MAXIMAL CURVES FROM SUBCOVERS OF THE GK-CURVE

MASSIMO GIULIETTI, LUCIANE QUOOS, AND GIOVANNI ZINI

ABSTRACT. For every $q = n^3$ with n a prime power greater than 2, the GK-curve is an $\mathbb{F}_{q^2}$-maximal curve that is not $\mathbb{F}_{q^2}$-covered by the Hermitian curve. In this paper some Galois subcovers of the GK curve are investigated. We describe explicit equations for some families of quotients of the GK-curve. New values in the spectrum of genera of $\mathbb{F}_{q^2}$-maximal curves are obtained. Finally, infinitely many further examples of maximal curves that cannot be Galois covered by the Hermitian curve are provided.

1. INTRODUCTION

Let $\mathbb{F}_{q^2}$ be a finite field with q^2 elements, where q is a power of a prime p. By a curve $\mathcal{X}$ over $\mathbb{F}_{q^2}$ we mean a projective, absolutely irreducible, non-singular algebraic curve defined over $\mathbb{F}_{q^2}$, and it 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 the curve. Maximal curves have interesting properties and have also been investigated for their applications in Coding Theory: sometimes the best known linear codes over finite fields of square order are obtained as one-point AG-codes from maximal curves, see e.g. [2, 3, 11].

One of the most important problems about maximal curves is determining the possible genera of maximal curves over $\mathbb{F}_{q^2}$. For a given q, the highest value of g for which an $\mathbb{F}_{q^2}$-maximal curve of genus g exists is $q(q-1)/2$, and equality holds if and only if the curve is isomorphic over $\mathbb{F}_{q^2}$ to the Hermitian curve. By a result of Serre, cited by Lachaud in [10], 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. However, not every maximal curve can be covered by the Hermitian curve. In fact, in 2009 Giulietti and Korchmáros constructed a maximal curve over $\mathbb{F}_{n^6}$ which cannot be covered by the Hermitian curve whenever $n > 2$; this curve is nowadays referred to as the GK-curve.

Serre's covering result has made it possible to obtain several genera of $\mathbb{F}_{q^2}$-maximal curves by applying the Riemann-Hurwitz formula to quotient curves of a known $\mathbb{F}_{q^2}$-maximal curve, such as the Hermitian curve, the Suzuki curve, the Ree curve, and the GK-curve, see [1, 4, 5, 7]. However, sometimes it can be hard to give *explicit equations* for a quotient curve. This problem is clearly relevant for applications to Coding Theory, but has been attacked only recently for the GK-curve. Equations of some quotients of the GK-curve with respect to p-groups of automorphisms have been obtained in [12, 14].

In this paper we deal with Galois subcovers of the GK-curve with respect to coverings of degree not divisible by p. We provide explicit equations for several such subcovers, see Theorem 3.2 and Equation (13), and in some cases we give an explicit description of the Galois group of the covering; see Section 4. Our starting point for computing such equations is a new non-singular model of the GK-curve; see Section 2. The genera of these subcovers are computed, see Theorem 3.3 and Formula (14), and sometimes they are new values in the spectrum of genera of $\mathbb{F}_{n^6}$-maximal curves; see Remark 3.4. Interestingly, it often happens that these curves are not Galois covered by the Hermitian curve; see Theorems 6.2, 6.3, 6.4. In some cases we are able to show they are not covered by the Hermitian curve at all; see Table 1.

2. A NEW MODEL OF THE GK-CURVE

Let p be a prime, n a power of p, $q = n^3$, $\mathbb{K} = \bar{\mathbb{F}}_{q^2}$ the algebraic closure of $\mathbb{F}_{q^2}$. Let $\mathcal{C}$ be the so-called GK curve, which is $\mathbb{F}_{q^2}$-maximal and is defined by the affine equations

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

Let $\rho \in \mathbb{F}_{n^2}$ with $\rho + \rho^n = 1$. Consider the $\mathbb{F}_{n^2}$-projectivity φ associated to the matrix A, where

$$A = \begin{pmatrix} 1 & 0 & 0 & 1-\rho \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & -\rho \end{pmatrix}.$$

Then $\mathcal{X} = \varphi(\mathcal{C})$ has equations

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

We will consider subgroups of the following tame $\mathbb{F}_{q^2}$-automorphism group G of $\mathcal{X}$ of size $(n+1)^2(n^2-n+1)$:

$$(1) \qquad G = \left\{ g_{a,b,\lambda} : (X,Y,Z,T) \mapsto (aX, bY, \lambda Z, T) \mid a^{n+1} = b^{n+1} = 1, \lambda^{n^2-n+1} = ab \right\}.$$

By conjugation, an $\mathbb{F}_{q^2}$-automorphism group $G^A = A^{-1}GA$ of $\mathcal{C}$ is obtained:

$$G^A = \left\{ g^A_{a,b,\lambda} \mid a^{n+1} = b^{n+1} = 1, \lambda^{n^2-n+1} = ab \right\}, \quad \text{where}$$

$$g^A_{a,b,\lambda} = \begin{pmatrix} a\rho + \rho^n & 0 & 0 & a\rho - a\rho^2 - \rho^{n+1} \\ 0 & b & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ a-1 & 0 & 0 & a - a\rho + \rho \end{pmatrix}.$$

According to the notation of [4], we compute the projection $\overline{G^A}$ of G^A over $\mathrm{PGU}(3,n)$ and the intersection G^A_Λ of G^A with

(2) $$\Lambda = \left\{ \alpha_\lambda : (X,Y,Z,T) \mapsto (X,Y,\lambda Z,T) \mid \lambda^{n^2-n+1} = 1 \right\}:$$

$$G^A_\Lambda = \Lambda, \quad \overline{G^A} = \left\{ \bar{g}_{a,b} \mid a^{n+1} = b^{n+1} = 1 \right\}, \quad \text{where}$$

$$\bar{g}_{a,b} = \begin{pmatrix} a\rho + \rho^n & 0 & a\rho - a\rho^2 - \rho^{n+1} \\ 0 & b & 0 \\ a-1 & 0 & a - a\rho + \rho \end{pmatrix}.$$

Note that $\overline{G^A} = \overline{A^{-1}GA} = \bar{A}^{-1}\bar{G}\bar{A}$, where $\bar{A}$ (resp. $\bar{G}$) is obtained by deleting the third row and column in A (resp. in the matrices of G). Note also that the set $\mathcal{X}(\mathbb{F}_{q^2})$ of $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$ has a short orbit $\mathcal{O}$ under the action of $\mathrm{Aut}(\mathcal{X})$, consisting of the set of $\mathbb{F}_{n^2}$-rational points of the cone $Y^{n+1} = X^{n+1} - 1$ in the plane $Z = 0$ (see [4, Section 3]). Hence, $\overline{G^A}$ acts naturally on $\bar{\mathcal{O}} = \mathcal{H}(\mathbb{F}_{n^2})$, where $\mathcal{H}$ is the Hermitian curve with equation $Y^{n+1} = X^{n+1} - 1$.

3. A FAMILY OF GALOIS SUBCOVERS OF $\mathcal{X}$

In this section we provide equations and genera for a family of curves covered by the curve $\mathcal{X}$ depending on three parameters. Let d_1, d_2, d_3 be divisors of $n+1$, and consider the rational functions

$$u = x^{\frac{n+1}{d_1}}, \quad v = y^{\frac{n+1}{d_2}}, \quad w = z^{\frac{n+1}{d_3}}$$

in the function field $\mathbb{K}(x,y,z)$ of $\mathcal{X}$. Then for the subfield $\mathbb{K}(u,v,w)$ we have the relations

(3) $$w^{d_3(n^2-n+1)} = u^{d_1}(u^{d_1} - 1)\left(\frac{u^{d_1(n-1)} - 1}{u^{d_1} - 1}\right)^{n+1}, \quad v^{d_2} = u^{d_1} - 1.$$

Let L be the following subgroup of the group G given in (1):

$$L = \left\{ (X,Y,Z,T) \mapsto (\lambda^3 b^n X, bY, \lambda Z, T) \mid b^{n+1} = \lambda^{n+1} = 1 \right\}.$$

Clearly, L has order $(n+1)^2$, and the fixed field $Fix(L)$ contains x^{n+1}, y^{n+1} and z^{n+1}. Actually, $Fix(L)$ coincides with $\mathbb{K}(x^{n+1}, y^{n+1}, z^{n+1})$, since $\mathbb{K}(x^{n+1}, y^{n+1}, z^{n+1})$ coincides with $\mathbb{K}(x^{n+1}, z^{n+1})$ and the degree of the extension

$$\mathbb{K}(x,y,z)/\mathbb{K}(x^{n+1}, z^{n+1})$$

is at most $(n+1)^2$. Then $Fix(L) \subseteq \mathbb{K}(u,v,w)$ and we can consider the double extension of function fields

$$Fix(L) \subseteq \mathbb{K}(u,v,w) \subseteq \mathbb{K}(x,y,z).$$

As $\mathbb{K}(x,y,z)/Fix(L)$ is a Galois extension, $\mathbb{K}(x,y,z)/\mathbb{K}(u,v,w)$ is Galois as well, that is, $\mathbb{K}(u,v,w)$ is the function field of the quotient curve of $\mathcal{X}/H$ of $\mathcal{X}$ with respect to some automorphism group $H \leq L$.

In order to provide irreducible equations for $\mathcal{X}/H$, consider the rational function $\alpha \in \mathbb{K}(u,v)$ defined as

$$\alpha = u^{d_1}(u^{d_1} - 1) \left(\frac{u^{d_1(n-1)} - 1}{u^{d_1} - 1} \right)^{n+1}.$$

After some computation, we get the principal divisor of α in $\mathbb{K}(u,v)$:

$$(4) \quad \mathrm{div}(\alpha) = d_1 \sum_{i=1}^{d_2} Q_{0,i} + d_2 \sum_{i=1}^{d_1} Q_{\alpha_i} + (n+1) \sum_{i=1}^{d_1(n-2)} \sum_{j=1}^{d_2} Q_{\beta_{i,j}} - \frac{d_1 d_2 n(n-1)}{(d_2, 2d_1)} \sum_{i=1}^{(d_2, 2d_1)} Q_{\infty,i},$$

where $Q_{0,i}$ lies over the zero P_0 of u, Q_{α_i} lies over the zero P_{α_i} of $u^{d_1} - 1$, $Q_{\beta_{i,j}}$ lies over the zero P_{β_i} of $(u^{d_1(n-1)} - 1)/(u^{d_1} - 1)$, and $Q_{\infty,i}$ lies over the pole P_∞ of u. Let

$$D = \gcd\left(d_1, d_2, n+1, \frac{d_1 d_2 n(n-1)}{(d_2, 2d_1)} \right),$$

$$M = \gcd\left(D, d_3(n^2 - n + 1)\right) = \gcd\left(d_1, d_2, d_3(n^2 - n + 1)\right).$$

If $M = 1$, then by equations (3), $\mathbb{K}(u,v,w)/\mathbb{K}(u,v)$ is a Kummer extension of degree $d_3(n^2 - n + 1)$, and the quotient curve has irreducible equations

$$\mathcal{X}/H : \begin{cases} W^{d_3(n^2-n+1)} = U^{d_1} V^{d_2} \left(\frac{U^{d_1(n-1)}-1}{U^{d_1}-1} \right)^{n+1} \\ V^{d_2} = U^{d_1} - 1 \end{cases}.$$

More generally, for $M \geq 1$, both sides of the first equation in (3) are a power of M, and we can factor the equation to obtain the irreducible curve

$$(5) \qquad \mathcal{X}/H : \begin{cases} W^{\frac{d_3}{M}(n^2-n+1)} = U^{\frac{d_1}{M}} V^{\frac{d_2}{M}} \left(\frac{U^{d_1(n-1)}-1}{U^{d_1}-1} \right)^{\frac{n+1}{M}} \\ V^{d_2} = U^{d_1} - 1 \end{cases}.$$

Remark 3.1. *We are in a position to compute the order of the group H, that is, the degree of the extension $[\mathbb{K}(x,y,z) : \mathbb{K}(u,v,w)]$. By the Fundamental Equality (see [13, Th. 3.1.11]), the divisor of zeros of x in $\mathbb{K}(x,y,z)$ has degree $\deg(x)_0 = [\mathbb{K}(x,y,z) : \mathbb{K}(x)] = n^3 + 1$, and*

$$[\mathbb{K}(x,y,z) : \mathbb{K}(u)] = \deg(x^{\frac{n+1}{d_1}})_0 = \frac{(n+1)^2(n^2-n+1)}{d_1}, \quad [\mathbb{K}(u,v) : \mathbb{K}(u)] = d_2;$$

hence,

$$[\mathbb{K}(x,y,z) : \mathbb{K}(u,v)] = \frac{(n+1)^2(n^2-n+1)}{d_1,d_2}, \quad [\mathbb{K}(u,v,w) : \mathbb{K}(u,v)] = \frac{d_3(n^2-n+1)}{M}.$$

Therefore

$$|H| = [\mathbb{K}(x,y,z) : \mathbb{K}(u,v,w)] = \frac{M(n+1)^2}{d_1 d_2 d_3}.$$

The general equations (5) of $\mathcal{X}/H$ have been obtained by working on $d_1, d_2, d_3(n^2 - n+1)/M$. If we start from $d_1/M, d_2, d_3$, or from $d_1, d_2/M, d_3$, then we get irreducible equations for other quotient curves:

$$\begin{cases} W^{d_3(n^2-n+1)} = U^{\frac{d_1}{M}}\left(U^{\frac{d_1}{M}(n-1)} - 1\right)\left(\frac{U^{\frac{d_1}{M}(n-1)}-1}{U^{\frac{d_1}{M}}-1}\right)^n \\ V^{d_2} = U^{\frac{d_1}{M}} - 1 \end{cases},$$

$$\begin{cases} W^{d_3(n^2-n+1)} = U^{d_1}\left(U^{d_1(n-1)} - 1\right)\left(\frac{U^{d_1(n-1)}-1}{U^{d_1}-1}\right)^n \\ V^{\frac{d_2}{M}} = U^{d_1} - 1 \end{cases}.$$

For any divisor e of $n^2 - n + 1$ let $s = w^{\frac{n^2-n+1}{e}}$; then $\mathbb{K}(u,v,s)$ is the function field of new subcovers of $\mathcal{X}$. The degree of the covering can be easily computed also for these subcovers, arguing as in Remark 3.1.

To sum up, the following result is obtained.

Theorem 3.2. *Let d_1, d_2, and d_3 be divisors of $n+1$, and let e be a divisor of $n^2 - n+1$. For*

$$M = \gcd\left(d_1, d_2, d_3(n^2 - n + 1)\right),$$

the following equations define $\mathbb{F}_{n^6}$-maximal curves which are Galois subcovers of $\mathcal{X}$:

(6) $$\mathcal{C}_1 : \begin{cases} S^{\frac{d_3}{M}e} = U^{\frac{d_1}{M}}V^{\frac{d_2}{M}}\left(\frac{U^{d_1(n-1)}-1}{U^{d_1}-1}\right)^{\frac{n+1}{M}} \\ V^{d_2} = U^{d_1} - 1 \end{cases},$$

(7) $$\mathcal{C}_2 : \begin{cases} S^{d_3 e} = U^{\frac{d_1}{M}}\left(U^{\frac{d_1}{M}(n-1)} - 1\right)\left(\frac{U^{\frac{d_1}{M}(n-1)}-1}{U^{\frac{d_1}{M}}-1}\right)^n \\ V^{d_2} = U^{\frac{d_1}{M}} - 1 \end{cases},$$

(8) $$\mathcal{C}_3 : \begin{cases} S^{d_3 e} = U^{d_1}\left(U^{d_1(n-1)} - 1\right)\left(\frac{U^{d_1(n-1)}-1}{U^{d_1}-1}\right)^n \\ V^{\frac{d_2}{M}} = U^{d_1} - 1 \end{cases}.$$

The degree of the covering is $\frac{(n^2-n+1)M(n+1)^2}{e d_1 d_2 d_3}$ for $\mathcal{C}_1$ and $\mathcal{C}_3$, and $\frac{(n^2-n+1)(n+1)^2}{e d_1 d_2 d_3}$ for $\mathcal{C}_2$.

Note that, when $\frac{(n^2-n+1)M(n+1)^2}{ed_1d_2d_3} = 1$ or $\frac{(n^2-n+1)(n+1)^2}{ed_1d_2d_3} = 1$, this theorem provides models for the GK-curve; in some cases they are plane models.

Now we compute the genera of the curves described in Theorem 3.2 for $e = n^2 - n + 1$, i.e. $s = w$. This is done via Kummer theory.

Theorem 3.3. *Let* $e = n^2 - n + 1$. *Then the genera of the curves* $\mathcal{C}_1$, $\mathcal{C}_2$, *and* $\mathcal{C}_3$ *described in Theorem* 3.2 *are the following:*

(9)
$$g(\mathcal{C}_1) = 1 + \frac{1}{2}\Big[d_1 d_2 \frac{d_3(n^2-n+1)}{M}(n-1) - d_2(\frac{d_1}{M}, \frac{d_3(n^2-n+1)}{M}) - d_1(\frac{d_2}{M}, \frac{d_3(n^2-n+1)}{M}) +$$
$$-d_1 d_2(n-2)(\frac{d_3(n^2-n+1)}{M}, \frac{n+1}{M}) - \Big((d_1,d_2)\frac{d_3(n^2-n+1)}{M}, \frac{2d_1d_2}{M} \Big) \Big]$$

and, for $i = 2, 3$,

(10) $g(\mathcal{C}_i) = 1 + \frac{1}{2}\left[hkr(n-1) - k(h,r) - h(k,r) - hk(n-2)(r,n+1) - ((h,k)r, 2hk) \right]$,

where
$$r = d_3(n^2 - n + 1), \quad h = \begin{cases} d_1/M & \text{for } \mathcal{C}_2 \\ d_1 & \text{for } \mathcal{C}_3 \end{cases}, \quad k = \begin{cases} d_2 & \text{for } \mathcal{C}_2 \\ d_2/M & \text{for } \mathcal{C}_3 \end{cases}.$$

Proof. We start with $\mathcal{C}_1$, and use the notation of equation (4) for the zeros and poles of
$$\alpha = u^{\frac{d_1}{M}} v^{\frac{d_2}{M}} \left(\frac{u^{d_1(n-1)} - 1}{u^{d_1} - 1} \right)^{\frac{n+1}{M}} \in \mathbb{K}(u,v).$$

By [13, Prop. 3.7.3] we compute the ramification indices in the Kummer extension $\mathbb{K}(u,v)/\mathbb{K}(u)$ of degree d_2:
$$e(Q_{\alpha_i} \mid P_{\alpha_i}) = d_2, e(Q_{0,i} \mid P_0) = 1, e(Q_{\beta_i,j} \mid P_{\beta_i}) = 1, e(Q_{\infty,i} \mid P_\infty) = \frac{d_2}{\gcd(d_1, d_2)}.$$

The Riemann-Hurwitz formula applied to the extension $\mathbb{K}(u,v)/\mathbb{K}(u)$ yields
$$g(\mathbb{K}(u,v)) = 1 + \frac{1}{2}(d_1 d_2 - d_1 - d_2 - \gcd(d_1, d_2)).$$

Let $\bar{P}_0$ be the zero and $\bar{P}_\infty$ the pole of v in $\mathbb{K}(v)$. Then, in the extension $\mathbb{K}(u,v)/\mathbb{K}(v)$, the places lying over $\bar{P}_0$ are $Q_{\alpha_1}, \ldots, Q_{\alpha_{d_1}}$, with ramification index 1; the places over $\bar{P}_\infty$ are $Q_{\infty,1}, \ldots, Q_{\infty,(d_1,d_2)}$, with ramification index $d_1/\gcd(d_1,d_2)$.

We compute the ramification indices in the Kummer extension $\mathbb{K}(u,v,s)/\mathbb{K}(u,v)$ of degree $\frac{d_3}{M}(n^2 - n + 1)$. We have

$$v_{Q_{\alpha_i}}(\alpha) = e(Q_{\alpha_i} \mid P_{\alpha_i}) \cdot v_{P_{\alpha_i}} \left(u^{\frac{d_1}{M}} \left(\frac{u^{d_1(n-1)} - 1}{u^{d_1} - 1} \right)^{\frac{n+1}{M}} \right) + e(Q_{\alpha_i} \mid \bar{P}_0) \cdot v_{\bar{P}_0} \left(v^{\frac{d_2}{M}} \right) = \frac{d_2}{M},$$

hence
$$e(R_{\alpha_i,j} \mid Q_{\alpha_i}) = \frac{\frac{d_3}{M}(n^2 - n + 1)}{\gcd\left(\frac{d_3}{M}(n^2 - n + 1), \frac{d_2}{M} \right)},$$

where $R_{\alpha_i,j}$ is a place of $\mathbb{K}(u,v,s)$ lying over Q_{α_i}. The theory of Kummer extensions also gives the ramification indices

$$\frac{\frac{d_3}{M}(n^2 - n + 1)}{\gcd\left(\frac{d_3}{M}(n^2 - n + 1), v_Q(\alpha)\right)}$$

of the places of $\mathbb{K}(u,v,s)$ lying over Q, for all places Q of $\mathbb{K}(u,v)$. Then the different divisor of $\mathbb{K}(u,v,s)/\mathbb{K}(u,v)$ has degree

$$\deg(\mathrm{Diff}) = d_1\left(m - \left(m, \frac{d_2}{M}\right)\right) + d_2\left(m - \left(m, \frac{d_1}{M}\right)\right) +$$

$$+d_1(n-2)d_2\left(m - \left(m, \frac{n+1}{M}\right)\right) + (d_1, d_2)\left(m - \left(m, \frac{d_1 d_2(n^2-n)}{M(d_1,d_2)}\right)\right) =$$

$$= d_1\left(m - \left(m, \frac{d_2}{M}\right)\right) + d_2\left(m - \left(m, \frac{d_1}{M}\right)\right) +$$

$$+d_1(n-2)d_2\left(m - \left(m, \frac{n+1}{M}\right)\right) + (d_1, d_2)\left(m - \left(m, \frac{2d_1 d_2}{M(d_1,d_2)}\right)\right),$$

where $m = d_3(n^2 - n + 1)/M$. Finally, the Riemann-Hurwitz formula applied to the extension $\mathbb{K}(u,v,s)/\mathbb{K}(u,v)$ provides the genus of $\mathcal{C}_1$.

The curves $\mathcal{C}_2$ and $\mathcal{C}_3$ are both defined by equations of the form

$$\mathcal{C}_i : \begin{cases} S^r = U^a\left(U^{a(n-1)} - 1\right)\left(\frac{U^{a(n-1)}-1}{U^a-1}\right)^n \\ V^b = U^a - 1 \end{cases}.$$

The genus of $\mathbb{K}(u,v)$ is obtained as above:

$$g(\mathbb{K}(u,v)) = 1 + \frac{1}{2}(ab - a - b - \gcd(a,b)).$$

Similar computations yield the degree of the different divisor of the Kummer extension $\mathbb{K}(u,v,s)/\mathbb{K}(u,v)$:

$$\deg(\mathrm{Diff}) = a\left(r - \gcd\left(r,b\right)\right) + b\left(r - \gcd\left(r,a\right)\right) +$$

$$+a(n-2)b\left(r - \gcd\left(r,n+1\right)\right) + \gcd(a,b)\left(r - \gcd\left(r, \frac{2ab}{\gcd(a,b)}\right)\right),$$

and the Riemann-Hurwitz formula applied to the extension $\mathbb{K}(u,v,s)/\mathbb{K}(u,v)$ provides the genus of $\mathcal{C}_i$, $i = 2, 3$.

$\square$

Remark 3.4. *The previous results provide new equations of $\mathbb{F}_{q^2}$-maximal curves for many genera. To exemplify this, consider the case $n = 5$. Then Theorem 3.2 provides new equations for the following genera:*

$$37, 74, 109, 121, 148, 220, 242, 361, 442, 484, 724, 1450,$$
$$160, 233, 469, 478, 496, 737, 1477, 1486$$

Up to our knowledge, the integers in the second row are new values in the spectrum of genera of $\mathbb{F}_{5^6}$-maximal curves.

4. THE GALOIS GROUPS

In this section we always assume

$$\gcd\left(d_1, d_2, d_3(n^2 - n + 1)\right) = 1.$$

In some cases we are able to give an explicit description of the automorphism groups H of order $\frac{(n+1)^2}{d_1 d_2 d_3}$ such that $Fix(H) = \mathbb{K}(u, v, w)$. We also provide an alternative computation of the genus of $\mathcal{X}/H$, by means of the Riemann-Hurwitz genus formula and [4, Prop. 3.2].

We state Proposition 3.2 from [4] in a slightly different form: in the original paper the authors consider the model $\mathcal{C}$ of the GK curve lying on the cone over the Hermitian curve $\mathcal{K}$ with equation $Y^n + Y = X^{n+1}$; it is not difficult to see that the same computations hold for the curve $\mathcal{X}$ lying on the cone over the Hermitian curve $\mathcal{H} : Y^{n+1} = X^{n+1} - 1$. This relies on the fact that $\mathcal{C}$ and $\mathcal{X}$ are projectively equivalent, with a projectivity defined over $\mathbb{F}_{n^2}$ which maps the Hermitian cone over $\mathcal{K}$ to the Hermitian cone over $\mathcal{H}$.

Proposition 4.1. [4, Prop. 3.2] *Let L be a tame subgroup of $Aut(\mathcal{X})$, $\bar{L}$ the projection of L to $PGU(n, 3)$ and $L_\Lambda = L \cap \Lambda$, where Λ is defined in equation (2). Assume that no non-trivial element in $\bar{L}$ fixes a point in $\mathcal{H} \setminus \mathcal{H}(\mathbb{F}_{n^2})$, where $\mathcal{H}$ is the Hermitian curve $Y^{n+1} = X^{n+1} - 1$. Then:*

$$g_L = g_{\bar{L}} + \frac{(n^3 + 1)(n^2 - |L_\Lambda| - 1) - |L_\Lambda|(n^2 - n - 2)}{2|L|},$$

where g_L is the genus of the quotient curve $\mathcal{H}/\bar{L}$.

Case 4.2. Suppose that $d_1 \mid 3d_3$ with $\gcd(d_1, d_2) = 1$. Then $\mathbb{K}(u, v, w)$ is the quotient curve of $\mathcal{X}$ with respect to the group

$$H = \left\{ (X, Y, Z, T) \mapsto (\lambda^3 b^n X, bY, \lambda Z, T) \mid b^{\frac{n+1}{d_1 d_2}} = \lambda^{\frac{n+1}{d_3}} = 1 \right\}.$$

In fact, by Remark 3.1, the size $\frac{(n+1)^2}{d_1 d_2 d_3}$ of H coincides with the degree of the extension

$$\mathbb{K}(x, y, z)/\mathbb{K}(u, v, w).$$

Also, u, v, and w are all fixed by H since

$$\lambda^{(n+1)/d_3} = 1, \qquad b^{(n+1)/d_2} = (b^{(n+1)/d_2 d_1})^{d_1} = 1,$$

and

$$(\lambda^3 b^n)^{(n+1)/d_1} = (\lambda^{(n+1)/d_3})^{3d_3/d_1} b^{-((n+1)/d_1)} = (b^{-((n+1)/d_1 d_2)})^{d_2} = 1.$$

The projection $\bar{H}$ of H on $PGU(3, n)$ is

$$\bar{H} = \left\{ [\lambda^3 b^n, b, 1] \mid b^{\frac{n+1}{d_2 d_1}} = \lambda^{\frac{n+1}{d_3}} = 1 \right\},$$

$$\text{with} \quad |\bar{H}| = \frac{(n+1)^2}{d_1 d_2 d_3 \gcd\left(3, \frac{n+1}{d_3}\right)},$$

where $[\lambda^3 b^n, b, 1]$ denotes the automorphism $(X, Y, T) \mapsto (\lambda^3 b^n X, bY, T)$. No non-trivial element in $\bar{H}$ fixes a point in $\mathcal{H} \setminus \mathcal{H}(\mathbb{F}_{n^2})$, and

$$H_\Lambda = \left\{ [1, 1, \lambda, 1] \mid \lambda^{n^2 - n + 1} = \lambda^{\frac{n+1}{d_3}} = 1 \right\}$$

has size $\gcd\left(\frac{n+1}{d_3}, 3\right)$. Then by Proposition 4.1 the genus of $\mathcal{X}/H$ is

$$g_H = g_{\bar{H}} + \frac{d_1 d_2 d_3 [(n^3 + 1)(n^2 - \gcd(3, (n+1)/d_3) - 1) - \gcd(3, (n+1)/d_3)(n^2 - n - 2)]}{2(n+1)^2},$$

where $g_{\bar{H}}$ is the genus of $\mathcal{H}/\bar{H}$. The only points of $\mathcal{H}$ that can be fixed by a non-trivial element in $\bar{H}$ are the points on the fundamental frame. It is easily seen that

(i) $[\lambda^3 b^n, b, 1]$ fixes $P_i = (0, \alpha_i, 1)$, $i = 1, \ldots, n+1$, if and only if $b = 1$;
(ii) $[\lambda^3 b^n, b, 1]$ fixes $Q_j = (\beta_j, 0, 1)$, $j = 1, \ldots, n+1$, if and only if $\lambda^3 = b$;
(iii) $[\lambda^3 b^n, b, 1]$ fixes $R_k = (\beta_k, 1, 0)$, $k = 1, \ldots, n+1$, if and only if $\lambda^3 = b^2$.

Let $\bar{H}_P$ denote the stabilizer of P in $\bar{H}$. We distinguish two cases.

(**A**) 3 does not divide $(n+1)/d_3$. Then $\lambda \mapsto \lambda^3$ is an automorphism of the multiplicative group of the $((n+1)/d_3)$-th roots of unity.

(i) We have

$$\bar{H}_{P_i} = \left\{ [\lambda^3, 1, 1] \mid \lambda^{\frac{n+1}{d_3}} = 1 \right\}, \quad \text{hence} \quad |\bar{H}_{P_i}| = \frac{n+1}{d_3}.$$

(ii) We have

$$\bar{H}_{Q_j} = \left\{ [1, b, 1] \mid b^{\frac{n+1}{d_2 d_1}} = 1, b = \lambda^3 \text{ for some } \lambda \text{ with } \lambda^{\frac{n+1}{d_3}} = 1 \right\},$$

hence

$$|\bar{H}_{Q_j}| = \gcd\left(\frac{n+1}{d_3}, \frac{n+1}{d_1 d_2} \right).$$

(iii) We distinguish two subcases.

$-$ $\frac{n+1}{d_1 d_2}$ is even. Then

$$\bar{H}_{R_k} = \left\{ [b, b, 1] \mid (b^2)^{\frac{n+1}{d_3}} = 1, (b^2)^{\frac{n+1}{2d_1 d_2}} = 1 \right\} \quad \text{and} \quad b \neq -b,$$

hence

$$|\bar{H}_{R_k}| = 2 \gcd\left(\frac{n+1}{d_3}, \frac{n+1}{2d_1 d_2} \right) = \gcd\left(\frac{2(n+1)}{d_3}, \frac{n+1}{d_1 d_2} \right).$$

$-$ $\frac{n+1}{d_1 d_2}$ is odd. Then $b \mapsto b^2$ is an automorphism of the multiplicative group of the $((n+1)/d_1 d_2)$-th roots of unity, and

$$\bar{H}_{R_k} = \left\{ [b, b, 1] \mid \lambda^{\frac{n+1}{d_3}} = b^{\frac{n+1}{d_1 d_2}} = 1, \lambda^3 = b^2 \right\};$$

hence,

$$|\bar{H}_{R_k}| = \gcd\left(\frac{n+1}{d_3}, \frac{n+1}{d_1 d_2}\right) = \gcd\left(\frac{2(n+1)}{d_3}, \frac{n+1}{d_1 d_2}\right).$$

Therefore, if $3 \nmid (n+1)/d_3$ then the Hurwitz formula applied to the covering $\mathcal{H} \to \mathcal{H}/\bar{H}$ provides the genus of $\mathcal{H}/\bar{H}$:

$$g_{\bar{H}} = 1 + \frac{1}{2\frac{(n+1)^2}{d_1 d_2 d_3}}\left[n^2 - n - 2 - (n+1)\left(\frac{n+1}{d_3} + \gcd(\frac{n+1}{d_1 d_2}, \frac{n+1}{d_3}) + \gcd(\frac{n+1}{d_1 d_2}, \frac{2(n+1)}{d_3}) - 3\right)\right],$$

that is,

$$g_{\bar{H}} = 1 + \frac{d_1 d_2 d_3}{2(n+1)}\left[n - 2 - \frac{n+1}{d_3} - \gcd(\frac{n+1}{d_1 d_2}, \frac{n+1}{d_3}) - \gcd(\frac{n+1}{d_1 d_2}, \frac{2(n+1)}{d_3}) + 3\right],$$

hence

$$g_H = 1 + \frac{d_1 d_2 d_3}{2(n+1)}\left(n + 1 - \frac{n+1}{d_3} - \gcd(\frac{n+1}{d_1 d_2}, \frac{n+1}{d_3}) - \gcd(\frac{n+1}{d_1 d_2}, \frac{2(n+1)}{d_3})\right) +$$

$$(11) \qquad\qquad + \frac{d_1 d_2 d_3 \left(n^3 - 2n^2 + n\right)}{2}.$$

(**B**) 3 divides $(n+1)/d_3$. Let $\lambda' = \lambda^3$, then

$$\bar{H} = \left\{[\lambda' b^n, b, 1] \mid (\lambda')^{\frac{n+1}{3d_3}} = b^{\frac{n+1}{d_1 d_2}} = 1\right\}.$$

The same arguments yield

$$g_H = 1 + \frac{3d_1 d_2 d_3}{2(n+1)}\left(n + 1 - \frac{n+1}{3d_3} - \gcd(\frac{n+1}{d_1 d_2}, \frac{n+1}{3d_3}) - \gcd(\frac{n+1}{d_1 d_2}, \frac{2(n+1)}{3d_3})\right) +$$

$$+ \frac{d_1 d_2 d_3 \left(n^3 - 2n^2 - n + 2\right)}{2}.$$

Case 4.3. Suppose $d_1 \mid d_2$, and $(d_1, d_3(n^2 - n + 1)) = 1$. Then $\mathbb{K}(u, v, w)$ is the quotient curve of $\mathcal{X}$ with respect to the group

$$H = \left\{(X, Y, Z, T) \mapsto (\lambda^3 b^n X, bY, \lambda Z, T) \mid b^{\frac{n+1}{d_2}} = \lambda^{\frac{n+1}{d_1 d_3}} = 1\right\}.$$

This follows from

$$\lambda^{(n+1)/d_3} = (\lambda^{(n+1)/d_1 d_3})^{d_1} = 1, \qquad b^{(n+1)/d_2} = 1,$$

and

$$(\lambda^3 b^n)^{(n+1)/d_1} = (\lambda^{\frac{n+1}{d_1 d_3}})^{3d_3} b^{-((n+1)/d_1)} = (b^{-((n+1)/d_2)})^{d_2/d_1} = 1.$$

Similar computations provide the genus of $\mathcal{X}/H$:

$$g_H = 1 + \frac{d_1 d_2 d_3 m}{2(n+1)}\left(n + 1 - \frac{n+1}{d_1 d_3 m} - \gcd(\frac{n+1}{d_2}, \frac{n+1}{d_1 d_3 m}) - \gcd(\frac{n+1}{d_2}, \frac{2(n+1)}{d_1 d_3 m})\right) +$$

$$+\frac{d_1 d_2 d_3 \left[n^3 - 2n^2 + (2 - m)n + m - 1\right]}{2},$$

where $m = \gcd(3, (n + 1)/(d_1 d_3))$.

5. ANOTHER FAMILY OF GALOIS SUBCOVERS OF $\mathcal{X}$

In this section we consider another subgroup of the group G given in (1). Let $c \mid (n+1)$, $d \mid (n^2 - n + 1)$, and consider the following automorphism group K of $\mathcal{X}$ of size $(n^3 + 1)/(cd)$:

$$K = \left\{ (X, Y, Z, T) \mapsto (b^{-1}X, bY, \lambda Z, T) \mid b^{\frac{n+1}{c}} = 1, \lambda^{\frac{n^2 - n + 1}{d}} = 1 \right\}.$$

Consider the following rational functions

$$u = x^{\frac{n+1}{c}}, \quad v = xy, \quad w = z^{\frac{n^2 - n + 1}{d}}$$

in the function field $\mathbb{K}(x, y, z)$ of $\mathcal{X}$; then the following relations hold:

(12) $$w^d = v \left(1 + u^c + u^{2c} + \ldots + u^{(n-2)c}\right), \quad v^{n+1} = u^{2c} - u^c.$$

In the double field extension $\mathbb{K}(u, v, w) \subseteq Fix(K) \subseteq \mathbb{K}(x, y, z)$ we have

$$[\mathbb{K}(x, y, z) : \mathbb{K}(u, v, w)] \le \frac{n^3 + 1}{cd} = [\mathbb{K}(x, y, z) : Fix(K)],$$

which implies $Fix(K) = \mathbb{K}(u, v, w)$.

Equations (12) define an irreducible curve. To show this, let $P = (0, a)$ be an affine point of the Hermitian plane curve $\mathcal{H} : Y^{n+1} = X^{n+1} - 1$, and let $\bar{P}$ be a place of the curve $\mathcal{W} : V^{n+1} = U^{2c} - U^c$ centered at the image $\varphi(P)$ of P under the rational map

$$\varphi : \mathcal{H} \to \mathcal{W}, \quad \varphi(X, Y, T) = (X^{\frac{n+1}{c}}, XY, T).$$

The rational function $\beta = xy(1 + x^{n+1} + x^{2(n+1)} \ldots + x^{(n-2)(n+1)}) \in \mathbb{K}(x, y)$ has valuation $v_P(\beta) = 1$ at P, hence the pull-back $\alpha = v(1 + u^c + \ldots + u^{(n-2)c}) \in \mathbb{K}(u, v)$ of β has valuation $v_{\bar{P}}(\alpha) = 1$ at $\bar{P}$, since $v_P(\beta) = e(P \mid \bar{P}) \cdot v_{\bar{P}}(\alpha)$. Hence the quotient curve $\mathcal{X}/K$ has irreducible equations

(13) $$\mathcal{X}/K : \begin{cases} W^d = V \left(1 + U^c + U^{2c} + \ldots + U^{(n-2)c}\right) \\ V^{n+1} = U^{2c} - U^c \end{cases}.$$

By the Hurwitz formula applied to the tame covering $\mathcal{X} \to \mathcal{X}/K$, it is easy to check that the genus of $\mathcal{X}/K$ is

(14) $$g(\mathcal{X}/K) = \frac{c}{2}\left[(d - 1)n^2 + n - d - \gcd\left(2, \frac{n+1}{c}\right)\right] + 1.$$

6. New examples of maximal curves not (Galois) covered by the Hermitian curve

Let a curve $\mathcal{Y}$ be a subcover of the Hermitian curve $\mathcal{H}$ by the $\mathbb{F}_{q^2}$-rational map

$$\varphi : \mathcal{H} \to \mathcal{Y}.$$

Then for the degree $\deg(\varphi)$ we have the following bounds:

$$\frac{\mathcal{H}(\mathbb{F}_{q^2})}{\mathcal{Y}(\mathbb{F}_{q^2})} \leq \deg(\varphi) \leq \frac{2g(\mathcal{H}) - 2}{2g(\mathcal{Y}) - 2}.$$

In particular, the lower bound $L_{\mathcal{H},\mathcal{Y}} = \mathcal{H}(\mathbb{F}_{q^2})/\mathcal{Y}(\mathbb{F}_{q^2})$ and the upper bound $U_{\mathcal{H},\mathcal{Y}} = (2g(\mathcal{H}) - 2)/(2g(\mathcal{Y}) - 2)$ satisfy $\lceil L_{\mathcal{H},\mathcal{Y}} \rceil \leq \lfloor U_{\mathcal{H},\mathcal{Y}} \rfloor$.

Therefore, a curve $\mathcal{Y}$ having $\lceil L_{\mathcal{H},\mathcal{Y}} \rceil > \lfloor U_{\mathcal{H},\mathcal{Y}} \rfloor$ cannot be a subcover of the Hermitian curve. By applying this argument to the curves given in Theorems 3.2 and 3.3, we get many new examples of curves which are not covered by the Hermitian curve.

To exemplify this, we list in the table below some genera of curves not covered by the Hermitian curve. We remark that for such curves we have both the genus and explicit equations.

TABLE 1. New maximal curves not covered by the Hermitian curve

g	n	(d_1, d_2, d_3)	Reference
233416	17	(1,18,6), (2,9,6), (2,18,3), (2,18,6), (3,18,6), (6,9,6), (6,18,3), (6,18,6), (9,2,6), (9,6,6), (9,18,2), (9,18,6), (18,1,6), (18,2,3), (18,2,6), (18,3,6), (18,6,3), (18,6,6), (18,9,2), (18,9,6)	Thm. 3.3 (9),(10)
233398	17	(9,18,2)	Thm. 3.3 (10)
1064701	23	(1,24,8), (8,3,8), (24,8,1), (24,1,8), (2,24,8), (3,8,8), (3,24,8), (4,24,8), (6,8,8), (6,24,8), (8,3,8), (8,6,8), (8,12,8), (8,24,1), (8,24,2)	Thm. 3.3 (9),(10)
1064689	23	(2,24,8), (4,24,8), (6,8,8), (6,24,8), (8,6,8), (8,12,8)	Thm. 3.3 (10)
3206257	23	(2,24,24), (4,24,24), (6,24,24), (8,6,24), (8,12,24)	Thm. 3.3 (10)
3402406	29	(30,10,1), (10,30,1), (10,15,2), (30,2,5), (10,6,5), (10,3,10)	Thm 3.3 (9)
5570731	32	(33,11,1), (11,33,1), (11,3,11)	Thm 3.3 (9)

Remark 6.1. *Let $\mathcal{H}$ be the Hermitian curve over $\mathbb{F}_{q^2}$, and $\mathcal{Y}$ an $\mathbb{F}_{q^2}$-maximal curve of genus g which is $\mathbb{F}_{q^2}$-covered by $\mathcal{H}$. If $g > f(q)$, where*

$$f(q) = \frac{\sqrt{q^5 + 2q^4 + q^3 + q^2 + 2q + 1} - q^2 - 1}{2q},$$

then the degree of the covering $\mathcal{H} \to \mathcal{Y}$ is uniquely determined as the unique integer d such that

$$L_{\mathcal{H},\mathcal{Y}} \leq d \leq U_{\mathcal{H},\mathcal{Y}}.$$

Proof. By direct computation, $g > f(q)$ is equivalent to $U_{\mathcal{H},\mathcal{Y}} - L_{\mathcal{H},\mathcal{Y}} < 1$, which implies $\lceil L_{\mathcal{H},\mathcal{Y}} \rceil = \lfloor U_{\mathcal{H},\mathcal{Y}} \rfloor$. $\qquad\square$

Theorem 6.2. *Let $n \geq 7$ be a power of a prime p, and k a divisor of $n+1$ with $k < \sqrt{n+1}+1$. Define $d_1 = (n+1)/k$, $d_2 = 1$, and $d_3 = n+1$. Then the curve $\mathcal{C}_1$ given in Theorem 3.2 is not Galois covered by the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{n^6}$.*

Proof. Let $\mathcal{H}$ be given in the form

$$\mathcal{H} : Y^{n^3+1} = X^{n^3+1} + X,$$

and denote by P_∞ the point at infinity of $\mathcal{H}$. Suppose $\mathcal{C}_1$ is Galois covered by $\mathcal{H}$; then $\mathcal{C}_1$ is isomorphic to the quotient curve $\mathcal{H}/N$ for some subgroup N of $\mathrm{Aut}(\mathcal{H})$.

The genus of $\mathcal{C}_1$ can be computed by equation (11), whence $L_{\mathcal{H},\mathcal{C}_1} > kn - 1$ if and only if

$$n^8 - k(k-2)n^7 - 2n^6 + n^5 - (k-1)[2k+1-(k,2)]n^4 + [2k-1-(k,2)]n^3 - k^2 n + 2k > 0,$$

while $U_{\mathcal{H},\mathcal{C}_1} < kn + 1$ if and only if

$$n^5 - 2kn^4 + 2(k-1)n^3 - [k(k,2)-k-1]n^2 - [(k,2)(k+1)+k-1]n + 2k - (k,2) - 1 > 0.$$

For $n \geq 7$, both conditions are implied by the hypothesis $k < \sqrt{n+1}+1$. Then $|N| = kn$.

Let S be a Sylow p-subgroup of N. S has a fixed $\mathbb{F}_{n^6}$-rational point $P \in \mathcal{H}$, since S acts on $\mathcal{H}(\mathbb{F}_{n^6})$ and $|\mathcal{H}(\mathbb{F}_{n^6})| \equiv 1 \pmod{p}$; as all Sylow p-subgroups of $\mathrm{Aut}(\mathcal{H})$ are conjugate, then we assume w.l.o.g. that S fixes P_∞. Moreover, the action of S on $\mathcal{H}(\mathbb{F}_{n^6}) \setminus \{P_\infty\}$ is semiregular, i.e. each element of S has no fixed point but P_∞; hence the orbit $\mathcal{O}$ of P_∞ under N satisfies $|\mathcal{O}| \equiv 1 \pmod{n}$.

Suppose P_∞ is not fixed by N, then $|\mathcal{O}| \geq n+1$. Hence, by the orbit-stabilizer theorem, n divides the cardinality of the stabilizer N_Q of Q in N, for all $Q \in \mathcal{O}$; then a Sylow p-subgroup M_Q of N_Q has size n. M_Q and M_R have trivial intersection for $Q \neq R$ in $\mathcal{O}$, by the semiregularity of S. Therefore N has at least $1 + (n+1)(n-1) = n^2$ elements, and $k \geq n$, against the hypothesis.

Therefore the whole N fixes P_∞. If $k = 1$, then $\mathcal{C}_1 \cong \mathcal{X}$, the GK curve, and the thesis holds; otherwise, the genus of $\mathcal{H}/N$ can be computed by [5, Th. 4.4]:

$$g(\mathcal{H}/N) = \frac{n^3 - p^w}{2kn}\left(n^3 - (k-1)p^v\right) = \frac{p^{5u} - p^{3u-v} - (k-1)p^{3u-w} + k - 1}{2k},$$

where $n = p^u$ and v, w are non-negative integers satisfying $u = v + w$.

On the other hand, the genus of $\mathcal{C}_1$ given in equation (11) is

$$g(\mathcal{C}_1) = \frac{n^5 - 2n^3 + n^2 + 2k - 1 - h}{2k}, \quad \text{where} \quad h = \begin{cases} n+2 & \text{if } k \text{ is even} \\ 1 & \text{if } k \text{ is odd} \end{cases}.$$

Hence $g(\mathcal{H}/N) = g(\mathcal{C}_1)$ reads

$$k = \frac{2p^{3u} + p^{3u-w} - p^{3u-v} - p^{2u} + h}{p^{3u-w} + 1}.$$

We have the following possibilities for v and w: either $v = 0$ and $w = u$, or $v \leq u/2$ and $w \geq u/2$, or $v > u/2$ and $w < u/2$. By considering separately each case, it is easily shown after some computation that

$$\left(p^{3u-w} + 1\right) \nmid \left(2p^{3u} + p^{3u-w} - p^{3u-v} - p^{2u} + h\right),$$

against the fact that k is integer. $\qquad\square$

Theorem 6.3. *Let $n > 3$ be a prime power, k a divisor of $n+1$ such that $3 \nmid (n+1)/k$ and $k < \sqrt{n+1}+1$; if $3 \mid (n+1)$, assume also $n \geq 23$. Define $d_1 = (n+1)/k$, $d_2 = n+1$, and $d_3 = 1$. Then the curve $\mathcal{C}_1$ given in Theorem 3.2 is not Galois covered by the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{n^6}$.*

Proof. By the choise of d_1, d_2, and d_3, the genus of the curve $\mathcal{C}_1$ can be computed as in Case 4.3.

By separating the cases $3 \mid (n + 1)$ and $3 \nmid (n + 1)$ and arguing as in the proof of Theorem 6.2, it is proved that a possible Galois covering has degree kn.

Suppose such a covering exists and $\mathcal{C}_1 \cong \mathcal{H}/N$ with $N \leq \mathrm{Aut}(\mathcal{H})$, then the same argument as in Theorem 6.2 allows to apply [5, Th. 4.4] and yields the following expression for k:

$$k = \frac{(1 + \gcd(3, k))\, p^{3u} + p^{3u-w} - p^{3u-v} - p^{2u} - \gcd(3, k)p^u}{p^{3u-w} - p^u - 2},$$

where $n = p^u$ with p prime, and v, w are non-negative integers satisfying $u = v + w$. But a case analysis shows that this fraction cannot be an integer. $\qquad\square$

Theorem 6.4. *Let n be a prime power, γ a divisor of $n + 1$, δ a divisor of $n^2 - n + 1$, and define $c = (n + 1)/\gamma$, $d = (n^2 - n + 1)/\delta$. Suppose that one of the following holds:*

- *$n = 5$, $\gamma = 2$, and $\delta = 1$;*
- *$n \geq 7$, $\gamma \leq 2$, and $\delta \leq (\sqrt{2\gamma n + 1} - 1)/2$;*
- *$n \geq 7$, $\gamma > 2$, and $\gamma\delta(\gamma\delta - \delta - 1) < n$.*

Then the curve $\mathcal{X}/K$ with equations (13) is not Galois covered by the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{n^6}$.

Proof. By arguing as in the proof of Theorem 6.2, it is proved that a possible Galois covering has degree $\gamma\delta n$.

Suppose such a covering exists and $\mathcal{X}/K \cong \mathcal{H}/N$ with $N \leq \mathrm{Aut}(\mathcal{H})$, then the same argument as in Theorem 6.2 allows to apply [5, Th. 4.4] and yields the following identity:

$$(15) \quad \delta\left[p^{3u} - \gamma p^{3u-w} + (\gcd(2, \gamma) - 1)\, p^u - \gamma + \gcd(2, \gamma)\right] = -p^{3u} + p^{3u-v} - p^{3u-w} + p^{2u},$$

where $n = p^u$ with p prime, and v, w are non-negative integers with $u = v + w$. By case analysis, it can be shown that (15) contradicts the hypothesis on the integers γ and δ. $\quad\square$

References

[1] Abdón, M., Quoos, L.: On the genera of subfields of the Hermitian function field. Finite Fields and Their Applications, **10**, 271–284 (2004).

[2] Fanali, S.: On Linear Codes from Maximal Curves. Lecture Notes in Computer Science **5921**, 91–111 (2009).

[3] Fanali, S., Giulietti, M.: One-point AG codes on the GK maximal curves. IEEE Trans. Inform. Theory **56**(1), 202–210 (2010).

[4] Fanali, S., Giulietti, M.: Quotient curves of the GK curve. Adv. Geom. **12**, 239–268 (2012).

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

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

[7] Giulietti, M., Torres, F., Korchmaros, G.: Quotient curves of the Suzuki curve. Acta Arithmetica, Polonia, **122**, n.3, 245–274 (2006).

[8] Hirschfeld, J.W.P., Korchmáros G., Torres F.: Algebraic curves over a finite field. Princeton Univ. Press (2008).

[9] Korchmáros, G., Torres, F.: Embedding of a Maximal Curve in a Hermitian Variety. Compositio Math. **128**, 95–113 (2001).

[10] Lachaud, G.: Sommes dEisenstein et nombre de points de certaines courbes algbriques sur les corps finis, C.R. Acad. Sci. Paris 305, 729-732 (1987).

[11] MinT: Tables of optimal parameters for linear codes. Univ. Salzburg, Salzburg, Austria. Online (2009). Available: http://mint.sbg.ac.at.

[12] Speziali, P.: Quotient curves in positive characteristic. Master Thesis, Department of Mathematics and Computer Science, University of Perugia (Italy), 2014.

[13] Stichtenoth, H.: Algebraic function fields and codes, Volume 254 of Graduate Texts in Mathematics, 2nd edn. Springer, Berlin (2009).

[14] Tafazolian, S., Teheran-Herrera, A., and Torres, F,: Further examples of maximal curves which cannot be covered by the Hermitian curve. Preprint. http://www.ime.unicamp.br/~ftorres/RESEARCH. Accessed 7 dec 2014.

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

(L. Quoos) Instituto de Matemática, Universidade Federal do Rio de Janeiro, Cidade Universitária, Rio de Janeiro, RJ 21941-909, Brazil
E-mail address: luciane@im.ufrj.br

(G. Zini) Dipartimento di Matematica e Informatica "Ulisse Dini", Università degli Studi di Firenze, Viale Morgagni, 67/a, 50134 Firenze - Italy
E-mail address: gzini@math.unifi.it