AG codes from the second generalization of the GK maximal curve

Montanucci, Maria; Pallozzi Lavorante, Vincenzo

Published in:
Discrete Mathematics

Link to article, DOI:
10.1016/j.disc.2020.111810

Publication date:
2020

Document Version
Peer reviewed version

AG CODES FROM THE SECOND GENERALIZATION OF THE GK MAXIMAL CURVE

MARIA MONTANUCCI AND VINCENZO PALLOZZI LAVORANTE

ABSTRACT. Let q be a prime-power, and $n \geq 3$ an odd integer. We determine the structure of the Weierstrass semigroup $H(P)$ where P is an arbitrary $\mathbb{F}_{q^2}$-rational point of $\mathcal{GK}_{2,n}$ where $\mathcal{GK}_{2,n}$ stands for the $\mathbb{F}_{q^{2n}}$-maximal curve of Beelen and Montanucci. We prove that these points are Weierstrass points, and we compute the Frobenius dimension of $\mathcal{GK}_{2,n}$. Using these results, we also show that $\mathcal{GK}_{2,n}$ is isomorphic to the Güneri-Garcìa-Stichtenoth only for $n = 3$. Furthermore, AG codes and AG quantum codes from the $GK_{2,n}$ are constructed and discussed. In some cases, they have better parameters compared with those of the known linear codes.

Keywords: Maximal curves, Weierstrass semigroups, algebraic-geometric codes

2000 MSC: Primary: 11G20. Secondary: 11R58, 14H05, 14H55.

1. INTRODUCTION

In this paper, $\mathcal{X}$ denotes a (projective, geometrically irreducible, non-singular algebraic) curve defined over a finite field $\mathbb{F}_q$ with q elements where $q = p^n$ with a prime number p. The curve $\mathcal{X}$ is $\mathbb{F}_q$-maximal if its number of points attains the Hasse-Weil upper bound, namely $|\mathcal{X}(\mathbb{F}_q)| = q + 1 + 2g\sqrt{q}$, where g is the genus of $\mathcal{X}$, and $\mathcal{X}(\mathbb{F}_q)$ stands for the set of all $\mathbb{F}_q$-rational points of $\mathcal{X}$. Obviously, $\mathbb{F}_q$-maximal curves only exist for square q's.

$\mathbb{F}_q$-maximal curves, more generally curves with many $\mathbb{F}_q$-rational points compared with their genera, are proven to be useful for the construction of AG (algebraic-geometry) codes with good performance. To compute the parameters of such codes, a useful tool is the Weierstrass semigroup $H(P)$ defined at a point $P \in \mathcal{X}$.

Although Weierstrass semigroup is truly an algebraic-geometry object, its explicit determination mostly require (sometimes cleaver and certainly non-standard) computations to carry out over a finite field. Indeed, there exists no method for the explicit computation of $H(P)$, unless the curve does have special features such as simple equations or many automorphisms. In particular, the search of enough non-gaps to generate $H(P)$ for an $\mathbb{F}_q$-rational point P of an $\mathbb{F}_q$-maximal curve $\mathcal{X}$ can benefit from the knowledge of the Frobenius dimension of $\mathcal{X}$ and the structure of the 1-point stabilizer of the automorphism group of $\mathcal{X}$.

Many of the known $\mathbb{F}_q$-maximal curves are $\mathbb{F}_q$-covered by the Hermitian, or the Suzuki, or the Ree curve, and they inherit several properties that are used to investigate their

features including the behavior of the structure of the Weierstrass semigroups. A different family consists of the $\mathbb{F}_q$-maximal curve, named GK-curve, constructed by Giulietti and Korchmáros in [6] together with its generalizations, such as the GGS-curve due to Garcìa, Güneri and Stichtenoth, see [5], and the curve recently introduced by Beelen and Montanucci, see [2].

In this paper we investigate the latter curve further using explicit computations performed over a finite field. Our goals are the explicit description of the Weierstrass semigroup $H(P)$ at some $\mathbb{F}_q$-rational points, and the determination of the Frobenius dimension. Our main results are stated in Theorem 1.1 where, as usual, q is replaced by q^2 to avoid the frequent use of $\sqrt{q}$, especially in equations.

Theorem 1.1. *For an odd prime-power q, and $n \geq 5$ odd, let $\mathcal{GK}_{2,n}$ be the $\mathbb{F}_{q^{2n}}$-maximal curve of Beelen and Montanucci. Let $m = (q^n+1)/(q+1)$.*

(I) *For any $P \in \mathcal{GK}_{2,n}(\mathbb{F}_{q^2})$, the Weierstrass semigroup $H(P)$ at P is*
- *$H(P) = \langle A_1, q^n+1\rangle$, for $A_1 := \{mq + i(q^2-q) \mid i = 0, \ldots, \frac{m-1}{q^2-q}\}$, if P is an infinite point of $\mathcal{GK}_{2,n}$;*
- *$H(P) = \langle q^n+1-m, A_2\rangle$, for $A_2 := \{q^n+1-k \mid k = 0, \ldots, \frac{m-1}{q^2-q}\}$, otherwise.*

(II) *The Frobenius dimension of $\mathcal{GK}_{2,n}$ equals $(m-1)/(q^2-q)+2$.*

Theorem 4.8 has the following corollary; see also Corollary 5.3 and Theorem 5.4.

Corollary 1.2. *Let q be a prime power and $n \geq 3$ be odd.*

- *The curve $\mathcal{GK}_{2,n}$ is isomorphic to GGS if and only if $n = 3$.*
- *All $\mathbb{F}_{q^{2n}}$-rational points of $\mathcal{GK}_{2,n}$ are Weierstrass points.*

As we have already pointed out AG codes constructed from algebraic curves have better parameters when the underlying curve has many rational points. In particular, most of the codes constructed from maximal curves are those having the best parameters known in the literature. Furthermore, maximal curves often have large automorphism groups which in many cases are inherited by the AG code itself. This is useful in Coding theory since it can ensure good performances in encoding [13] and decoding [10]. Also, the parameters of an AG code arising from a curve rely on the inner structure of its Weierstrass semigroups; see e.g. [21]. Section 6 is dedicated to the construction of AG codes and AG quantum codes from the curve $\mathcal{GK}_{2,n}$. Comparison with codes known in the literature are also provided. In some cases our AG codes have better parameters; see Remark 6.3.

2. Preliminary results

From a result commonly known as the Kleiman-Serre covering result [14], we know that every curve which is $\mathbb{F}_{q^2}$-covered by an $\mathbb{F}_{q^2}$-maximal curve is itself also $\mathbb{F}_{q^2}$-maximal. The

most important example of $\mathbb{F}_{q^2}$-maximal curve is the Hermitian curve $\mathcal{H}_q$, with affine equation

$$Y^{q+1} = X^{q+1} - 1.$$

The automorphisms group of $\mathcal{H}_q$ is very large compared to $g(\mathcal{H}_q)$. Indeed it is isomorphic to $\mathrm{PGU}(3,q)$ and its order is larger than $16(g(\mathcal{H}_q))^4$. Moreover $\mathcal{H}_q$ has the largest genus admissible for an $\mathbb{F}_{q^2}$-maximal curve and it is the unique curve having this property up to birational isomorphism, see [16]. Few examples of maximal curves not covered by $\mathcal{H}_q$ are known in the literature. In [6] Giulietti and Korchmáros constructed an $\mathbb{F}_{q^6}$-maximal curve which is not a subcover of the Hermitian curve $\mathcal{H}_{q^3}$. Two generalizations of the Giulietti-Korchmàros curve (GK curve) into infinite families of maximal curves are known in the literature and they are not Galois subcovers of the Hermitian curve. The first generalization $\mathcal{GK}_{1,n}$ was introduced by Garcìa, Güneri and Stichtenoth in [5]. For a prime power q and an odd integer $n \geq 3$ the curve $\mathcal{GK}_{1,n}$ is given by the affine space model

$$\mathcal{GK}_{1,n} : \begin{cases} Z^m = Y^{q^2} - Y \\ Y^{q+1} = X^q + X \end{cases} \tag{2.1}$$

where $m := \frac{q^n+1}{q+1}$. The curve $\mathcal{GK}_{1,n}$ is $\mathbb{F}_{q^{2n}}$-maximal of genus

$$g(\mathcal{GK}_{1,n}) = (q-1)(q^{n+1} + q^n - q^2)/2$$

and $\mathcal{GK}_{1,3}$ is the GK curve.

Recently Beelen and Montanucci [2] constructed another infinite family $\mathcal{GK}_{2,n}$ of maximal curves generalizing the GK curve. For any prime power q and odd $n \geq 3$ the curve $\mathcal{GK}_{2,n}$ is given by

$$\mathcal{GK}_{2,n} : \begin{cases} Z^m & = Y \frac{X^{q^2} - X}{X^{q+1} - 1} \\ Y^{q+1} & = X^{q+1} - 1 \end{cases} \tag{2.2}$$

where again $m := \frac{q^n+1}{q+1}$. The main properties of $\mathcal{GK}_{2,n}$, for a fixed n, are summarized in the next propositions.

Proposition 2.1. [2, Section 2] *Let $\mathcal{GK}_{2,n}$ be defined as above. Then the following hold.*

- *$\mathcal{GK}_{2,n}$ is an absolutely irreducible $\mathbb{F}_{q^{2n}}$-maximal curve. The genus of $\mathcal{GK}_{2,n}$ is*

$$g(\mathcal{GK}_{2,n}) = \frac{(q-1)(q^{n+1} + q^n - q^2)}{2}.$$

  The curve $\mathcal{GK}_{2,3}$ is $\mathbb{F}_{q^6}$-isomorphic to the GK curve. Even though $g(\mathcal{GK}_{1,n}) = g(\mathcal{GK}_{2,n})$, the curves $\mathcal{GK}_{1,n}$ and $\mathcal{GK}_{2,n}$ are not isomorphic over $\overline{\mathbb{F}}_{q^{2n}}$ for any $n \geq 5$.
- *For any odd $n \geq 3$ and $q > 2$, $\mathcal{GK}_{2,n}$ is not Galois covered by the Hermitian curve $\mathcal{H}_{q^n}$. If $q = 2$ then $\mathcal{GK}_{2,n}$ is Galois covered by $\mathcal{H}_{q^n}$ over $\mathbb{F}_{q^{2n}}$ for every odd $n \geq 3$.*
- *The automorphism group of $\mathcal{GK}_{2,n}$ is isomorphic to $\mathrm{SL}(2,q) \rtimes C_{q^n+1}$ where C_k denotes the cyclic group with k elements.*

Let $\mathbb{F}_{q^{2n}}(x,y,z)$ be the function field of $\mathcal{GK}_{2,n}$ where

$$y^{q+1} = x^{q+1} - 1 \text{ and } z^m = y\frac{x^{q^2}-x}{x^{q+1}-1}.$$

Then $\mathbb{F}_{q^{2n}}(x,y,z)$ is an extension of the Hermitian function field $\mathbb{F}_{q^{2n}}(x,y)$. The following proposition describes the ramification structure in the function fields extension $\mathbb{F}_{q^{2n}}(x,y,z)/\mathbb{F}_{q^{2n}}(x,y)$ and the short-orbits structure of the automorphism group of $\mathcal{GK}_{2,n}$ over the algebraic closure of $\mathbb{F}_{q^{2n}}$.

Proposition 2.2. [2, Section 4] *For the function field $\mathbb{F}_{q^{2n}}(x,y,z)$ of $\mathcal{GK}_{2,n}$ the following hold.*

- *The places centered at the q^3+1 $\mathbb{F}_{q^2}$-rational points of the Hermitian curve $\mathcal{H}_q$ are totally ramified in the function fields extension $\mathbb{F}_{q^{2n}}(x,y,z)/\mathbb{F}_{q^{2n}}(x,y)$. Moreover, $\mathbb{F}_{q^{2n}}(x,y,z)/\mathbb{F}_{q^{2n}}(x,y)$ is a Kummer extension of degree $m=(q^n+1)/(q+1)$.*
- *The full automorphism group $\mathrm{Aut}(\mathcal{GK}_{2,n})$ of $\mathcal{GK}_{2,n}$ acts on the set of $\mathbb{F}_{q^2}$-rational points of $\mathcal{GK}_{2,n}$ with two orbits, say O_1 and O_2, with*

  $$O_1 := \{P_1, \dots, P_{q+1}\},$$

  lying over the $q+1$ points at infinity of $\mathcal{H}_q$, and

  $$O_2 := \{R_1, \dots, R_{q^3-q}\},$$

  lying over the remaining $\mathbb{F}_{q^2}$-rational points.

Before proceeding with the investigation of Weierstrass semigroups at points in O_1 and O_2, we describe the divisor associated to some algebraic functions on $\mathcal{GK}_{2,n}$ that we will use in the following.

Lemma 2.3. [2, Lemma 4.2] *Let $P_1 := (1:-1:0:0) \in O_1$. Then: see* [2]

1. $(z) = \sum_{\substack{P \in \mathcal{GK}_{2,n}(\mathbb{F}_{q^2}) \\ P \notin \{P_1,\dots,P_{q+1}\}}} P - (q^2-q)\sum_{i=1}^{q+1} P_i$
2. $(dz) = (q^{n+1}-q^n-q^2+2q-2)\sum_{i=1}^{q+1} P_i = \frac{2g(\mathcal{GK}_{2,n})-2}{(q+1)}\sum_{i=1}^{q+1} P_i$.

3. The Weierstrass semigroup at points in O_1

The semigroup $H(P)$ is defined to be the set of all integers k for which there exists a rational function on $\mathcal{X}$ having pole divisor kP. Clearly $H(P)$ is a subset of $\mathbb{N} = \{0,1,2,\dots\}$. The Weierstrass gap Theorem [20, Theorem 1.6.8], states that the set $G(P) := \mathbb{N} \setminus H(P)$ contains exactly g elements, called *gaps*.

In this section we investigate the structure of the Weierstrass semigroup $H(P)$ for $P \in O_1 = \{P_1, \dots, P_{q+1}\}$. Note that

$$P_i := (1 : a_i : 0 : 0) \text{ and } a_i^{q+1} = 1.$$

These are all the points at infinity of $\mathcal{GK}_{2,n}$. Furthermore, in the function fields extension $\mathbb{F}_{q^{2n}}(x,y,z)/\mathbb{F}_{q^{2n}}(x,y)$ we have $P_i \mid \bar{P}_i$, with $i = 1,\dots,q+1$ where $\{\bar{P}_i\}_i$ denotes the $q+1$ points at infinity of $\mathcal{H}_q$. We can take

$$P_1 := (1 : -1 : 0 : 0)$$

as a representative of points in O_1 to compute $H(P)$ for every $P \in O_1$. Indeed, it is known that the structure of Weierstrass semigroups is invariant under the action of automorphism groups see [20, Lemma 3.5.2] and O_1 is an $\mathrm{Aut}(\mathcal{GK}_{2,n})$-orbit. Thus, $\bar{P}_1 := (1 : -1 : 0)$.

Lemma 3.1. *For all $k = 0,\dots,\frac{m-1}{q^2-q}$ we have $mq + k(q^2-q) \in H(P_1)$.*

Proof. Let $\varrho = x + y$. In [2, Lemma 3.1] the function fields extension $\mathbb{F}_{q^{2n}}(x,y)/\mathbb{F}_{q^{2n}}(\varrho)$ is shown to be an Artin–Schreier extension of degree q and in [2, Proposition 2.1] it is pointed out that $\mathbb{F}_{q^{2n}}(x,y,z)/\mathbb{F}_{q^{2n}}(x,y)$ is a Kummer extension of degree m. This implies that

$$(\varrho) = mqP_1^{\infty} - m\sum_{i=2}^{q+1} P_i^{\infty}, \tag{3.1}$$

see [2, Equation (3.1)]. By Lemma 2.3 we can define for all $k = 0,\dots,\frac{m-1}{q^2-q}$ the rational function $\vartheta_k = \frac{z^k}{\varrho}$. Then:

$$\begin{aligned}(\vartheta_k) &= k \sum_{\substack{P\in\mathcal{GK}_{2,n}(\mathbb{F}_{q^2})\\ P\notin\{P_1,\dots,P_{q+1}\}}} P - (q^2-q)k\sum_{i=1}^{q+1} P_i - qmP_1 + m\sum_{i=2}^{q+1} P_i \\ &= k \sum_{\substack{P\in\mathcal{GK}_{2,n}(\mathbb{F}_{q^2})\\ P\notin\{P_1,\dots,P_{q+1}\}}} P + (m - k(q^2-q))\sum_{i=2}^{q+1} P_i - (mq - k(q^2-q))P_1.\end{aligned}$$

Note that

- $k \sum\limits_{\substack{P\in\mathcal{GK}_{2,n}(\mathbb{F}_{q^2})\\ P\notin\{P_1,\dots,P_{q+1}\}}} P \geq 0$;
- $(m - k(q^2-q))\sum_{i=2}^{q+1} P_i \geq 0$ as $k \leq \frac{m-1}{q^2-q}$.

Thus,

$$(\vartheta_k) = E - (mq - k(q^2-q))P_1,$$

where $E \geq 0$. This concludes the proof. □

Observation 3.2. From Proposition *2.1*, the curve $\mathcal{GK}_{2,n}$ is $\mathbb{F}_{q^{2n}}$-maximal for odd $n \geq 3$. The fundamental equation [11, Page xix (ii)] guarantees that if $\mathcal{X}$ is an $\mathbb{F}_{q^2}$-maximal curve and $P \in \mathcal{X}$ then

$$qP + \Phi^2(P) \equiv (q+1)P_0,$$

where $P_0 \in \mathcal{X}(\mathbb{F}_{q^2})$ and Φ is the Frobenius homomorphism ($\alpha \mapsto \alpha^q$). Thus, if P and Q are $\mathbb{F}_{q^{2n}}$-rational points of $\mathcal{GK}_{2,n}$ then

$$(q^n+1)P \equiv (q^n+1)Q, \tag{3.2}$$

as also $\Phi^{2n}(P) = P$. In particular this implies that q^n+1 is a non-gap for every $P \in \mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}})$. For more details see also [11, Proposition 10.6].

The following result allows us to construct explicitly a rational function which realizes q^n+1 as a non-gap.

Lemma 3.3. *Let* $\alpha := \left(\frac{x-1}{\varrho}\right)$. *Then*

$$(\alpha) = (q^n+1)(Q - P_1),$$

where $Q := (1:0:1:0)$.

Proof. Let $\bar{Q}$ be the affine point $\bar{Q} = (1:0:1)$. Then clearly $\bar{Q}$ is $\mathbb{F}_{q^2}$-rational. The tangent line at $\mathcal{H}_q$ in $\bar{Q}$ is $t : X - 1 = 0$. This line meets $\mathcal{H}_q$ only in $\bar{Q}$, so the intersection multiplicity is $q+1$. Thus the divisor of t is

$$(t)_{\mathbb{F}_{q^{2n}}(x,y)} = (q+1)\bar{Q} - \sum_{i=1}^{q+1} \bar{P}_i.$$

Using that $\mathbb{F}_{q^{2n}}(x,y,z)/\mathbb{F}_{q^{2n}}(x,y)$ is a Kummer extension, we obtain:

$$(t) = m(q+1)Q - m\sum_{i=1}^{q+1} P_i = (q^n+1)Q - m\sum_{i=1}^{q+1} P_i.$$

Considering now the quotient given by the rational functions t and $\varrho = x+y$, we get

$$\begin{aligned}\left(\frac{x-1}{\varrho}\right) &= (q^n+1)Q - mP_1 - m\sum_{i=2}^{q+1} P_i + m\sum_{i=2}^{q+1} P_i - mqP_1 \\ &= (q^n+1)Q - (q^n+1)P_1.\end{aligned}$$

□

Our aim is now to prove the following theorem, which is the main result of this section.

Theorem 3.4. *Let* $H_1 := \langle A_1, q^n+1\rangle$, *for* $A_1 := \{mq + i(q^2-q) \mid i = 0,\dots,\frac{m-1}{q^2-q}\}$. *Then* $H_1 = H(P_1)$.

From Lemma 3.1 and Lemma 3.3, H_1 is contained in $H(P_1)$, so we only need to show the other inclusion to prove Theorem 3.4.

3.1. **Computing the genus of H_1.** We recall that for a numerical semigroup $G \subset \mathbb{N}$, the *genus* of G is $g(G) :=\mid \mathbb{N} \setminus G \mid$. In order to prove $H_1 = H(P_1)$, we can equivalently show that the two semigroups H_1 and $H(P_1)$ have the same genus. Indeed, this means

that there are no elements in $H(P_1) \setminus H_1$ and hence $H_1 = H(P_1)$. We start by recalling the definition of an important class of numerical semigroups, called *telescopic semigroups*, see [12].

Let $(a_1, \ldots, a_k)$ be a sequence of positive integers with greatest common divisor equal to 1. Define

$$d_i := \gcd(a_1, \ldots, a_i) \quad \text{and} \quad A_i := \left\{ \frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i} \right\},$$

for $i = 1, \ldots, k$. Let $d_0 := 0$ and G_i be the semigroup generated by A_i. If $\frac{a_i}{d_i} \in G_{i-1}$ for all $i = 2, \ldots, k$ then the sequence $(a_1, \ldots, a_k)$ is *telescopic*. A numerical semigroup is called *telescopic* if it is generated by a telescopic sequence.

From [12, Proposition 5.35] the genus of a telescopic semigroup S generated by a telescopic sequence $(a_1, \ldots, a_k)$ is

$$g(S) = \frac{1}{2}\left(1 + \sum_{i=1}^{k} \left(\frac{d_{i-1}}{d_i} - 1 \right) a_i \right). \tag{3.3}$$

In order to compute the genus of H_1 we will proceed according to the following steps.

- We construct a telescopic semigroup $S \subset H_1$;
- we use Equation (3.3) to compute the genus of S, so that $g(H_1) \leq g(S)$;
- we compute explicitly the elements in $H_1 \setminus S$ and hence their number. In this way we get $g(H_1) \leq g(S) - \mid H_1 \setminus S \mid \leq g$. Since $g(H_1) \geq g$ as $H_1 \subseteq H(P_1)$ we get that $g(H_1) = g$.

Let $S := \langle mq, mq + (q^2 - q), q^n + 1 \rangle$.

Lemma 3.5. *The numerical semigroup S is telescopic. In particular,*

$$g(S) = \frac{1}{2}(q(m^2 - 3m + 2) + q^2(m - 1) - q^n + q^{n+1}).$$

Proof. The sequence $(mq, mq + (q^2 - q), q^n + 1)$ has GCD equal to 1. Furthermore we have $q^n + 1 = m(q + 1)$ and $A_2 = \{m, m + q - 1\}$, so we can apply the equation (3.3). Thus,

$$\begin{aligned} g(S) &= \frac{1}{2}(1 + mq(-1) + (mq + q^2 - q)(m - 1) + (q - 1)(q^n + 1)) \\ &= \frac{1}{2}(1 - mq + m^2q + mq^2 - mq - mq + q^2 + q + q^{n+1} + q - q^n - 1) \\ &= \frac{1}{2}(q(m^2 - 3m + 2) + q^2(m - 1) - q^n + q^{n+1}). \end{aligned}$$

□

The following remark describes the elements in $H_1 \setminus S$.

Remark 3.6. For every integer n there exist uniquely determined a, b and c such that $n = a(mq) + b(q^2 - q) + c(q^n + 1)$, $0 \leq b \leq m - 1$ and $0 \leq c \leq q - 1$. In fact if $a(mq) + b(q^2 - q) + c(q^n + 1) = a_1(mq) + b_1(q^2 - q) + c_1(q^n + 1)$ then we have $b \equiv b_1 \bmod m$ and $c \equiv c_1 \bmod q$.
Moreover, $n \in S$ if and only if $n = a(mq) + b(q^2 - q) + c(q^n + 1)$ with $0 \leq b \leq m - 1$, $0 \leq c \leq q - 1$ and $a \geq b$, because $n = (a - b)(mq) + b(mq + q^2 - q) + c(q^n + 1)$.

Lemma 3.7. *Let $n \in \mathbb{N}$ such that $n = a(mq) + b(q^2 - q) + c(q^n + 1)$, $0 \leq b \leq m - 1$ and $0 \leq c \leq q - 1$. Then $n \in S$ if and only if $a \geq b$.*

Proof. If $a \geq b$, then $n = (a-b)(mq)+b(mq+q^2-q)+c(q^n+1)$, so $n \in S$. On the other hand, if $n \in S$ then $n = a(mq) + b(mq + q^2 - q) + c(q^n + 1) = (a + b)(mq) + b(q^2 - q) + c(q^n + 1)$. □

Proposition 3.8. *For all $i = 1, \ldots, q^2 - q - 1$ and $j = q^2 - q, \ldots, (q^2 - q)s - 1$ with $s = (m - 1)/(q^2 - q)$, define*

$$S_i = \{i(mq) + (i + k_1)(q^2 - q) + k_3(q^n + 1) \mid k_1 = 1, \ldots, is - i \text{ and } k_3 = 0, \ldots, q - 1\},$$

$$S_j = \{j(mq) + (j + k_2)(q^2 - q) + k_3(q^n + 1) \mid 1 \leq k_2 \leq (q^2 - q)s - j,\ 0 \leq k_3 \leq q - 1\}.$$

Then

1. *S_i, $S_j \subset H_1 \setminus S$;*
2. *$\{S_i\}_i$ and $\{S_j\}_j$ are families of mutually disjoint sets; we also have $S_i \cap S_j = \emptyset$ for all i, j in the corresponding ranges;*
3. *$|S_i| = (is - i)q$ and $|S_j| = ((q^2 - q)s - j)q$.*

Proof.
1. If $x \in S_i$ then $x = i(mq) + (i + k_1)(q^2 - q) + k_3(q^n + 1) = i(mq + \frac{i+k_1}{i})(q^2 - q) + k_3(q^n + 1)$ with $\frac{i+k_1}{i} \leq s$, so $x \in H_1$. Moreover $k_1 > 0$ and we get $x \notin S$. The same argument can be used for S_j.
2. If $i(mq) + (i + k_1)(q^2 - q) + k_3(q^n + 1) = j(mq) + (j + k_2)(q^2 - q) + k_3'(q^n + 1)$, by Remark 3.6, we have $i = j$, $k_3 = k_3'$ and consequently $k_1 = k_2$. In the same way it can be proved that the families are disjoint.
3. From 1. and 2., we get the cardinality of S_i (respectively S_j) simply multiplying the number of possibilities for k_1 (respectively k_2) by those for k_3.

□

Figure 1 describes the sets S_i and S_j for $q = 2$ and $n = 5$. In this picture a point with coordinates (a, b) is used to represent the element $amq + b(q^2 - q) + c(q^n + 1)$ for some $0 \leq c \leq q - 1$. Black dots represent elements of the numerical semigroup S, while white dots represent the elements contained in S_i and S_j for some i and j.

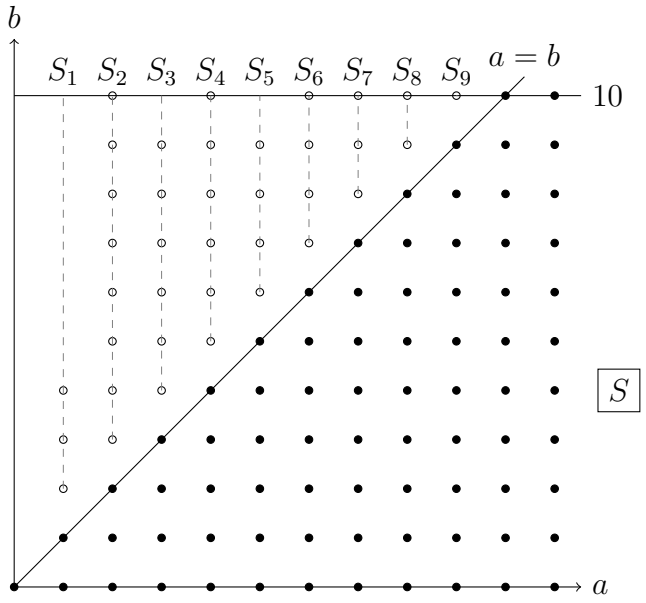

FIGURE 1. The sets S_i, S_j and S for $q = 2$ and $n = 5$
$\circ$: Elements in S_i and S_j $\bullet$: Elements in S

We are in a position to prove our claim.

Theorem 3.9. *We have $g(H_1) = g$. In particular $H_1 = H(P_1)$.*

Proof. By Proposition 3.8 we obtain the upper bound,

$$g(H_1) \leq g(S) - \sum_{i=1}^{q^2-q-1} (is - i)q - \sum_{j=q^2-q}^{(q^2-q)s-1} ((q^2 - q)s - j)q.$$

Thus we get

$$\begin{aligned} g(H_1) &\leq g(S) - \sum_{i=1}^{q^2-q-1} (is-i)q - \sum_{j=q^2-q}^{(q^2-q)s-1} ((q^2-q)s-j)q \\ &= g(S) - \frac{1}{2}q(-1-q+q^2)(-q+q^2)(-1+s) - \sum_{k=1}^{(q^2-q)s-(q^2-q)} kq \\ &= g(S) - \frac{1}{2}q(-1-q+q^2)(-q+q^2)(-1+s)+ \\ &\quad - \frac{1}{2}q(q-q^2+(-q+q^2)s)(1+q-q^2+(-q+q^2)s) \\ &= g(S) - \frac{1}{2}q(-1-q+q^2)(-q+q^2)(-1+s)+ \\ &\quad - \frac{1}{2}q(q^2-q)(s-1)(1+(q^2-q)(s-1)) \\ &= g(S) - \frac{1}{2}(-1+q)^2q^3(-1+s)s. \end{aligned}$$

Now, using that $s = \frac{m-1}{q^2-q}$ together with Lemma 3.5,

$$\begin{aligned} g(H_1) &\leq g(S) - \frac{1}{2}q(m-q^2+q-1)(m-1) \\ &= \frac{1}{2}((2-3m+m^2)q+(-1+m)q^2-q^n+q^{n+1}) \\ &\quad - \frac{1}{2}q(m-q^2+q-1)(m-1). \end{aligned}$$

Finally,

$$\begin{aligned} g(H_1) &\leq \frac{1}{2}(mq^3-mq+q-q^3-q^n+q^{n+1}) \\ &= \frac{1}{2}(\frac{q^{n+1}}{q+1}q(q^2-1)+q-q^3-q^n+q^{n+1}) \\ &= \frac{1}{2}(q^{n+2}+q^2-q^3-q^n) \\ &= \frac{1}{2}(-1+q)(-q^2+q^n+q^{1+n}) = g. \end{aligned}$$

□

4. Weierstrass semigroup at points in O_2

The second orbit of $\mathbb{F}_{q^2}$-rational points of $\mathcal{GK}_{2,n}$ is $O_2 = \mathcal{GK}_{2,n}(\mathbb{F}_{q^2})\backslash O_1 = \{R_1, \ldots, R_{q^3-q}\}$, that is, O_2 is the set of the $\mathbb{F}_{q^2}$-rational affine points of $\mathcal{GK}_{2,n}$. As already mentioned, the corresponding places are totally ramified in the function fields extension $\mathbb{F}_{q^{2n}}(x,y,z)/\mathbb{F}_{q^{2n}}(x,y)$; see Proposition 2.2. Let α be a given $(q+1)$-th root of -1 in

$\mathbb{F}_{q^2}$ and let R be the point

$$R = (0 : a : 0 : 1).$$

Note that R is in O_2. In fact $a^{q^2-1} = a^{2(q+1)} = 1$ and $R \in \mathcal{GK}_{2,n}$. Denote by $\bar{R}$ the point

$$\bar{R} = (0 : a : 1).$$

Clearly, $\bar{R}$ is an affine $\mathbb{F}_{q^2}$-rational point of the Hermitian curve $\mathcal{H}_q$ and looking at the corresponding places, $R \mid \bar{R}$ in the function fields extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(x, y)$. As for the previous case, we can take R to be a representative in O_2 because $H(R) = H(Q)$ for every $Q \in O_2$.

Lemma 4.1. *$q^n + 1 - k \in H(R)$ for all $k = 0, \ldots, \frac{m-1}{q^2-q}$.*

Proof. Let t_R be the tangent line in $\bar{R}$ at $\mathcal{H}_q$. Then $t_R : Y - a = 0$,

$$(y - a)_{\mathbb{F}_{q^{2n}}(x,y)} = (q + 1)\bar{R} - \sum_{i=1}^{q+1} \bar{P}_i,$$

and hence the divisor of $y - a$ in $\mathbb{F}_{q^{2n}}(x, y, z)$ is

$$(y - a) = m(q + 1)R - m\sum_{i=1}^{q+1} P_i = (q^n + 1)R - m\sum_{i=1}^{q+1} P_i.$$

Define the algebraic function

$$f_k = \frac{z^k}{y - a},$$

where z is defined as in Lemma 2.3 and $k = 0, \ldots, (m - 1)/(q^2 - q)$. We get,

$$\begin{aligned}(f_k) &= k \sum_{\substack{Q \in \mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}}) \setminus H \\ Q \neq R}} Q + kR - k(q^2 - q)\sum_{i=1}^{q+1} P_i - (q^n + 1)R + m\sum_{i=1}^{q+1} P_i \\ &= E - (q^n + 1 - k)R,\end{aligned}$$

where E is an effective divisor. The claim now follows. □

Lemma 4.2. *$mq = q^n + 1 - m \in H(R)$.*

Proof. Since $T^{q+1} + 1 \in \mathbb{F}_{q^2}[T]$ has $q + 1$ distinct zeros in $\mathbb{F}_{q^2}$, the function x has $q + 1$ affine zeros in $\mathbb{F}_{q^{2n}}(x, y)$, namely the points $(0 : \alpha : 1)$ with $\alpha^{q+1} = -1$. Thus,

$$(x)_{\mathbb{F}_{q^{2n}}(x,y)} = \bar{R} + \sum_{\alpha^{q+1}=-1, \alpha \neq a} \bar{R}_{(0:\alpha:0:1)} - \sum_{i=1}^{q+1} \bar{P}_i,$$

and hence

$$(x) = mR + m \sum_{\alpha^{q+1}=-1, \alpha \neq a} R_{(0:\alpha:0:1)} - m\sum_{i=1}^{q+1} P_i.$$

Let $f = x/(y-a)$. Then,

$$\begin{aligned}(f) &= mR + m \sum_{\alpha^{q+1}=-1, \alpha \neq a} R_{(0:\alpha:0:1)} - m \sum_{i=1}^{q+1} R_i^{\infty} - (q^n+1)R + m \sum_{i=1}^{q+1} R_i^{\infty} \\ &= m \sum_{\alpha^{q+1}=-1, \alpha \neq a} R_{(0:\alpha:0:1)} - (q^n + 1 - m)R,\end{aligned}$$

proving the statement. □

We are going to prove the following theorem, which is the main result of this section.

Theorem 4.3. *The semigroup*

$$H(R) = \langle q^n + 1 - m, A_2 \rangle, \quad \text{for} \quad A_2 := \{q^n + 1 - k \mid k = 0, \ldots, \frac{m-1}{q^2-q}\}$$

for every $R \in O_2$.

In order to prove Theorem 4.3, we proceed in a different way with respect to Section 3. Indeed this time we will determine the set of gaps $G(R)$ in R instead of $H(R)$. Doing so, we will then show that $H(R) = \mathbb{N} \setminus G(R)$ is exactly the semigroup $\langle q^n+1-m, q^n+1-k \mid k = 0, \ldots, (m-1)/(q^2-q) \rangle$.

4.1. **Holomorphic differentials and gaps.** We first recall some basic facts about holomorphic differentials on algebraic curves and function fields. A differential w on a function field $\mathbb{K}(x,y)$ is said to be *holomorphic* if $(w) \geq 0$, see [20] for details. For a divisor D we set $\Omega(D) := \{w \mid w \text{ differential and } (w) \geq D\}$, so $\Omega(0)$ denotes the set of all holomorphic differentials. It is known that $\Omega(0)$ is a $\mathbb{K}$-vector space, with $\dim \Omega(0) = g$, where $g = g(\mathbb{K}(x,y))$, see [20, Remark 1.5.12].

The main ingredient that we use to compute $G(R)$ is given by the following result.

Proposition 4.4. [22, Corollary 14.2.5]. *The integer $n \in \mathbb{N}$ is a gap at a place P of $\mathbb{K}(x,y)$ if and only if there exists an holomorphic differential ω in $\mathbb{K}(x,y)$ such that*

$$\omega \in \Omega((n-1)P) \quad \text{and} \quad \omega \notin \Omega(nP).$$

In other words, n is a gap at P if and only if there exists an holomorphic differential ω such that

$$v_P(\omega) = n - 1.$$

According to this proposition, since $|G(R)| = g(\mathcal{GK}_{2,n}) = \dim \Omega(0)$, our aim is to construct a basis for $\Omega(0)$ made by a class of holomorphic differentials having all distinct evaluations in R.

First, we show that the function z is a separating variable in the function field of the curve $\mathcal{GK}_{2,n}$ so that every differential of $\mathbb{F}_{q^{2n}}(x,y,z)$ can be written as $f dz$ for some f in $\mathbb{F}_{q^{2n}}(x,y,z)$, see [20, Proposition 4.1.8 (a)].

By Lemma 2.3,

$$(dz) = (q^{n+1} - q^n - q^2 + 2q - 2)\sum_{i=1}^{q+1} P_i = \frac{2g(\mathcal{GK}_{2,n}) - 2}{(q+1)}\sum_{i=1}^{q+1} P_i$$

and z is a separating variable from [20, Proposition 4.1.8 (c)].

We also observe that a differential fdz is holomorphic if and only if for every $P \in \mathcal{GK}_{2,n}$ we have $v_P(f) \geq -v_P(dz)$. Thus, by definition, fdz is holomorphic if and only if

$$f \in \mathscr{L}(dz) = \mathscr{L}((q^{n+1} - q^n - q^2 + 2q - 2)\sum_{i=1}^{q+1} P_i),$$

where $\mathscr{L}(dz)$ denotes the Riemann-Roch space of the divisor (dz). Then we can construct an holomorphic differential fdz provided that f has only P_i $(i = 1\ldots, q+1)$ as poles, with multiplicity less than or equal to $q^{n+1} - q^n - q^2 + 2q - 2$.

From Section 3,

$$(z) = \sum_{\substack{P \in \mathcal{GK}_{2,n}(\mathbb{F}_{q^2}) \\ P \notin \{P_1,\ldots,P_{q+1}\}}} P - (q^2 - q)\sum_{i=1}^{q+1} P_i,$$

$$(x) = mR + m\sum_{\alpha^{q+1}=-1, \alpha \neq a} R_{(0:\alpha:0:1)} - m\sum_{i=1}^{q+1} P_i,$$

$$(y-a) = m(q+1)R - m\sum_{i=1}^{q+1} P_i = (q^n+1)R - m\sum_{i=1}^{q+1} P_i.$$

Consider the family of differentials

$$\mathrm{I} := \{f_{j,k,l}dz \mid 0 \leq k \leq m-1,\ 0 \leq l \leq q,\ 0 \leq j \leq q^2 - 2 \text{ with } k(q^2-q) + (j+l)m \leq q^{n+1} - q^n - q^2 + 2q - 2\},$$

where

$$f_{j,k,l} = z^k(y-a)^j x^l.$$

Lemma 4.5. *The family* I *satisfies the following properties.*

1. $\mathrm{I} \subseteq \Omega(0)$.
2. *Let* $f_{j,k,l}dz \in \mathrm{I}$. *Then* $v_R(f_{j,k,l}dz) = v_R(f_{j,k,l}) = k + (q^n+1)j + lm$.
3. *If* $f_{j,k,l}dz, f_{\tilde{j},\tilde{k},\tilde{l}} \in \mathrm{I}$ *with* $v_R(f_{i,j,k}dz) = v_R(f_{\tilde{i},\tilde{j},\tilde{k}}dz)$ *then* $(i,j,k) = (\tilde{i},\tilde{j},\tilde{k})$.

Proof. (1) We want to show that $f_{j,k,l} \in \mathscr{L}((q^{n+1} - q^n - q^2 + 2q - 2)\sum_{i=1}^{q+1} R_i^\infty)$ for all $0 \leq k \leq m-1$, $0 \leq l \leq q$, $0 \leq j \leq q^2 - 2$ with $k(q^2-q) + (j+l)m \leq$

$q^{n+1}-q^n-q^2+2q-2$. We observe that with j, k and l fixed,

$$\begin{aligned}(f_{j,k,l}) &= (z^k(y-a)^j x^l)\\ &= k \sum_{\substack{Q\in\mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}})\setminus H\\ Q\neq R}} Q + kR - k(q^2-q)\sum_{i=1}^{q+1} P_i + lmR +\\ &+ lm \sum_{\substack{\alpha^{q+1}=-1\\ \alpha\neq a}} R_{(0:\alpha:0:1)} - lm\sum_{i=1}^{q+1} R_i^\infty + j(q^n+1)R - jm\sum_{i=1}^{q+1} R_i^\infty\\ &= E + (k+lm+j(q^n+1))R - (k(q^2-q)+lm+jm)\sum_{i=1}^{q+1} P_i,\end{aligned}$$

where E is an effective divisor whose support is disjoint from $\{R, P_1, \dots, P_{q+1}\}$. By definition, $f_{j,k,l} \in \mathscr{L}((q^{n+1}-q^n-q^2+2q-2)\sum_{i=1}^{q+1} P_i)$ if and only if $f_{j,k,l}$ has poles only in $\{P_i\}_i$ with multiplicity at most $q^{n+1}-q^n-q^2+2q-2$. This is equivalent to require that $k(q^2-q)+lm+jm \leq q^{n+1}-q^n-q^2+2q-2$, which is satisfied by construction. We show that the bound considered for j, k, l is not in contradiction with the previous inequality. Actually we have

$$\left\lfloor \frac{q^{n+1}-q^n-q^2+2q-2}{m} \right\rfloor = q^2-1-\left\lceil \frac{q^2-q+1}{m} \right\rceil = q^2-2,$$

that is the greatest value for j (note that it is strictly greater than the greatest value reached by l). Also,

$$\left\lfloor \frac{q^{n+1}-q^n-q^2+2q-2}{q^2-q} \right\rfloor = q^{n-1}-1 > m-1 = q\frac{q^{n-1}-1}{q+1}.$$

(2) It follows directly by the computation of the divisor of $f_{i,j,k}$, as $v_R(dz)=0$.

(3) Suppose that

$$k+(q^n+1)j+lm = v_R(f_{i,j,k}dz) = v_R(f_{\tilde{i},\tilde{j},\tilde{k}}dz) = \tilde{k}+(q^n+1)\tilde{j}+\tilde{l}m.$$

By considering the above equality modulo m, and using that k and $\tilde{k}$ are at most $m-1$ we obtain $k=\tilde{k}$. We need to show that

$$(q+1)j+l = (q+1)\tilde{j}+\tilde{l}.$$

As before, consider the equality modulo $q+1$. We have that l and $\tilde{l}$ are less than or equal to q, so $l=\tilde{l}$. Clearly at this point $j=\tilde{j}$ and this proves the statement.

□

Corollary 4.6. *We have that*

$$\begin{aligned}L := \{k+(q^n+1)j+lm+1 \mid\ & 0\leq k\leq m-1,\ 0\leq l\leq q,\ 0\leq j\leq q^2-2 \text{ and}\\ & k(q^2-q)+(j+l)m \leq q^{n+1}-q^n-q^2+2q-2\} \subseteq G(R).\end{aligned}$$

Moreover, the differentials $f_{j,k,l}dz$ are linearly independent over $\mathbb{F}_{q^{2n}}$, as they have all distinct evaluations in R.

The following observation explains our next step.

Observation 4.7. If we show that for a subset $L \subseteq G(R)$,

$$|L| = g(\mathcal{GK}_{2,n}) = (q-1)(q^{n+1}+q^n-q^2)/2$$

then

- $L = G(R)$,
- I is a $\mathbb{F}_{q^{2n}}$-basis for the vector space $\Omega(0)$ of $\mathcal{GK}_{2,n}$.

According to Observation 4.7, we only need to show that L contains exactly $g(\mathcal{GK}_{2,n})$ elements. Doing so, the following theorem is established.

Theorem 4.8. *Let q be a prime power and $n \geq 5$ odd. Let also R be an affine $\mathbb{F}_{q^2}$-rational point of the curve $\mathcal{GK}_{2,n}$. Let L be the set*

$$L = \{k + (q^n+1)j + lm + 1 \mid 0 \leq k \leq m-1,\ 0 \leq l \leq q,\ 0 \leq j \leq q^2-2 \text{ with } k(q^2-q) + (j+l)m \leq q^{n+1} - q^n - q^2 + 2q - 2\}.$$

Then we have

$$|L| = g(\mathcal{GK}_{2,n}) = \frac{1}{2}(q-1)(q^{n+1}+q^n-q^2).$$

In particular, $L = G(R)$.

In order to prove Theorem 4.8 we are going to proceed with a direct computation of the number of distinct elements in L. First, we make clear the range of the entries of (k,l,j) for elements in L.

Observation 4.9. Note that if k could always reach the value $m-1$, the set L would be the whole $\mathbb{N}$. As a matter of fact, we can move from $h \in L$, with associated value (k,l,j), to $h+1$ simply putting $k=0$ and by replacing l (or j) with $l+1$ (or $j+1$). This clearly cannot be possible by the bound $k(q^2-q)+(j+l)m \leq q^{n+1}-q^n-q^2+2q-2$. However when $k_{max}(j,l)$ coincides with $m-1$ then from $(q^n+1)j+lm$ to $(q^n+1)j+(l+1)m$ there are not non-gaps.

For the sake of simplicity, in the following we identify an element in L with the associated triple (k,l,j). Also k_{max} always denotes $k_{max} := k_{max}(l+j)$.

Lemma 4.10. *Let (k,l,j) be in L, then $j+l < q^2-1$ for all $k \geq 0$.*

Proof. Suppose that $j+l \geq q^2-1$. Then

$$\begin{aligned}(j+l)m &\geq (q^2-1)m \\ &= (q+1)(q-1)\frac{q^n+1}{q+1} \\ &= (q-1)(q^n+1) \\ &= q^{n+1}-q^n+q-1 > q^{n+1}-q^n-q^2+2q-2.\end{aligned}$$

In the last equation we used that $q^2-q+1>0$ for every integer q. □

Lemma 4.11. *Let (k,l,j) be in L with $j+l<q-1$. Then $k_{max}=m-1$.*

Proof. By direct computation,

$$\begin{aligned}(m-1)(q^2-q)+(q-2)m &= mq^2-q^2-mq+q+mq-2m \\ &= m(q^2-2)-q(q-1) \\ &< m(q^2-1)-q(q-1) = (q^n+1-q)(q-1) \\ &= q^{n+1}-q^n-q^2+2q-1.\end{aligned}$$

Hence $(m-1)(q^2-q)+(q-2)m \leq q^{n+1}-q^n-q^2+2q-2$ and the claim follows. □

Lemma 4.12. *Let (k,l,j) be in L. Then $k_{max}=m-1-(s(j+l-q+1)+1)$ for all $q-1\leq j+l<q^2-1$.*

Proof. Let $\bar{k}=m-1-(s(j+l-q+1)+1)$. We note that if $j+l\geq q-1$ then $\bar{k}\leq m-2$. If on the contrary $j+l<q^2-1$, then

$$\begin{aligned}\bar{k}(q^2-q)+(j+l)m &< (m-1-(s(q^2-1-q+1)+1))(q^2-q)+(q^2-1)m \\ &= (m-2-s(q^2-q))(q^2-q)+(q^2-1)m \\ &= (m-2-m+1)(q^2-q)+m(q+1)(q-1) \\ &= -q(q-1)+(q^n+1)(q-1) \\ &= (q-1)(q^n+1-q) = q^{n+1}-q^n-q^2+2q-1.\end{aligned}$$

So we prove that $\bar{k}(q^2-q)+(j+l)m \leq q^{n+1}-q^n-q^2+2q-2$. Using that $j+l\geq q-1$, we get

$$\begin{aligned}(\bar{k}+1)(q^2-q)+(j+l)m &\geq (m-1-s(q-1-q+1))(q^2-q)+(q-1)m \\ &= (m-1)(q^2-q)+m(q-1) \\ &= m(q^2-1)-q(q-1) \\ &= (q^n-q+1)(q-1) = q^{n+1}-q^n-q^2+2q-1,\end{aligned}$$

and thus $(\bar{k}+1)(q^2-q)+(j+l)m > q^{n+1}-q^n-q^2+2q-2$, proving that $\bar{k}=k_{max}$. □

Observation 4.13. The value k_{max} depends on the sum of j and l, i.e. $k_{max}(j,l) = k_{max}(j+l)$.

We are now in a position to prove Theorem 4.8.

Proof, Theorem 4.8. Let $M_q = q^{n+1} - q^n - q^2 + 2q - 2$. Then L can be described as follows

$$L := \{k + (q^n+1)j + lm + 1 \mid 0 \le k \le k_{max},\ 0 \le l \le q,\ 0 \le j + l \le q^2 - 2 : \\ k(q^2-q) + (j+l)m \le M_q\}.$$

From Lemma 4.11 and Lemma 4.12 we can partition L into two subsets

$$L_1 := \{k+(q^n+1)j+lm+1 \mid 0 \le k \le m-1,\ 0 \le j+l \le q-2\ :\ k(q^2-q)+(j+l)m \le M_q\}$$

and

$$L_2 := \{k + (q^n+1)j + lm + 1 \mid 0 \le k \le k_{max},\ 0 \le l \le q, \\ q - 1 \le j + l \le q^2 - 2\ :\ k(q^2-q) + (j+l)m \le M_q\}.$$

Since every element of L is uniquely determined by (k,l,j), we just need to compute the number of triples which are contained in L_1 and L_2.

- *The computation of* $|L_1|$. We note that k_{max} in L_1 does not depend on l and j. Let l be fixed. Then we have m choices for k, while $j = 0, \dots, q-2-l$. Thus,

$$|L_1| = \sum_{l=0}^{q-2} m(q-l-1) = m\frac{q(q-1)}{2}.$$

- *The computation of* $|L_2|$. We distinguish two cases, namely $l \le q-1$ and $l = q$. If $l \le q-1$, then $j = q-1-l, \dots, q^2-2-l$; while in the latter case $j = 0, \dots, q^2-2-l$. Suppose now that (l,j) is fixed. Repeating the previous argument we note that at each step $k = 0, \dots, m-2-s(j+l-q+1)$; so we have $m-1-s(j+l-q+1)$

choices for k . By adding up for every value of l and j, we obtain

$$\begin{aligned}
|L_2| &= \sum_{l=0}^{q-1} \sum_{j+l=q-1}^{q^2-2} (m-1-s(j+l-q+1)) + \sum_{j=0}^{q^2-q-2} (m-1-s(j+1)) \\
&= \sum_{l=0}^{q-1} ((q^2-q)(m-1) - s\frac{(q^2-q)(q^2-q-1)}{2}) + \\
&\quad + \sum_{j=0}^{q^2-q-2} (m-1-s(j+1)) \\
&= \frac{1}{2}q(q^2-q)(2(m-1)-s(q^2-q-1)) + \sum_{j=0}^{q^2-q-2} (m-1-s(j+1)) \\
&= \frac{1}{2}q(q^2-q)(2(m-1)-s(q^2-q-1)) + ((q^2-q-1)(m-1) + \\
&\quad - \frac{1}{2}s(q^2-q)(q^2-q-1)) \\
&= \frac{1}{2}q(q^2-q)(2(m-1)-s(q^2-q-1)) + \\
&\quad + \frac{1}{2}(q^2-q-1)(2(m-1)-s(q^2-q)).
\end{aligned}$$

Putting $m-1 = s(q^2-q)$ in the equation we have

$$\begin{aligned}
|L_2| &= \frac{1}{2}q(q^2-q)s(2q^2-2q-q^2+q+1) + \frac{1}{2}(q^2-q-1)s(q^2-q) \\
&= \frac{1}{2}q(q^2-q)s(q^2-q+1) + \frac{1}{2}(q^2-q-1)s(q^2-q) \\
&= \frac{1}{2}s(q^2-q)(q^3-q^2+q+q^2-q-1) = \frac{1}{2}(m-1)(q^3-1).
\end{aligned}$$

Hence,

$$\begin{aligned}
|L| = |L_1| + |L_2| &= \frac{1}{2}mq(q-1) + \frac{1}{2}(m-1)(q-1)(q^2+q+1) \\
&= \frac{1}{2}(q-1)(mq+mq^2+mq+m-q^2-q-1) \\
&= \frac{1}{2}(q-1)(m(q+1)+m(q)(q+1)-q^2-q-1) \\
&= \frac{1}{2}(q-1)(q^n+1+(q^n+1)(q)-q^2-q-1) \\
&= \frac{1}{2}(q-1)(q^{n+1}+q^n-q^2) = g(\mathcal{GK}_{2,n}),
\end{aligned}$$

proving the statement. □

5. On the Frobenius dimension of $\mathcal{GK}_{2,n}$

In this section we investigate the Frobenius dimension of the curves $\mathcal{GK}_{2,n}$. In particular, we are interested in comparing it with the Frobenius dimension of the first generalized GK curve $\mathcal{GK}_{2,n}$.

Recall that for any $\mathbb{F}_{q^{2n}}$-maximal curve $\mathcal{X}_n$, the Fundamental Equation (3.2) is written as

$$q^n P + \Phi^{2n}(P) \equiv (q^n+1)P_0,$$

where $P \in \mathcal{X}_n$, $P_0 \in \mathcal{X}_n(\mathbb{F}_{q^{2n}})$ and Φ is the Frobenius automorphism.

The complete linear series given by $\mathcal{D} := |\ (q^n+1)P_0\ |$ is said to be the *Frobenius linear series* of $\mathcal{X}_n$ and $r := \dim \mathcal{D}$ is the *Frobenius dimension* of $\mathcal{X}_n$. This dimension is one of the most important (birational) invariants of a maximal curve.

The following proposition allows us to easily compute the Frobenius dimension of any maximal curve, see [11, Section 10.2].

Proposition 5.1. [11, Propositions 10.6 and 10.9] *Let $\mathcal{X}_n$ be an $\mathbb{F}_{q^{2n}}$-maximal curve having Frobenius dimension r. Let P be an $\mathbb{F}_{q^{2n}}$-rational point of $\mathcal{X}_n$. Then the following holds.*

1. *The Frobenius dimension r coincides with the number of non-trivial non-gaps at P which are less than or equal to q^n, i.e.*
$$0 < m_1(P) < \cdots < m_{r-1}(P) \leq q < m_r(P).$$
2. *$r \geq 2$ holds. If $r \geq 3$ and $m_{r-2}(P) < q^n - 1$, then P is a Weierstrass point of $\mathcal{X}_n$.*

The following theorem is obtained using the results of Sections 3 and 4 together with Proposition 5.1.

Theorem 5.2. *Let q be a prime power and $n \geq 5$ an odd integer. The Frobenius dimension of the second generalized GK curves $\mathcal{GK}_{2,n}$ is*

$$r = \frac{m-1}{q^2-q} + 2, \text{ where } m = \frac{q^n+1}{q+1}.$$

We now show two applications of Theorem 5.2.

It is known that if $H(P)$ is symmetric for $P \in \mathcal{GK}_{2,n}$, that is, $2g-1 \in G(P)$, then P is a Weierstrass point of $\mathcal{GK}_{2,n}$; see [15, Proposition 50]. However, the converse is not necessarily true. The results obtained in Sections 3 and 4 together with Theorem 5.2 allow us to provide a counterexample.

Corollary 5.3. *If $P \in \mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}})$ then P is a Weierstrass point of $\mathcal{GK}_{2,n}$. In particular, if $P \in O_1 \cup O_2$ then $H(P)$ is not symmetric even though P is a Weierstrass point of $\mathcal{GK}_{2,n}$.*

Proof. The fact that $H(P)$ is not symmetric follows from a direct computation from Theorems 3.4 and 4.3. The claim regarding the points in $\mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}})$ follows from [4, Corollary 4.5.] and Theorem 5.2 noting that $q^n + 1 - r < g(\mathcal{GK}_{2,n})$. □

Theorem 5.2 has also the following second application. It allows us to exhibit another way to prove that the curves $\mathcal{GK}_{2,n}$ and $\mathcal{GK}_{1,n}$ are not isomorphic for any $n \geq 5$ odd. Indeed in [2, Corollary 2.6], the authors proved the following theorem.

Theorem 5.4. *Let q be a prime power and $n \geq 3$ be odd. Then $\mathcal{GK}_{2,n}$ is isomorphic to $\mathcal{GK}_{1,n}$ if and only if $n = 3$.*

In order to prove Theorem 5.4 Beelen and Montanucci made use of the theory of automorphism groups of algebraic curves. In fact, since the full automorphism group of an algebraic curve is invariant under (birational) isomorphisms, it is sufficient to note that $\mathrm{Aut}(\mathcal{GK}_{1,n}) \neq \mathrm{Aut}(\mathcal{GK}_{2,n})$, see [2] and [9, 8].

We instead are going to compute the Frobenius dimension of the curves $\mathcal{GK}_{1,n}$ and compare it with the value obtained in Theorem 5.2.

Remember that the function field of $\mathcal{GK}_{1,n}$ is the compositum of the function fields $\mathbb{F}_{q^{2n}}(x, y)$ and $\mathbb{F}_{q^{2n}}(y, z)$, where x, y and z satisfy Equation (2.1). Let P_∞ denote the common pole of x, y and z. In [8], the following result is proved.

Proposition 5.5. *The set of non-gaps at P_∞ in $\mathcal{GK}_{1,n}$ is*

$$\{i(q^n + 1) + jmq + kq^3 \mid i, j, k \in \mathbb{N} \text{ with } 0 \leq i \leq q,\ 0 \leq j \leq q^2,\ k \geq 0\}.$$

As for the curve $\mathcal{GK}_{2,n}$ we can now compute the Frobenius dimension of $\mathcal{GK}_{1,n}$.

Corollary 5.6. [19, Corollary 3.43] *The Frobenius dimension of the $\mathcal{GK}_{1,n}$ curve is equal to*

$$r' = q^{n-3} + \sum_{i=2}^{n-2} (-1)^{i+1} q^i + 1.$$

Finally, we show how this computation allows us to obtain another proof of Theorem 5.4.

Theorem 5.7. *Let q denote a prime power and $n \geq 3$ an odd integer. For a fixed n, let $\mathcal{GK}_{1,n}$ and $\mathcal{GK}_{2,n}$ be the first and the second generalized GK curve respectively. Then $\mathcal{GK}_{1,n}$ and $\mathcal{GK}_{2,n}$ are not isomorphic for every $n \geq 5$.*

Proof. The proof follows directly by comparing the Frobenius dimensions of $\mathcal{GK}_{1,n}$ and $\mathcal{GK}_{2,n}$. Indeed, we have

$$q^{n-3} + \sum_{i=2}^{n-2} (-1)^{i+1} q^i + 1 \geq q^{n-3} + q^{n-2} - q^{n-3} + 1,$$

and we want to show that

$$
\begin{aligned}
q^{n-3}+q^{n-2}-q^{n-3}+1 &\geq \frac{m-1}{q^2-q}+2\\
&= \frac{\frac{q^n+1}{q+1}-1}{q^2-q}+2\\
&= \frac{q^{n-1}-1}{q^2-1}+2.
\end{aligned}
\tag{5.1}
$$

However, we obtain equation (5.1) by computing

$$
\begin{aligned}
&q^{n-2}+1-\frac{q^{n-1}-1}{q^2-1}-2\\
=&(q^{n-2}-1)(q^2-1)-q^{n-1}+1\\
=&q^n-q^{n-2}-q^{n-1}-q^2+2,
\end{aligned}
\tag{5.2}
$$

which is a positive integer for $n \geq 5$. □

6. Applications to AG codes

In this section we will apply the results obtained in Sections 3 and 4 to construct AG codes and AG quantum codes from the second generalized GK curve. Explicit tables containing the parameters of the resulting codes for $q = 2$ and $n = 5$ can be found in Subsection 6.1.

As before, $\mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}})$ denotes the set of all $\mathbb{F}_{q^{2n}}$-rational points of $\mathcal{GK}_{2,n}$ while $\mathbb{F}_{q^{2n}}(\mathcal{GK}_{2,n})$ denotes the set of $\mathbb{F}_{q^{2n}}$-rational functions on $\mathcal{GK}_{2,n}$. A divisor D is $\mathbb{F}_{q^{2n}}$-rational if it is fixed by the Frobenius endomorphism Φ^{2n}.

We briefly recall the definition of an AG code; see [20, Chapter 2] and [12] for a more detailed description. Let $P_1, \dots P_N \in \mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}})$ be distinct points and consider the divisor $D := P_1 + \cdots + P_N$. Let G be another $\mathbb{F}_{q^{2n}}$-rational divisor whose support is disjoint from that of D. Let e denote the following linear map

$$
\begin{cases}
e\colon \mathscr{L}(G) \to \mathbb{F}_{q^{2n}}^N,\\
\alpha \mapsto e(\alpha) := (\alpha(P_1), \dots, \alpha(P_N)).
\end{cases}
$$

The AG code associated to D and G is $C(D,G) := e(\mathscr{L}(G))$. The code $C(D,G)$ is an $[N,k,d]_{q^{2n}}$-code with $d \geq N - \deg G$ and $k = \ell(G) - \ell(G-D)$. When $G := n_P P$, $n_P \in \mathbb{N}$, then $C(D,G)$ is a *one-point code*. The dual code $C^\perp(D,G)$ is an AG code with dimension $k^\perp := N - k$ and minimum distance $d^\perp \geq \deg G - 2g + 2$, where g is the genus of $\mathcal{GK}_{2,n}$.

Let $P \in \mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}})$ and set

$$H(P) = \{\varrho_1 := 0 < \varrho_2 < \cdots\}$$

the Weierstrass semigroup at P. For $\ell > 0$ the *Feng-Rao function* is defined as

$$\nu_\ell := \mid \{(i,j) \in \mathbb{N}^2 : \varrho_i + \varrho_j = \varrho_\ell\} \mid .$$

Consider now the AG code $C_\ell := C^\perp(P_1 + \cdots + P_N, \varrho_\ell P)$, with $N > \ell + 1$ and $P_1, \ldots, P_N, P$ distinct points.

Proposition 6.1. [12, Theorem 5.24] *C_ℓ is a linear $[N,k,d]_{q^{2n}}$-code with $k = N - \ell$ and $d \geq d_{ORD}(C_\ell)$, where*

$$d_{ORD}(C_\ell) := \min\{\nu_m \mid m \geq \ell\}$$

is the Feng-Rao designed minimum distance.

From [12, Theorem 5.24] we have also the following proposition which shows that, for large values in $H(P)$, d_{ORD} can be easily computed.

Proposition 6.2. *Let $H(P)$ be a Weierstrass semigroup. Then $d_{ORD}(C_\ell(P)) \geq \ell + 1 - g$ and equality holds if $\varrho_\ell + 1 \geq 4g$.*

6.1. **Tables of AG codes.** Here we are going to show how to construct AG dual codes on the curve $\mathcal{GK}_{2,n}$. We examine just the case $q := 2$ and $n := 5$. Consider the set $\mathcal{GK}_{2,5}(\mathbb{F}_{2^{10}})$, with $\mid \mathcal{GK}_{2,5}(\mathbb{F}_{2^{10}}) \mid = 3969$. If we take a point $P \in O_1$, then we have

$$H(P) := \langle mq + i(q^2 - q), q^n + 1 \mid i = 0, \ldots, s \rangle,$$

by Theorem 3.4. Thus, we can calculate the parameters of $C^1_\ell := C^\perp(P_1 + \cdots + P_{3968}, \varrho_\ell P)$. Similarly, fix a point $R \in O_2$. From Theorem 4.3 we know that

$$H(R) = \langle q^n + 1 - m, q^n + 1 - k \mid k = 0, \ldots, (m-1)/(q^2 - q) \rangle.$$

Applying the same argument as above, we can compute the parameters of the AG code $C^2_\ell := C^\perp(P_1 + \cdots + P_{3968}, \varrho_\ell R)$. For the complete table of codes we refer to the ArXiv version of this paper; see [1].

Remark 6.3. In [5, Table 1] dual AG codes from the first generalized GK curves $\mathcal{GK}_{1,n}$ are constructed. As already recalled, the curves $\mathcal{GK}_{1,n}$ and $\mathcal{GK}_{2,n}$ have the same genus. This allows us to compare the codes obtained in this section with the ones constructed from the curves $\mathcal{GK}_{1,n}$. In particular some of the codes C^2_ℓ are shown to have better parameters. The following tables collects some comparisons of our codes from the curve $\mathcal{GK}_{2,n}$ and the ones from the curves $\mathcal{GK}_{1,n}$

n	k	$d_{ORD}(\mathcal{GK}_{1,n})$	$d_{ORD}(\mathcal{GK}_{2,n})$
3968	3910	16	18
3968	3909	16	21
3968	3908	16	24
3968	3907	16	25
3968	3906	22	26
3968	3905	22	27
3968	3904	22	28
3968	3903	22	28
3968	3902	22	28
3968	3901	22	29
3968	3900	24	30
3968	3899	24	30

TABLE 1. AG codes from the first and second generalized GK curves

6.2. **AG quantum codes for the second generalized GK curve.** In this section we construct quantum codes from the curves $\mathcal{GK}_{2,n}$ as an application of the so called *CSS construction* to families of one point AG codes from the curves $\mathcal{GK}_{2,n}$. For more details on quantum codes, we refer the reader to [18, Section 2]. Let q be a prime power. A q-ary quantum code of length N and dimension k is defined to be a Hilbert subspace Q, with $\dim Q = q^k$, of a q^n-dimensional Hilbert space $\mathbb{H} := (\mathbb{C}^q)^{\otimes n} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$. If Q has minimum distance D, we will write $Q = [[N, k, D]]_{q^{2n}}$-code.

Proposition 6.4. [18, Lemma 2.5] *Let C_1 and C_2 be two linear codes with parameters $[N, k_i, d_i]_q$, $i = 1, 2$, and assume that $C_1 \subset C_2$. Then there exists an $[[N, k_2 - k_1, D]]_q$-code with $D = \min\{wt(c) \mid c \in (C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\}$, where $wt(c)$ is the weight of c.*

The construction given in Proposition 6.4 is known as the *CSS construction*. An application can be obtained looking at the dual of the one point codes from the curves $\mathcal{GK}_{2,n}$. Let $P \in \mathcal{GK}_{2,n}$. Consider $C_2 := C_\ell = C(D, G_2)$ and $C_1 := C_{\ell+s} = C(D, G_1)$, where $s \geq 1$, $G_1 = \rho_\ell P$, $G_2 = \rho_{\ell+s} P$ and $D = \sum_{Q \in \mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}}) \setminus \{P\}} Q$. Then we have $C_1 \subset C_2$ and the dimensions of C_1 and C_2 are $k_2 = N - h_\ell$ and $k_1 = N - h_\ell - s$ respectively where h_i denotes the number of non-gaps at P which are smaller than or equal to i and $N = \mid \mathcal{GK}_{2,n}(\mathbb{F}_{q^{2n}}) \mid -1$. Hence $k_1 - k_2 = s$. From Proposition 6.4 this induces an $[[N, s, D]]_{q^{2n}}$-quantum code, where

$$\begin{aligned} D &= \min\{wt(c) \mid c \in (C_2 \setminus C_1) \bigcup (C_1^\perp \setminus C_2^\perp)\} \\ &= \min\{wt(c) \mid c \in (C_\ell \setminus C_{\ell+s}) \bigcup (C(P_1 + \cdots + P_{N-1}, G_1) \setminus C(P_1 + \cdots + P_{N-1}, G_2))\}. \end{aligned}$$

In particular we get

$$D \geq \min\{d_{ORD}(C_\ell), d_1\},$$

where d_1 denotes the minimum distance of the code $C(D, G_1)$.

Hence the following result follows as a corollary of Proposition 6.2.

Corollary 6.5. *Let $g = (q-1)(q^{n+1}+q^n-q^2)/2$ and $N = q^{2n+2} - q^{n+3} + q^{n+2}$. For every $\ell \in [3g-1, N-g]$ and $s \in [1, N-2\ell]$, there exists a quantum code with parameters $[[N, s, D]]_{q^{2n}}$, where $D \geq \ell + 1 - g$.*

Proof. Since there are exactly $g+1$ non-gaps which are less than or equal to $2g$ and $\ell \geq 3g-1$, we have $\rho_{\ell+s} = 2g + (\ell + s - (g+1)) = g - 1 + \ell + s$, and hence $d_1 \geq N - \deg(G_1) = N - \rho_{\ell+s} = N - \ell - s - g + 1$. Also from $\ell \geq 3g-1$ we can apply Proposition 6.2 and Proposition 6.4 to get $D \geq \min\{d_{ORD}(C_\ell), d_1\} = \ell + 1 - g$. The claim follows. □

Using the results of Subsection 6.1 and applying the general strategy written before, AG quantum codes for which Proposition 6.2 does not apply can also be constructed for $q = 2$ and $n = 5$. Indeed assume in general that $\ell \in [g, 3g-1]$. For $s \in [\max\{2g-\ell, 1\}, N-2\ell]$ we have that $\ell + s \geq 2g$ and $d_1 \geq N - \ell - s - g + 1$ as in the proof of Corollary 6.5. If $d_{ORD}(C_\ell) \leq N - \ell - s - g + 1$ then arguing as in Corollary 6.5 there exists a quantum code with parameters $[[N, s, D]]_{q^{2n}}$ where $D \geq d_{ORD}(C_\ell)$. This shows the following proposition.

Proposition 6.6. *Let $\ell \in [g, 3g-1]$ and $s \in [\max\{2g-\ell, 1\}, \min\{N-2\ell, N-\ell-g+1-d_{ORD}(C_\ell)\}]$. Then there exists a quantum code with parameters $[[N, s, D]]_{q^{2n}}$ where $D \geq d_{ORD}(C_\ell)$.*

Using the data collected in Subsection 6.1, the parameters of the AG quantum codes constructed as in Proposition 6.6 can be determined for $q = 2$ and $n = 5$. For more details see [1].

Acknowledgments

This research was partially supported by Ministry for Education, University and Research of Italy (MIUR) (Project PRIN 2012 "Geometrie di Galois e strutture di incidenza" - Prot. N. 2012XZE22K_005) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

References

[1] M. Montanucci, V. Pallozzi Lavorante. AG codes from the second generalization of the GK maximal curve, Preprint arXiv:1901.08897

[2] P. Beelen and M. Montanucci. A new family of maximal curves. *Journal of the London Math. Soc.* **2** (2018), 1–20.

[3] W. Bosma, J. Cannon and C. Playoust. The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.
[4] R. Fuhrmann and F. Torres. On Weierstrass points and optimal curves. *Rend. Circ. Mat. Palermo*, Suppl. **51** (Recent Progress in Geometry E. Ballico and G. Korchmáros Eds.) (1998), 25–46.
[5] A. Garcia, C. Güneri, and H. Stichtenoth. A generalization of the Giulietti-Korchmáros maximal curve. *Advances in Geometry* (10) **3** (2010), 427–434.
[6] M. Giulietti and G. Korchmáros. A new family of maximal curves over a finite field. *Math. Ann.* **343** (2009), 229–245.
[7] V. D. Goppa. *Geometry and Codes*. Mathematics and its Applications (Soviet Series) **24**. Kluwer Academic Publishers Group, Dordrecht, 1988.
[8] C. Güneri, M. Özdemir, and H. Stichtenoth. The automorphism group of the generalized Giulietti-Korchmáros function field. *Adv. Geom.* **13** (2013), 369–380.
[9] R. Guralnick, B. Malmskog, and R. Pries. The automorphism group of a family of maximal curves. *J. Algebra* **361** (2012), 92–106.
[10] C. Heegard, J. Little, and K. Saints. Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes. *IEEE Trans. Inf. Theory* **41** (1995), 1752–1761.
[11] J.W.P. Hirschfeld, G. Korchmáros and F. Torres. *Algebraic Curves over a Finite Field*. Princeton Series in Applied Mathematics, Princeton, 2008.
[12] T. Høholdt, J. H. van Lint, and R. Pellikaan. Algebraic geometry codes. In Handbook of Coding Theory, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier **1** (1998), 871–961.
[13] D. Joyner. An error-correcting codes package. *SIGSAM Comm. Computer Algebra* **39** (2) (2005), 65–68.
[14] S.L. Kleiman. *Algebraic cycles and the Weil conjectures*, in: Dix exposés sur la cohomologie des schémas, in: Adv. Stud. Pure Math. **3** (1968), 359–386.
[15] S. Karanikolopoulos and A. Kontogeorgis. Automorphisms of curves and Weierstrass semigroups. Preprint, arXiv:1005.2871.
[16] H.G. Rück and H. Stichtenoth. A characterization of the Hermitian function fields over finite fields. *J. Reine Angew. Math.* **457** (1994), 185–188.
[17] K.O. Stöhr and J.F. Voloch. Weierstrass points and curves over finite fields. textitProc. London Math. Soc. **52**(3) (1986), 1–19.
[18] G. G. La Guardia and F. R. F. Pereira. Good and asymptotically good quantum codes derived from Algebraic geometry codes. Preprint, arXiv:1612.07150.
[19] P. Speziali. *Quotient Curves in Positive Characteristic*. Master Degree Thesis. Universitá degli Studi di Perugia, 2014.
[20] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer, 2009.
[21] M.A. Tsfasman and G. Vladut. *Algebraic-geometric Codes*. Kluwer, Dordrecht, 1991.
[22] G.D.V. Salvador. *Topics in the theory of algebraic function fields*. Mathematics: Theory and Applications. Birkhäuser Boston, Inc., Boston, 2006.

Maria Montanucci

Technical University of Denmark,
Department of Applied Mathematics and Computer Science,
Kongens Lyngby, Denmark,
marimo@dtu.dk

Vincenzo Pallozzi Lavorante

Università degli Studi di Modena e Reggio Emilia,
Dipartimento di Matematica Pura e Applicata,
Via Giuseppe Campi 213/b, 41125 Modena, Italy,
vincenzo.pallozzi.lavorante@gmail.com