{O}$. Then, by [20, Thm. 20.7.1], G is isomorphic to the group of affine transformations of a near-field F; also, G has a regular normal subgroup N, and hence $G = N \rtimes Q_1$. The order f of F satisfies $q(q+1) = (f-1)f$, hence $f = q + 1$. This implies that F cannot be one of the seven exceptional near-fields listed in [35] and then F is a Dickson near-field; see [20, Thm. 20.7.2]. In particular, N is isomorphic to the additive group $(\mathbb{Z}_{p'})^s$ of a finite field. □

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

Proof. Suppose q is odd. Then all involutions of $\mathrm{PGU}(3,q^3)$ are conjugate, and they are homologies of $\mathrm{PG}(2,q^6)$; see [25, Lemma 2.2]. The maximum number of pairwise commuting involutions is 3; in fact, two homologies commute if and only if the center of one homology lies on the axis of the other (see [6, Thm. 3.1.12]). Then $q+1=4$ by Lemma 4.7, contradicting $q>3$.

Suppose q is even, and $\mathcal{X}_q \cong \mathcal{H}_{q^3}/G$. The group Q_1 is isomorphic to the multiplicative group of F, hence Q_1 is metacyclic; see e.g. [3, Ex. 1.19]. Also, Q_1 has exponent 2 or 4 by [25, Lemma 2.1]. Therefore, $q \in \{2,4,8,16\}$. The case $q=2$ is excluded. If $q=16$, then F has prime order 17 and F is a field; hence Q_1 has exponent 16, a contradiction.

For $q \in \{4,8\}$ we apply the Riemann–Hurwitz formula [31, Thm. 3.4.13] to the covering $\mathcal{H}_{q^3} \to \mathcal{X}_q$ to get a contradiction on the degree $\Delta = \big(2g(\mathcal{H}_{q^3})-2\big) - |G|\,(2g(\mathcal{X}_q)-2)$ of the different divisor. By [31, Thm. 3.8.7]

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

where $i(\sigma) \geq 0$ satisfies the following conditions.

- If σ has order 2, then $i(\sigma) = q^3+2$; if σ has order 4, then $i(\sigma)=2$ (see [31, Eq. (2.12)]).
- If σ has odd order, then $i(\sigma)$ equals the number of fixed points of σ on $\mathcal{H}_{q^3}$, see [31, Cor. 3.5.5]; also, by [22, 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 $i(\sigma) = q^3+1$.

If $q=4$, then $\Delta = 470$ 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 of the Q_i's to Δ sum up to $5\cdot 66 + 10\cdot 2 = 350$. The remaining four non-trivial elements of G are generators of $\mathbb{Z}_5$; then either all of them are homologies, or all of them fix 3 points. In both cases, their contribution cannot be equal to $120 = \Delta - 350$.

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 for at least $18\cdot 514 > \Delta$. Hence, Q_1 is the quaternion group, and the sum of Q_i's contributions to Δ is $9\cdot 514 + 54\cdot 2 = 4734$. The contribution to Δ of the elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$ is either 513 or less than 4; hence, it cannot sum up to $3024 = \Delta - 4734$. $\square$

By Lemma 4.5 and Propositions 4.6 and 4.8, the following result follows.

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

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

Acknowledgments

This research was supported by the Italian Ministry MIUR, Strutture Geometriche, Combinatoria e loro Applicazioni, PRIN 2012 prot. 2012XZE22K, and by GNSAGA of the Italian INdAM.

References

[1] M. Abdón, J. Bezerra, L. Quoos, Further examples of maximal curves, J. Pure Appl. Algebra 213 (6) (2009) 1192–1196.
[2] W. Burnside, Theory of Groups of Finite Order, Cambridge University Press, Cambridge, 1897.
[3] P.J. Cameron, Permutation Groups, Cambridge University Press, 1999.
[4] A. Cossidente, G. Korchmáros, F. Torres, On curves covered by the Hermitian curve, J. Algebra 216 (1) (1999) 56–76.
[5] A. Cossidente, G. Korchmáros, F. Torres, Curves of large genus covered by the Hermitian curve, Commun. Algebra 28 (10) (2000) 4707–4728.
[6] P. Dembowski, Finite Geometries, Springer, Berlin, 1968.
[7] L.E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, Teubner, Leipzig, 1902.
[8] I. Duursma, K.-H. Mak, On maximal curves which are not Galois subcovers of the Hermitian curve, Bull. Braz. Math. Soc. (N. S.) 43 (3) (2012) 453–465.
[9] R. Fuhrmann, F. Torres, On Weierstrass points and optimal curves, Rend. Circ. Mat. Palermo Suppl. 51 (1998) 25–46 (Recent Progress in Geometry, Ballico E., Korchmáros G. (Eds.)).
[10] A. Garcia, Curves over finite fields attaining the Hasse–Weil upper bound, in: European Congress of Mathematics, vol. II, Barcellona, 2000, in: Prog. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 199–205.
[11] A. Garcia, On curves with many rational points over finite fields, in: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer, Berlin, 2002, pp. 152–163.
[12] A. Garcia, C. Güneri, H. Stichtenoth, A generalization of the Giulietti–Korchmáros maximal curve, Adv. Geom. 10 (3) (2010) 427–434.
[13] A. Garcia, H. Stichtenoth, Algebraic function fields over finite fields with many rational places, IEEE Trans. Inf. Theory 41 (1995) 1548–1563.
[14] A. Garcia, H. Stichtenoth, A maximal curve which is not a Galois subcover of the Hermitian curve, Bull. Braz. Math. Soc. (N. S.) 37 (1) (2006) 139–152.
[15] A. Garcia, H. Stichtenoth, C.P. Xing, On subfields of the Hermitian function field, Compos. Math. 120 (2000) 137–170.
[16] A. Garcia, F. Torres, On unramified coverings of maximal curves, in: Proceedings of AGCT-10 2005, in: Semin. Congr., vol. 21, 2010, pp. 35–42.
[17] M. Giulietti, G. Korchmáros, A new family of maximal curves over a finite field, Math. Ann. 343 (1) (2009) 229–245.
[18] C. Güneri, M. Özdemir, H. Stichtenoth, The automorphism group of the generalized Giulietti–Korchmáros function field, Adv. Geom. 13 (2) (2013) 369–380.
[19] R. Guralnick, B. Malmskog, R. Pries, The automorphism of a family of maximal curves, J. Algebra 361 (2012) 92–106.
[20] M. Hall, The Theory of Groups, Macmillan, New York, 1959.
[21] P. Hall, A note on soluble groups, J. Lond. Math. Soc. 3 (1928) 98–105.
[22] R.W. Hartley, Determination of the ternary collineation group whose coefficients lie in the $GF(2^n)$, Ann. of Math. Second Series 27 (2) (1925) 140–158.
[23] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Ser. Appl. Math., Princeton, 2008.
[24] B. Huppert, Endliche Gruppen I, Grundlehren Math. Wiss., vol. 134, Springer, Berlin, 1967.
[25] W.N. Kantor, M.E. O'Nan, G.M. Seitz, 2-transitive groups in which the stabilizer of two points is cyclic, J. Algebra 21 (1972) 17–50.
[26] G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C.R. Acad. Sci. Paris 305 (Série I) (1987) 729–732.
[27] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, Cambridge, 1986.

[28] I.D. Macdonald, The Theory of Groups, Oxford University Press, Oxford, 1968.
[29] K.-H. Mak, On congruence function fields with many rational points, PhD Thesis. Available at www.ideals.illinois.edu.
[30] H.H. Mitchell, Determination of the ordinary and modular ternary linear groups, Trans. Am. Math. Soc. 12 (2) (1911) 207–242.
[31] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd edn., Grad. Texts Math., vol. 254, Springer, Berlin, 2009.
[32] G. van der Geer, Curves over finite fields and codes, in: European Congress of Mathematics, vol. II, Barcellona, 2000, in: Prog. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 225–238.
[33] G. van der Geer, Coding theory and algebraic curves over finite fields: a survey and questions, in: Applications of Algebraic Geometry to Coding Theory, Physics and Computation, in: NATO Sci. Ser. II Math. Phys. Chem., vol. 36, Kluwer, Dordrecht, 2001, pp. 139–159.
[34] O. Veblen, J.W. Young, Projective Geometry, The Atheneum Press, Boston, 1910.
[35] H. Zassenhaus, Über endliche Fastkörper, Abh. Math. Semin. Univ. Hamb. 11 (1936) 132–145.