FURTHER EXAMPLES OF MAXIMAL CURVES WHICH CANNOT BE COVERED BY THE HERMITIAN CURVE

SAEED TAFAZOLIAN, ARNOLDO TEHERÁN-HERRERA, AND FERNANDO TORRES

ABSTRACT. We construct examples of curves defined over the finite field $\mathbb{F}_{q^6}$ which are covered by the GK-curve. Thus such curves are maximal over $\mathbb{F}_{q^6}$ although they cannot be covered by the Hermitian curve for $q > 2$. We also give examples of maximal curves that cannot be Galois covered by the Hermitian curve over the finite field $\mathbb{F}_{q^{2n}}$ with $n > 3$ odd and $q > 2$. We point out some applications to codes related to an array coming from telescopic semigroups.

1. INTRODUCTION

Let $\mathcal{C}$ be a projective, nonsingular, geometrically irreducible, algebraic curve defined over the finite field $\mathbb{F}_\ell$ of order ℓ. A very basic topic in the study of $\mathcal{C}$ is concerning the size of the set $\mathcal{C}(\mathbb{F}_\ell)$ of its $\mathbb{F}_\ell$-rational points. The fundamental result here is the so-called Hasse-Weil bound, namely

$$|\#\mathcal{C}(\mathbb{F}_\ell) - (\ell + 1)| \leq 2g\sqrt{\ell}\,,$$

where g is the genus of $\mathcal{C}$; see, e.g., [21, Thm. 5.2.3], [13, Thm. 9.18]. The curve $\mathcal{C}$ is called *maximal over* $\mathbb{F}_\ell$, with $\ell = q^2$, if the upper bound above is attained; that is, whenever

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq\,.$$

Not all the curves over $\mathbb{F}_{q^2}$ can be maximal. As a matter of fact, a necessary condition is a result pointed out by Ihara [21, Prop. 5.3.3]: The genus g of a maximal curve over $\mathbb{F}_{q^2}$ does satisfy the inequality

$$g \leq q(q-1)/2\,.$$

The Hermitian curve $\mathcal{H}_1$ over $\mathbb{F}_{q^2}$ which can be defined by the affine equation

$$v^{q+1} = u^q + u\,,$$

is up to $\mathbb{F}_{q^2}$-isomorphism the unique maximal curve over $\mathbb{F}_{q^2}$ of genus $q(q-1)/2$ [20]. Further examples of maximal curves over $\mathbb{F}_{q^2}$ can be obtained via an important remark which is commonly presented as Serre's covering result: Any curve (nontrivially) $\mathbb{F}_{q^2}$-covered by a maximal curve over $\mathbb{F}_{q^2}$ is also maximal over $\mathbb{F}_{q^2}$; cf. [22], [18], [16, Prop. 2.3]. As a matter of fact, one can obtain a huge number of explicit examples of maximal

2010 MSC: 11G20, 11M38, 14G15, 14H25.
Key words: finite field, maximal curve, Hermitian curve, GK-curve, generalized GK-curve.

curves by taking advantage of the fact that the $\mathbb{F}_{q^2}$-automorphism group of the Hermitian curve is also huge; see, e.g., [8], [1], [10]. However, the converse of the aforementioned Serre's remark is not true: In 2008, Giulietti and Korchmáros [9] constructed a maximal curve over $\mathbb{F}_{q^6}$ which cannot be covered by the Hermitian curve whenever $q > 2$; such a curve is nowadays referred as the *GK-curve* (see Section 2).

In this paper we present two further examples of maximal curves which cannot be covered by the Hermitian curve, see Theorems 3.4 and 4.4 below. In fact, such examples are closely related to the GK-curve as they arise as subcovers of this curve; moreover, they might be considered as concrete models of the quotient curves computed by Fanali and Giulietti in [4, Thm. 4.5(iv)(v)] (see Remark 4.6 here). We also exhibit examples of maximal curves that cannot be Galois covered by the Hermitian curve over an appropriate finite field (see Theorem 3.5 below); these examples are subcovers of maximal curves proposed by Güneri, Garcia and Stichtenoth [6] and their genera coincide with previous results of Güneri, Özdemir and Stichtenoth [11, Remark 3.14]. Finally in Section 5 we point out some applications to coding theory via one-point AG codes arising from a telescopic Weierstrass semigroup (cf. Proposition 5.1); we mainly use Kirfel and Pellikaan approach [17].

Conventions. Throughout this paper, unless otherwise stated, by a curve we shall mean a projective, nonsingular, geometrically irreducible algebraic curve defined over a finite field. By $\mathbb{P}^r$ we denote the r-dimensional projective space over the algebraic closure of the respective base field.

Remark. While working out the details of this paper we had learned that Bartoli and Speziali [2] also constructed quotient curves of the GK-curve toward the determination of further examples of maximal curves which are not dominated by the Hermitian curve. Our method is slightly more elementary than theirs and in fact, our results are subsumed by theirs.

2. On the GK-curve and the GGS-curve

Let q be a prime power. The *GK-curve*, introduced by Giulietti and Korchmáros in [9], is the curve $\mathcal{C}_3 \subseteq \mathbb{P}^3$ defined over $\mathbb{F}_{q^6}$ by the (affine) equations

$$v^{q+1} = u^q + u \quad \text{and} \quad w^{\frac{q^3+1}{q+1}} = vh(u)\,,$$

where $h(u) = (u^q + u)^{q-1} - 1$. This curve is maximal over $\mathbb{F}_{q^6}$ and it is so far the only known example of a maximal curve which cannot be dominated by the Hermitian curve.

It turns out that $\mathcal{C}_3$ can also be defined by the equations [6]

$$v^{q+1} = u^q + u \quad \text{and} \quad w^{\frac{q^3+1}{q+1}} = v^{q^2} - v\,.$$

As a matter of fact, $\mathcal{C}_3$ is a member of a family $\mathcal{C}_n$ of maximal curves over $\mathbb{F}_{q^{2n}}$, $n \geq 3$ odd, introduced by Garcia, Güneri and Stichtenoth [6] being $\mathcal{C}_n$ the nonsingular model over $\mathbb{F}_{q^{2n}}$ of the (possible singular) space curve defined by the (affine) equations

$$v^{q+1} = u^q + u \quad \text{and} \quad w^{\frac{q^n+1}{q+1}} = v^{q^2} - v\,.$$

The curve $\mathcal{C}_n$ will be refer as the *GGS-curve* (or the *generalized GK-curve*). Its genus g_n is given by [6, Prop. 2.2]

$$g_n = \frac{(q-1)(q^{n+1}+q^n-q^2)}{2} = \frac{q^{n+2}-q^n-q^3+q^2}{2}\,.$$

We point out that Duursma and Mak [3] noticed that $\mathcal{C}_n$ cannot be Galois covered by the Hermitian curve over $\mathbb{F}_{q^{2n}}$ whenever $n > 3$ and $q > 2$; in this case, it is an open problem to decide whether the GGS-curve is non-Galois covered by the Hermitan curve or not.[1]

3. The curve $\mathcal{X}_{a,b,n,s}$

Let $a, b, s \geq 1$, $n \geq 3$ be integers, let $q = p^a$ be a power of a prime number p. Throughout we also assume that

- n is odd;
- b is a divisor of a;
- s is a divisor of $\frac{q^n+1}{q+1}$.

Let us consider the morphism

$$\varphi_{a,b,n,s} : \mathcal{C}_n \to \mathbb{P}^3, \quad (u,v,w,1) \mapsto (x,y,z,1) := (cu - (cu)^{p^b}, v, w^s, 1)\,,$$

where $\mathcal{C}_n$ is the GGS-curve (Section 2) and we fix $c \in \mathbb{F}_{q^2}$ with $c^{q-1} = -1$.

Definition 3.1. The curve $\mathcal{X}_{a,b,n,s}$ is the nonsingular model over $\mathbb{F}_{q^{2n}}$ of $\varphi_{a,b,n,s}(\mathcal{C}_n) \subseteq \mathbb{P}^3$.

We notice that $\varphi_{a,b,n,s}(\mathcal{C}_n)$ is in fact a (possible singular) space curve defined by the (affine) equations

$$cy^{q+1} = t(x) := \sum_{i=0}^{f-1} x^{p^{ib}} \quad \text{and} \quad z^M = y^{q^2} - y\,, \tag{3.1}$$

where $f := \frac{a}{b}$ and $M := \frac{q^n+1}{s(q+1)}$.

[1] The authors in [3] claimed that the GGS-curve $\mathcal{C}_n$ is covered by the Hermitian curve over $\mathbb{F}_{q^{2n}}$ for $n > 3$ and $q = 2$; however, according to [12, Remark 3.21], this would be false.

Proposition 3.2. *With the above notations and assumptions, the curve $\mathcal{X} := \mathcal{X}_{a,b,n,s}$ is maximal over $\mathbb{F}_{q^{2n}}$ of genus*

$$\alpha = \alpha_{a,b,n,s} = \frac{q^{n+2} - p^b q^n - sq^3 + q^2 + (s-1)p^b}{2sp^b}\,.$$

Proof. By construction, the curve $\mathcal{X}$ is maximal over $\mathbb{F}_{q^{2n}}$ since it is covered by the GGS-curve over $\mathbb{F}_{q^{2n}}$ (Serre's remark stated in the introduction). To compute the genus α of $\mathcal{X}$, we notice that a plane model of $\mathcal{X}$ is $\mathcal{D}$ given by the equation

$$cz^{\frac{q^n+1}{s}} = t(x)((t(x))^{q-1} + 1)^{q+1}\,. \tag{3.2}$$

By applying the Riemmann-Hurwitz formula to the morphism $x : \mathcal{D} \to \mathbb{P}^1$ of Kummer type we obtain (see e.g. [21, Prop. 3.7.3])

$$2\alpha - 2 = \frac{q^n+1}{s}(\frac{q^2}{p^b} - 1) - (\frac{q^3}{p^b} + 1)\,, \tag{3.3}$$

and the formula for α follows after some computations. □

Remark 3.3. With the above notation, the curve $\mathcal{X}_{a,b,n,s}$ has genus 0 if and only if $b = a$ and $s = \frac{q^n+1}{q+1}$.

Let $\mathcal{H}_n : v^{q^n+1} = u^{q^n} + u$ be the Hermitian curve over $\mathbb{F}_{q^{2n}}$; we recall that its genus is $G_n = q^n(q^n-1)/2$ and $\#\mathcal{H}_n(\mathbb{F}_{q^{2n}}) = q^{3n} + 1$. Suppose that there exists a nontrivial $\mathbb{F}_{q^{2n}}$-morphism

$$\phi = \phi_{a,b,n,s} : \mathcal{H}_n \to \mathcal{X}_{a,b,n,s}\,. \tag{3.4}$$

Let $d = d_{a,b,n,s}$ be the degree of ϕ. From $\phi(\mathcal{H}(\mathbb{F}_{q^{2n}})) \subseteq \mathcal{X}_{a,b,n,s}(\mathbb{F}_{q^{2n}})$ it follows that

$$d \cdot \#\mathcal{X}_{a,b,n,s}(\mathbb{F}_{q^{2n}}) \geq \#\mathcal{H}_n(\mathbb{F}_{q^{2n}})$$

and hence

$$d \geq sp^b q^{n-2} + \frac{-(s-1)sp^{2b}q^{3n-2} + s^2p^bq^{2n+1} - sp^bq^{2n} - (s-1)sp^{2b}q^{2n-2} - s^2p^{2b}q^{n-2} + sp^b}{q^{2n+2} + (s-1)p^bq^{2n} - sq^{n+3} + q^{n+2} + (s-1)p^bq^n + sp^b}\,. \tag{3.5}$$

On the other hand, the Riemann-Hurwitz formula [21, Thm. 3.4.13] implies

$$2G_n - 2 \geq d(2\alpha_{a,b,n,s} - 2)$$

and thus

$$d \leq sp^b q^{n-2} + \frac{sp^{2b}q^{2n-2} + s^2p^bq^{n+1} - 2sp^bq^n + s(s+1)p^{2b}q^{n-2} - 2sp^b}{q^{n+2} - p^bq^n - sq^3 + q^2 - (s+1)p^b}\,. \tag{3.6}$$

Theorem 3.4. *Let $q = p^a$ be a power of a prime number p. Let b be a divisor of a and suppose that $q > p^{2b} + p^b$; or equivalently, $a \geq 2b+1$. Then the above curve $\mathcal{X}_{a,b} := \mathcal{X}_{a,b,3,1}$ of genus*

$$\alpha_{a,b} = \frac{q^5 - (p^b+1)q^3 + q^2}{2p^b}$$

cannot be covered by the Hermitian curve $\mathcal{H}_3$ over $\mathbb{F}_{q^6}$.

Proof. The proof is similar to [9, Thm. 5]. Suppose that $\mathcal{X}_{a,b}$ is dominated by $\mathcal{H}_3$ as in (3.4). Then from (3.5) and (3.6), with $n = 3$ and $s = 1$, we would have, respectively,

$$d \geq p^b q + \frac{p^b q^7 - p^b q^6 - p^{2b} q + p^b}{q^8 - q^6 + q^5 + p^b}, \quad \text{and}$$

$$d \leq p^b q + \frac{(p^{2b} + p^b)q^4 - 2p^b q^3 + 2p^{2b} q - 2p^b}{q^5 - p^b q^3 - q^3 + q^2 - 2p^b}.$$

Thus $d > p^b q$ and $d < p^b q + 1$ since $q > p^{2b} + p^b$, a contradiction. □

Let $s = 1$ and suppose further that the morphism $\phi_{a,b,n,1}$ in (3.4) is Galois. Let $d = d_{a,b,n,1}$ be its degree and let $\alpha = \alpha_{a,b,n,1}$ be the genus of $\mathcal{X}_{a,b,n,1}$. According to (3.3) we can write

$$2\alpha - 2 = (q^n + 1)C - D$$

with $C = \frac{q^2}{p^b} - 1$ and $D = \frac{q^3}{p^b} + 1$. Then thanks to Duursma and Mak [3, Prop. 5.1] we can improve (3.5) so that

$$d \geq \frac{(q+1)(q^n+1)}{D}$$

and hence

$$d \geq p^b q^{n-2} + \frac{p^b q^n - p^{2b} q^{n-2} + p^b q + p^b}{q^3 + p^b}.$$

From this inequality and (3.6) (with $s = 1$) we conclude that

$$\frac{p^b q^n - p^{2b} q^{n-2} + p^b q + p^b}{q^3 + p^b} \leq \frac{p^{2b} q^{2n-2} + p^b q^{n+1} - 2p^b q^n + 2p^{2b} q^{n-2} - 2p^b}{q^{n+2} - p^b q^n - q^3 + q^2 - 2p^b}.$$

After some computation we then find the relation

$$q^{2n+1} - 2p^b q^{2n-1} + 2q^{n+1} - 2p^b q^{n-1} - q^3 + q - 2p^b \leq p^b q^{2n} + q^{n+3} - 2q^{n+2} + 3p^b q^n - q^2. \tag{3.7}$$

Theorem 3.5. *With the above notation, the curve $\mathcal{X}_{a,b,n,1}$ above cannot be Galois covered by the Hermitian curve $\mathcal{H}_n$ over $\mathbb{F}_{q^{2n}}$ provided that $b < a$.*

Proof. It follows from the computations above and (3.7). □

Question 3.6. Let $s > 1$. Can the curve $\mathcal{X}_{a,b,n,s}$ be covered (Galois covered) by the Hermitian curve $\mathcal{H}_n$ over $\mathbb{F}_{q^{2n}}$?

We finish this section by computing some polar divisors which will be quite useful for application to codes (see Section 5 below). Let us recall that x, y, z are the rational functions in (3.1), and $M = \frac{q^n+1}{s(q+1)}$.

Lemma 3.7. *The function x has just one pole $P_0 \in \mathcal{X} := \mathcal{X}_{a,b,n,s}$; moreover, $P_0 \in \mathcal{X}(\mathbb{F}_{q^{2n}})$ and the following computations hold true*:

- $\mathrm{div}_\infty(x) = (q+1)MP_0$;
- $\mathrm{div}_\infty(y) = \frac{q}{p^b}MP_0$;
- $\mathrm{div}_\infty(z) = \frac{q^3}{p^b}P_0$.

Proof. Let $Q \in \mathcal{X}$ be a pole of x and let v be the valuation at Q. Let e be the ramification index of Q over $x(Q) = \infty$. By using (3.1) we have

$$(q+1)v(y) = -\frac{q}{p^b}e\,, \quad \text{and} \quad Mv(z) = q^2v(y)$$

so that

$$M(q+1)v(z) = -\frac{q^3}{p^b}e\,.$$

Thus $M(q+1)$ divides e and hence $e = M(q+1)$ by (3.2). Therefore $P_0 := Q$ is the unique pole of x; it is $\mathbb{F}_{q^{2n}}$-rational by the Fundamental Equality on places; see e.g. [21, Thm. 3.1.11]. Finally from (3.1), P_0 is also the unique pole of y and z and the computations of the polar divisors of x, y and z follow. □

4. The curve $\mathcal{Y}_{n,s}$

Throughout this section we fix the following notation:

- $n \geq 3$ is an odd integer;
- q is a prime power;
- $s \geq 1$ is a divisor of $\frac{q^n+1}{q+1}$.

Let $\mathcal{C}_n$ be the GGS-curve (Section 2) and consider the morphism

$$\varphi_{n,s} : \mathcal{C}_n \to \mathbb{P}^3, \quad (u,v,w,1) \mapsto (x,y,z,1) := (u,v,w^s,1)\,.$$

Definition 4.1. We let $\mathcal{Y}_{n,s}$ be the nonsingular model over $\mathbb{F}_{q^{2n}}$ of $\varphi_{n,s}(\mathcal{C}_n) \subseteq \mathbb{P}^3$.

It turns out that $\varphi_{n,s}(\mathcal{C}_n)$ can be defined by the affine equations

$$y^{q+1} = x^q + x \quad \text{and} \quad z^M = y^{q^2} - y\,, \tag{4.1}$$

where $M = \frac{q^n+1}{s(q+1)}$ is as in Section 3.

Proposition 4.2. *The curve $\mathcal{Y}_{n,s}$ is maximal over $\mathbb{F}_{q^{2n}}$ of genus*

$$\beta_{n,s} := \frac{q^{n+2} - q^n - sq^3 + q^2 + s - 1}{2s}\,.$$

Proof. The proof is similar to Proposition 3.2; in particular, it is only necessary to prove the formula for $\beta_{n,s}$. We observe that $\mathcal{Y}_{n,s}$ has a plane model $\mathcal{D}$ of type

$$z^{\frac{q^n+1}{s}} = (x^q + x)((x^q + x)^{q-1} - 1)^{q+1}\,. \tag{4.2}$$

Then the Riemann-Hurwitz formula [21, Prop. 3.7.3] applied to the morphism $x : \mathcal{D} \to \mathbb{P}^1$ (which is of Kummer type) gives

$$2\beta_{n,s} - 2 = \frac{q^n+1}{s}(q^2-1) - (q^3+1)\,;$$

now the result follows after some computations. □

Remark 4.3. Notation as above. The curve $\mathcal{Y}_{n,s}$ has genus $\beta_{n,s} = q(q-1)/2$ if and only if $s = \frac{q^n+1}{q+1}$. In this case from (4.2), the curve $\mathcal{Y}_{n,s}$ is the Hermitian curve over $\mathbb{F}_{q^2}$.

Theorem 4.4. *Let q be a prime power, and s be a divisor of q^2-q+1 such that $q > s(s+1)$. Then the curve $\mathcal{Y}_s := \mathcal{Y}_{3,s}$ above of genus*

$$\beta_s := \beta_{3,s} = \frac{q^5 - (s+1)q^3 + q^2 + s - 1}{2s}$$

cannot be covered by the Hermitian curve $\mathcal{H}_3$ over $\mathbb{F}_{q^6}$.

Proof. The formula for β_s is $\beta_{3,s}$ in Proposition 4.2. To prove the second claimed part, we argue as in Theorem 3.4. In the context of Proposition 4.2, suppose that there is a (nontrivial) $\mathbb{F}_{q^{2n}}$-morphism $\phi : \mathcal{H}_n \to \mathcal{Y}_{n,s}$, where $\mathcal{H}_n$ is the Hermitian curve over $\mathbb{F}_{q^{2n}}$. Let d be the degree of ϕ. Then

$$d \cdot \#\mathcal{Y}_{n,s}(\mathbb{F}_{q^{2n}}) \geq q^{3n} + 1 \quad \text{so that}$$

$$d \geq sq^{n-2} + \frac{-(s-1)sq^{3n-2} + s^2q^{2n+1} - sq^{2n} - (s-1)sq^{2n-2} - s^2q^{n-2} + s}{q^{2n+2} + (s-1)q^{2n} - sq^{n+3} + q^{n+2} + (s-1)q^n + s}\,. \tag{4.3}$$

Moreover the Riemann-Hurwitz formula [21, Thm. 3.1.13] implies

$$2G_n - 2 \geq d(2\beta_{n,s} - 2)\,,$$

where $G_n = q^n(q^n-1)/2$ is the genus of $\mathcal{H}_n$, and hence

$$d \leq sq^{n-2} + \frac{sq^{2n-2} + s^2q^{n+1} - 2sq^n + s(s+1)q^{n-2} - 2s}{q^{n+2} - q^n - sq^3 + q^2 - (s+1)}\,. \tag{4.4}$$

Let $n = 3$. From Eq. (4.3)

$$d \geq sq + \frac{sq^7 - sq^6 - (s-1)sq^4 - s^2q + s}{q^8 - q^6 + q^5 + (s-1)q^3 + s}$$

and hence $d \geq sq + 1$; on the other hand, Eq. (4.4) reads

$$d \leq sq + \frac{s(s+1)q^4 - 2sq^3 + s(s+1)q - 2s}{q^5 - (s+1)q^3 + q^2 - (s+1)}$$

so that $d \leq sq$ for $q > s(s+1)$, a contradiction. □

Question 4.5. Let $n \geq 5$ be odd. Can the curve $\mathcal{Y}_{n,s}$ above be covered (Galois covered) by the Hermitian curve $\mathcal{H}_n$ over $\mathbb{F}_{q^{2n}}$?

Remark 4.6. Fanali and Giulietti [4] computed the genus of several quotient curves of the GK-curve $\mathcal{C}_3$. Their computations in [4, Thm. 4.5(iv)(v)] subsume the genera of the curves $\mathcal{X}_{a,b,3,1}$ and $\mathcal{Y}_{3,s}$ (Theorems 3.4 and 4.4 here). As a matter of fact, these values of the genus were also obtained in [2, Sect. 3].

Remark 4.7. Let $n \geq 5$ be odd. Güneri, Özdemir and Stichtenoth computed the genus of several quotient curves of the GGS-curve $\mathcal{C}_n$. Their computations in [11, Remark 3.13] subsume the genera of the curves $\mathcal{X}_{a,b,n,s}$ and $\mathcal{Y}_{n,s}$ in Proposition 3.2 and 4.2 above.

Remark 4.8. Let $n \geq 3$ be odd. Let $\mathcal{C} = \mathcal{X}_{a,b,n,s}$ (or $\mathcal{C} = \mathcal{Y}_{n,s}$) be the curve in Section 3 (or in Section 4). It is plausible the existence of a subgroup G of automorphisms of $\mathcal{C}_n$ (cf. [11], [12]) such that $\mathcal{C} = \mathcal{C}_n/G$.

We end up this section with a result concerning polar divisor. The result is similar to Lemma 3.7 and we omit its proof (in fact, it can be considered as the formal case $b = 0$ of such a Lemma). Let x, y, z be the functions in (4.1) and recall that $M = \frac{q^n+1}{s(q+1)}$.

Lemma 4.9. *The function x has just one pole $P_0 \in \mathcal{Y}_{n,s}$; moreover, $P_0 \in \mathcal{Y}_{n,s}(\mathbb{F}_{q^{2n}})$ and the following computations hold true*:

- $\mathrm{div}_\infty(x) = (q+1)MP_0$;
- $\mathrm{div}_\infty(y) = qMP_0$;
- $\mathrm{div}_\infty(z) = q^3P_0$.

5. Application to codes

Let a, b, n, s, p, $q = p^a$, $M = \frac{q^n+1}{s(q+1)}$ be as above; in addition, throughout we fix the following notation:

- $\mathcal{C}$ denotes either the curve $\mathcal{X}_{a,b,n,s}$ in Section 3, or the curve $\mathcal{Y}_{n,s}$ in Section 4;
- g denotes the genus of $\mathcal{C}$ computed in Proposition 3.2 or in Proposition 4.9;
- $P_0 \in \mathcal{C}(\mathbb{F}_{q^{2n}})$ is the unique common pole of the functions x, y, z which define the function field of $\mathcal{C}$ in (3.1) or in (4.1).

We notice that the morphism $\mathcal{C}_n \to \mathbb{P}^3$ which was used to define $\mathcal{C}$ can be lifted to a morphism $\bar{\varphi} : \mathcal{C}_n \to \mathcal{C}$ of degree $\bar{d}$ in such a way that $\#\bar{\phi}^{-1}(P_0) = 1$, and that either $\bar{d} = sp^b$ if $\mathcal{C} = \mathcal{X}_{a,b,n,s}$, or $\bar{d} = s$ if $\mathcal{C} = \mathcal{Y}_{n,s}$.

Next we compute the Weierstrass semigroup $H(P_0)$ of $\mathcal{C}$ at P_0. To do so, let us consider the following sequence of integers

$$(a_1, a_2, a_3) := \begin{cases} (\frac{q}{p^b}M, \frac{q^3}{p^b}, (q+1)M) & \text{if } n = 3\,, \\ (\frac{q^3}{p^b}, \frac{q}{p^b}M, (q+1)M) & \text{if } n > 3\,. \end{cases}$$

As a matter of fact, the members of this sequence are exactly the pole orders computed in Lemma 3.7; we also obtain the pole orders in Lemma 4.9 if we (formally) set $b = 0$ in the definition of (a_1, a_2, a_3) above.

For $i = 1, 2, 3$, let $d_i := \gcd(a_1, \ldots, a_i)$ (thus, $d_3 = 1$), and let S_i be the semigroup generated by $a_1/d_i, \ldots, a_i/d_i$. We see that $a_i/d_i \in S_{i-1}$ for $i = 2, 3$; that is to say, the semigroup $S_3 = \langle a_1, a_2, a_3 \rangle$ is *telescopic* (cf. [14, Sect. 5.4]). In particular, its genus $g(S_3) = \#(\mathbb{N}_0 \setminus S_3)$ is given by the formula (see e.g. [14, Prop. 5.35])

$$g(S_3) = g(S_2)d_2 + \frac{(d_2 - 1)(a_3 - 1)}{2}\,,$$

where $g(S_2) = \#(\mathbb{N}_0 \setminus S_2)$ is the genus of S_2. After some computation, it turns out that

$$g(S_3) = \frac{q^{n+2} - p^b q^n - sq^3 + q^2 + (s-1)p^b}{2sp^b}$$

which is equal to the genus g of $\mathcal{C}$ computed in Proposition 3.2 (or in Proposition 4.2, where we set $b = 0$ in the formula of $g_3(S)$ above). Thus we obtain the following.

Proposition 5.1. *With the above notation, the Weierstrass semigroup $H(P_0)$ of $\mathcal{C}$ at P_0 is telescopic and*

$$H(P_0) = S_3 = \langle a_1, a_2, a_3 \rangle\,.$$

We notice that the case $\mathcal{C} = \mathcal{Y}_{n,s}$ of Proposition 5.1 generalizes [9, Prop. 1] and [11, Sect. 2] as $\mathcal{Y}_{n,1}$ coincides with the GGS-curve $\mathcal{C}_n$ in Section 2.

Remark 5.2. Notations as above. Since the semigroup $H(P_0)$ is telescopic, we have a nice description for each $h \in H(P_0)$ [14, Lemma 5.34]: There exist unique integers $x_1 \geq 0$, $0 \leq x_2 < d_1/d_2$, $0 \leq x_3 < d_2/d_3 = d_2$ such that $h = x_1a_1 + x_2a_2 + x_3a_3$. In particular, the following set of rational functions is a base over $\mathbb{F}_{q^{2n}}$ of the Riemann-Roch space $\mathcal{L}(hP_0)$:

$$\{f_1^{\alpha_1} f_2^{\alpha_2} f_3^{\alpha_3} : \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 \leq h\,,\ \alpha_1 \geq 0\,,\ 0 \leq \alpha_2 < d_1/d_2\,, 0 \leq \alpha_3 < d_2\}\,,$$

where $\mathrm{div}_\infty(f_i) = a_i P_0$, $i = 1, 2, 3$.

Let $(\rho_\ell)_{\{\ell \in \mathbb{N}\}}$ be the sequence that enumerates the Weierstrass semigroup $H(P_0)$ in such a way that $\rho_1 = 0$ and $\rho_\ell < \rho_{\ell+1}$ for each ℓ. By the Riemann-Roch theorem, $\rho_\ell = \ell - 1 + g$ for $\ell \geq g + 1$ and hence the largest element ℓ_g of $\mathbb{N}_0 \setminus H(P_0)$ (*the set of gaps* at P_0) satisfies $\ell_g \leq 2g - 1$ (Weirstrass gap theorem).

Remark 5.3. Notation as above; in particular, let ℓ_g be the largest gap at P_0. The semigroup $H(P_0)$ is in fact *symmetric* [14, Prop. 5.35]; i.e., $\ell_g = 2g-1$. Thus the gaps at P_0 are completely determined, namely

$$\ell_g - \rho_g < \ell_g - \rho_{g-1} < \ldots < \ell_g - \rho_2 < \ell_g = 2g-1\,.$$

Therefore, as $g > 0$, $\rho_g = 2g-2$.

For $h \in \mathbb{N}$, let C_h denote the one-point Algebraic Geometry (AG) code on $\mathcal{C}$ defined by the divisors

$$G_h := hP_0\,, \qquad E = P_1 + \ldots + P_N\,,$$

where for each i, $P_i \in \mathcal{C}(\mathbb{F}_{q^{2n}})$, $P_i \neq P_j$ for $i \neq j$ and $N = \#\mathcal{C}(\mathbb{F}_{q^{2n}}) - 1$. We recall that a codeword in C_h is of type $(f(P_1), \ldots, f(P_N))$ with f in the Riemann-Roch space $\mathcal{L}(G_h)$; thus C_h is $\mathbb{F}_{q^{2n}}$-isomorphic to $\mathcal{L}(G_h)/\mathcal{L}(G_h - E)$. In particular,

$$k_h := \dim_{\mathbb{F}_{q^{2n}}} C_h = \#\{\rho \in H(P_0) : \rho \leq h\} \quad \text{whenever } h < N\,.$$

Let C_h^t be the dual code of C_h. Thus the length word of both codes C_h and C_h^t is N which is "large" with respect to g (this is related to the construction of "good codes", cf. e.g. [19, Sect. 10.8]). Let d_h and d_h^t denote the minimum distance of C_h and C_h^t, respectively. The Goppa lower bound on these parameters reads (see e.g. [14, Thms. 2.65 and 2.69]):

$$d_h \geq N - h\,, \qquad d_h^t \geq d_{\mathrm{G}}(h) := h - (2g-2)\,. \tag{5.1}$$

The objective of this Section is to improve on $d_{\mathrm{G}}(h)$ in (5.1) by using the fact that $H(P_0)$ is telescopic (Proposition 5.1 above). In fact we use the so-called designed (minimum distance) Feng-Rao d_{FR} numerical function which is defined via the concept of *error-correcting array* and that was elucidated by Feng and Rao [5] (see also [17], [14]). We notice that we can assume $h = \rho_\ell \in H(P_0)$ for some $\ell \in \mathbb{N}$, since $\rho_\ell \leq h < \rho_{\ell+1}$ implies $\mathcal{L}(G_h) = \mathcal{L}(\rho_\ell P_0)$.

Now we introduce the function d_{FR}. For $\ell \in \mathbb{N}_0$ set

$$\nu_\ell := \#\{(i,j) \in \mathbb{N}^2 : \rho_i + \rho_j = \rho_{\ell+1}\}\,, \qquad \text{and define}$$

$$d_{\mathrm{FR}}(\ell) := \min\{\nu_m : \ell \leq m\}\,.$$

Therefore, with $h = \rho_\ell$, from [5], (see also [17, Thm. 2.5]), the following holds true

$$d_h^t \geq d_{\mathrm{FR}}(\ell)\,. \tag{5.2}$$

Thus our objective is to compare the lower bounds on d_h^t stated in (5.1) and (5.2); see Corollary 5.5 and Remark 5.6 below.

Lemma 5.4. *Notation as above. In particular, $q = p^a$ and b is a divisor of a with $b < a$ whenever $\mathcal{C} = \mathcal{X}_{a,b,n,s}$. Let $H(P_0) = \langle a_1, a_2, a_3\rangle : 0 = \rho_1 < \rho_2 < \ldots$ be the Weierstrass*

semigroup of $\mathcal{C}$ *at* P_0*, and suppose that* $a_3 = \max\{a_1, a_2, a_3\}$*. Let* $d_2 = \gcd(a_1, a_2)$ *and* $g = \#(\mathbb{N}_0 \setminus H(P_0))$ *be the genus of* $\mathcal{C}$*. Then*

(5.3)

$$d_{\mathrm{FR}}(\ell) = \begin{cases} \min\{\rho_m : \rho_m \geq \ell + 1 - g\} & \text{if } 3g - 2 - (d_2 - 1)a_3 < \ell \leq 3g - 2 \text{ and } \ell \geq g\,; \\ j + 1 & \text{if } (j-1)a_3 < \rho_{\ell+1} \leq ja_3 \leq (d_2 - 1)a_3\,. \end{cases}$$

Proof. The claimed formula for $d_{\mathrm{FR}}(\ell)$ follows from Theorems 6.10 and 6.11 in [17] since our semigroup $H(P_0)$ is telescopic (Proposition 5.1) and $d_2 = q/p^b > 1$ as $b < a$ or $d_2 = q$ in case $\mathcal{C} = \mathcal{Y}_{n,s}$. □

Next we compute an explicit formula for the first part of (5.3) by taking advantage of the symmetry property of $H(P_0)$ which was already noticed in Remark 5.3 above.

Corollary 5.5. *Let* g, d_2, a_3 *be as in Lemma 5.4. Let* U *be an integer such that* $0 \leq U \leq \min\{2g - 2, (d_2 - 1)a_3 - 1\}$*,* $\ell = 3g - 2 - U$ *and* $h = \rho_\ell$*.*

(1) *If* $U \in \mathbb{N}_0 \setminus H(P_0)$*, then* $d_{\mathrm{FR}}(\ell) = \ell + 1 - g$*;*
(2) (cf. [7]) *Let* $U = \rho_i \in H(P_0)$ *and* $F \in \mathbb{N}_0$ *such that* $\rho_i > \rho_{i-1} > \ldots > \rho_{i-F}$ *are* $F + 1$ *consecutive elements in* $H(P_0)$*, but* $\rho_{i-F} > \rho_{i-F-1} + 1$*. Then*

$$d_{\mathrm{FR}}(\ell) = \ell + F + 2 - g\,.$$

Proof. We have $\ell + 1 - g = \ell_g - U$ and the result is a direct application of Lemma 5.4 and Remark 5.3. □

Remark 5.6. Let $\ell \geq g+1$ and so $h = \rho_\ell = \ell - 1 + g$. Thus in (5.1) $d^t_\ell \geq d_{\mathrm{G}}(h) = \ell + 1 - g$. In general it is known that $d_{\mathrm{FR}}(\ell) \geq \ell + 1 - g$; equality holds if $\ell > 3g - 2$ since $H(P_0)$ is symmetric (see [14, Thm. 5.24]). Thus we have extended and improved these results to $g \leq \ell \leq 3g - 2$; e.g., notice that $d_{\mathrm{FR}}(g) = \rho_2$.

We conclude this paper with an observation concerning Suzuki and Ree curves.

Remark 5.7. In the context of curves with many rational points over a finite field $\mathbb{F}_\ell$ there is an important class of such curves, namely the Deligne-Lusztig curves associated to either projective special linear groups (Hermitian curves, where $\ell = q^2$, and which we already dealt with), or to Suzuki groups (Suzuki curves, where $\ell = 2\ell_0^2$), or to Ree groups (Ree curves, where $\ell = 3\ell_0^2$); see e.g. [15, §1.16,§4]. We have that a Suzuki (resp. Ree) curve is a maximal curve over $\mathbb{F}_{\ell^4}$ and thus over $\mathbb{F}_{\ell^{12}}$ (resp. $\mathbb{F}_{\ell^6}$). The genus of a Suzuki (Ree) curve is $g_S = \ell_0(\ell - 1)$ (resp. $g_R = 3\ell_0(\ell - 1)(\ell + \ell_0 + 1)$.

Let $\mathcal{C} = \mathcal{X}_{a,b,3,s}$ or $\mathcal{C} = \mathcal{Y}_{3,s}$ over $\mathbb{F}_{q^6}$. Then we can extend Theorems 3.4 and 4.4 as follows: "The curve $\mathcal{C}$ cannot be $\mathbb{F}_{q^6}$-covered by a Suzuki curve or Ree curve, where $q = \ell^2$ in the former case". The very simple reason for this is that the genus of $\mathcal{C}$ (Propositions 3.2 and 4.2) is larger than g_S and g_R.

Acknowledgments. We thank Massimo Giulietti who pointed out to us Remark 4.6 and share with us the paper [2]. The first and second author were supported, respectively, by Industrial University of Santander, Colombia, and FAPESP/SP-Brazil (Grant 2012/02255-3); the third author was partially supported by CNPq-Brazil (Grant 306324/2011-3).

References

[1] A. Aguglia, G. Korchmáros and F. Torres, *Plane maximal curves*, Acta Arith. **98** (2001), 165–179.

[2] D. Bartoli and P. Speziali, *On some quotient curves of the GK curve*, preprint, 2014.

[3] I. Duursma and K.H. Mak, *On maximal curves which are not Galois subcovers of the Hermitian curve*, Bull. Braz. Math. Soc. New Series **43**(3) (2012), 453–465.

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

[5] G.L. Feng and T.R.N. Rao, *A simple approach for construction of algebraic-geometric codes from plane curves*, IEEE Trans. Inform. Theory **IT-40** (1994), 1003–1012.

[6] A. Garcia, C. Güneri and H. Stichtenoth, *A generalization of the Giulieti-Korchmáros maximal curve*, Adv. Geom. **10** (2010), 427–434.

[7] A. Garcia, S.J. Kim and R.F. Lax, *Consecutive Weirstrass gaps and minimum distance of Goppa codes*, J. Pure Appl. Algebra **84** (1993), 199–207.

[8] A. Garcia, H. Stichtenoth and C. P. Xing, *On subfields of Hermitian function fields*, Composito Math. **120** (2000), 137–170.

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

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

[11] C. Güneri, M. Özdemir and H. Stichtenoth, *The automorphism group of the generalized Giulietti-Korchmáros function field*, Adv. Geom. **13** (2013), 369–380.

[12] R. Guralnick, B. Malmskog and R. Pries, *The Automorphism Group of a Family of Maximal Curves*, J. Algebra **361**, (2012), 92–116.

[13] J. W.P, Hirschfeld, G. Korchmáros and F. Torres, "Algebraic curves over a finite field", Princeton Univ. Press, 2008.

[14] T. Høholdt, J.H. van Lint and R. Pellikaan, *Algebraic geometry codes*, Handbook of Coding Theory, vol. 1, V.S. Pless, W.C. Huffman and R.A. Brualdi (Eds.), Elsevier, Amsterdam (1998), 871–961.

[15] N.E. Hurt, "Many rational points, Coding theory and algebraic geometry", Kluwer Academic Publishers, 2003.

[16] A. Kazemifard, A. R. Naghipour and S. Tafazolian, *A note on superspecial and maximal curves*, Bull. Iranian Math. Soc. **39** (2013), 405–413.

[17] C. Kirfel and R. Pellikann, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inform. Theory **41** (1995), 1720–1732.

[18] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris, Sér. I Math. **305** (1987), 729–732,

[19] J.H. van Lint, "Introduction to coding theory", third ed., Grad. Texts in Math., vol. **86**, Springer-Verlag, 1999.

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

[21] H. Stichtenoth, "Algebraic function fields and codes", second ed., Grad. Texts in Math., vol. **254**, Springer-Verlag, 2009.

[22] J. Tate, *Endomorphisms of Abelian Varieties over Finite Fields*, Invent. Math. **2** (1966), 134–144.

IMECC-UNICAMP, R. Sérgio Buarque de Holanda, 651, Cidade Universitária "Zeferino Vaz", 13083-859, Campinas, SP, Brazil.
E-mail address: tafazolian@ime.unicamp.br

Industrial University of Santander, Bucaramanga, Cra. 27 calle 9 pbx: (57(7) 6344000 nit 890201213-4, Colombia
E-mail address: ateheran@uis.edu.co

IMECC-UNICAMP, R. Sérgio Buarque de Holanda, 651, Cidade Universitária "Zeferino Vaz", 13083-859, Campinas, SP, Brazil
E-mail address: ftorres@ime.unicamp.br