On the floor and the ceiling of a divisor

Hiren Maharaj * and Gretchen L. Matthews [1]

Department of Mathematical Sciences

Clemson University

Clemson, SC 29634-0975 USA

Abstract

Given a divisor A of a function field, there is a unique divisor of minimum degree that defines the same vector space of rational functions as A and there is a unique divisor of maximum degree that defines the same vector space of rational differentials as A. These divisors are called the floor and the ceiling of A. A method is given for finding both the floor and the ceiling of a divisor. The floor and the ceiling of a divisor give new bounds for the minimum distance of algebraic geometry codes. The floor and the ceiling of a divisor supported by collinear places of the Hermitian function field are determined. Finally, we find the exact code parameters for a large class of algebraic geometry codes constructed from the Hermitian function field.

Key words: Riemann-Roch space, algebraic geometry code

PACS:

* Corresponding author.
Email addresses: hmahara@clemson.edu (Hiren Maharaj),
gmatthe@clemson.edu (Gretchen L. Matthews).

[1] Work supported in part by NSF grant DMS-0201286.

1 Introduction

The vector space $\mathcal{L}(A)$ of rational functions and the vector space $\Omega(A)$ of rational differentials associated to a divisor A have been studied for some time now. It is natural to ask when two divisors A and A' define the same space of rational functions or the same space of differentials. This is motivated further by the fact that Goppa used these vector spaces to construct algebraic geometry codes [5,6]. In [14,18] the question of when two algebraic geometry codes are equal is addressed by considering which divisors of the same degree define the same space of rational functions. Here, we allow the degree of the divisors to vary. It makes sense to do so since the parameters of an algebraic geometry code are estimated using the degree of the defining divisor. Thus, by considering divisors of varying degrees that define the same vector space of rational functions or rational differentials, improved estimates of code parameters are obtained.

The notion of "growing" or "shrinking" a divisor in such a way that the same space of rational functions or rational differentials is maintained has been suggested repeatedly in the literature (for instance, see [13]). In this paper, we provide a careful study of this by defining the floor of a divisor as well as its counterpart, the ceiling of a divisor. The floor of a divisor, introduced in [11], is a divisor of minimum degree that defines the same space of rational functions. The ceiling of a divisor is a divisor of maximum degree that defines the same space of rational differentials. We show that both the floor and the ceiling of a divisor are unique. Moreover, we provide a method of finding both the floor and the ceiling of a divisor. Using floors and ceilings, we obtain improved bounds on the parameters of algebraic geometry codes. These bounds generalize many of those found previously using Weierstrass gap sets of places (even r-tuples of places) of a function field (cf. [4], [12], [8], [3]). We also determine the floor and ceiling of divisors supported by collinear places of the Hermitian function field. In addition, we determine the exact minimum distances of a large class of algebraic geometry codes constructed from the Hermitian function field.

This paper is organized as follows. In Section 2 we review the main results on floors of divisors from [11]. Section 3 concerns the ceiling of a divisor. Several new results regarding floors and ceilings of divisors are presented here. In Section 4, applications to coding theory are considered. In Section 5 we consider applications to the Hermitian function field: we give a formula for the ceiling of divisors whose support consists of collinear points, and we exhibit a large class of functional and differential codes with exact formulaes for the parameters (length, dimension, and minimum distance).

Notation Unless stated otherwise, we will use notation as in [15]. We write $F/\mathbb{F}_q$ to mean that F is a global function field with full field of constants $\mathbb{F}_q$. Let $g = g(F)$ denote the genus of F. If P is a rational place of F, that is, a place of F of degree one, then v_P denotes the discrete valuation corresponding to P. Given two divisors A, A' of F, the greatest common divisor of A and A' is

$$\gcd(A, A') := \sum_P \min\{v_P(A), v_P(A')\}P$$

and the least common multiple of A and A' is

$$\operatorname{lcm}(A, A') := \sum_P \max\{v_P(A), v_P(A')\}P.$$

The support of a divisor A will be denoted by supp A. The divisor of a function $f \in F \setminus \{0\}$ (resp. differential $\eta \in \Omega \setminus \{0\}$, where Ω denotes the space of differentials of F) is denoted by (f) (resp. (η)). Given a function $f \in F \setminus \{0\}$, the zero divisor of f is denoted by $(f)_0$ and the pole divisor of f is denoted by $(f)_\infty$. Given a divisor A of F, the Riemann-Roch space of A is the vector space

$$\mathcal{L}(A) := \{f \in F : (f) \geq -A\} \cup \{0\}$$

of rational functions associated to A, and the dimension of $\mathcal{L}(A)$ over $\mathbb{F}_q$ is denoted by $\ell(A)$. The vector space of differentials associated to A is

$$\Omega(A) := \{\eta \in \Omega : (\eta) \geq A\} \cup \{0\},$$

and its dimension over $\mathbb{F}_q$ is denoted by $i(A)$.

Let $Q_1, \ldots, Q_m$, $P_1, \ldots, P_n$ be distinct rational places of F. Define the divisor $G := \sum_{i=1}^m \alpha_i Q_i$, where $\alpha_i \in \mathbb{Z}$ for all $1 \leq i \leq m$, and set $D := P_1 + \ldots + P_n$. We will consider the following two algebraic geometry codes defined using the divisors G and D:

$$C_{\mathcal{L}}(D, G) := \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$$

and

$$C_\Omega(D, G) := \{(res_{P_1}(\eta), \ldots, res_{P_n}(\eta)) : \eta \in \Omega(G - D)\}.$$

It is well known that $C_{\mathcal{L}}(D, G)$ has length n, dimension $\ell(G) - \ell(G - D)$, and minimum distance at least $n - \deg G$ while $C_\Omega(D, G)$ has length n, dimension $i(G - D) - i(G)$, and minimum distance at least $\deg G - (2g - 2)$. The designed distance of $C_{\mathcal{L}}(D, G)$ is $n - \deg G$ and the designed distance of $C_\Omega(D, G)$ is $\deg G - (2g - 2)$. As usual, a code of length n, dimension k, and minimum distance d is called an $[n, k, d]$ code.

2 The floor of a divisor

In this section we review of some results from [11] concerning the floor of a divisor.

Let A be a divisor of a function field $F/\mathbb{F}_q$ with $\ell(A) > 0$. In [11] it is shown that there is a unique divisor A' of F of minimum degree such that $\mathcal{L}(A) = \mathcal{L}(A')$. Hence we have the following definition.

Definition 1 Given a divisor A of a function field $F/\mathbb{F}_q$ with $\ell(A) > 0$, the *floor* of A is the unique divisor A' of F of minimum degree such that $\mathcal{L}(A) = \mathcal{L}(A')$. The floor of A will be denoted by $\lfloor A \rfloor$.

It is always the case the $\lfloor A \rfloor \leq A$. The next two results aid in searching for the floor of a divisor. The first shows that the floor of the divisor A is obtained from A by removing the base-points of the projective linear system of A. Hence, the floor of a divisor is base-point free by definition.

Proposition 2 *Let A be a divisor of $F/\mathbb{F}_q$ with $\ell(A) > 0$. Define the effective divisor $E := \gcd(A + (x) : x \in \mathcal{L}(A) \setminus \{0\})$. Then $\lfloor A \rfloor = A - E$.*

Theorem 3 *Let A be a divisor of $F/\mathbb{F}_q$ and let $\{b_1, \ldots, b_t\} \subseteq \mathcal{L}(A) \setminus \{0\}$ be a spanning set for $\mathcal{L}(A)$. Then*

$$\lfloor A \rfloor = -\gcd((b_i) : i = 1, \ldots, t).$$

The next result is useful, because it implies that if a divisor G is effective and $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$ for some divisor D, then $\operatorname{supp} \lfloor G \rfloor \cap \operatorname{supp} D = \emptyset$.

Proposition 4 *If A is an effective divisor of $F/\mathbb{F}_q$, then $\lfloor A \rfloor$ is also effective.*

In particular, if A is effective, then the support of $\lfloor A \rfloor$ is contained in the support of A.

3 The ceiling of a divisor

Throughout this section, $F/\mathbb{F}_q$ denotes a global function field. Given a divisor A, we consider divisors A' that define the same vector space of rational differentials as A. In particular, we are interested in those divisors A' satisfying $\Omega(A) = \Omega(A')$ that have degree as large as possible.

Proposition 5 *Let A be a divisor of a function field $F/\mathbb{F}_q$ with $i(A) > 0$. Suppose A' is a divisor of F of maximum degree such that $\Omega(A) = \Omega(A')$. Then $A \leq A'$. Consequently, A' is the unique divisor with respect to the above property.*

Proof: Since $\Omega(A) = \Omega(A') \cap \Omega(A) = \Omega(\mathrm{lcm}(A', A))$, it follows from the maximality property of the degree of A' that

$$\deg A' \geq \deg \mathrm{lcm}(A', A).$$

On the other hand, $\mathrm{lcm}(A', A) \geq A'$. It follows that $A' = \mathrm{lcm}(A', A)$, whence $A' \geq A$.

Now suppose that A' and A'' are two divisors of F of maximum degree such that $\Omega(A') = \Omega(A) = \Omega(A'')$. From the above, the fact that A'' is a divisor of F of maximum degree such that $\Omega(A') = \Omega(A'')$ implies $A' \leq A''$. Similarly, $A'' \leq A'$ since A' is a divisor of F of maximum degree such that $\Omega(A'') = \Omega(A')$. Therefore, $A' = A''$. Hence, there is a unique divisor A' of F of maximum degree satisfying $\Omega(A) = \Omega(A')$. □

Definition 6 Given a divisor A of a function field $F/\mathbb{F}_q$ with $i(A) > 0$, the *ceiling* of A is the unique divisor A' of F of maximum degree such that $\Omega(A) = \Omega(A')$. The ceiling of A will be denoted by $\lceil A \rceil$.

Corollary 7 *Let A_1 and A_2 be divisors of a function field $F/\mathbb{F}_q$ with $i(A_1) > 0$ and $i(A_2) > 0$. Then $\Omega(A_1) = \Omega(A_2)$ if and only if $\lceil A_1 \rceil = \lceil A_2 \rceil$.*

PROOF: The forward implication follows from Proposition 5. Assume that $\lceil A_1 \rceil = \lceil A_2 \rceil$. Then $\Omega(A_1) = \Omega(\lceil A_1 \rceil) = \Omega(\lceil A_2 \rceil) = \Omega(A_2)$. □

The next two results will aid in searching for the ceiling of a divisor.

Proposition 8 *Let A be a divisor of $F/\mathbb{F}_q$ with $i(A) > 0$. Define the divisor $E := \gcd((\eta) : \eta \in \Omega(A) \setminus \{0\})$. Then $\lceil A \rceil = E$.*

PROOF: Observe that for any place P, we have

$$\min_{\eta \in \Omega(A) \setminus \{0\}} v_P(\eta) = v_P(E).$$

Then for any $\eta \in \Omega(A) \setminus \{0\}$, $v_P(\eta) \geq v_P(E)$, whence $\eta \in \Omega(E)$. Thus, $\Omega(A) \subseteq \Omega(E)$. Since $E \geq A$, we also have $\Omega(E) \subseteq \Omega(A)$. Hence, $\Omega(E) = \Omega(A)$. By Proposition 5, we have $E \leq \lceil A \rceil$. Suppose that there is a place P such that $v_P(E) < v_P(\lceil A \rceil)$. Then $E + P \leq \lceil A \rceil$, and so

$$\Omega(A) = \Omega(\lceil A \rceil) \subseteq \Omega(E + P) \subseteq \Omega(E).$$

Since $\Omega(A) = \Omega(E)$, it follows that $\Omega(E) = \Omega(E+P)$. By the definition of E, there exists $\eta \in \Omega(A) = \Omega(E)$ such that $v_P(\eta) = v_P(E)$. Clearly, $\eta \notin \Omega(E+P)$ which is a contradiction. Therefore, $v_P(E) = v_P(\lceil A \rceil)$ for all places P of F, and so $E = \lceil A \rceil$. □

Theorem 9 *Let A be a divisor of $F/\mathbb{F}_q$ and let $\{\eta_1, \ldots, \eta_t\} \subseteq \Omega(A) \setminus \{0\}$ be a spanning set for $\Omega(A)$. Then*

$$\lceil A \rceil = \gcd((\eta_i) : i = 1, \ldots, t).$$

Proof: Put $E := \gcd((\eta_i) : i = 1, \ldots, t)$. For each $i = 1, \ldots, t$, $\eta_i \in \Omega(A) = \Omega(\lceil A \rceil)$ so that $(\eta_i) \geq \lceil A \rceil$. Thus

$$\lceil A \rceil \leq \gcd((\eta_i) : i = 1, \ldots, t) = E.$$

From Proposition 8 we have that $\lceil A \rceil = \gcd((\eta) : \eta \in \Omega(A) \setminus \{0\})$. Let P be a place of F and choose $\eta \in \Omega(A)$ such that $v_P(\eta) = v_P(\lceil A \rceil)$. Choose a uniformizing element x for P and for each i, let $x_i \in F$ such that $\eta_i = x_i dx$. Then there exist $a_i \in \mathbb{F}_q$ such that $\eta = a_1 \cdot x_1 dx + a_2 \cdot x_2 dx + \ldots + a_t \cdot x_t dx = (a_1 x_1 + a_2 x_2 + \ldots + a_t x_t) dx$. We have $v_P(\eta) = v_P(a_1 x_1 + a_2 x_2 + \ldots + a_t x_t) \geq \min_{a_i \neq 0}(v_P(x_i)) = v_P\left(\gcd_{a_i \neq 0}(\eta_i)\right) \geq v_P\left(\gcd((\eta_i), 1 \leq i \leq t)\right)$. This implies that $\lceil A \rceil \geq E$. Thus $\lceil A \rceil = E$. □

Given a divisor A of $F/\mathbb{F}_q$ and a spanning set $\{\eta_1, \ldots, \eta_t\} \subseteq \Omega(A) \setminus \{0\}$ for $\Omega(A)$, Theorem 9 shows that the support of the ceiling of A is contained in the union of the supports of $(\eta_1), \ldots, (\eta_t)$:

$$\operatorname{supp} \lceil A \rceil \subseteq \operatorname{supp}(\eta_1) \cup \ldots \cup \operatorname{supp}(\eta_t).$$

This illustrates how much one can "grow" the divisor A without changing the space of rational differentials associated to it.

Proposition 10 *Let A be a divisor of $F/\mathbb{F}_q$ with $i(A) > 0$. If W is a canonical divisor of F with the property that $W \geq A$ then $W \geq \lceil A \rceil$.*

PROOF: Choose any differential η such that $W = (\eta)$. Then $W \geq A$ implies that $(\eta) \geq A$, whence $\eta \in \Omega(A) = \Omega(\lceil A \rceil)$. Thus, $W = (\eta) \geq \lceil A \rceil$. □

The following result establishes a relationship between the floor and ceiling of a divisor. It also provides a convenient way of computing the ceiling of a divisor.

Theorem 11 *Let A be a divisor of $F/\mathbb{F}_q$ and let W be a canonical divisor of F.*

(a) If $i(A) > 0$, then

$$W - \lceil A \rceil = \lfloor W - A \rfloor. \tag{1}$$

(b) If $\ell(A) > 0$ then

$$W - \lfloor A \rfloor = \lceil W - A \rceil. \tag{2}$$

PROOF: Choose a differential η such that $W = (\eta)$. Then $\mathcal{L}(\lfloor W - A \rfloor) = \mathcal{L}(W - A) \cong \Omega(A) = \Omega(\lceil A \rceil) \cong \mathcal{L}(W - \lceil A \rceil)$. The first isomorphism is given by $x \mapsto x\eta$ and the second is given by $\omega \mapsto \omega/\eta$ so that the composite of these maps is the identity map. This implies that $\mathcal{L}(W - \lceil A \rceil) = \mathcal{L}(\lfloor W - A \rfloor) = \mathcal{L}(W - A)$ so that $W - \lceil A \rceil \geq \lfloor W - A \rfloor$. Suppose that $W - \lceil A \rceil > \lfloor W - A \rfloor$. Then there is a place P such that $\mathcal{L}(W - \lceil A \rceil - P) = \mathcal{L}(W - \lceil A \rceil)$. But this implies that $\Omega(\lceil A \rceil + P) = \Omega(\lceil A \rceil) = \Omega(A)$ contradicting the fact that $\lceil A \rceil$ is the divisor of maximum degree such that $\Omega(\lceil A \rceil) = \Omega(A)$. Thus $W - \lceil A \rceil = \lfloor W - A \rfloor$. Now (2) follows from (1) by replacing A by $W - A$. □

Remark 12 Let W be a canonical divisor and A be a divisor with $i(A) > 0$. As mentioned in the proof of Theorem 11, there is an isomorphism $\Omega(A) \cong$

$\mathcal{L}(W-A)$. Hence, according to Definition 6, the ceiling of A is the unique divisor $\lceil A\rceil$ such that $\mathcal{L}(W-\lceil A\rceil)=\mathcal{L}(W-A)$ and

$$\deg\lceil A\rceil = \max\left\{\deg A' : \mathcal{L}(W-A')=\mathcal{L}(W-A)\right\}.$$

Note that by Proposition 2

$$\lceil A\rceil = A + E_{W-A}$$

where $E_{W-A} := \gcd\left(W-A+(f) : f\in\mathcal{L}(W-A)\setminus\{0\}\right)$.

Next we give a large class of divisors which equal their floors or ceilings.

Corollary 13 *Let f be a nonzero function, A a divisor of F, and W a canonical divisor of F.*

(a) If $i(A)>0$ then

$$\lceil A+(f)\rceil = \lceil A\rceil + (f).$$

(b) If $\ell(A)>0$ then

$$\lfloor A+(f)\rfloor = \lfloor A\rfloor + (f).$$

(c) $\lfloor (f)\rfloor = (f)$, $\lfloor (f)_0\rfloor = (f)_0$ and $\lfloor (f)_\infty\rfloor = (f)_\infty$.

(d) $\lceil W-(f)_0\rceil = W-(f)_0$, $\lceil W-(f)_\infty\rceil = W-(f)_\infty$ and $\lceil W-(f)\rceil = W-(f)$.

Proof: *(a)* Let $x\in F$ be a separating element. Then since the divisor of a differential is a canonical divisor, it follows from Theorem 11 that

$$\lfloor (dx)-((f)+A)\rfloor = (dx)-((f)+\lceil A\rceil).$$

and

$$\lfloor (dx) - ((f) + A) \rfloor = (dx) - \lceil (f) + A \rceil .$$

Thus $\lceil (f) + A \rceil = (f) + \lceil A \rceil$.

(b) The proof is similar to (a).

(c) The first result follows from (b) by putting $A = 0$. Now put $A = (f)_\infty$. Then $f \in \mathcal{L}(A)$ so that $\ell(A) > 0$ and from (b) we have that

$$\lfloor (f)_\infty + (f) \rfloor = \lfloor (f)_\infty \rfloor + (f)$$

whence $\lfloor (f)_0 \rfloor = \lfloor (f)_\infty \rfloor + (f)_0 - (f)_\infty$ so that

$$\lfloor (f)_0 \rfloor - (f)_0 = \lfloor (f)_\infty \rfloor - (f)_\infty . \tag{3}$$

From Proposition 4 we have that the support of $\lfloor (f)_0 \rfloor$ is contained in the support of $(f)_0$ and the support of $\lfloor (f)_\infty \rfloor$ is contained in the support of $(f)_\infty$. Since the divisors $(f)_0$ and $(f)_\infty$ have disjoint supports, that same must be true for the divisors on both sides of (3). This implies $\lfloor (f)_0 \rfloor = (f)_0$ and $\lfloor (f)_\infty \rfloor = (f)_\infty$.

(d) Observe that since $W - (f)_0 \leq W$, $i(W - (f)_0) > 0$. Now, putting $A = W - (f)_0$ in (a), it follows that $\lceil W - (f)_0 + (f) \rceil = \lceil W - (f)_0 \rceil + (f)$. But $\lceil W - (f)_0 + (f) \rceil = \lceil W - (f)_\infty \rceil = W - \lfloor (f)_\infty \rfloor = W - (f)_\infty$ by Theorem 11, (a) and (c). Thus $\lceil W - (f)_0 \rceil + (f) = W - (f)_\infty$ so that $\lceil W - (f)_0 \rceil = W - (f)_0$. The second result now follows by replacing W by $W + (f)$ and the third result is a special case of the previous results by replacing W by $W + (f)$ (which is also a canonical divisor) and f by any nonzero constant function. □

4 Bounds on parameters of codes

The main motivation for studying the floor and the ceiling of a divisor is that it leads to improved estimates of the minimum distance of algebraic geometric codes. The idea of changing the defining divisor of an algebraic geometry code so that a better bound on the code parameters is obtained not a new one. In fact, it was suggested by Goppa that special divisors might be used to define better codes [5], [6].

Several authors have used the Weierstrass gap set to obtain estimates on the parameters of algebraic geometry codes (see [9], [4], [10], [12], [8], [3]). Recall that $(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$ is an element of the Weierstrass gap set of an m-tuple $(P_1, \ldots, P_m)$ of rational places of a function field $F/\mathbb{F}_q$ if

$$\mathcal{L}\left(\sum_{i=1}^{m} \alpha_i P_i\right) = \mathcal{L}\left(\sum_{i=1,\ i\neq j}^{m} \alpha_i P_i + (\alpha_j - 1)P_j\right) \tag{4}$$

for some j, $1 \leq j \leq m$ ([1], [2]). The idea is that consecutive elements of the Weierstrass gap set give some information on how to appropriately “grow” or “shrink” a divisor supported by the places $P_1, \ldots, P_m$ while maintaining the same set of rational functions or rational differentials. However, when $m \geq 2$, it is not so obvious what consecutive should mean. A first step around this was made by Kirfel and Pellikaan in [10] where they use consecutive B-gaps at a place P (considered previously in [7] and [4]) where B is a divisor. For instance, if $B = \sum_{i=1, i\neq j}^{m} \alpha_i P_i$, then α_j is a B-gap at P_j if (4) holds. In [8], Homma and Kim define a pure gap to be an element of the Weierstrass gap set such that (4) holds for all j, $1 \leq j \leq m$, and use consecutive pure gaps to derive a better bound on the minimum distance of certain algebraic geometry codes.

The floor and ceiling of a divisor allow one to recover many of the results obtained using techniques described in the preceding paragraph and is much more general. In particular, the floor and ceiling do not require the symmetry that is necessary in many of the previous results (including those using B-gaps and pure gaps). While Weierstrass gap sets may be used to find a divisor that defines the same vector space, it may not necessarily give the best one in the sense that the divisor may not be the one of largest or smallest possible degree.

The first improved estimate of the minimum distance of an AG code follows immediately from the definition of the floor of a divisor. This estimate which appears in [11] is a generalization of [9] and [4, Theorem 3]. Recall that given a divisor A, $\deg A \geq \deg\lfloor A \rfloor$. Given a divisor A, let $E_A := A - \lfloor A \rfloor$. Then $\deg E_A \geq 0$.

Theorem 14 *Let $F/\mathbb{F}_q$ be a function field of genus g. Let $D := P_1 + \ldots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let G be a divisor of F such that the support of $\lfloor G \rfloor$ does not contain any of the places $P_1, \ldots, P_n$. Then $C_{\mathcal{L}}(D, G)$ is an $[n, k, d]$ code whose parameters satisfy*

$$k \geq \deg G - g + 1$$

and

$$d \geq n - deg\lfloor G \rfloor = n - \deg G + \deg E_G.$$

Next, we state a bound on the minimum distance of $C_\Omega(D, G)$.

Theorem 15 *Let $F/\mathbb{F}_q$ be a function field of genus g. Let $D := P_1 + \ldots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let G be a divisor of*

F such that the support of $\lceil G-D \rceil + D$ does not contain any of the places $P_1, \ldots, P_n$. Then $C_\Omega(D,G)$ is an $[n,k,d]$ code whose parameters satisfy

$$k \geq n - \deg G + g - 1$$

and

$$d \geq \deg \lceil G-D \rceil + n + g - 1 = \deg G - (2g-2) + \deg E_{W-G+D}$$

where W is any canonical divisor.

Proof: The result follows immediately from the fact that

$$\Omega(G-D) = \Omega(\lceil G-D \rceil) = \Omega(\lceil G-D \rceil + D - D) = \Omega(G - D + E_{W-G+D}).$$

□

Typically, an algebraic geometry code is defined by taking G to be a divisor supported by a few rational places of $F/\mathbb{F}_q$ and setting D to be the sum of all rational places of $F/\mathbb{F}_q$ other than those in the support of G. In order to construct a long code, there must be many rational places in the support of D. For this reason, the task of finding the ceiling of $G-D$ might seem rather daunting as the support of $G-D$ is quite large. However, recall that there exists a differential η with divisor $(\eta) = A - D$ where $\mathrm{supp} A \cap \mathrm{supp} D = \emptyset$ [15, Lemma II.2.9]. Then to compute the ceiling of $G-D$, we can use that

$$\lceil G-D \rceil = W - \lfloor W - G + D \rfloor = W - \lfloor A - G \rfloor$$

where $W = (\eta)$ is a canonical divisor.

In order for Theorem 15 to give an improvement over the designed distance of $C_\Omega(D,G)$, we need $W + D - G > \lfloor W + D - G \rfloor$, which means we need

$n - 2 \leq \deg G$. Such codes will have small dimension but large minimum distance. Next, we include a result from [11] that yields an improvement over the designed distance for certain codes $C_\Omega(D, G)$ with larger dimensions.

Theorem 16 *Let $F/\mathbb{F}_q$ be a function field of genus g. Let $D := P_1 + \ldots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let $G := H + \lfloor H \rfloor$ be a divisor of F where H is an effective divisor whose support does not contain any of the places $P_1, \ldots, P_n$. Then $C_\Omega(D, G)$ is an $[n, k, d]$ code whose parameters satisfy*

$$k \geq n - \deg G + g - 1$$

and

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

The next corollary shows how one may apply Theorem 16 to an even larger class of codes. We remark that this result yields a generalization of [8, Theorem 3.3], [3, Theorem 3.4], and [10, Proposition 3.10].

Corollary 17 *Let $F/\mathbb{F}_q$ be a function field of genus g. Let $D := P_1 + \ldots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let $G := H + A$ where H and A are effective divisors of F such that the support of H does not contain any of the places $P_1, \ldots, P_n$ and $\lfloor H \rfloor \leq A \leq H$. Then $C_\Omega(D, G)$ is an $[n, k, d]$ code whose parameters satisfy*

$$k \geq n - \deg G + g - 1$$

and

$$d \geq \deg G - (2g-2) + \deg(H-A).$$

PROOF: This follows immediately from Theorem 16 as $H + \lfloor H \rfloor - D \leq H + A - D$ implies $C_\Omega(D, H+A) \subseteq C_\Omega(D, H + \lfloor H \rfloor)$. □

Proposition 18 *Let $F/\mathbb{F}_q$ be a function field of genus g. Let $D := P_1 + \ldots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let G be a divisor of F such that the support of $\lceil G \rceil$ does not contain any of the places $P_1, \ldots, P_n$. Then $C_\Omega(D, \lceil G \rceil)$ is an $[n, k, d]$ code whose parameters satisfy*

$$k \geq n - \deg\lceil G \rceil + g - 1$$

and

$$d \geq \deg\lceil G \rceil - (2g-2) = \deg G - (2g-2) + \deg(\lceil G \rceil - G).$$

The floor and ceiling of a divisor can also be used to improve the bounds on the generalized Hamming weights of algebraic geometry codes. If C is a code of length n and dimension k and $1 \leq r \leq k$, the r^{th} generalized Hamming weight of C is defined to be

$$d_r(C) := \min\{|\text{supp } V| : V \text{ is a linear subcode of } C, \dim V = r\}$$

where supp $V := \{i : 1 \leq i \leq n, c_i \neq 0 \text{ for some } c \in V\}$ is the support of the subcode V [17]. Clearly, $d_1(C) = d(C)$, the minimum distance of C. In [19, Theorem 12] it is shown that if $C_\mathcal{L}(D, G)$ is a code over $\mathbb{F}_q$ of length n and dimension k and $1 \leq r \leq k$, then

$$d_r(C_\mathcal{L}(D,G)) \geq n - \deg G + \gamma_r$$

where $\{\gamma_r : r \geq 1\}$ denotes the gonality sequence of $F/\mathbb{F}_q$. The next two results follow immediately from Definition 1 and Definition 6. The first generalizes [16, Theorem 4.3].

Proposition 19 *Let $F/\mathbb{F}_q$ be a function field. Let $D := P_1 + \ldots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let G be a divisor of F such that the support of $\lfloor G \rfloor$ does not contain any of the places $P_1, \ldots, P_n$. If $C_{\mathcal{L}}(G, D)$ is nontrivial, then*

$$\begin{aligned} d_r(C_{\mathcal{L}}(D, G)) &\geq n - \deg\lfloor G \rfloor + \gamma_r \\ &= n - \deg G + \gamma_r + \deg(G - \lfloor G \rfloor). \end{aligned}$$

Proposition 20 *Let $F/\mathbb{F}_q$ be a function field of genus g. Let $D := P_1 + \ldots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let G be a divisor of F such that the support of $\lceil G - D \rceil + D$ does not contain any of the places $P_1, \ldots, P_n$. If $C_{\Omega}(G, D)$ is nontrivial, then*

$$\begin{aligned} d_r(C_{\Omega}(D, G)) &\geq \deg(G + E_{W-G+D}) - (2g - 2) + \gamma_r \\ &= \deg G - (2g - 2) + \gamma_r + \deg E_{W-G+D}. \end{aligned}$$

5 Applications to the Hermitian function field

In this section, we restrict our attention to the Hermitian function field $H = \mathbb{F}_{q^2}(x, y)$ with defining equation $y^q + y = x^{q+1}$. We determine the floor and the ceiling of divisors of H with collinear support. First, we set up some notation. Let

$$\mathcal{K} := \{(\alpha, \beta) \in \mathbb{F}_{q^2}^2 : \beta^q + \beta = \alpha^{q+1}\}.$$

For each $\alpha \in \mathbb{F}_{q^2}$, set

$$K_\alpha := \{\beta : \beta^q + \beta = \alpha^{q+1}\},$$

and for each $(\alpha, \beta) \in \mathcal{K}$, let $P_{\alpha,\beta}$ denote the common zero of $x - \alpha$ and $y - \beta$. For $(\alpha, \beta) \in \mathcal{K}$, we define the function $\tau_{\alpha,\beta} := y - \beta - \alpha^q(x - \alpha)$. Throughout the next two subsections, α is a fixed element of $\mathbb{F}_{q^2}$ and r and k_β (for each $\beta \in K_\alpha$) are fixed integers.

5.1 The floor and ceiling of divisors with collinear support

In [11], the floor of a divisor with collinear support is found. We include this result and determine the ceiling of such a divisor as a corollary.

Theorem 21 *[11] Let $A := rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta}$ be a divisor of the Hermitian function field $H/\mathbb{F}_{q^2}$ where $r \in \mathbb{Z}$, $\alpha \in \mathbb{F}_{q^2}$, and $k_\beta \in \mathbb{Z}$ for each $\beta \in K_\alpha$. Then the floor of A is given by*

$$\lfloor A \rfloor = bQ_\infty + \sum_{\beta \in K_\alpha} a_\beta P_{\alpha,\beta}$$

where

$$a_\beta = -\min\left\{ i - (q+1)\left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor : 0 \leq i \leq q \text{ and } a(i) > 0 \right\},$$

$$b := \max\left\{ (q+1)\left\lfloor \frac{r - iq}{q+1} \right\rfloor + qi : 0 \leq i \leq q \textit{ and } a(i) > 0 \right\}$$

and

$$a(i) := \left\lfloor \frac{r - iq}{q+1} \right\rfloor + \sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor + 1$$

for $1 \leq i \leq q$.

Recall that even though $\lfloor A \rfloor \leq A$, it is not necessarily the case that supp$\lfloor A \rfloor \subseteq$ supp$A$ if A is not effective. However, Theorem 21 shows that if A is supported by collinear places of the Hermitian function field, then supp$\lfloor A \rfloor \subseteq$ supp$A$ even if A is not an effective divisor.

As an immediate corollary of Theorem 21, we obtain a formula for the ceiling of a divisor supported by collinear rational places of the Hermitian function field. Note that the support of the ceiling of such a divisor is contained in the support of the divisor.

Corollary 22 *Let* $A := rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta}$ *be a divisor of the Hermitian function field* $H/\mathbb{F}_{q^2}$ *where* $r \in \mathbb{Z}$, $\alpha \in \mathbb{F}_{q^2}$, *and* $k_\beta \in \mathbb{Z}$ *for each* $\beta \in K_\alpha$. *The ceiling of* A *is given by*

$$\lceil A \rceil = (2g - 2 - b)Q_\infty - \sum_{\beta \in K_\alpha} a_\beta P_{\alpha,\beta}$$

where

$$a_\beta = -\min \left\{ i - (q+1) \left\lfloor \frac{-k_\beta + i}{q+1} \right\rfloor : 0 \leq i \leq q \text{ and } a(i) > 0 \right\},$$

$$b := \max \left\{ (q+1) \left\lfloor \frac{2g - 2 - r - iq}{q+1} \right\rfloor + qi : 0 \leq i \leq q \ \textit{and} \ a(i) > 0 \right\}$$

and

$$a(i) := \left\lfloor \frac{2g - 2 - r - iq}{q+1} \right\rfloor + \sum_{\beta \in K_\alpha} \left\lfloor \frac{-k_\beta + i}{q+1} \right\rfloor + 1$$

for $1 \leq i \leq q$.

PROOF: Let $W := (2g-2)Q_\infty$. Then W is a canonical divisor ([15, Lemma VI.4.4]). According to Remark 12,

$$\begin{aligned}\lceil A\rceil &= (2g-2)Q_\infty - \lfloor W-A\rfloor \\ &= (2g-2)Q_\infty - \lfloor (2g-2-r)Q_\infty - \textstyle\sum_{\beta\in K_\alpha} k_\beta P_{\alpha,\beta}\rfloor.\end{aligned}$$

According to Theorem 21, this gives

$$\begin{aligned}\lceil A\rceil &= (2g-2)Q_\infty - bQ_\infty - \textstyle\sum_{\beta\in K_\alpha} a_\beta P_{\alpha,\beta} \\ &= (2g-2-b)Q_\infty - \textstyle\sum_{\beta\in K_\alpha} a_\beta P_{\alpha,\beta}\end{aligned}$$

where b, $a(i)$, $1\le i\le q$, and a_β are as described in Corollary 22. □

5.2 The exact dimension and minimum distance of a class of codes.

In Theorem 14 we give improved lower bounds for the minimum distance and dimension of codes from divisors G which are not equal to their floors. However, if one can compute the dimension of the Riemann-Roch spaces $\mathcal{L}(G)$ exactly, then in order to get the best possible lower bound on the minimum distance, it makes sense to work only with those divisors which equal their floors. In [11] the exact dimension of Riemann-Roch spaces of a class of divisors with collinear support is computed: it is shown that the dimension of $\mathcal{L}\left(rQ_\infty + \sum_{\beta\in K_\alpha} k_\beta P_{\alpha,\beta}\right)$ is given by

$$\sum_{i=0}^{q} \max\left\{\left\lfloor\frac{r-iq}{q+1}\right\rfloor + \sum_{\beta\in K_\alpha}\left\lfloor\frac{k_\beta+i}{q+1}\right\rfloor + 1, 0\right\}. \tag{5}$$

In Corollary 13 we exhibit large classes of divisors which equal their floors. For divisors G of the form $(f)_\infty$, the pole divisor of f, there is a large class of AG codes for which we can give the exact minimum distance [15, Remark II.2.5]:

Theorem 23 *Let $F/\mathbb{F}_q$ be a function field and let $f \in F$. Put $G = (f)_\infty$ and let D be the divisor $D := P_1 + \ldots + P_n$ whose support consists of rational places disjoint from the support G. Suppose that all of the zeroes of f are simple and contained in the support of D. Then the minimum distance of the code $C_\mathcal{L}(G, D)$ is exactly $n - \deg(G)$.*

PROOF: The function f belongs to $\mathcal{L}(G)$ and the corresponding codeword $(f(P_1), f(P_2), \ldots, f(P_n))$ has weight exactly $n - \deg(f)_0$ so that the minimum distance of the code $C_\mathcal{L}(G, D)$ is at most $n - \deg(f)_0 = n - \deg G$. But the minimum distance of the code $C_\mathcal{L}(G, D)$ is at least $n - \deg G$ [15, Theorem II.2.2]. Thus the minimum distance is exactly $n - \deg G$. □

For divisors G of the form $W + (f)_0$, where W is a canonical divisor, there is a large class of differential codes for which we can give the exact minimum distance:

Theorem 24 *Let $F/\mathbb{F}_q$ be a function field of genus g and let $f \in F$. Suppose that P_1, …, P_n are rational places of F and put $D := P_1 + \ldots + P_n$. Suppose that f has only simple zeroes contained in the support of D and that η is a differential such that $G := (\eta) + (f)_0$ has support disjoint from the support of D. Then the minimum distance of the code $C_\Omega(G, D)$ is exactly* $\deg G - (2g - 2) = \deg(f)_0$.

PROOF: It is clear that $\eta \in \Omega(G - D)$. Observe that since G has support disjoint from the support of D and since f has only simple zeroes, it follows that for each place P in the support D, P belongs to the support of

$(f)_0$ if and only if $v_P(\eta) = -1$. But at any place P in the support of D, we have that $\mathrm{res}_P(\eta) \neq 0$ if and only if $v_P(\eta) = -1$. Thus $\mathrm{res}_P(\eta) \neq 0$ iff P belongs to the support of $(f)_0$ and consequently the corresponding codeword $(res_{P_1}(\eta), res_{P_2}(\eta), \ldots, res_{P_n}(\eta))$ has weight exactly $\deg(f)_0$ so that the minimum distance of the code $C_\Omega(G, D)$ is at most $\deg(f)_0 = \deg G - (2g-2)$. But the minimum distance of the code $C_\Omega(G, D)$ is at least $\deg G - (2g-2)$ [15, Theorem II.2.7]. Thus the minimum distance is exactly $\deg G - (2g-2)$. □

Corollary 25 *Suppose that the numbers k_β, $\beta \in K_\alpha$, are non-negative and belong to the same congruence class modulo $q+1$. Furthermore, assume that $b \leq q^2 - 1$ where $b := \sum_{\beta \in K_\alpha} k_\beta$ and let t be a non-negative integer such that $\lceil b/q \rceil \leq t < q^2 - 1$. Let $G = \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta} + rQ_\infty$ where $r = qt - b$. Let $\alpha \in \mathbb{F}_{q^2}$ and let D be the sum of all rational places of the Hermitian function field H, none of which are zeroes of the function $x - \alpha$ or the place Q_∞. Then the code $C_\mathcal{L}(D, G)$ is an $[n, k, d]$ code where*

(i) $n = q^3 - q$,

(ii) $k = \sum_{j=0}^{q} \max\left\{\left\lfloor \frac{r-jq}{q+1} \right\rfloor + \sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + j}{q+1} \right\rfloor + 1, 0\right\}$ *and*

(iii) $d = q^3 - q - b - r = q^3 - q(t+1)$.

Proof: There are $q^3 + 1$ rational places in H and q of them are zeroes of $x - \alpha$. Thus $n = q^3 + 1 - (q+1) = q^3 - q$. The dimension follows from (5). Choose a set S of t elements of $\mathbb{F}_{q^2} \setminus \{\alpha\}$. Let i be the integer in the interval $0 \leq i \leq q$ such that $-k_\beta \equiv i \bmod q+1$ for all $\beta \in K_\alpha$. For each $\beta \in K_\alpha$ let e_β

be the integer such that $-k_\beta - i = (q+1)e_\beta$. Let f be the function

$$f := \left((x-\alpha)^i \prod_{\beta \in K_\alpha} \tau_{\alpha,\beta}^{e_{\beta,i}} \right) \cdot \prod_{\gamma \in S} (x-\gamma).$$

In [11] it is shown that

$$\begin{aligned}
&\left((x-\alpha)^i \prod_{\beta \in K_\alpha} \tau_{\alpha,\beta}^{e_{\beta,i}} \right) \\
&= \sum_{\beta \in K_\alpha} (e_{\beta,i}(q+1)+i)P_{\alpha,\beta} - ((q+1)\sum_{\beta \in K_\alpha} e_{\beta,i} + iq)Q_\infty \\
&= \sum_{\beta \in K_\alpha} -k_\beta P_{\alpha,\beta} + bQ_\infty
\end{aligned}$$

and $\left(\prod_{\gamma \in S}(x-\gamma)\right) = D' - qtQ_\infty$ where D' is a sum of qt rational places in the support of D. Thus

$$(f) = \sum_{\beta \in K_\alpha} -k_\beta P_{\alpha,\beta} + (b-qt)Q_\infty + D'$$

so that

$$(f)_\infty = \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta} + rQ_\infty = G.$$

and $(f)_0 = D'$. Observe that the zeroes of f are all simple and are contained in the support of D. Thus by Theorem 23 it follows tht $d = n - \deg(f)_\infty = q^3 - q - (b+r) = q^3 - q(t+1)$ as required. □

Corollary 26 *Suppose that the numbers k_β, $\beta \in K_\alpha$, are non-negative and belong to the same congruence class modulo $q+1$. Furthermore, assume that $b \leq q^2-1$ where $b := \sum_{\beta \in K_\alpha} k_\beta$ and let t be a non-negative integer such that $\lceil b/q \rceil \leq t \leq q^2-1$. Let $G = \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta} + rQ_\infty$. where $r = qt - b + q^2 - q - 2$. Let $\alpha \in \mathbb{F}_{q^2}$ and let D be the sum of all rational places of the Hermitian function field H none of which are zeroes of the function $x-\alpha$ or the place*

Q_∞.

Then the code $C_\Omega(D, G)$ is an $[n, k, d]$ code where

(i) $n = q^3 - q$,

(ii) $k = \sum_{i=0}^{q} \max\left\{\left\lfloor \frac{q^3-q-r-iq}{q+1} \right\rfloor + \sum_{\beta \in K_\alpha} \left\lfloor \frac{-k_\beta+i}{q+1} \right\rfloor + 1, 0\right\}$ and

(iii) $d = qt$.

Proof: There are q^3+1 rational places in H and q of them are zeroes of $x-\alpha$. Thus $n = q^3+1-(q+1) = q^3-q$. Choose a set S of t elements of $\mathbb{F}_{q^2} \setminus \{\alpha\}$. Let i be the integer in the interval $0 \le i \le q$ such that $-k_\beta \equiv i \mod q+1$ for all $\beta \in K_\alpha$. For each $\beta \in K_\alpha$ let e_β be the integer such that $-k_\beta - i = (q+1)e_\beta$. Let f be the function

$$f := \left((x-\alpha)^i \prod_{\beta \in K_\alpha} \tau_{\alpha,\beta}^{e_{\beta,i}}\right) \cdot \prod_{\gamma \in S} (x-\gamma).$$

As in the proof of Corollary 25 it follows that

$$(f) = \sum_{\beta \in K_\alpha} -k_\beta P_{\alpha,\beta} + (b-qt)Q_\infty + D'$$

where D' is a sum of qt rational places in the support of D. Consequently

$$(f)_\infty = \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta} + (qt-b)Q_\infty.$$

and $(f)_0 = D'$.

Put $\eta = dx/f$. Observe that

$$\begin{aligned} &(dx) + (f)_\infty \\ =&(q^2-q-2)Q_\infty + (f)_\infty \end{aligned}$$

$$= \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta} + (qt - b + q^2 - q - 2)Q_\infty$$

equals G and has disjoint support from D. Hence $(\eta)+(f)_0 = (dx)+(f)_\infty = G$. Note also that the zeroes of f are all simple and are contained in the support of D. Thus by Theorem 24 it follows that $d = \deg(f)_0 = \deg D' = qt$ as required.

Put $W = dx/\prod_{\gamma\neq\alpha}(x-\gamma)$. Since $\Omega(G-D) \cong \mathcal{L}(W-G+D)$, it suffices to compute the dimension of $\mathcal{L}(W-G+D)$. Observe that

$W - G + D = (dx) - (D - q(q^2-1)Q_\infty) - G + D = (dx) + (q^3-q)Q_\infty - ((dx) + (f)_\infty) = (q^3-q)Q_\infty - (f)_\infty = (q^3 - q - (qt-b))Q_\infty - \sum_{\beta\in K_\alpha} k_\beta P_{\alpha,\beta}$

so that by (5) the code has dimension

$$\sum_{i=0}^{q} \max\left\{ \left\lfloor \frac{q^3 - q - (qt-b) - iq}{q+1} \right\rfloor + \sum_{\beta\in K_\alpha} \left\lfloor \frac{-k_\beta + i}{q+1} \right\rfloor + 1, 0 \right\}$$

as required. □

References

[1] E. Arbarello, M. Cornalba, P. Griffiths, and J. Harris, Geometry of Algebraic Curves, Springer-Verlag, 1985.

[2] E. Ballico and S. J. Kim, Weierstrass multiple loci of n-pointed algebraic curves, J. Algebra **199** (1998), 455–471.

[3] C. Carvalho and F. Torres, On Goppa codes and Weierstrass gaps at several points, in press.

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

[5] V. D. Goppa, Algebraico-geometric codes, Math. USSR-Izv. **21** (1983), 75–91.

[6] V. D. Goppa, Geometry and Codes, Kluwer, 1988.

[7] M. Homma, Funny plane curves in characteristic p¿0, Commun. Algebra **15** (1987), 1469–1501.

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

[9] H. Janwa, On the parameters of algebraic geometry codes, Applied Algebra, Algebraic Algorithms, and Error-correcting Codes (New Orleans, LA, 1991), Lecture Notes in Computer Science **539**, Springer, Berlin 1991, 19–28.

[10] C. Kirfel and R. Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, IEEE Trans. Inform. Theory **41** no. 5 part 1 (1995), 1720–1732.

[11] H. Maharaj, G. L. Matthews, and G. Pirsic, Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences, in review.

[12] G. L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, Des. Codes and Cryptog. **22** (2001), 107–121.

[13] R. Miranda, Algebraic curves and Riemann surfaces, Graduate Studies in Mathematics **5**, American Mathematical Society, Providence, RI, 1995.

[14] C. Munuera and R. Pellikaan, Equality of geometric Goppa codes and equivalence of divisors, J. Pure Appl. Algebra **90** (1993), 229–252.

[15] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.

[16] L. Tang, Consecutive Weierstrass gaps and weight hierarchy of geometric Goppa codes, Algebra Colloq. **3** no. 1 (1996), 1–10.

[17] V. K. Wei, Generalized Hamming weights for linear codes, IEEE Trans. Inform. Theory **37** (1991), 1412–1418.

[18] C. P. Xing, When are two geometric Goppa codes equal?, IEEE Trans. Inform. Theory **38** no. 3 (1992), 1140–1142.

[19] K. Yang, P. V. Kumar, and H. Stichtenoth, On the weight hierarchy of geometric Goppa codes, IEEE Trans. Inform. Theory **40** (1994), 913–920.