A note about theory of codes of Goppa

Abstract

In this paper, we study about 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 a quota for the minimum distance of a geometric code of Goppa. A such quota involve the floor of a divisor and provide a estimate for the minimum distance of this code.

1 Introduction

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

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

Keywords: divisors, minimum distance, floor of a divisor, floor quota.

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*.

Moreover, we speak about the floor of a divisor. We obtain a quota for the minimum distance of a geometric code of Goppa involving the floor of a divisor, which is given in the Theorem 4.6.

2 Preliminary

The contents of this section it follows of [9].

Definition 2.1. 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 2.2. 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 2.2, 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 2.3. (see [9]) *We have that:*

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

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

Definition 2.4. 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 2.5. 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 2.5 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 2.6. 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 2.7. 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 2.8. 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 2.9. 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 2.10. ([9]) *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 2.10.

Definition 2.11. (*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 2.11 that:

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

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

Theorem 2.12. (see [9])[**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 2.13. (see [9]) *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

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 an 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 $\text{supp}(G) \cap \text{supp}(D) = \emptyset$. 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 $\text{supp}(G) \cap \text{supp}(D) = \emptyset$). 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 [9]) *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.

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

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

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

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

4.2 The results

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

Proof. By hypothesis, we have that $\mathcal{L}\left(G\right) = \mathcal{L}\left(G^{'}\right) \cap \mathcal{L}\left(G\right)$. Thus $\mathcal{L}\left(G^{'}\right) \cap \mathcal{L}\left(G\right) = \mathcal{L}\left(\text{m.d.c.}\left(G^{'}, G\right)\right)$: in fact, if $0 \neq x \in \mathcal{L}\left(G^{'}\right) \cap \mathcal{L}\left(G\right)$ then, by Definition 2.2, $\left(x\right) + G^{'} \geq 0$, $\left(x\right) + G \geq 0$. So, $\min\left\{v_P\left(\left(x\right) + G^{'}\right), v_P\left(\left(x\right) + G\right)\right\} = \min\left\{v_P\left(\left(x\right)\right) + v_P\left(G^{'}\right), v_P\left(\left(x\right)\right) + v_P\left(G\right)\right\} \geq 0, \ \forall\ P\ \in\ \mathbb{P}_F$.

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

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

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

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

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

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

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

Thus $\mathcal{L}\left(G\right) = \mathcal{L}\left(G\right) \cap \mathcal{L}\left(G^{'}\right) = \mathcal{L}\left(\text{m.d.c.}\left(G^{'}, G\right)\right)$. 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 $\min\left\{v_P\left(G^{'}\right), v_P\left(G\right)\right\} \leq v_P\left(G^{'}\right)$ for all place P, we obtain

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

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, $\mathcal{L}\left(G\right) = \mathcal{L}\left(G^{'}\right)$ and $\mathcal{L}\left(G\right) = \mathcal{L}\left(G^{''}\right)$. 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 $\mathcal{L}\left(G\right) = \mathcal{L}\left(G^{'}\right)$. □

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

4.3 The theorem of the quota of the floor

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 $\mathcal{L}\left(G\right)$. Thus, we have that

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

We take $E := \text{m.d.c.}\left(G + \left(x\right) \mid x \in \mathcal{L}\left(G\right) \setminus \{0\}\right)$. So, it follows that $\lfloor G \rfloor = G - E$. So, $v_P\left(\lfloor G \rfloor\right) = -\min\left\{v_P\left(x\right) \mid x \in \mathcal{L}\left(G\right) \setminus \{0\}\right\}$ the that implies $v_P\left(\lfloor G \rfloor\right) \geq 0$, $\forall P \in \mathbb{P}_F$. Thus, $\lfloor G \rfloor$ is a divisor effective. As $G \geq \lfloor G \rfloor$, we have $v_P\left(G\right) \geq v_P\left(\lfloor G \rfloor\right), \forall P \in \mathbb{P}_F$, 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 [9]) *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 differents 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 $\operatorname{supp}(\lfloor H \rfloor) \subseteq \operatorname{supp}(H)$. 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 2.11, 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 2.13) 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 2.12) 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,

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

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, $\min\left\{v_P\left(H - D^{'}\right), v_P\left(\lfloor H \rfloor\right)\right\} \leq v_P\left(H - D^{'}\right), \forall$ 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 $x \in \mathcal{L}\left(H - D^{'}\right) \subseteq \mathcal{L}\left(\lfloor H \rfloor\right)$ and then $x \in \mathcal{L}\left(H - D^{'}\right) \cap \mathcal{L}\left(\lfloor H \rfloor\right)$. Therefore, $\mathcal{L}\left(\text{m.d.c.}\left(H - D^{'}, \lfloor H \rfloor\right)\right) \subseteq \mathcal{L}\left(H - D^{'}\right) \cap \mathcal{L}\left(\lfloor H \rfloor\right)$. So, $\mathcal{L}\left(\text{m.d.c.}\left(H - D^{'}, \lfloor H \rfloor\right)\right) = \mathcal{L}\left(H - D^{'}\right) \cap \mathcal{L}\left(\lfloor H \rfloor\right)$.

By hypothesis, $\text{supp}\left(H\right) \cap \text{supp}\left(D\right) = \emptyset$ and as $D^{'}$ is a divisor effective such that $D^{'} \leq D$ we have that $\text{supp}\left(H\right) \cap \text{supp}\left(D^{'}\right) = \emptyset$ and as $\text{supp}\left(\lfloor H \rfloor\right) \subseteq \text{supp}\left(H\right)$ it follows that $\text{supp}\left(\lfloor H \rfloor\right) \cap \text{supp}\left(D^{'}\right) = \emptyset$. 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:

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

□

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]. Moreover, see also [6], and, [7].

The author of the article also recommends viewing the following articles [10], [11], and, [12], and, [13].

6 Acknowledgment

The author thanks the anonymous referees for their comments that helped improve the article.

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] Carvalho, C., Chara, M., Quoos, L., *On evaluation codes coming from a tower of function fields*, JOURNAL OF SYMBOLIC COMPUTATION, 89, 121 - 128, 2018.

[7] Carvalho, C., LOPEZ, HIRAM H., MATTHEWS, GRETCHEN L., *Decreasing norm-trace codes*, Designs, Codes And Cryptography (Dordrecht. Online), 92, 1143 - 1161, 2024.

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

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

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

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

[12] 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.

[13] C.H. Tognon, *A Result for the Formal Local Cohomology Module and Vanishing Results*, APPLIED MATHEMATICS & INFORMATION SCIENCES (PRINT), 11, 993 - 997, 2017.