NEAR ORDERS AND CODES

C. CARVALHO, C. MUNUERA, E. SILVA, AND F. TORRES

Abstract. Høholdt, van Lint and Pellikaan used order functions to construct codes by means of Linear Algebra and Semigroup Theory only. However, Geometric Goppa codes that can be represented by this method are mainly those based on just one point. In this paper we introduce the concept of near order function with the aim of generalize this approach in such a way that a of wider family of Geometric Goppa codes can be studied on a more elementary setting.

1. Introduction

Geometric Goppa codes (or GG codes, for short) were constructed by Goppa [6], [7] based on a curve $\mathcal{X}$ over a finite field $\mathbb{F}$, and two $\mathbb{F}$-rational divisors D and G on $\mathcal{X}$. Here, by a *curve* we mean a projective, geometrically irreducible, non-singular algebraic curve. Usually the divisors D and G are chosen as

- $D = P_1 + \ldots + P_n$;
- $G = \alpha_1 Q_1 + \ldots + \alpha_\ell Q_\ell$,

where the P_i's and Q_j's are pairwise different $\mathbb{F}$-rational points of $\mathcal{X}$. Then, there are two GG codes associated to the triple $(\mathcal{X}, D, G)$, defined as the images $C_{\mathcal{L}} = C_{\mathcal{L}}(\mathcal{X}, D, G)$ and $C_\Omega = C_\Omega(\mathcal{X}, D, G)$ of the maps

$$ev : f \in \mathcal{L}(G) \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}^n \quad \text{and}$$

$$res : \omega \in \Omega(G - D) \mapsto (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)) \in \mathbb{F}^n$$

Keywords and Phrases: Error-correcting codes, algebraic geometric Goppa codes, Weierstrass semigroups, order function.

2000 Math. Subj. Class.: 94B27; 14G50.

The work of C. Carvalho was partially supported by FAPEMIG, grant CEX 605/05; research done under a joint project of the Millennium Institute for the Global Advancement of Brazilian Mathematics (IM-AGIMB) and Universidade Federal de Uberlândia (UFU).

The work of C. Munuera was supported by the "Junta de Castilla y León", España, under Grant VA020-02.

The work of E. Silva was partially supported by FAPEMIG; this paper is based on his Ph.D dissertation [21] done at IMECC-UNICAMP, SP-Brazil.

The work of F. Torres was supported by CNPq-Brazil (306676/03-6) and PRONEX (66.2408/96-9).

This paper will be published elsewhere.

respectively. According to the residue theorem, these codes are dual to the other, $C_{\mathcal{L}} = C_{\Omega}^{\perp}$, hence both constructions provide the same family of codes. Bounds on the dimension and minimum distance of such codes are available from their definition, as they satisfy $k = \ell(G) - \ell(G-D)$, $d \geq n - \deg(G)$ for $C_{\mathcal{L}}$ and $k = i(G-D) - i(G)$, $d \geq \deg(G) - 2\gamma + 2$ for C_{Ω} (where γ is the genus of $\mathcal{X}$). Soon after its introduction, GG codes became a very important tool in Coding Theory; for example, Tsfasman, Vladut and Zink [22] showed that the Varshamov-Gilbert bound can be attained by using these codes. The way of dealing with the dimension and minimum distance of C is via the Riemann-Roch theorem; in particular one needs to compute the genus of the underlying curve which may be a difficult task. Thus it will be of interest to construct and manage GG codes by using "elementary methods" only. An important step in this direction was given by Høholdt, van Lint and Pellikaan [8] (see also [2]), who used order functions (see Section 2.2) to construct codes from an $\mathbb{F}$-algebra $\mathbf{R}$. Order functions and the obtained codes have benn studied in detail by Pellikaan, Geil and other authors (see [5], [20]). This technique allows us to do mainly with "one-point GG" codes –that is to say, when $\ell = 1$ in the definition of divisor G above–. The objective of this paper is to introduce and study a wider class of "order-like" functions (the called *near order* functions; see Section 3) in such a way that more GG codes could be represented by those elementary methods.

2. Background

2.1. *Weierstrass Semigroups and Geometric Goppa Codes.* Let $\mathcal{X}$ be a curve over a finite field $\mathbb{F}$. For a point $P \in \mathcal{X}$, let $\mathcal{O}_P$ and v_P denote the local ring and valuation of $\mathcal{X}$ at P respectively. Following [8], we consider the $\mathbb{F}$-algebra

$$\mathbf{R} = \mathbf{R}(Q_1, \ldots, Q_\ell) := \bigcap_{R \neq Q_1, \ldots, Q_\ell} \mathcal{O}_R \,,$$

where the Q_i's are as in Section 1; we shall consider also the Weierstrass semigroup of $\mathcal{X}$ at $Q_1, \ldots, Q_\ell$, namely

$$\begin{aligned} H &= H(Q_1, \ldots, Q_\ell) \\ &= \{(\beta_1, \ldots, \beta_\ell) \in \mathbb{N}_0^\ell : \text{ there exists } f \in \mathbf{R} \text{ with } \mathrm{div}_\infty(f) = \beta_1 Q_1 + \ldots + \beta_\ell Q_\ell\} \,. \end{aligned}$$

These semigroups have been intensively studied in connection with Coding Theory; see for example [1], [3], [4], [9], [10], [11] [12] [13], [14], [16], [17], [18], [19]. The relationship between $\mathbf{R}$ and H above suggests that Goppa codes can be represented by elementary means. As was already mentioned, this was noticed in [8] for the case $\ell = 1$ (see also [15]).

2.2. *Order Functions.* Our reference in this section is the paper [8]. Let $\mathbf{R}$ be an $\mathbb{F}$-algebra. A function $\rho : \mathbf{R} \to \mathbb{N}_0 \cup \{-\infty\}$ is called an *order* function if the following properties

(O0) $\rho(f) = -\infty$ if and only if $f = 0$;
(O1) $\rho(\lambda f) = \rho(f)$ for all $\lambda \in \mathbb{F}^*$;
(O2) $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$;
(O3) If $\rho(f) < \rho(g)$ and $h \neq 0$, then $\rho(fh) < \rho(gh)$; and
(O4) If $\rho(f) = \rho(g) \neq -\infty$, then there exists $\lambda \in \mathbb{F}^*$ such that $\rho(f - \lambda g) < \rho(g)$,

are satisfied for all $f, g, h \in \mathbf{R}$. If in addition

(O5) $\rho(fg) = \rho(f) + \rho(g)$,

then ρ is called a *weight* function. We collect some properties of order functions.

Lemma 2.1. ([8, Lemma 3.9]) *With notation as above*:

(1) *If* $\rho(f) = \rho(g)$, *then* $\rho(fh) = \rho(gh)$ *for all* $h \in \mathbf{R}$;
(2) *If* $f \in \mathbf{R} \setminus \{0\}$, *then* $\rho(1) \leq \rho(f)$;
(3) $\mathbb{F}^* = \{f \in \mathbf{R} : \rho(f) = \rho(1)\}$;
(4) *If* $f \neq 0$, $g \neq 0$ *and* $\rho(f) = \rho(g)$, *then there exists a unique nonzero* $\lambda \in \mathbb{F}$ *such that* $\rho(f - \lambda g) < \rho(f)$;
(5) *If* $\rho(f) \neq \rho(g)$, *then* $\rho(f + g) = \max\{\rho(f), \rho(g)\}$.

Remark 2.2. According to the lemma above, the $\mathbb{F}$-algebra $\mathbf{R}$ splits as $\mathbf{R} = \mathcal{M} \cup \mathcal{U}$, where

$$\mathcal{M} = \{f \in \mathbf{R} : \rho(f) > \rho(1)\}, \quad \text{and} \quad \mathcal{U} = \{f \in \mathbf{R} : \rho(f) \leq \rho(1)\}.$$

As a matter of fact, $\mathcal{U}^* := \mathcal{U} \setminus \{0\} = \{f \in \mathbf{R} \setminus \{0\} : \rho(f) = \rho(1)\} = \mathbb{F}^*$.

3. Near Order Functions

In this section we study a "weak" version of the concept of order and weight function discussed in Section 2. The starting point for our discussion is Remark 2.2.

3.1. *Near Order Functions.* Let $\mathbf{R}$ be an $\mathbb{F}$-algebra and let $\rho : \mathbf{R} \to \mathbb{N}_0 \cup \{-\infty\}$ be a function with $\rho(0) = -\infty$. Associated to ρ we can consider the sets:

$$\begin{aligned} \mathcal{U} = \mathcal{U}_\rho &:= \{f \in \mathbf{R} : \rho(f) \leq \rho(1)\}, \\ \mathcal{U}^* = \mathcal{U}_\rho^* &:= \mathcal{U} \setminus \{0\}, \\ \mathcal{M} = \mathcal{M}_\rho &:= \{f \in \mathbf{R} : \rho(f) > \rho(1)\}. \end{aligned}$$

In addition, let $\mathcal{U} = \mathcal{U}_\rho := \mathcal{U}^* \cup \{0\}$. We say that ρ is a *near order* function (or *n-order* function, for short) if properties

(N0) $\rho(f) = -\infty$ if and only if $f = 0$;
(N1) $\rho(\lambda f) = \rho(f)$ for all $\lambda \in \mathbb{F}^*$;
(N2) $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$;

similar to the corresponding concerning order functions hold true, and for $f, g, h \in \mathbf{R}$ we have:

(N3) If $\rho(f) < \rho(g)$ then $\rho(fh) \leq \rho(gh)$. Furthermore, if $h \in \mathcal{M}$, then $\rho(fh) < \rho(gh)$;
(N4) If $\rho(f) = \rho(g)$ with $f, g \in \mathcal{M}$, then there exists $\lambda \in \mathbb{F}^*$ such that $\rho(f - \lambda g) < \rho(f)$.

Clearly an order function is also a n-order (cf. Remark 2.2). We can also construct n-orders functions on $\mathbf{R}$ which are not orders functions.

Example 3.1. (a) Let $\rho(0) = -\infty$ and for $f \in \mathbf{R} \setminus \{0\}$ put $\rho(f) := c \in \mathbb{N}_0$ (constant). Here $\mathcal{M} = \emptyset$ and $\mathcal{U} = \mathbf{R}$, so ρ is trivially a n-order on $\mathbf{R}$ which is not an order (it is an order function if and only if $\mathbf{R} = \mathbb{F}$).

(b) Fix $g \in \mathbf{R} \setminus \mathbb{F}$ and define $\rho(f) = -\infty$ if and only if $f = 0$; $\rho(f) := 0$ if $f \in \langle g \rangle, f \neq 0$; $\rho(f) = 1$ otherwise. Then ρ is a n-order function with $\rho(1) = 1$ and $\mathcal{U} = \mathbf{R}$.

The examples above shows the existence of n-order functions on an arbitrary $\mathbb{F}$-algebra. Note that in both cases it holds that $\mathcal{U} = \mathbf{R}$ hence $\mathcal{M} = \emptyset$. N-orders verifying this condition will be called *trivial*. For non-trivial n-orders both sets $\mathcal{M}$ and $\rho(\mathcal{M})$ have infinitely many elements. This is a consequence of (N3), since $\rho(1) < \rho(f)$ implies $\rho(f^i) < \rho(f^{i+1})$. An example of a nontrivial n-order is the following.

Example 3.2. Let $\mathbf{R} = \mathbb{F}[X, Y]/(XY - 1) = \mathbb{F}[x, y]$ with x, y being the class of X and Y respectively. Every $f \in \mathbf{R}$ admits a unique decomposition of type $f = f_1(x) + f_2(y)$, where $f_1, f_2 \in \mathbb{F}[T]$ with $f_2(0) = 0$. It is known that $\mathbf{R}$ does not admit any order function, [8, Ex. 3.11]. However, $\mathbf{R}$ admits a non-trivial n-order function, namely

$$\rho(f) := \begin{cases} -\infty & \text{if } f = 0, \\ 0 & \text{if } f_1 \neq 0 \text{ and } f_2 = 0, \\ \deg(f_2) & \text{if } f_2 \neq 0. \end{cases}$$

Here $\rho(1) = 0$, $\mathcal{M} = \{f_1(x) + f_2(y) : f_2 \in \mathbb{F}[t],\ f_2 \neq 0 \text{ and } f_2(0) = 0\}$, $\mathcal{U} = \{f_1(x) : f_1 \in \mathbb{F}[t]\}$; an straightforward computation shows that ρ is in fact a n-order function.

The relation between orders and n-orders is clarified by the following result, which complements Remark 2.2.

Lemma 3.3. *Let $\rho : \mathbf{R} \to \mathbb{N}_0 \cup \{-\infty\}$ be a function defined on a $\mathbb{F}$-algebra $\mathbf{R}$. Let $\mathcal{U} = \mathcal{U}_\rho$ be the set of elements $f \in \mathbf{R}$ with $\rho(f) \leq \rho(1)$. Then the following statements are equivalent:*

(1) *ρ is an order*;
(2) *ρ is a n-order and $\mathcal{U} = \mathbb{F}$.*

Note that, as a consequence of property (N1), for any n-order on $\mathbf{R}$ it holds that $\mathbb{F} \subseteq \mathcal{U}$. The above lemma shows that equality holds just for orders. On the other hand, it was

noticed in [8, Prop. 3.10] that any $\mathbb{F}$-algebra equipped with an order function is an integral domain but the inverse statement is false; cf. Example 3.2. We stress the fact that any $\mathbb{F}$ algebra can be equipped with a n-order function; cf. Examples 3.1, 3.2.

Lemma 3.4. *Let $\mathbf{R}$ be an $\mathbb{F}$-algebra and ρ a n-order on $\mathbf{R}$. Then the set $\mathcal{M}_\rho$ does not contain zero divisors.*

Proof. Let $g \in \mathbf{R} \setminus \{0\}$ and $f \in \mathcal{M}$. Since $\rho(1) < \rho(f)$ it holds that $\rho(g) \leq \rho(fg)$ by Axiom $(N3)$. Hence $fg \neq 0$. □

Let us see one more example. As said in the Introduction, our purpose is to manage Goppa codes over more that one point by means of "order-like" functions. This example shows a way to obtain n-order functions from points on curves (cf. Section 5).

Example 3.5. Let $\mathcal{X}$ be a curve over a finite field $\mathbb{F}$. Let $Q_1, \ldots, Q_\ell$ be pairwise different $\mathbb{F}$-rational points of $\mathcal{X}$ and $\mathbf{R} = \mathbf{R}(Q_1, \ldots, Q_\ell)$ the algebra defined in Section 2.1. For each point Q_i, define the function $\rho_i = \rho_{Q_i} : \mathbf{R} \to \mathbb{N}_0 \cup \{-\infty\}$ by $\rho_i(f) = -\infty$ if and only if $f = 0$, and

$$\rho_i(f) = \begin{cases} 0 & \text{if } v_{Q_i}(f) \geq 0, \\ -v_{Q_i}(f) & \text{if } v_{Q_i}(f) < 0. \end{cases}$$

Then $\rho_i(1) = 0$ and hence $\mathcal{U}_i^* = \{f \in \mathbf{R}^* : v_{Q_i}(f) \geq 0\}$. As a consequence of properties regarding valuation maps, ρ_i is indeed a n-order function (and in fact a n-weight as we shall define it later).

Note that in the one-point case ($\ell = 1$) it holds that

$$H(Q_1) = \{-v_{Q_1}(f) : f \in \mathbf{R}^*\}.$$

In the multiple-point case ($\ell > 1$) we must use the functions ρ_i's instead of the valuations $-v_{Q_i}$'s in order to describe the Weierstrass semigroup; indeed,

$$H(Q_1, \ldots, Q_\ell) = \{(\rho_1(f), \ldots, \rho_\ell(f)) : f \in \mathbf{R}^*\}.$$

This fact gives a motivation to define the concept of near order.

Now we subsume further properties of n-order functions that are similar to those of order functions (cf. [8, Lemma 3.9]).

Lemma 3.6. *Let ρ be a n-order function on a $\mathbb{F}$-algebra $\mathbf{R}$. The following statements hold:*

(1) *If $f, g, h \in \mathcal{M}_\rho$ and $\rho(f) = \rho(g)$, then $\rho(fh) = \rho(gh)$;*
(2) *The element λ in Axiom $(N4)$ is unique;*
(3) *If $\rho(f) \neq \rho(g)$, then $\rho(f + g) = \max\{\rho(f), \rho(g)\}$.*

Proof. Similar to the proof of [8, Lemma 3.9(1),(2),(4)]. □

3.2. *Normalized Near Orders and Near Weights Functions.* Let ρ be a n-order function on $\mathbf{R}$. As we shall see in the forthcoming sections, we will be interested in the value of $\rho(f)$ when $f \in \mathcal{M}$ but not when $f \in \mathcal{U}$. Thus we can consider the *normalization* of ρ as the function $\tilde{\rho}$ defined as $\tilde{\rho}(0) = -\infty$ and for $f \neq 0$

$$\tilde{\rho}(f) = \begin{cases} 0 & \text{if } f \in \mathcal{U}_\rho; \\ \rho(f)/d & \text{if } f \in \mathcal{M}_\rho, \end{cases}$$

where $d = \gcd(\rho(\mathcal{M}))$. It is clear that $\tilde{\rho}$ is also a n-order function, $\mathcal{M}_{\tilde{\rho}} = \mathcal{M}_\rho$ and $\mathcal{U}_{\tilde{\rho}} = \mathcal{U}_\rho$. The n-order function ρ is said to be *normal* if $\rho = \tilde{\rho}$. In what follows, all the n-orders functions we consider will be understood as normal.

A (normal) n-order function ρ is called a *near weight* (or *n-weight*, for short) if it verifies the supplementary condition

(N5) $\rho(fg) \leq \rho(f) + \rho(g)$. If $f, g \in \mathcal{M}$, then equality holds.

Two interesting properties of n-weights arise at once from its definition

Proposition 3.7. *Let ρ be a n-weight function on the $\mathbb{F}$-algebra $\mathbf{R}$. Then*

1. *the set $\rho(\mathbf{R} \setminus \{0\})$ is a numerical semigroup of finite genus;*
2. *the set $\mathcal{U}_\rho$ is closed under product and so it is a subalgebra of $\mathbf{R}$.*

Next, motivated by Proposition 3.12 and Theorem 3.14 in [8], we point out a relation between n-order functions ρ on $\mathbf{R}$ and subspaces of $\mathbf{R}$. Set $\rho(\mathbf{R} \setminus \{0\}) = \{0 = \rho_0 < \rho_1 < \rho_2 < \ldots\}$ and

- For $i \in \mathbb{N}_0$, $L_i := \{f \in \mathbf{R} : \rho(f) \leq \rho_i\}$;
- For $f \neq 0$ define $\iota(f)$ as being the least non-negative integer ℓ such that $f \in L_\ell$;
- For $i, j \in \mathbb{N}_0$, $\ell(i,j) := \max\{\iota(fg) : f \in L_i \text{ and } g \in L_j\}$.

Proposition 3.8. *Let ρ be a n-order function on a $\mathbb{F}$-algebra $\mathbf{R}$ whose set of non-units is not empty. Then the following statements hold true*:

1. *(L_i) is an increasing sequence of vector subspaces of $\mathbf{R}$ such that*:
   (a) $\mathbb{F} \subseteq L_0$;
   (b) $\dim(L_{i+1}) = \dim(L_i) + 1$;
   (c) $\cup_i L_i = \mathbf{R}$;
2. *$\ell(i,j) = \ell(j,i)$, and for all $i \in \mathbb{N}_0$:*
   (a) *If $j \geq 1$, then $\ell(i,j) < \ell(i+1,j)$;*
   (b) *If $j = 0$, then $\ell(i,0) \leq \ell(i+1,0)$;*
3. *If ρ is a n-weight function, then $\rho_{\ell(i,j)} \leq \rho_i + \rho_j$ for $i, j \in \mathbb{N}_0$. If $i, j \geq 1$ the equality holds.*

Proof. (1) The fact that the L_i's are vector spaces follows from properties (N0),(N1) and (N2) of n-order functions. (1.a) was already noted. (1.b) holds as a consequence

of properties (N2) and (N4). Statement (1.c) is obvious; (2) is a direct consequence of property (N3); (3) follows from (N5). □

Remark 3.9. As doing in [8], the above proposition can be partially written in terms of functions instead of subspaces. Indeed, for $i \in \mathbb{N}$, let $f_i \in L_i \setminus L_{i-1}$. Then

(1) $\iota(f_i) = i$ and $\rho(f_i) = \rho_i$;
(2) The set (f_i) is linearly independent and $\mathbf{R} = \mathcal{U} \oplus \langle f_1, f_2 \ldots \rangle$.
(3) For $i, j \in \mathbb{N}$, $\ell(i, j) = \iota(f_i f_j)$.

Conversely, we will prove that certain sequences of subspaces of $\mathbf{R}$ defines a n-order function on $\mathbf{R}$. Let $L_0 \subseteq L_1 \subseteq \ldots$ be an increasing sequence of vector subspaces of $\mathbf{R}$ verifying the conditions:

(1a) $\mathbb{F} \subseteq L_0$;
(1b) $\dim(L_{i+1}) = \dim(L_i) + 1$;
(1c) $\cup_i L_i = \mathbf{R}$.

Let $0 = \rho_0 < \rho_1 < \ldots$ be a sequence of positive integers whose cardinality is the same as the sequence (L_i) and such that $\gcd(\rho_i) = 1$. For $f \neq 0$ define $\iota(f)$ as being the least non-negative integer ℓ such that $f \in L_\ell$. For $i, j \in \mathbb{N}_0$, set

$$\ell(i, j) := \max\{\iota(fg) : f \in L_i \text{ and } g \in L_j\}.$$

The following proposition arises:

Proposition 3.10. *Notation as above. Let $\rho : \mathbf{R} \to \mathbb{N}_0 \cup \{-\infty\}$ be the function defined by $\rho(0) = -\infty$ and $\rho(f) = \rho_{\iota(f)}$ for $f \neq 0$. If the following two conditions*:

(2a) *If $j \geq 1$, then $\ell(i, j) < \ell(i + 1, j)$,*
(2b) *If $j = 0$, then $\ell(i, 0) \leq \ell(i + 1, 0)$*

hold, then ρ is a n-order function; *if, in addition, $\rho_{\ell(i,j)} \leq \rho_i + \rho_j$ with equality if $i, j \geq 1$, then ρ is a n-weight function. In both cases, $L_0 \setminus \{0\}$ is the set of unities of $\mathbf{R}$.*

4. Well-Agreeing n-weights

The subject matter of this section can be applied to finitely many n-weight functions. However, for simplicity we shall consider the case of just two n-weights. Then, let ρ, σ be two n-weights on $\mathbf{R}$. We consider the following subsemigroup of $(\mathbb{N}_0^2, +)$:

$$H(\rho, \sigma) = \{(\rho(f), \sigma(f)) : f \in \mathbf{R} \setminus \{0\}\}.$$

It can have, or have not, a finite genus.

Proposition 4.1. *If $H(\rho, \sigma)$ has a finite genus, then $\rho(\mathbf{R}\setminus\{0\}) = \mathbb{N}_0$ and $\sigma(\mathbf{R}\setminus\{0\}) = \mathbb{N}_0$.*

Proof. Let $n \in \mathbb{N}_0$. The set $\{(n,m) \notin H(\rho,\sigma) : m \in \mathbb{N}_0\}$ is finite, hence $n \in \rho(\mathbf{R})$. Analogously for σ. □

In what follows we shall assume that $H(\rho,\sigma)$ has a finite genus. As said before, both $\mathcal{U}_\rho$ and $\mathcal{U}_\sigma$ are subalgebras of $\mathbf{R}$. Then, the sets

$$H(\sigma) := \sigma(\mathcal{U}_\rho^*) = \{m : (0,m) \in H(\rho,\sigma)\} \quad \text{and}$$
$$H(\rho) := \rho(\mathcal{U}_\sigma^*) = \{m : (m,0) \in H(\rho,\sigma)\}$$

are numerical semigroups. Write $H(\sigma) = \{0 = m_0 < m_1 < m_2 < \ldots\}$.

Lemma 4.2. *The semigroups $H(\sigma)$ and $H(\rho)$ have at most the genus of $H(\rho,\sigma)$.*

Proof. Note that $H(\sigma) = \sigma(\mathcal{U}_\rho \cap \mathcal{M}_\sigma) \cup \{0\}$. Now if ℓ is a gap of $H(\sigma)$, then $(0,\ell)$ is a gap of $H(\rho,\sigma)$. The same argument for $H(\rho)$. □

Proposition 4.3. *Let $f_0 = 1$ and for $i \in \mathbb{N}$ take functions $f_i \in \mathbf{R}$, $g_i \in \mathcal{U}_\rho$ such that $\rho(f_i) = i$, $\sigma(g_i) = m_i$. Set $\mathcal{B} := \{f_i : i \in \mathbb{N}_0\} \cup \{g_j : j \in \mathbb{N}\} \subseteq \mathbf{R}$. If $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$, then $\mathcal{B}$ is a basis of $\mathbf{R}$ as a $\mathbb{F}$-vector space.*

Proof. We first show that $\mathcal{B}$ is a linearly independent set. If $\lambda_0 f_0 + \ldots + \lambda_r f_r = \mu_1 g_1 + \ldots + \mu_s g_s$, then

$$\rho(\lambda_0 f_0 + \ldots + \lambda_r f_r) = \rho(\mu_1 g_1 + \ldots + \mu_s g_s) = 0\,,$$

by (N2) and $g_j \in \mathcal{U}_\rho$. Then $\lambda_i = 0$ for $i \geq 1$ by 3.6(3), and so

$$-\lambda_0 + \mu_1 g_1 + \ldots + \mu_s g_s = 0\,.$$

As above it follows that $\mu_1 = \ldots = \mu_s = 0$ and so $\mathcal{B}$ is in fact a linearly independent set.

We show next that $\mathcal{B}$ generates $\mathbf{R}$. Let $h \in \mathbf{R}$ such that $\rho(h) = i \in \mathbb{N}_0$. By applying iteratively (N4), there exist elements $\lambda_1, \ldots, \lambda_r \in \mathbb{F}$ such that

$$\tilde{h} := h - \lambda_1 f_1 - \ldots - \lambda_r f_r \in \mathcal{U}_\rho\,.$$

Let $\sigma(\tilde{h}) = m_s = \sigma(g_s)$. Arguing as above, we find elements $\beta_1, \ldots, \beta_s \in \mathbb{F}$ so that

$$\tilde{h} - \beta_1 g_1 - \ldots - \beta_s g_s \in \mathcal{U}_\sigma\,.$$

The proof now follows by the hypothesis $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$. □

Definition 4.4. We say that the n-weights ρ and σ *agree well* if the semigroup $H(\rho,\sigma)$ has a finite genus and $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$.

Example 4.5. (Continuation of Example 3.5) Let $\mathcal{X}$ be a curve of genus γ over $\mathbb{F}$ and let Q_1, Q_2 be two rational points. Let $\mathbf{R} = \mathbf{R}(Q_1, Q_2)$ and ρ, σ be the n-weights associated to the points Q_1, Q_2 respectively. Then $H(\rho,\sigma)$ is just the Weierstrass semigroup at Q_1, Q_2, $H(\rho,\sigma) = H(Q_1, Q_2)$. By the Riemann-Roch theorem this semigroup has finite genus. Furthermore since $\mathcal{U}_\rho$ (resp. $\mathcal{U}_\sigma$) is the set of rational functions having poles only at Q_2 (resp. at Q_1), then $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$, hence ρ and σ agree well. Moreover, it is easy to see

that $H(\rho) = H(Q_1)$ and $H(\sigma) = H(Q_2)$. In this case (n-weights associated to points on a curve), both semigroups have the same genus, γ. As we shall see next, this is also true for general well agreeing n-weights; see Corollary 4.8.

If the n-weights ρ and σ agree well, then the functions f_i in the basis $\mathcal{B}$ can be taken in such a way that (cf. [14])

$$\sigma(f_i) = \min\{\sigma(f) : f \in \mathbf{R} \text{ and } \rho(f) = i\}\,. \tag{4.1}$$

Definition 4.6. A basis with the property above will be called *good* (with respect to the n-weights ρ and σ).

The next proposition and its corollary states some properties of good basis.

Proposition 4.7. *Let ρ and σ be two well agreeing n-weights on $\mathbf{R}$ and let $\mathcal{B} = \{f_i : i \in \mathbb{N}_0\} \cup \{g_j : j \in \mathbb{N}\}$ be a good basis. Then*

1. *For all $i = 0, 1, \ldots,$ either $\sigma(f_i) = 0$ or $\sigma(f_i)$ is a gap of $H(\sigma)$;*
2. *Conversely, for every gap m of $H(\sigma)$ there exists exactly one index i such that $\sigma(f_i) = m$;*
3. *$\sigma(f_i) = 0$ if and only if i is a nongap of $H(\rho)$.*

Proof. (1) Suppose that $\sigma(f_i) = m_j \in H(\sigma)$, $m_j \neq 0$; then $\sigma(f_i) = \sigma(g_j)$ and by (N4) there exists $\mu_j \in \mathbb{F}^*$ such that $\sigma(f_i - \mu_j g_j) < m_j$. Proceeding iteratively in this way we find a $\tilde{f}_i := f_i + \sum_j \mu_j g_j$ such that $\sigma(\tilde{f}_i) \in \mathrm{Gaps}(H(\sigma)) \cup \{0\}$. Since $\rho(\tilde{f}_i) = \rho(f_i) = i$ by Lemma 2.1(5), the proof is complete.

(2) Let $t \in \mathbb{N}$ be a gap of $H(\sigma)$. Let us prove first that there are at most one r such that $\sigma(f_r) = t$. If, on the contrary, $\sigma(f_i) = \sigma(f_j) = t$ for some $i > j$, then there is a $\lambda \in \mathbb{F}^*$ such that $\sigma(f_i - \lambda f_j) < m$. Then $\tilde{f}_i = f_i - \lambda f_j$ verifies $\rho(\tilde{f}_i) = i$, contradicting the defining property of the function f_i. Let us prove now that there is an index r such that $\sigma(f_r) = t$. From 4.1 there is $h \in \mathbf{R}$ such that $\sigma(h) = m$. Write

$$h = \sum_{i \in I} \lambda_i f_i + \sum_{j \in J} \mu_j g_j\,.$$

with $I \subseteq \mathbb{N}_0, J \subset \mathbb{N}$ and $\lambda_i, \mu_j \neq 0$. Since all the elements in the family $\{\sigma(f_i) : i \in I, \sigma(f_i) \neq 0\}$ are pairwise distinct gaps of $H(\sigma)$, and all the elements in the family $\{\sigma(g_j) : j \in J\}$ are pairwise distinct nongaps of $H(\sigma)$, according to the properties of n-weights, we conclude that

$$t = \sigma(h) = \max(\{\sigma(f_i) : i \in I\} \cup \{\sigma(g_j) : j \in J\}) = \sigma(f_r)$$

for some r (because m is a gap).

(3) $\sigma(f_i) = 0$ if and only if there exists $f \in \mathcal{U}_\sigma$ with $\rho(f) = i$, that is, if and only if i is a nongap of $H(\rho)$. □

Corollary 4.8. *Let ρ and σ be two well agreeing n-weights on $\mathbf{R}$ and let $\mathcal{B}$ be a good basis. Then*

(1) *$\sigma(f_i)$ is a gap of $H(\sigma)$ if and only if i is a gap of $H(\rho)$. In particular, both semigroups have equal genus.*
(2) *$\sigma(f_i) = 0$ except for finitely many i's; for all i, $\sigma(f_i) \leq \Lambda_\sigma$, where Λ_σ is the largest gap of $H(\sigma)$.*

Well agreeing n-weights and good basis can be used to construct codes from $\mathbf{R}$, as we shall see in the next Section.

5. The Codes and a Bound on the Minimum Distance

5.1. *N-order Codes.* Let ρ, σ be two well agreeing n-weights on a $\mathbb{F}$-algebra $\mathbf{R}$ and let $\mathcal{B} := \{f_i : i \in \mathbb{N}_0\} \cup \{g_j : j \in \mathbb{N}\}$ be a good basis. Let γ be the genus of $H(\sigma)$ (or equivalently the genus of $H(\rho)$) and Λ_σ its largest gap. For a pair of non-negative integers $\ell, m \in \mathbb{N}_0$, set a to be the (only) integer such that

$$m_a \leq m < m_{a+1}$$

and let us consider the set

$$\mathbf{R}_\ell^m = \{h \in \mathbf{R} : \rho(h) \leq \ell \text{ and } \sigma(h) \leq m\}.$$

Proposition 5.1. *$\mathbf{R}_\ell^m$ is a vector subspace of $\mathbf{R}$. Furthermore, if $m \geq \Lambda_\sigma$ then*

$$\mathbf{R}_\ell^m = \langle f_0, \ldots, f_\ell, g_0, g_1, \ldots, g_a \rangle,$$

where $g_0 = f_0 = 1$. In this case $\dim(\mathbf{R}_\ell^m) = \ell + m + 1 - \gamma$.

Let $*$ denote the product in $\mathbb{F}^n$ defined by the coordinatewise multiplication, and let $\varphi : \mathbf{R} \to \mathbb{F}^n$ be a morphism of $\mathbb{F}$-algebras. Let m be an integer such that $m \geq \Lambda_\sigma$ and $\varphi(\cup_\ell \mathbf{R}_\ell^m) = \mathbb{F}^n$. We define the codes

$$E_\ell^m := \varphi(\mathbf{R}_\ell^m) \quad \text{and} \quad C_\ell^m := (E_\ell^m)^\perp. \tag{5.1}$$

Note that, since $\varphi(\cup_\ell \mathbf{R}_\ell^m) = \mathbb{F}^n$, there exists L such that $E_0^m \subseteq E_1^m \subseteq \ldots \subseteq E_L^m = \mathbb{F}^n$ and hence $C_0^m \supseteq C_1^m \supseteq \ldots \supseteq C_L^m = (0)$.

Example 5.2. (Continuation of Example 4.5) Let $\mathcal{X}$ be a curve of genus γ over $\mathbb{F}$ and let Q_1, Q_2 be two rational points. Let $\mathbf{R} = \mathbf{R}(Q_1, Q_2)$ and ρ, σ be the n-weights associated to the points Q_1, Q_2 respectively. Since $\mathbf{R}_\ell^m = \mathcal{L}(\ell Q_1 + m Q_2)$, if we take a divisor $D = P_1 + \cdots + P_n$, sum of n distinct rational points on $\mathcal{X}$ and $\varphi = ev$, the evaluation at these points, we obtain the codes $E_\ell^m = C_\mathcal{L}(\mathcal{X}, D, \ell Q_1 + m Q_2)$ and $C_\ell^m = C_\Omega(\mathcal{X}, D, \ell Q_1 + m Q_2)$.

The dimension of E_ℓ^m and C_ℓ^m depends on the dimension of the subspaces $\mathbf{R}_\ell^m$ and the morphism φ. With regard to their minimum distances, we shall show a bound on the minimum distance of C_ℓ^m, analogous to the order bound in [8, Section 4].

5.2. *The n-order bound on the minimum distance.* For a vector $\mathbf{y} \in \mathbb{F}^n$ and $i, j = 0, \ldots, L$, let us consider the two-dimensional syndromes

$$s_{ij}(\mathbf{y}) = (\mathbf{h}_i * \mathbf{h}_j) \cdot \mathbf{y}\,,$$

where $\mathbf{h}_t = \varphi(f_t)$. The *matrix of syndromes* of $\mathbf{y}$ is $S(\mathbf{y}) = (s_{ij}(\mathbf{y}))_{i,j=0,\ldots,L}$.

Proposition 5.3. $\mathrm{wt}(\mathbf{y}) \geq \mathrm{rank}(S(\mathbf{y}))$.

Proof. Analogous to [8, Lemma 4.7]. □

For a nonnegative integer s, set

$$\Sigma(s) = \max\{\sigma(f_0), \ldots, \sigma(f_s)\}\,, \quad \text{and}$$
$$N_\ell^m = \{(i,j) \in \mathbb{N}_0^2 : i + j = \ell + 1 \text{ and } \sigma(f_i) + \Sigma(j) \leq m\}\,.$$

Note that for all i, j it holds that $\rho(f_i f_j) = \rho(f_i) + \rho(f_j)$. Thus, if $(i,j) \in N_\ell^m$ then $f_i f_j \in \mathbf{R}_{\ell+1}^m \setminus \mathbf{R}_\ell^m$.

Proposition 5.4. *Write $N_\ell^m = \{(i_1, j_1), \ldots, (i_t, j_t)\}$ ordered in increasing lexicographical order. Then*

(1) *$i_1 < \ldots < i_t$ and $j_1 > \ldots > j_t$;*
(2) *If $\mathbf{y} \in C_\ell^m$ and $u < v$, then $s_{i_u j_v}(\mathbf{y}) = 0$;*
(3) *If $\mathbf{y} \in C_\ell^m \setminus C_{\ell+1}^m$, then $s_{i_u j_u}(\mathbf{y}) \neq 0$.*

Proof. (1) Note that $i_u + j_u = \ell + 1$.

(2) Since $j_v < j_u$ then $\rho(f_{i_u}) + \rho(f_{j_v}) < \rho(f_{i_u}) + \rho(f_{j_u}) = \ell + 1$ and $\sigma(f_{i_u}) + \sigma(f_{j_v}) \leq \sigma(f_{i_u}) + c(j_u) \leq m$. Thus $f_{i_u} f_{j_v} \in R_\ell^m$, hence $\mathbf{h}_{i_u} * \mathbf{h}_{j_v} \in E_\ell^m$ and $(\mathbf{h}_{i_u} * \mathbf{h}_{j_v}) \cdot \mathbf{y} = 0$.

(3) Since $f_{i_u} f_{j_u} \in R_{\ell+1}^m \setminus R_\ell^m$, then $f_{i_u} f_{j_u} = \lambda f_{\ell+1} + f$ with $\lambda \neq 0$ and $\rho(f) \leq \ell$. Furthermore, since $m \geq \Lambda_\sigma$ it holds that $\sigma(f) \leq m$, hence $f \in \mathbf{R}_\ell^m$. Then $\mathbf{h}_{i_u} * \mathbf{h}_{j_u} = \lambda \mathbf{h}_{\ell+1} + \mathbf{h}$, with $\mathbf{h} \in E_\ell^m$, so $(\mathbf{h}_{i_u} * \mathbf{h}_{j_u}) \cdot \mathbf{y} = \lambda \mathbf{h}_{\ell+1} \cdot \mathbf{y} \neq 0$. □

Corollary 5.5. *If $\mathbf{y} \in C_\ell^m \setminus C_{\ell+1}^m$, then* $\mathrm{rank}(S(\mathbf{y})) \geq \#N_\ell^m$.

Proof. The minor obtained from $S(\mathbf{y})$ by taking the rows $i_1 < \ldots < i_t$ and the columns $j_1 > \ldots > j_t$ is nonsingular. □

Definition 5.6. The *n-order bound* on the minimum distance of C_ℓ^m is defined as

$$d_{NORD}(\ell, m) := \min\{\#N_r^m : r \geq \ell\}\,.$$

As a direct consequence of the above results we have the following.

Theorem 5.7. *The minimum distance of the code C_ℓ^m is lower bounded by $d_{NORD}(\ell, m)$, that is*

$$d(C_\ell^m) \geq d_{NORD}(\ell, m)\,.$$

Next we shall give a bound on the cardinality $\#N_r^m$.

Proposition 5.8. *We have $\#N_r^m \geq \#(H(\rho) \cap [1, r+1])$. In particular, if $r \geq \gamma$ then $\#N_r^m \geq r - \gamma + 1$.*

Proof. If $i \in H(\rho) \cap [1, r+1]$ then, according to 4.7 (3), it holds that $\sigma(f_i) = 0$, hence $(i, r+1-i) \in N_r^m$ (because $\Sigma(r+1-i) \leq \Lambda_\sigma \leq m$). Since $H(\rho)$ is a semigroup of genus γ then $\#(H(\rho) \cap [1, r+1]) \geq r - \gamma + 1$ for $r \geq \gamma$. □

Corollary 5.9. *If $\ell \geq \gamma$, then $d(C_\ell^m) \geq d_{NORD}(\ell, m) \geq \ell - \gamma + 1$.*

As another consequence of the proposition, the computation of $d_{NORD}(\ell, m)$ only requires the knowledge of a finite number of terms $\#N_r^m$.

Corollary 5.10. $d_{NORD}(\ell, m) = \min\{\#N_\ell^m, \ldots, \#N_{\ell+\gamma}^m\}$.

Proof. Note that $\#N_r^m \leq r + 2$ by definition. Thus, according to the above proposition, if $r > \ell + \gamma$ then $\#N_r^m \geq \ell + 2 \geq \#N_\ell^m$ and hence $\min\{\#N_r^m : r \geq \ell\}$ must be attained in the set $\{\#N_\ell^m, \ldots, \#N_{\ell+\gamma}^m\}$. □

Remark 5.11. Note that the n-order bound does not depend on the good basis chosen. In fact, since (4.1) is equivalent to

$$\sigma(f_i) = \min\{t \in \mathbb{N}_0 : (i, t) \in H(\rho, \sigma)\},$$

each $\#N_r^m$ (and hence $d_{NORD}(\ell, m)$) can be computed, in finite time, from only the information given by the semigroup $H(\rho, \sigma)$.

5.3. *Performance of the n-order bound.* Next we study the performance of the obtained bound. To that end we shall compare it to the Goppa bound, $d_G(\ell, m) := \ell + m - 2\gamma + 2$ by means of the number

$$\Delta(\ell, m) := d_{NORD}(\ell, m) - d_G(\ell, m).$$

Remark that when the code C_ℓ^m is obtained from two points on an algebraic curve, $C_\ell^m = C_\Omega(\mathcal{X}, D, \ell Q_1 + m Q_2)$, then its minimum distance verifies $d(C_\ell^m) \geq d_G(\ell, m)$.

Let Λ_ρ and Λ_σ be the largest gaps of $H(\rho)$ and $H(\sigma)$ respectively. Furthermore, let s be the integer defined by

$$\sigma(f_s) = \max\{\sigma(f_i) : i \in \mathbb{N}\} = \Lambda_\sigma = c_\sigma - 1 .$$

For large values of m the n-order bound is easy to compute.

Lemma 5.12. *If $m \geq 2\Lambda_\sigma$, then $d_{NORD}(\ell, m) = \ell + 2$. In particular, $\Delta(\ell, m) = 2\gamma - m$, hence $\Delta(\ell, m) < 0$ for $m > 2\gamma$ and $d_{NORD}(\ell, m) = d_G$ if and only if $m = 2\gamma$ (and thus $\Lambda_\sigma = \gamma$).*

Proof. Since $\sigma(f_i) \leq \Lambda_\sigma$ and $\Sigma(i) \leq \Lambda_\sigma$ for all i, $\#N_r^m = r+2$ by hypothesis; thus $d_{NORD}(\ell, m) = \ell + 2$ and the result follows. □

Thus, the remaining case to study is $\Lambda_\sigma \leq m < 2\Lambda_\sigma$. Write

$$N_r^m = \{(0, r+1), (r+1, 0)\} \cup \{(i,j) \in \mathbb{N}^2 : i \in A_r^m \cup B_r^m \cup C_r^m\},$$

where

$$\begin{aligned} A_r^m &= H(\rho) \cap [1, r], \\ B_r^m &= \{i \in \mathrm{Gaps}(H(\rho)) \cap [1, r+1-s] : \sigma(f_i) + \Lambda_\sigma \leq m\} \quad \text{and} \\ C_r^m &= \{i \in \mathrm{Gaps}(H(\rho)) \cap [r+2-s, r] : \sigma(f_i) + \Sigma(r+1-i) \leq m\}. \end{aligned}$$

The following lemma holds true.

Lemma 5.13. *Assume $\Lambda_\sigma \leq m < 2\Lambda_\sigma$ and let $\ell \geq \Lambda_\rho + s - 1$. Then*

(1) $d_{NORD}(\ell, m) = \ell + 2 - \gamma + \#A_\ell^m$;
(2) *If $\Lambda_\sigma \geq \gamma + 1$, then $d_{NORD}(\ell, m) < d_G(\ell, m)$;*
(3) $d_{NORD}(\ell, m) = d_G(\ell, m)$ *if and only if* $\Lambda_\sigma = \gamma$.

Proof. (1) We have $r \geq \Lambda_\rho + 1$ for $r \geq \ell$; on the other hand, $\ell + 2 - s \geq \Lambda_\rho + 1$ and the proof follows from the fact that $\#A_r^m$ increases with r.

(2) By (1), and since $\#A_r^m \leq m - \Lambda_\sigma$, we have $\Delta(\ell, m) = \gamma + \#A_\ell^m - m \leq \gamma - \Lambda_\sigma$.

(3) If $\Delta(\ell, m) = 0$, then clearly $\Lambda_\sigma = \gamma$. Conversely, if $\Lambda_\sigma = \gamma$, then $\#A_\ell^m = m - \gamma$. □

After this lemma, one may expect to obtain $\Delta(\ell, m) > 0$ only in the case

$$\Lambda_\sigma \leq m < 2\Lambda_\sigma \quad \text{and} \quad \ell \leq \Lambda_\rho + s - 2\,.$$

In fact, this can occur as the next example shows.

Example 5.14. Suppose $\sigma(f_i) = i$ for $i = 1, \ldots, \gamma$ (this case can occur on points of the Hyperelliptic curve, see [9]). Then $H(\rho) = \{\gamma+1, \gamma+2, \ldots\}$ and $s = \gamma$. Take $\gamma \leq m < 2\gamma$ and $\ell \geq \gamma + 1$; thus for $r \geq \gamma$

$$\begin{aligned} \#N_r^m = r + 2 - \gamma + \\ \#\{i \in [1, r+1-\gamma] \cap \mathrm{Gaps}(H_\rho) : i + \gamma \leq m\} + \\ \#\{i \in [r+2-\gamma, r+1] \cap \mathrm{Gaps}(H_\rho) : i + \Sigma(r+1-i)\}\,. \end{aligned}$$

Since $m < \gamma$,

$$\#N_r^m = r + 2 - \gamma + \min\{r+1-\gamma, m-\gamma\} + c(m, r)\,,$$

where $c(m, r) = 0$ if $r + 1 > m$ and $c(m, r) = 2\gamma - r - 1$ if $r + 1 \leq m + 1$. Thus

$$\#N_r^m = \begin{cases} r + m - 2\gamma + 2 & \text{if } r+1 > m, \\ r + 2 & \text{if } r+1 \leq m. \end{cases}$$

Observe that $\#N_\ell^m = d_G(\ell, m)$ if $\ell + 1 > m$ and $\#N_\ell^m > d_G(\ell, m)$ otherwise. Thus $d_{ORD}(\ell, m)$ is greater than $d_G(\ell, m)$ whenever $\gamma \leq \ell < m < 2\gamma$.

Finally, for the case $\gamma < m < 2\gamma$ and $\ell < \gamma$, a direct computation shows that $\#N_r^m = r+2$ and hence the n-order bound on the minimum distance improves also on the Goppa bound.

References

[1] Carvalho C. and Torres F., *On Goppa codes and Weierstrass gaps at several points*, Des. Codes Cryptogr. **35**(2) (2005), 211–225.

[2] Feng G.L. and Rao T.R.N., *Improved geometric Goppa codes part I, basic theory*, IEEE Trans. Inf. Theory **41**(6) (1995), 1678–1693.

[3] Garcia A. and Lax R., *Goppa codes and Weierstrass gaps*, Lecture Note in Math., Springer-Verlag, Berlin-Heildelberg, **1518**, 33–42, 1992.

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

[5] Geil, O. and Pellikaan R., *On the structure of order domains*, Finite Fields and their Applications **8** (2002), 369–396.

[6] Goppa, V.D., *Codes associated with divisors*, Problems Inform. Transmission **13** (1977), 22–26.

[7] Goppa, V.D. "Geometry and Codes", Mathematics and its Applications, vol 24, Kluwer, Dordrecht (1991).

[8] Høholdt, T., van Lint J.V. and Pellikaan R., *Algebraic Geometry Codes*, Handbook of Coding Theory, eds. V. Pless and W.C. Huffman, 871–961, Elsevier, 1998.

[9] Homma, M., *The Weierstrass semigroup of a pair of points on a curve*, Arch. Math. **67** (1996), 337–348.

[10] Homma, M. and Kim, S.J., *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra **162** (2001), 273–290.

[11] Homma, M. and Kim, S.J., *Toward the determination of the minimum distance of two-point codes on a Hermitian curve*, Des. Codes Cryptogr., to appear.

[12] Homma, M. and Kim, S.J., *The two-point codes on a Hermitian curve with the designed minimum distance*, Des. Codes Cryptogr., to appear.

[13] Homma, M. and Kim, S.J., *The two-point codes with the designed distance on a Hermitian curve in even characteristic*, preprint.

[14] Kim, S.J., *On the index of the Weiertrass semigroup of a pair of points on a curve*, Arch. Math. **62** (1994), 73–82.

[15] Matsumoto, R., *Miura's generalization of one-point AG codes is equivalent to Høholdt, van Lint and Pellikaan's*, IEICE TRANS. FUNDAMENTALS **E82**-A(10) (1999), 2007–2010.

[16] Matthews, G., *Weierstrass pairs and minimum distance of Goppa codes*, Designs Codes Cryptogr. **22** (2001), 107–221.

[17] Matthews, G., *The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve* (A. Poli, H. Stichtenoth Eds.) Fq7 2003, LNCS **2948**, 12–24, 2004.

[18] Matthews, G., *Weierstrass semigroups and codes from a quotient of the Hermitian curve*, preprint.

[19] Matthews, G., *Some computational tools for estimating the parameters of algebraic geometry codes*, Contemporary Mathematics **381** (2005), 19–26.

[20] Pellikaan R., *On the existence of order functions*, Journal of Statistical Planning and Inference **94** (2001), 287–301.

[21] Silva, E., "Funcões Ordens Fracas e a Distância Mínima dos Códigos de Goppa Geométricos", Tese (Doutorado), http://libdigi.unicamp.br/document/?code=vtls000333125, IMECC-UNICAMP, Cx. P. 6065, 13083-970, Campinas SP-Brazil.

[22] Tsfasman M.A., Vlăduţ S.G. and Zink T. *Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.

Faculdade de Matemática, Universidade Federal de Uberlândia, Av. J.N. de Ávila 2160, Uberlândia, 38408-100, Uberlândia, MG-Brazil.

E-mail address: cicero@ufu.br

Department of Applied Mathematics, University of Valladolid (ETS Arquitectura) 47014 Valladolid, Castilla, Spain.

E-mail address: cmunuera@modulor.arq.uva.es

Faculdade de Matemática, Universidade Federal de Uberlândia, Av. J.N. de Ávila 2160, Uberlândia, 38408-100, Uberlândia, MG-Brazil

E-mail address: ercilio@ufu.br

IMECC-UNICAMP, Cx.P. 6065, 13083-970, Campinas SP-Brazil.

E-mail address: ftorres@ime.unicamp.br