Quotas for the minimum distance of codes of Goppa involving the floor of a divisor

Abstract

In this paper, we study some fundaments of the theory of field of algebraic functions, a small introduction to theory of codes, highlighting at this point the study of geometric codes of Goppa, and some results involving the definition of floor of a divisor. This paper provides two quotas for the minimum distance of a geometric code of Goppa; these quotas involve the floor of a divisor and provide a good estimate for the minimum distance of this code. We introduce a code over a determined field of algebraic functions and we obtain a quota for the minimum distance using the content of the paper.

2010 Mathematics Subject Classification: 14H55, 14G50.

Keywords: divisors; minimum distance; floor of a divisor; floor quota; generalized floor quota.

1 Introduction

This paper resolves the problem of quotas for the minimum distance of a given code. This work has two parts.

In the first part we introduce the theory of field of algebraic functions, such as discrete valuation, places, divisors, genus and adeles of a field of algebraic functions, Weil differentials and the Riemann-Roch theorem. We put also the definition of local components of the Weil differentials and the theory of codes. We define the minimum distance of a code and a geometric code of Goppa. Now, we have a motivation for the definition of a geometric

code of Goppa; we consider the Reed Solomon code, a vector space over the field finite with q elements $\mathbb{F}_q$. The geometric codes of Goppa are a generalization of Reed-Solomon codes.

We consider $n = q - 1$ and $\beta \in \mathbb{F}_q$ an element such that

$$\mathbb{F}_q \setminus \{0\} = \left\{\beta, \beta^2, \ldots, \beta^n = 1\right\}.$$

For $k \in \mathbb{Z}$, with $1 \leq k \leq n$, we consider the $\mathbb{F}_q$-vector space k-dimensional,

$$\mathcal{L}_k := \{f \in \mathbb{F}_q[X] \mid \deg(f) \leq k - 1\},$$

and the application

$$e_v : \mathcal{L}_k \longrightarrow \mathbb{F}_q^n \text{ given by } e_v(f) := \left(f(\beta), f\left(\beta^2\right), \ldots, f\left(\beta^n\right)\right) \in \mathbb{F}_q^n.$$

Note that this application is $\mathbb{F}_q$-linear, since given $\lambda \in \mathbb{F}_q$ and f, $g \in \mathcal{L}_k$, we have that $e_v(f + \lambda g) = e_v(f) + \lambda(e_v(g))$.

Observe that e_v also is injective, because given a polynomial not null $f \in \mathbb{F}_q[X]$ such that $f \in \mathcal{L}_k$, we have that the $\deg(f) \leq k - 1 \leq n - 1 < n$ and hence f has a number of zeros small than n and thus,

$$\operatorname{Ker}(e_v) = \{f \in \mathcal{L}_k \mid e_v(f) = 0\} = \{0\}$$

and so e_v is injective (observe that $\operatorname{Ker}(e_v) = \{0\}$, since if there exists f not null in $\mathcal{L}_k$ such that $e_v(f) = 0$, the polynomial f has n roots $\beta, \beta^2, \ldots, \beta^n$, which is absurd). Therefore,

$$C_k := \{e_v(f) \mid f \in \mathcal{L}_k\}$$

is a code of length n and dimension k over the field $\mathbb{F}_q$. This code is called Reed-Solomon code.

The second part is about the floor of a divisor. We obtain quotas for the minimum distance of a geometric code of Goppa involving the floor of a divisor. We define a code over the field of Hermitian algebraic functions. With the results we obtain quotas for the minimum distance of this code.

2 Preliminary results

The contents of this section it follows of [7].

2.1 Prerequisites

Definition 2.1. A field of algebraic functions $F|K$ in a variable over the field K is an extension of fields $F \supset K$ such that F is an extension algebraic finite of $K(x)$ for some element $x \in F$ which is transcendent over K.

A valuation ring of the field of algebraic functions $F|K$ is a ring O of the field F with the following properties:

(1) $K \subset O \subset F$, and

(2) for all $z \in F$, we have that $z \in O$ or $z^{-1} \in O$.

We have that O (the valuation ring) is a local ring with ideal maximal $P = O \setminus O^*$ where $O^* := \{z \in O \mid \text{ there exists } w \in O \text{ with } z.w = 1\}$ is the group of units of O. Moreover, we have that P is a principal ideal.

Definition 2.2. A place P of the field of algebraic functions $F|K$ is the maximal ideal of some valuation ring O of $F|K$. All element $t \in P$ such that $P = tO = \{tp \mid p \in O\}$ is called a local parameter for P.

We denote by $\mathbb{P}_F := \{P \mid P \text{ is a place of } F|K\}$.

If O is a valuation ring of $F|K$ and P is its maximal ideal then O is determined by P, i.e.,

$$O := \left\{z \in F \mid z^{-1} \notin P\right\}.$$

Thus, $O_P := O$ is called the valuation ring of the place P or the valuation ring associated to the place P.

The next we define the concept of discrete valuation, which will be used in the sequel.

Definition 2.3. A discrete valuation of the field of algebraic functions $F|K$ is a function $v : F \to \mathbb{Z} \cup \{\infty\}$, which has the following properties:

(1) $v(x) = \infty \Leftrightarrow x = 0$.

(2) $v(xy) = v(x) + v(y)$ for all $x, y \in F$.

(3) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in F$.

(4) There exists an element $z \in F$ with $v(z) = 1$.

(5) $v(a) = 0$ for all $0 \neq a \in K$.

In this context, the symbol ∞ is not a number integer, and is such that $\infty + \infty = \infty + n = n + \infty = \infty$ and $\infty > m$ for all $m, n \in \mathbb{Z}$.

For all place P of the field of algebraic functions $F|K$, we associate the function $v_P : F \to \mathbb{Z} \cup \{\infty\}$. This function is defined as it follows: for t a local parameter for P we have that all element z not null in F has an unique representation $z = t^n u$, with $u \in O_P^* = O^*$ and $n \in \mathbb{Z}$; we define $v_P(z) := n$ and $v_P(0) := \infty$. This function so defined is a discrete valuation.

Definition 2.4. Let P be a place of the field of algebraic functions $F|K$.

(a) $\mathbb{F}_P := O_P/P$ is the residue field of P. The application $x \mapsto x(P)$ of F for $\mathbb{F}_P \cup \{\infty\}$ is called of function of residue classes with respect to P. We use also the notation $x(P) := x + P$, for $x \in O_P$.

(b) $\deg(P) := [\mathbb{F}_P : K]$ is called the degree of P.

We have that if P is a place of the field of algebraic functions $F|K$ and $0 \neq x \in P$, then $\deg(P) \leq [F : K(x)] < \infty$.

We take $z \in F$ and let P be a place of the field of algebraic functions $F|K$. We say that P is a zero of z iff $v_P(z) > 0$; P is a pole of z iff $v_P(z) < 0$. If $v_P(z) = m > 0$, P is a zero of z of order m; if $v_P(z) = -m < 0$, P is a pole of z of order m.

The group abelian free which has as base free the places of $F|K$ will be denoted by $\mathbb{D}_F$. Is called group of divisors of $F|K$. The elements uniques of $\mathbb{D}_F$ are called divisors of $F|K$, i.e., a divisor is a formal sum $D = \sum_{P \in \mathbb{P}_F} n_P P$, with $n_P \in \mathbb{Z}$ and almost all $n_P = 0$, i.e., $n_P \neq 0$ in a number finite of installments of this sum.

The support of the element $D \in \mathbb{D}_F$ is defined by

$$\operatorname{supp}(D) := \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

Two divisors D and D', with $D = \sum n_P P$ and $D' = \sum n'_P P$ are summed as it follows: $D + D' = \sum_{P \in \mathbb{P}_F} \left(n_P + n'_P\right) P$.

The neutral element for the sum of the group of divisors $\mathbb{D}_F$ is the divisor $0 = \sum_{P \in \mathbb{P}_F} r_P P$, with all $r_P = 0$. For Q a place and D a divisor of $F|K$, where $D = \sum_{P \in \mathbb{P}_F} n_P P$, we define $v_Q(D) = n_Q$ and therefore, $\operatorname{supp}(D) = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\}$ and $D = \sum_{P \in \operatorname{supp}(D)} v_P(D) P$.

A divisor $D \geq 0$, i.e., $v_P(D) \geq 0$ for all place P, is called divisor effective. The degree of a divisor is defined as

$$\deg(D) = \sum_{P \in \mathbb{P}_F} v_P(D) .\deg(P).$$

Definition 2.5. We take $0 \neq x \in F$ and we denote by Z, respectively N, the set of zeros, and the set of poles, of x in $\mathbb{P}_F$. Then we define:

$(x)_0 := \sum_{P \in Z} v_P(x) P$, the divisor of zeros of x; $(x)_\infty := \sum_{P \in N} -v_P(x) P$, the divisor of poles of x; $(x) := (x)_0 - (x)_\infty$, the divisor principal of x.

As $v_P(x) > 0$ for all $P \in Z$ it follows that $(x)_0 \geq 0$, and as $v_P(x) < 0$ for all $P \in N$ we have that $-v_P(x) > 0$, and then $(x)_\infty \geq 0$.

Moreover, $(x) = \sum_{P \in \mathbb{P}_F} v_P(x) P$.

Definition 2.6. For a divisor $A \in \mathbb{D}_F$ we define,

$$\mathcal{L}(A) := \{x \in F \mid (x) + A \geq 0\} \cup \{0\}.$$

We have that $\mathcal{L}(A)$, according to Definition 2.6, is a vector space over the field K. The dimension of each K-vector space V will be denoted by $\ell(V)$. Moreover, the vector space $\mathcal{L}(A)$ has dimension finite, for all divisor A of the field of algebraic functions $F|K$.

Lemma 2.7. (see [7]) *We have that:*

(a) $\mathcal{L}(0) = K$.

(b) *If* $A \in \mathbb{D}_F$ *and* $A < 0$ *then* $\mathcal{L}(A) = \{0\}$.

Definition 2.8. For $A \in \mathbb{D}_F$, we define the dimension of the divisor A, and we denote by $\ell(A)$, as the dimension of the vector space $\mathcal{L}(A)$, i.e., $\ell(A) = \ell(\mathcal{L}(A))$.

The genus g of the field of algebraic functions $F|K$ is defined by

$$g := \max\{\deg(A) - \ell(A) + 1 \mid A \in \mathbb{D}_F\}.$$

The genus of $F|K$ is a non-negative integer.

Definition 2.9. An adele of the field of algebraic functions $F|K$ is an application $\alpha : \mathbb{P}_F \longrightarrow F$, given by $\alpha(P) = \alpha_P$, such that $\alpha_P \in O_P$, for almost all the places P of $F|K$.

According to the Definition 2.9 we can consider an adele as a sequence in the field F, and therefore we use the notation $\alpha = (\alpha_P)_{P\in\mathbb{P}_F}$ or $\alpha = (\alpha_P)$. The set

$$\mathbb{A}_F := \{\alpha \mid \alpha \text{ is an adele of } F|K\},$$

is called the space of adeles of $F|K$. This set is a vector space over the field K.

The principal adele of an element $x \in F$ is the adele whose components are all equals to x, and note that $\alpha_P = x \in O_P$, for almost all the places P of $F|K$ make sense, since x not null in F has a finite quantity of poles and zeros. We take the application that take $x \in F$ in the your principal adele; this is a diving of F in $\mathbb{A}_F$, since is a bijective application, and then we can write $F \hookrightarrow \mathbb{A}_F$.

As we have this diving, the discrete valuation v_P associated to the place P of $F|K$ naturally extends to $\mathbb{A}_F$, where we put $v_P(\alpha) := v_P(\alpha_P)$, being that we have α_P the P component of the adele α. By definition $v_P(\alpha) \geq 0$, for almost all the places P of $F|K$.

Definition 2.10. For $A \in \mathbb{D}_F$ we define the following set

$$\mathbb{A}_F(A) := \{\alpha \in \mathbb{A}_F \mid v_P(\alpha) \geq -v_P(A), \text{ for all place } P \text{ of } F|K\}.$$

This set is an K-vector subspace of $\mathbb{A}_F$. We introduce now the concept of Weil differential.

Definition 2.11. A Weil differential of the field of algebraic functions $F|K$ is an application K-linear

$$\omega : \mathbb{A}_F \longrightarrow K,$$

that is null in $\mathbb{A}_F(A) + F$, for some divisor $A \in \mathbb{D}_F$. We define the module of Weil differential of $F|K$ by

$$\Omega_F := \{\omega \mid \omega \text{ is a Weil differential of } F|K\},$$

and we have that Ω_F is an F-vector space.

For $A \in \mathbb{D}_F$ we consider

$$\Omega_F(A) := \{\omega \in \Omega_F \mid \omega \text{ is null in } \mathbb{A}_F(A) + F\}.$$

We have that $\Omega_F(A)$ is a vector space over the field K.

Definition 2.12. For $x \in F$ and $\omega \in \Omega_F$, we define the Weil differential

$$x\omega : \mathbb{A}_F \longrightarrow K \text{ by } (x\omega)(\alpha) := \omega(x\alpha).$$

Definition 2.13. Let P be a place of the field of algebraic functions $F|K$.

(*a*) For $x \in F$ we put $\iota_P(x) \in \mathbb{A}_F$ the adele whose P-component is x and all the others components are equals to zero.

(*b*) For a Weil differential $\omega \in \Omega_F$ we define the your local component as the function $\omega_P : F \longrightarrow K$ given by

$$\omega_P(x) := \omega(\iota_P(x)).$$

We have that ω_P is an application K-linear.

We want has a divisor for any Weil differential $\omega \neq 0$. We consider for a given ω the set

$$M(\omega) := \{A \in \mathbb{D}_F \mid \omega \text{ is null over } \mathbb{A}_F(A) + F\}.$$

Lemma 2.14. ([7]) *We take $0 \neq \omega \in \Omega_F$. Then, there exists an unique divisor $W \in M(\omega)$ such that $A \leq W$, for any $A \in M(\omega)$.*

The next definition make sense by the Lemma 2.14.

Definition 2.15. (*a*) The divisor (ω) of a Weil differential ω not null is the unique divisor of the field of algebraic functions $F|K$ such that:

(1) ω is null over $\mathbb{A}_F((\omega)) + F$.
(2) If ω is null over $\mathbb{A}_F(A) + F$ then $A \leq (\omega)$.

(*b*) For $\omega \in \Omega_F \setminus \{0\}$ and P a place of $F|K$, we define $v_P(\omega) := v_P((\omega))$.

(*c*) A place P is said to be a zero, respectively a pole, of ω if $v_P(\omega) > 0$, respectively $v_P(\omega) < 0$. We say that ω is regular in P if $v_P(\omega) \geq 0$ and ω is called regular, if ω is regular for any place P of $F|K$.

(*d*) A divisor W is called a canonical divisor of $F|K$ if $W = (\omega)$, for some ω Weil differential not null of $F|K$.

It follows of the Definition 2.15 that:

(1) $\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0 \text{ or } (\omega) \geq A\}$.

(2) $\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ is regular }\}$.

We presented now one of the most important theorems of the theory of fields of algebraic functions.

Theorem 2.16. (see [7])**[Riemann-Roch]** *Let W be a canonical divisor of the field of algebraic functions $F|K$ of genus g. Then, for any divisor A of $F|K$, we have that the dimension of A satisfies the following equality:*

$$\ell(A) = \deg(A) + 1 - g + \ell(W - A).$$

Corollary 2.17. (see [7]) *For a canonical divisor W of the field of algebraic functions $F|K$ of genus g we have that*

$$\deg(W) = 2g - 2 \text{ and } \ell(W) = g.$$

3 On the definition of codes

The contents of this section it follows of [7].

3.1 The basic definitions

Let $\mathbb{F}_q$ be a field finite with q elements. We consider the vector space of dimension n over $\mathbb{F}_q$, $\mathbb{F}_q^n$, where the elements are of the following form $(a_1, \ldots, a_n)$, with a_i in the field $\mathbb{F}_q$, for all $i = 1, \ldots, n$.

For $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in $\mathbb{F}_q^n$, we take

$$d(a, b) := |\{i \mid a_i \neq b_i\}|.$$

The function d, that we presented above, define a distance in $\mathbb{F}_q^n$ and is called of *Hamming Distance* in $\mathbb{F}_q^n$. The weight of a element $a \in \mathbb{F}_q^n$ is defined as $\omega(a) := d(a, 0) = |\{i \mid a_i \neq 0\}|$.

Definition 3.1. A code C over the field $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$. The elements of C are called of words of the code. The natural number n, that appear in $\mathbb{F}_q^n$, is called the length of the code C and $\ell(C)$ is the dimension of C as $\mathbb{F}_q$-vector space. A code of length n and dimension k is denoted by $[n, k]$. The *minimum distance* of a code $C \neq \{0\}$ is denoted by $d(C)$ and is defined as

$$d(C) := \min\{d(a,b) \mid a,b \in C \text{ and } a \neq b\}.$$

As $d(a,b) = |\{i \mid a_i - b_i \neq 0\}| = d(a-b,0) = \omega(a-b)$ and $a-b \in C$, since C is a vector space, it follows that the minimum distance is such that

$$d(C) := \min\{\omega(c) \mid 0 \neq c \in C\}.$$

A code $[n,k]$ with minimum distance d will be refered as a code $[n,k,d]$.

The canonical inner product over $\mathbb{F}_q^n$ is defined by,

$$\langle a,b\rangle := \sum_{i=1}^{n} a_i b_i,$$

for $a = (a_1,\ldots,a_n)$ and $b = (b_1,\ldots,b_n) \in \mathbb{F}_q^n$.

Definition 3.2. If $C \subseteq \mathbb{F}_q^n$ is a code then

$$C^{\perp} := \left\{u \in \mathbb{F}_q^n \mid \langle u,c\rangle = 0, \forall c \in C\right\}$$

is called the code dual of C.

The code C is called self-dual, respectively self-orthogonal, if $C = C^{\perp}$, respectively, if $C \subseteq C^{\perp}$. Moreover, we have that $\left(C^{\perp}\right)^{\perp} = C$.

Now, let $F|\mathbb{F}_q$ be a field of algebraic functions of genus g and let $P_1,\ldots,P_n$ be places two to two differents of $F|\mathbb{F}_q$ of degree one. Moreover, we take $D = P_1+\ldots+P_n$. And let G be a divisor of $F|\mathbb{F}_q$ such that $\operatorname{supp}(G)\cap\operatorname{supp}(D) = \emptyset$. According to these considerations, the geometric code of Goppa $C_{\mathcal{L}}(D,G)$, associated with the divisors D and G, is defined by:

$$C_{\mathcal{L}}(D,G) := \{(x(P_1),\ldots,x(P_n)) \mid x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Definition 3.3. The integer $d^* := n - \deg(G)$ is called the *designated distance* of the code $C_{\mathcal{L}}(D,G)$.

We have that the minimum distance d of a geometric code of Goppa is such that $d^* \leq d$.

Now, we define an other code associated with the divisors G and D.

Definition 3.4. Let G and $D = P_1 + \ldots + P_n$ be divisors as before (i.e., we have that, for each i, P_i are places two to two differents of degree one and $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \emptyset$). Then, we define the code $C_{\Omega}(D,G) \subseteq \mathbb{F}_q^n$ by:

$$C_{\Omega}(D,G) := \{(\omega_{P_1}(1),\ldots,\omega_{P_n}(1)) \mid \omega \in \Omega_F(G-D)\}.$$

The following theorem will be used in the next section.

Theorem 3.5. (see [7]) *The codes $C_{\mathcal{L}}(D,G)$ and $C_{\Omega}(D,G)$ are dual, i.e.,*

$$C_{\Omega}(D,G) = C_{\mathcal{L}}(D,G)^{\perp}.$$

4 On the floor of a divisor

In this section we presented the results.

Given a divisor A of a field of algebraic functions $F|K$, there exists an unique divisor of minimum degree B that define the same vector space $\mathcal{L}(A)$, i.e., such that $\mathcal{L}(A) = \mathcal{L}(B)$.

A such divisor is called the floor of the divisor A.

4.1 The floor of a divisor

Throughout this section, $F|\mathbb{F}_q$ is a field of algebraic functions on the finite field $\mathbb{F}_q$ which has q elements.

Definition 4.1. Given two divisors A and $A^{'}$ of $F|\mathbb{F}_q$ the greatest common divisor of A and $A^{'}$ is the divisor

$$\text{m.d.c.}\left(A, A^{'}\right) := \sum_{P \in \mathbb{P}_F} \min\left\{v_P(A), v_P\left(A^{'}\right)\right\} P,$$

and the least common multiple between the divisors A and $A^{'}$ is the divisor

$$\text{m.m.c.}\left(A, A^{'}\right) := \sum_{P \in \mathbb{P}_F} \max\left\{v_P(A), v_P\left(A^{'}\right)\right\} P.$$

4.2 The results

Proposition 4.2. *Let G be a divisor of the field of algebraic functions $F|\mathbb{F}_q$ with $\ell(G) > 0$. Suppose that $G^{'}$ is a divisor of $F|\mathbb{F}_q$ of minimum degree such that $\mathcal{L}(G) = \mathcal{L}\left(G^{'}\right)$. Then, $G \geq G^{'}$. Hence, $G^{'}$ is the unique divisor with this property.*

Proof. By hypothesis, we have that $\mathcal{L}(G) = \mathcal{L}\left(G^{'}\right) \cap \mathcal{L}(G)$. Thus $\mathcal{L}\left(G^{'}\right) \cap \mathcal{L}(G) = \mathcal{L}\left(\text{m.d.c.}\left(G^{'}, G\right)\right)$: in fact, if $0 \neq x \in \mathcal{L}\left(G^{'}\right) \cap \mathcal{L}(G)$ then, by Definition 2.6, $(x) + G^{'} \geq 0$, $(x) + G \geq 0$. So, $\min\left\{v_P\left((x) + G^{'}\right), v_P((x) + G)\right\} = \min\left\{v_P((x)) + v_P\left(G^{'}\right), v_P((x)) + v_P(G)\right\} \geq 0, \ \forall\ P \in \mathbb{P}_F$.

On the other hand, it is seen that the minimum value of the set given previous is as it follows, $v_P(x) + \min\left\{v_P\left(G'\right), v_P(G)\right\}$. Therefore,

$$\sum_P \left(v_P(x) + \min\left\{v_P\left(G'\right), v_P(G)\right\}\right) P \geq 0,$$

for all $P \in \mathbb{P}_F$, i.e., $(x) + \text{m.d.c.}\left(G', G\right) \geq 0$. Thus, $x \in \mathcal{L}\left(\text{m.d.c.}\left(G', G\right)\right)$.

Conclusion: $\mathcal{L}\left(G'\right) \cap \mathcal{L}(G) \subseteq \mathcal{L}\left(\text{m.d.c.}\left(G', G\right)\right)$.

We consider $x \in \mathcal{L}\left(\text{m.d.c.}\left(G', G\right)\right)$. As $\min\left\{v_P(G), v_P\left(G'\right)\right\} \leq v_P(G)$ $\forall P \in \mathbb{P}_F$, it follows that:

$\sum_P \min\left\{v_P(G), v_P\left(G'\right)\right\} P \leq \sum_P v_P(G) P \Rightarrow 0 \leq (x) + \text{m.d.c.}\left(G, G'\right) \leq (x) + G \Rightarrow x \in \mathcal{L}(G) = \mathcal{L}\left(G'\right) \Rightarrow x \in \mathcal{L}(G) \cap \mathcal{L}\left(G'\right)$.

Conclusion: $\mathcal{L}\left(\text{m.d.c.}\left(G', G\right)\right) \subseteq \mathcal{L}\left(G'\right) \cap \mathcal{L}(G)$.

Thus $\mathcal{L}(G) = \mathcal{L}(G) \cap \mathcal{L}\left(G'\right) = \mathcal{L}\left(\text{m.d.c.}\left(G', G\right)\right)$. Therefore, it follows of the minimum degree of G' that, $\deg\left(G'\right) \leq \deg\left(\text{m.d.c.}\left(G', G\right)\right)$.

As $\min\left\{v_P\left(G'\right), v_P(G)\right\} \leq v_P\left(G'\right)$ for all place P, we obtain

$$\sum_P \min\left\{v_P\left(G'\right), v_P(G)\right\} P \leq \sum_P v_P\left(G'\right) P,$$

and then we have that $\text{m.d.c.}\left(G', G\right) \leq G'$. Therefore, we have: $\deg\left(G'\right) \leq \deg\left(\text{m.d.c.}\left(G', G\right)\right)$ and $\text{m.d.c.}\left(G', G\right) \leq G'$. Thus, $\deg\left(\text{m.d.c.}\left(G', G\right)\right) \leq \deg\left(G'\right)$ and therefore we have that $\deg\left(G'\right) = \deg\left(\text{m.d.c.}\left(G', G\right)\right)$; as $\text{m.d.c.}\left(G', G\right) \leq G'$ we have that, $G' = \text{m.d.c.}\left(G', G\right)$. Hence, $G' \leq G$, since $\text{m.d.c.}\left(G', G\right) \leq G$.

Suppose now that G' and G'' are two divisors of $F|\mathbb{F}_q$ of minimum degree such that, $\mathcal{L}(G) = \mathcal{L}\left(G'\right)$ and $\mathcal{L}(G) = \mathcal{L}\left(G''\right)$. Now, of G'' divisor of minimum degree such that $\mathcal{L}\left(G'\right) = \mathcal{L}\left(G''\right)$ it follows, of the done previously, that $G' \geq G''$ and of G' divisor of minimum degree such that $\mathcal{L}\left(G''\right) = \mathcal{L}\left(G'\right)$, we have that $G'' \geq G'$. Therefore, $G' = G''$. Hence, there exists an unique divisor G' of $F|\mathbb{F}_q$ of minimum degree such that $\mathcal{L}(G) = \mathcal{L}\left(G'\right)$. $\square$

Definition 4.3. Given a divisor G of the field of algebraic functions $F|\mathbb{F}_q$ with $\ell(G) > 0$, the floor of G is the unique divisor G' of $F|\mathbb{F}_q$ of minimum degree such that $\mathcal{L}(G) = \mathcal{L}\left(G'\right)$. The floor of G will be denoted by $\lfloor G \rfloor$.

4.3 The quotas of the floor and of the generalized floor

We introduce the floor's quota theorem, that we will give a generalization called generalized floor quota. Next, we will give an example where we will apply this quota for to estimate improvement of the minimum distance of a code.

The next proposition will be used in the sequel.

Proposition 4.4. *If G is a divisor effective of the field of algebraic functions $F|\mathbb{F}_q$ then the floor of G also is a divisor effective. In particular, if G is a divisor effective then the support of $\lfloor G \rfloor$ is a subset of the support of G.*

Proof. As $G \geq 0$, the elements of $\mathbb{F}_q$ belongs to $\mathcal{L}(G)$. Thus, we have that

$$-\min\{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\} \geq 0.$$

We take $E := \text{m.d.c.}(G + (x) \mid x \in \mathcal{L}(G) \setminus \{0\})$. So, it follows that $\lfloor G \rfloor = G - E$. So, $v_P(\lfloor G \rfloor) = -\min\{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\}$ the that implies $v_P(\lfloor G \rfloor) \geq 0$, $\forall P \in \mathbb{P}_F$. Thus, $\lfloor G \rfloor$ is a divisor effective. As $G \geq \lfloor G \rfloor$, we have $v_P(G) \geq v_P(\lfloor G \rfloor), \forall P \in \mathbb{P}_F$, and hence the support of the floor of G is contained in the support of G. □

Moreover, also will be used in the sequel the following result.

Lemma 4.5. (see [7]) *Let A and B be two divisors of the field of algebraic functions $F|K$ with $A \leq B$. Then, we have that $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ and $\ell(B) - \ell(A) \leq \deg(B) - \deg(A)$.*

Theorem 4.6 (Floor quota). *Let $F|\mathbb{F}_q$ be a field of algebraic functions of genus g. Let $D = P_1 + \ldots + P_n$ be a divisor, where $P_1, \ldots, P_n$ are places two to two different of $F|\mathbb{F}_q$, where each divisor have degree equal to one, and let $G := H + \lfloor H \rfloor$ be a divisor of $F|\mathbb{F}_q$ such that H is a divisor effective whose support does not contain any of the places $P_1, \ldots, P_n$. Let $E_H := H - \lfloor H \rfloor$ be a divisor. Then, $C_\Omega(D, G)$ is a code $[n, k, d]$ whose minimum distance satisfies:*

$$d = d(C_\Omega(D, G)) \geq \deg(G) - (2g - 2) + \deg(E_H) = 2\deg(H) - (2g - 2).$$

Proof. As H is a divisor effective, we have, according to the Proposition 4.4, that $\lfloor H \rfloor$ is effective and $\text{supp}(\lfloor H \rfloor) \subseteq \text{supp}(H)$. Thus, $G := H + \lfloor H \rfloor$ is a divisor effective and as the supports of the divisors H and D are disjoint,

it follows that the supports of the divisors G and D are also disjoint. We chose a Weil differential $\eta \in \Omega_F(G-D)$ such that the code word $c_0 := (\eta_{P_1}(1), \ldots, \eta_{P_n}(1))$ is of minimum weight. By definition, the minimum distance of a code is the minimum of the set of the weights of the code words not nulls; thus, we can assume, without loss of generality, that the first d-coordinates of c_0 are not nulls and that the remaining coordinates are nulls. Then, with $D' := P_1 + \ldots + P_d$ we obtain, according to Definition 2.15, that $(\eta) \geq G - D'$, since as $\operatorname{supp}(D') \subseteq \operatorname{supp}(D)$ and $(\eta) \geq G - D$ it follows that $v_Q(\eta) \geq v_Q(G-D)$, for all place Q of $F|\mathbb{F}_q$ that belongs to the support of D and then, in particular, this is applied to every place that belongs to the support of D'. Thus, there exists a divisor effective A such that $(\eta) = G - D' + A$ and whose support does not contain any of the places $P_1, \ldots, P_d$. In the equality $(\eta) = G - D' + A$, we take the degree of the divisors on both sides, and hence we have that $\deg((\eta)) = \deg(G) - d + \deg(A)$, and as $\deg((\eta)) = 2g-2$, (see the Corollary 2.17) since (η) is canonical divisor, it follows that $2g-2 = \deg(G) - d + \deg(A)$, and therefore $d = \deg(G) - (2g-2) + \deg(A)$. In order to prove the assertion about the minimum distance quota, it is sufficient to show that $\deg(A) \geq \deg(E_H)$. Observe that $\deg(A) \geq \ell(H+A) - \ell(H) = \ell(H+A) - \ell(\lfloor H \rfloor) \geq \ell(H+A) - \ell(\lfloor H \rfloor + A)$. In fact,
(1) $\deg(A) \geq \ell(H+A) - \ell(H)$, since as $A \geq 0$ we have that $H + A \geq H$ and then, by the Lemma 4.5, it follows that $\ell(H+A) - \ell(H) \leq \deg(H+A) - \deg(H) = \deg(A)$. Therefore, $\deg(A) \geq \ell(H+A) - \ell(H)$.
(2) $\ell(H+A) - \ell(H) = \ell(H+A) - \ell(\lfloor H \rfloor)$, since as $\mathcal{L}(H) = \mathcal{L}(\lfloor H \rfloor)$, we have that $\ell(H) = \ell(\lfloor H \rfloor)$, as desired.
(3) $\ell(H+A) - \ell(\lfloor H \rfloor) \geq \ell(H+A) - \ell(\lfloor H \rfloor + A)$, since as $\lfloor H \rfloor \leq \lfloor H \rfloor + A$ it follows that $\mathcal{L}(\lfloor H \rfloor) \subseteq \mathcal{L}(\lfloor H \rfloor + A)$; thus, $\ell(\lfloor H \rfloor) \leq \ell(\lfloor H \rfloor + A)$ and then $-\ell(\lfloor H \rfloor) \geq -\ell(\lfloor H \rfloor + A)$ and adding $\ell(H+A)$ on both sides of this inequality we have the result.

We show now that $\deg(E_H) = \ell(H+A) - \ell(\lfloor H \rfloor + A)$. We have $W = G - D' + A$ canonical divisor. We take the divisor $H + A$ and the divisor $\lfloor H \rfloor + A$; by the Riemann-Roch Theorem (Theorem 2.16) we obtain the following equalities:

(1) $\ell(H+A) = \deg(H+A) + 1 - g + \ell(W - H - A)$ and
(2) $\ell(\lfloor H \rfloor + A) = \deg(\lfloor H \rfloor + A) + 1 - g + \ell(W - \lfloor H \rfloor - A)$.

Thus, $\ell(H+A) - \ell(\lfloor H \rfloor + A) = \deg(H) + \ell(W - H - A) - \deg(\lfloor H \rfloor) - \ell(W - \lfloor H \rfloor - A)$.

Therefore, $\ell(H+A)-\ell(\lfloor H\rfloor+A)=\deg(H-\lfloor H\rfloor)+\ell(W-H-A)-\ell(W-\lfloor H\rfloor-A)=\deg(E_H)+\ell(W-H-A)-\ell(W-\lfloor H\rfloor-A)$.

As $W-A=G-D'$ and $G=H+\lfloor H\rfloor$, we obtain that:

$$\ell(H+A)-\ell(\lfloor H\rfloor+A)=\deg(E_H)+\ell\left(\lfloor H\rfloor-D'\right)-\ell\left(H-D'\right).$$

We show now that $\mathcal{L}\left(\lfloor H\rfloor-D'\right)=\mathcal{L}\left(H-D'\right)$. As $H-D'\leq H$, it follows that $\mathcal{L}\left(H-D'\right)\subseteq\mathcal{L}(H)$ and then $\mathcal{L}\left(H-D'\right)\subseteq\mathcal{L}(\lfloor H\rfloor)$, and thus $\mathcal{L}\left(H-D'\right)=\mathcal{L}\left(H-D'\right)\cap\mathcal{L}(\lfloor H\rfloor)$. Note that $\mathcal{L}\left(H-D'\right)\cap\mathcal{L}(\lfloor H\rfloor)=\mathcal{L}\left(\text{m.d.c.}\left(H-D';\lfloor H\rfloor\right)\right)$.

In fact, for $0\neq x\in\mathcal{L}\left(H-D'\right)\cap\mathcal{L}(\lfloor H\rfloor)$, $(x)+H-D'\geq 0$ and $(x)+\lfloor H\rfloor\geq 0$ and then for all place P we have that $v_P\left((x)+H-D'\right)\geq 0$ and $v_P((x)+\lfloor H\rfloor)\geq 0$ and thus,

$$\begin{gathered}\min\left\{v_P\left((x)+H-D'\right);v_P((x)+\lfloor H\rfloor)\right\}=\\ v_P((x))+\min\left\{v_P\left(H-D'\right);v_P(\lfloor H\rfloor)\right\}\geq 0,\end{gathered}$$

for all place P of $F|\mathbb{F}_q$. Therefore,

$$\sum_P\left(v_P((x))+\min\left\{v_P\left(H-D'\right);v_P(\lfloor H\rfloor)\right\}\right)P\geq 0.$$

Thus it follows that, $(x)+\text{m.d.c.}\left(H-D';\lfloor H\rfloor\right)\geq 0$ and then $x\in\mathcal{L}\left(\text{m.d.c.}\left(H-D',\lfloor H\rfloor\right)\right)$. Therefore,

$$\mathcal{L}\left(H-D'\right)\cap\mathcal{L}(\lfloor H\rfloor)\subseteq\mathcal{L}\left(\text{m.d.c.}\left(H-D',\lfloor H\rfloor\right)\right).$$

If $0\neq x\in\mathcal{L}\left(\text{m.d.c.}\left(H-D',\lfloor H\rfloor\right)\right)$ by definition we have that, $(x)+\text{m.d.c.}\left(H-D',\lfloor H\rfloor\right)\geq 0$. We have that, $\min\left\{v_P\left(H-D'\right),v_P(\lfloor H\rfloor)\right\}\leq v_P\left(H-D'\right),\forall$ place P. Thus, $0\leq(x)+\text{m.d.c.}\left(H-D',\lfloor H\rfloor\right)\leq(x)+\left(H-D'\right)$; and so $x\in\mathcal{L}\left(H-D'\right)\subseteq\mathcal{L}(\lfloor H\rfloor)$ and then $x\in\mathcal{L}\left(H-D'\right)\cap\mathcal{L}(\lfloor H\rfloor)$. Therefore, $\mathcal{L}\left(\text{m.d.c.}\left(H-D',\lfloor H\rfloor\right)\right)\subseteq\mathcal{L}\left(H-D'\right)\cap\mathcal{L}(\lfloor H\rfloor)$. So, $\mathcal{L}\left(\text{m.d.c.}\left(H-D',\lfloor H\rfloor\right)\right)=\mathcal{L}\left(H-D'\right)\cap\mathcal{L}(\lfloor H\rfloor)$.

By hypothesis, $\text{supp}(H)\cap\text{supp}(D)=\emptyset$ and as D' is a divisor effective such that $D'\leq D$ we have that $\text{supp}(H)\cap\text{supp}\left(D'\right)=\emptyset$ and as $\text{supp}(\lfloor H\rfloor)\subseteq\text{supp}(H)$ it follows that $\text{supp}(\lfloor H\rfloor)\cap\text{supp}\left(D'\right)=\emptyset$. By the definition, the maximum common divisor between $H-D'$ and $\lfloor H\rfloor$ is the divisor whose coefficients of the places are the minimum of the coefficients of the places of $H-D'$ and $\lfloor H\rfloor$, and as $H\geq\lfloor H\rfloor$ we conclude that $\text{m.d.c.}\left(H-D',\lfloor H\rfloor\right)=\lfloor H\rfloor-D'$.

It follows then that $\mathcal{L}\left(\text{m.d.c.}\left(H-D^{'},\lfloor H\rfloor\right)\right)=\mathcal{L}\left(\lfloor H\rfloor-D^{'}\right)$ and, as we have $\mathcal{L}\left(\text{m.d.c.}\left(H-D^{'},\lfloor H\rfloor\right)\right)=\mathcal{L}\left(H-D^{'}\right)\cap\mathcal{L}\left(\lfloor H\rfloor\right)=\mathcal{L}\left(H-D^{'}\right)$, since $\mathcal{L}\left(H-D^{'}\right)\subseteq\mathcal{L}\left(\lfloor H\rfloor\right)$, we obtain that $\mathcal{L}\left(\lfloor H\rfloor-D^{'}\right)=\mathcal{L}\left(H-D^{'}\right)$. Therefore:

$$\begin{aligned} d &= d\left(C_{\Omega}\left(D,G\right)\right) \\ &= \deg\left(G\right)-\left(2g-2\right)+\deg\left(A\right) \\ &\geq \deg\left(G\right)-\left(2g-2\right)+\deg\left(E_{H}\right) \\ &= \deg\left(H\right)+\deg\left(\lfloor H\rfloor\right)-\left(2g-2\right)+\deg\left(H\right)-\deg\left(\lfloor H\rfloor\right) \\ &= 2\deg\left(H\right)-\left(2g-2\right). \end{aligned}$$

□

Next, we presented the generalized floor quota theorem.

Theorem 4.7 (**Generalized floor quota).** *Let $F|\mathbb{F}_q$ be a field of algebraic functions of genus g. Let $P_1,\ldots,P_n$ be places two to two different of $F|\mathbb{F}_q$, of degree one. With $D:=P_1+\ldots+P_n$, let A, B, G, Z be divisors with the support disjoint of the support of D such that Z is effective and with $\ell\left(A\right)=\ell\left(A-Z\right)$, $\ell\left(B\right)=\ell\left(B+Z\right)$ and $G=A+B$. Then, the minimum distance d of the code $C_{\Omega}\left(D,G\right)$ is such that:*

$$d=d\left(C_{\Omega}\left(D,G\right)\right)\geq\deg\left(G\right)-\left(2g-2\right)+\deg\left(Z\right).$$

Proof. We consider $\eta\in\Omega_{F}\left(G-D\right)$, such that the code word

$$c_0:=\left(\eta_{P_1}\left(1\right),\ldots,\eta_{P_n}\left(1\right)\right),$$

is of minimum weight not null. As the minimum distance d of $C_{\Omega}\left(D,G\right)$ is such that

$$d\left(C_{\Omega}\left(D,G\right)\right)=\min\left\{\omega\left(c\right)\ |\ 0\neq c\in C_{\Omega}\left(D,G\right)\right\},$$

we can suppose, without loss of generality, that $c_i\neq 0$, for $1\leq i\leq d$ and $c_i=0$, for $d<i\leq n$. We put $D^{'}:=P_1+\ldots+P_d$. By hypothesis, we have that $\text{supp}\left(G\right)\cap\text{supp}\left(D\right)=\emptyset$, since $G=A+B$, A and B are divisors with support disjoint of the support of D. As $\text{supp}\left(D^{'}\right)\subseteq\text{supp}\left(D\right)$ it follows that $\text{supp}\left(G\right)\cap\text{supp}\left(D^{'}\right)=\emptyset$. Since $v_Q\left(\eta\right)\geq v_Q\left(G-D\right)$, for all place Q of $F|\mathbb{F}_q$, such that $Q\in\text{supp}\left(D\right)$ it follows, in particular, that we have for all $Q\in\text{supp}\left(D^{'}\right)$. Therefore, we should have $\left(\eta\right)\geq G-D^{'}$. Thus, there exists

a divisor effective E, with support disjoint of the support of $D^{'}$, such that $W := (\eta) = G - D^{'} + E$, and so we have that W is a canonical divisor and so $\deg(W) = 2g-2$. We consider the degree of the divisors on both sides of equality $W := G - D^{'} + E$ and we obtain that, $2g-2 = \deg(G) - d + \deg(E)$ and this implies that $d = \deg(G) - (2g-2) + \deg(E)$.

Observe that $\deg(E) \geq \ell(A+E) - \ell(A) = \ell(A+E) - \ell(A-Z)$. In fact, by Lemma 4.5, we have that $\ell(A+E) - \ell(A) \leq \deg(A+E) - \deg(A) = \deg(E)$, and thus $\deg(E) \geq \ell(A+E) - \ell(A)$; as, by hypothesis, $\ell(A) = \ell(A-Z)$ it follows that $\ell(A+E) - \ell(A) = \ell(A+E) - \ell(A-Z)$. Therefore, $\deg(E) \geq \ell(A+E) - \ell(A-Z)$. Since E is a divisor effective it follows that, $A+E-Z \geq A-Z$ and thus, $\mathcal{L}(A-Z) \subseteq \mathcal{L}(A+E-Z)$. So, $\ell(A-Z) \leq \ell(A+E-Z)$, and hence $-\ell(A-Z) \geq -\ell(A+E-Z)$. Therefore, $\deg(E) \geq \ell(A+E) - \ell(A+E-Z)$. By applying the Riemann-Roch Theorem (Theorem 2.16) to the divisors $A+E$ and $A+E-Z$, we obtain that:

(1) $\ell(A+E) = \deg(A+E) + 1 - g + \ell(W - (A+E))$,
(2) $\ell(A+E-Z) = \deg(A+E-Z) + 1 - g + \ell(W - (A+E-Z))$.

Thus, we obtain the following equality:

$$\begin{aligned}&\ell(A+E) - \ell(A+E-Z) = \\ &\ell(W-(A+E)) - \ell(W-(A+E-Z)) + \deg(Z) = \\ &\deg(Z) + \ell\left(W - A + G - D^{'} - W\right) - \ell\left(W + Z - A + G - D^{'} - W\right),\end{aligned}$$

and then, we have that

$$\ell(A+E) - \ell(A+E-Z) = \deg(Z) + \ell\left(B - D^{'}\right) - \ell\left(B + Z - D^{'}\right).$$

Now, as $B + Z - D^{'} \leq B + Z$ we have that $\mathcal{L}\left(B+Z-D^{'}\right) \subseteq \mathcal{L}(B+Z)$.

Since Z is effective, $B + Z \geq B$ and so $\mathcal{L}(B) \subseteq \mathcal{L}(B+Z)$; by hypothesis we have, $\ell(B) = \ell(B+Z)$ and thus it follows the equality, $\mathcal{L}(B) = \mathcal{L}(B+Z)$. Therefore, $\mathcal{L}\left(B+Z-D^{'}\right) \subseteq \mathcal{L}(B)$ and then $\mathcal{L}\left(B+Z-D^{'}\right) = \mathcal{L}\left(B+Z-D^{'}\right) \cap \mathcal{L}(B)$.

We show now that $\mathcal{L}\left(B+Z-D^{'}\right) = \mathcal{L}\left(\text{m.d.c.}\left(B+Z-D^{'}; B\right)\right)$. We consider $x \in \mathcal{L}\left(B+Z-D^{'}\right) = \mathcal{L}\left(B+Z-D^{'}\right) \cap \mathcal{L}(B)$. Then $(x) + B + Z - D^{'} \geq 0$ and $(x) + B \geq 0$. So, for all place P of $F|\mathbb{F}_q$, we have that $v_P\left((x) + B + Z - D^{'}\right) \geq 0$ and $v_P\left((x) + B\right) \geq 0$, and then we obtain that

$v_P((x)) + \min\left\{v_P\left(B + Z - D'\right); v_P(B)\right\} \geq 0$; therefore

$$x \in \mathcal{L}\left(\text{m.d.c.}\left(B + Z - D'; B\right)\right),$$

and thus $\mathcal{L}\left(B + Z - D'\right) \subseteq \mathcal{L}\left(\text{m.d.c.}\left(B + Z - D'; B\right)\right)$.

Now, if $x \in \mathcal{L}\left(\text{m.d.c.}\left(B + Z - D'; B\right)\right)$ we have

$$\min\left\{v_P\left(B + Z - D'\right); v_P(B)\right\} \leq v_P\left(B + Z - D'\right),$$

for all place P of $F|\mathbb{F}_q$, and so,

$$0 \leq (x) + \text{m.d.c.}\left(B + Z - D'; B\right) \leq (x) + B + Z - D'.$$

Therefore, $x \in \mathcal{L}\left(B + Z - D'\right) = \mathcal{L}\left(B + Z - D'\right) \cap \mathcal{L}(B)$.

Thus, $\mathcal{L}\left(\text{m.d.c.}\left(B + Z - D'; B\right)\right) \subseteq \mathcal{L}\left(B + Z - D'\right)$.

Conclusion: $\mathcal{L}\left(B + Z - D'\right) = \mathcal{L}\left(\text{m.d.c.}\left(B + Z - D'; B\right)\right)$.

We have that $\text{supp}\left(D'\right) \subseteq \text{supp}(D)$ and so, $\text{supp}(B) \cap \text{supp}\left(D'\right) = \emptyset$ and $\text{supp}(Z) \cap \text{supp}\left(D'\right) = \emptyset$. Since Z is effective, we have $B + Z \geq B$ and then $\text{m.d.c.}\left(B + Z - D'; B\right) = B - D'$. Thus, $\mathcal{L}\left(B + Z - D'\right) = \mathcal{L}\left(B - D'\right)$ and then $\ell\left(B + Z - D'\right) = \ell\left(B - D'\right)$. So,

$$\deg(E) \geq \ell(A + E) - \ell(A + E - Z) + \deg(Z)$$

which implies $\deg(E) \geq \ell\left(B - D'\right) - \ell\left(B + Z - D'\right) + \deg(Z) = \deg(Z)$. So, we have that $\deg(E) \geq \deg(Z)$. Therefore, $d = d\left(C_\Omega(D, G)\right) = \deg(G) - (2g - 2) + \deg(E) \geq \deg(G) - (2g - 2) + \deg(Z)$. □

Next, we exemplify as the floor quota and the generalized floor quota can be applieds. In this example we use the following result.

Theorem 4.8. (see [7])[**Weierstrass Gaps Theorem**] *Let $F|K$ be a field of algebraic functions of genus $g > 0$ and let P be a place of degree one of $F|K$. Then there are g gaps $i_1 < i_2 < \ldots < i_g$ of P. Moreover, we have that $i_1 = 1$ and $i_g \leq 2g - 1$.*

Example 4.9 (**Hermitian code of one place).** A Hermitian code is a code on the field of Hermitian functions. A field of functions $F|K$, where $K = \mathbb{F}_{q^2}$ with q a power rating of some prime number p and $F = K(x, y)$,

with equation given by $y^q + y = x^{q+1}$, is said to be a field of Hermitian functions. According to [7, Lemma $VI.4.4.$], this field of functions has genus $g = \frac{q(q-1)}{2}$ and $q^3 + 1$ places of degree one.

We consider a field finite with 16 elements $\mathbb{F}_{16}$ and the field of functions $\mathbb{F}_{16}(x, y) | \mathbb{F}_{16}$ with equation defined by $y^4 + y = x^5$. In this case, we have $q = 4$ and then the field of functions previously described is a field of Hermitian functions. So, the genus g of the field of functions is $g = 6$ and the same has $q^3+1 = 65$ places of degree one. We denote these places by $P_0, P_1, \ldots, P_{63}, P_\infty$ where, according to [7, Lemma $VI.4.4.$], P_∞ is the unique pole in commum of x and y. We consider the Weierstrass semigroup of the place P_∞, i.e., the set of the pole orders of P_∞:

$$H(P_\infty) := \{n \in \mathbb{N}_0 \mid \text{ there exists } x \in F \text{ with } (x)_\infty = nP_\infty\},$$

where $\mathbb{N}_0$ denote the set of non-negative integers. Thus, we define the set of the Weierstrass gaps of the place P_∞ by $G(P_\infty) := \mathbb{N}_0 \setminus H(P_\infty)$. We have that the Weierstrass semigroup of the place P_∞ is such that $H(P_\infty) \supset \langle 4, 5\rangle = \{0, 4, 5, 8, 9, 10, 12, 13, 14, \ldots\}$, since by [7, Proposition $VI.4.1.$] we have $(x)_\infty = qP_\infty$ and $(y)_\infty = (q+1)P_\infty$, with $q = 4$.

By the Theorem 4.8 we have that P_∞ has $g = 6$ gaps, which will be are denoted by n_1, n_2, n_3, n_4, n_5 and n_6, with $n_1 < n_2 < n_3 < n_4 < n_5 < n_6$ and by the Weierstrass Gaps Theorem $n_1 = 1$ and $n_i \leq 2g - 1 = 11$, for all $i = 1, \ldots, 6$. We show now that $n_2 = 2$, $n_3 = 3$, $n_4 = 6$, $n_5 = 7$ and $n_6 = 11$. Suppose that $n_6 < 11$. We could then have $n_6 = 10$, 9 or 8, but this is not possible, since 8, 9 and 10 belongs to $\langle 4, 5\rangle \subset H(P_\infty)$. Then, let $n_6 = 7$. In this case, at best we will have that $n_2 = 2$, $n_3 = 3$, $n_4 = 6$ and thus there are no possible values for n_5, what is absurd. Therefore, we can not have $n_6 = 7$. Now, if $n_6 = 6$, at best we will have that $n_2 = 2$, $n_3 = 3$ and then we have no values for n_4 and n_5, what is absurd. If $n_6 = 3$, at best we will have that $n_2 = 2$ and hence n_3, n_4 and n_5 do not receive any value, what is absurd. If $n_6 = 2$ there are no values for n_2, n_3, n_4 and n_5, what is absurd. We can then conclude that $n_6 = 11$ and thus we should have $n_2 = 2$, $n_3 = 3$, $n_4 = 6$ and $n_5 = 7$. Therefore, $\{1, 2, 3, 6, 7, 11\}$ is the set of the gaps of P_∞ and hence $\mathbb{N}_0 \setminus \{1, 2, 3, 6, 7, 11\}$ is the set of the pole orders of P_∞. Thus, it follows that $H(P_\infty) = \mathbb{N}_0 \setminus \{1, 2, 3, 6, 7, 11\}$.

Conclusion: $H(P_\infty) = \langle 4, 5\rangle$.

We recall that we have characterized a gap by the following:

i is a gap of a place of degree one Q if and only if $\mathcal{L}((i-1)Q) = \mathcal{L}(iQ)$.

Thus, since 11 is a gap of P_∞ we obtain that $\mathcal{L}(11P_\infty) = \mathcal{L}(10P_\infty)$ and as 7 also is a gap of P_∞ it follows that $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$. We consider the divisors $A = 11P_\infty$, $B = 6P_\infty$ and $Z = P_\infty$ and we put $G = A + B = 17P_\infty$ and $D := P_0 + P_1 + \ldots + P_{63}$. We consider the code $C_\Omega(D, G)$.

Definition 4.10. Let $F|K$ be a field of algebraic functions. If $G = mP$, for some place P of degree one, $m \in \mathbb{N}$ and D is a divisor which is the soma of all others places of degree one of $F|K$, we called the code $C_\Omega(D, G)$ of code of one place on the $F|K$.

According to the Definition 4.10 we have that $C_\Omega(D, G)$ is a code of one place on the field of Hermitian functions, i.e., is a Hermitian code of one place. Therefore, we have A, B, G and Z divisors whose support is disjoint of the support of D, Z is effective, $G = A + B$ and $\ell(A) = \ell(A - Z)$, since $\mathcal{L}(11P_\infty) = \mathcal{L}(10P_\infty)$ and $\ell(B) = \ell(B + Z)$, since $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$.

By the theorem of the Generalized Floor Quota (Theorem 4.7) it follows that:

$$d = d(C_\Omega(D, G)) \geq \deg(G) - (2g - 2) + \deg(Z) = 17 - 10 + 1 = 8.$$

We know that the designated distance of $C_\Omega(D, G)$ (see Definition 3.3) is given by

$$d^* = \deg(G) - (2g - 2) = 17 - 10 = 7.$$

As $d(C_\Omega(D, G))$ is at least 8, we obtain an improvement of at least one for the minimum distance of $C_\Omega(D, G)$ in relation to the your designated distance.

While the generalized floor quota provides this improvement the floor quota does not provides, since there is no way to write the divisor $G = 17P_\infty$ as $G = H + \lfloor H \rfloor$, where H is a divisor effective whose support is disjoint of the support of D. In fact, suppose that $G = 17P_\infty$ can be written in the manner previous described. Thus, H is of the form $H = aP_\infty$ and as H is a divisor effective we have that the floor of H also is effective and $\mathrm{supp}(\lfloor H \rfloor) \subseteq \mathrm{supp}(H)$ (see Proposition 4.4).

If H was equal to $0P_\infty$, $1P_\infty$, $2P_\infty$, $3P_\infty$, $4P_\infty$, $5P_\infty$, $6P_\infty$, $7P_\infty$ or $8P_\infty$ we should have, respectively, $\lfloor H \rfloor$ equal to $17P_\infty$, $16P_\infty$, $15P_\infty$, $14P_\infty$, $13P_\infty$, $12P_\infty$, $11P_\infty$, $10P_\infty$ and $9P_\infty$; in all these cases whether contrary the fact that $\lfloor H \rfloor \leq H$. If $H = 9P_\infty$ then we should has $\lfloor H \rfloor = 8P_\infty$ and so $\mathcal{L}(9P_\infty) = \mathcal{L}(8P_\infty)$, which implies that 9 is a gap, what is absurd. If $H = 10P_\infty$ then we should has $\lfloor H \rfloor = 7P_\infty$; if this occurs then $\mathcal{L}(10P_\infty) = \mathcal{L}(7P_\infty)$ and as 7 is a

gap it follows that $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$ and hence $\lfloor 10P_\infty \rfloor \neq 7P_\infty$, since the floor of H is the divisor of minimum degree such that $\mathcal{L}(H) = \mathcal{L}(\lfloor H \rfloor)$ and in this case we have $\deg(6P_\infty) < \deg(7P_\infty)$. If $H = 11P_\infty$ then, since G is written as the sum of H with the floor of H, we should has $\lfloor H \rfloor = 6P_\infty$; thus we have $\mathcal{L}(11P_\infty) = \mathcal{L}(6P_\infty) = \mathcal{L}(5P_\infty)$ and so $\lfloor 11P_\infty \rfloor \neq 6P_\infty$, by the same reason previously explained. If $H = 12P_\infty$, we should has $\lfloor H \rfloor = 5P_\infty$; thus we have $\mathcal{L}(12P_\infty) = \mathcal{L}(5P_\infty) = \mathcal{L}(6P_\infty) = \mathcal{L}(7P_\infty)$ and hence $\lfloor 7P_\infty \rfloor = 5P_\infty$ and therefore two different divisors have the same floor, which is absurd. If $H = 13P_\infty$ we should has $\lfloor H \rfloor = 4P_\infty$; while 13 is pole order and so $\mathcal{L}(13P_\infty) \neq \mathcal{L}(12P_\infty)$ and so, if we have that $\mathcal{L}(13P_\infty) = \mathcal{L}(4P_\infty)$ we should has $\mathcal{L}(4P_\infty) = \mathcal{L}(12P_\infty)$, since $4P_\infty \leq 12P_\infty$, thus $\mathcal{L}(13P_\infty) = \mathcal{L}(12P_\infty)$, what is absurd; therefore, $\lfloor 13P_\infty \rfloor \neq 4P_\infty$. If $H = 14P_\infty$, we should has $\lfloor H \rfloor = 3P_\infty$ and then $\mathcal{L}(14P_\infty) = \mathcal{L}(3P_\infty)$, and as 3 is gap it follows that, $\mathcal{L}(3P_\infty) = \mathcal{L}(2P_\infty)$ and so we have a divisor whose degree is smaller than the degree of $3P_\infty$ and $\mathcal{L}(2P_\infty) = \mathcal{L}(14P_\infty)$; it follows that we can not have $\lfloor 14P_\infty \rfloor = 3P_\infty$. If $H = 15P_\infty$ we should then has $\lfloor H \rfloor = 2P_\infty$; while 2 is gap and thus $\mathcal{L}(H) = \mathcal{L}(2P_\infty) = \mathcal{L}(1P_\infty)$ and so the floor of H can not be $2P_\infty$. If $H = 16P_\infty$ then your floor must be $1P_\infty$; while, 1 is gap and so, by the same argument, we can not have that $\lfloor H \rfloor = 1P_\infty$. Finally, if $H = 17P_\infty$ then we should has $\lfloor H \rfloor = 0P_\infty$; thus $\mathcal{L}(17P_\infty) = \mathcal{L}(0) = \mathbb{F}_{16}$ (see Lemma 2.7 (a)), which is absurd.

Conclusion: G it is not written as $G = H + \lfloor H \rfloor$, where H is a divisor effective whose support is disjoint of the support of D.

Remark 4.11. We show now that $C_\Omega(D, 17P_\infty) = C_\mathcal{L}(D, 57P_\infty)$.

In fact, by [7, Proposition VII.4.2.], we have, according to the Definition 3.2, that

$$C_\mathcal{L}(D, 57P_\infty)^\perp = C_{q^3+q^2-q-2-57} = C_{17} = C_\mathcal{L}(D, 17P_\infty).$$

By Theorem 3.5 we have that $C_\mathcal{L}(D, G)$ and $C_\Omega(D, G)$ are dual codes. Thus, $C_\mathcal{L}(D, 17P_\infty)^\perp = C_\Omega(D, 17P_\infty)$.

Now, note that as seen above

$$C_\mathcal{L}(D, 17P_\infty)^\perp = \left(C_\mathcal{L}(D, 57P_\infty)^\perp\right)^\perp = C_\mathcal{L}(D, 57P_\infty),$$

according to the Definition 3.2. Therefore, $C_\Omega(D, 17P_\infty) = C_\mathcal{L}(D, 57P_\infty)$, as required. Thus, by [6], we have that the minimum distance of this code is exactly 8.

5 Conclusion

In general, to obtain quotas for the minimum distance of a given code is not a very easy problem. One of the reasons for the interest in Goppa Geometric codes is that, for this great class of codes, it is possible to evaluate a good quota for the minimum distance.

For more references on this theory, see [1], [2], [3], [4], and [5].

The author of the article also recommends viewing the following articles [8], [9], and, [10].

References

[1] Carvalho, C., *On the distribution of ramification points in trigonal curves*, International Journal of Mathematics and Mathematical Sciences, 22, 489 - 496, 1999.

[2] Carvalho, C., *Weierstrass Gaps and Curves on a Scroll*, Contributions to Algebra and Geometry/Beitrage zur Algebra und Geometrie, 43, 209 - 216, 2002.

[3] Carvalho, C., *Pure gaps and bounds for the generalized Hamming weights of Goppa codes*, Contemporary Mathematics - American Mathematical Society (Print), 537, 123 - 128, 2011.

[4] Carvalho, C., *On semigroups, Gröbner basis and algebras admitting a complete set of near weights*, Semigroup Forum, 93, 17 - 33, 2016.

[5] Carvalho, C., *On generalized monomial codes defined over sets with a special vanishing ideal*, BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY, 55, number 15, 2024.

[6] Kumar, P. V., Stichtenoth, H., Yang, K., *On the Weight Hierarchy of Geometric Goppa Codes*, IEEE Transactions on Information Theory 40 (1994) 913 - 920.

[7] Stichtenoth, H., *Algebraic Function Fields and Codes*, Berlin Heidelberg New York: Springer-Verlag, 1993.

[8] Tognon, C.H., *Local Cohomology and Maximal Generalized Modules*, Asian Journal of Mathematics and Computer Research, 31, 1 - 7, 2024.

[9] C.H. Tognon, LOTAYIF, M., *A Note on Modules and Submodules over Polynomial Rings*, APPL MATH INFORM SCI, 15, 555 - 560, 2021.

[10] C.H. Tognon, Radwan A. Kharabsheh, *Some Properties of the Formal Local Cohomology Module and Application in the Theory of Graphs*, APPL MATH INFORM SCI, 16, 45 - 49, 2022.