ON THE MINIMUM DISTANCE OF ALGEBRAIC GEOMETRY CODES

by

İHSAN TAŞKIN

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

Sabancı University
Fall 2008

ON THE MINIMUM DISTANCE OF ALGEBRAIC GEOMETRY CODES

APPROVED BY

Assist. Prof. Dr. Cem Güneri .....
(Thesis Supervisor)

Prof. Dr. Henning Stichtenoth .....
(Thesis Coadvisor)

Prof. Dr. Alev Topuzoğlu .....

Assoc. Prof. Dr. Erkay Savaş .....

Prof. Dr. Ferruh Özbudak .....

DATE OF APPROVAL: .....

to my father

Acknowledgements

First of all, it is with sincere appreciation that I here express my deepest gratitude to my supervisor Assist. Prof. Dr. Cem Güneri and my coadvisor Prof. Dr. Henning Stichtenoth for their friendliness. They expertly and patiently guided my research up to this point and this thesis would never be finished without their support.

Moreover, I would thank to my colleagues at UEKAE for all they have done for me also thanks to my managers, Önder Yetiş, Alparslan Babaoğlu and Ali Murat Apohan for their helps.

Finally, many thanks goes to my wife for her unfailing support and to my parent for their love and patience.

ON THE MINIMUM DISTANCE OF ALGEBRAIC GEOMETRY CODES

İhsan Taşkın

Mathematics, Doctor of Philosophy Thesis, 2008

Thesis Supervisor: Assist. Prof. Dr. Cem Güneri

Thesis Coadvisor: Prof. Dr. Henning Stichtenoth

Keywords: function fields, algebraic geometry codes, minimum distance of codes, Goppa bound.

Abstract

In the literature about algebraic geometry codes one finds a lot of results improving Goppa's minimum distance bound. These improvements often use the idea of "shrinking" or "growing" the defining divisors of the codes under certain technical conditions. The main contribution of this thesis is to show that most of these improvements can be obtained in a unified way from one theorem. Our results do not only simplify previous results but they also improve them further.

CEBİRSEL GEOMETRİ KODLARININ MİNİMUM UZAKLIĞI

İhsan Taşkın

Matematik, Doktora Tezi, 2008

Tez Danışmanı: Yard. Doç. Dr. Cem Güneri

Tez Eş Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: fonksiyon cisimleri, cebirsel geometri kodları, kodların minimum uzaklığı, Goppa sınırı

Özet

Goppa'nın cebirsel geometri kodlarının minimum uzaklıkları için bulduğu sınırı iyileştirme üzerine literatürde birçok çalışma vardır. Bu çalışmalar, genellikle kodları tanımlayan bölenleri "daraltma" veya "genişletme" fikrine dayanan teknik koşullar içerir. Bu tezin en önemli katkısı, bahsi geçen iyileştirmelerin birçoğunun tek bir teoremden elde edilebileceğini göstermesidir. Bulduğumuz sonuçlar, daha önceki çalışmaları basitleştirmekle kalmayıp onları daha da iyileştirmektedir.

Contents

CHAPTER 1

INTRODUCTION

In this chapter, we recall earlier bounds on the minimum distance of Algebraic Geometry (AG) codes. A necessary background on function fields and AG codes is also provided. We use standard notations, cf. [16].

1.1 Preliminaries

Let $F/\mathbb{F}_q$ be an algebraic function field of genus g with full constant field $\mathbb{F}_q$ and G be a divisor of $F/\mathbb{F}_q$. There are two vector spaces over $\mathbb{F}_q$ that are associated with G. These are:

$$\mathcal{L}(G) = \{x \in F | (x) \geq -G\} \cup \{0\}$$

and

$$\Omega_F(G) = \{\omega \in \Omega_F | (\omega) \geq G\} \cup \{0\}.$$

The dimension of $\mathcal{L}(G)$ (resp. $\Omega_F(G)$) over $\mathbb{F}_q$ is denoted by $\ell(G)$ (resp. $i(G)$). The space $\mathcal{L}(G)$ is also known as the *Riemann-Roch space* of G. The dimension of $\mathcal{L}(G)$ can be computed via Riemann-Roch Theorem ([16, Theorem I.5.15]):

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

Here W is a canonical divisor of F. We can replace $\ell(W - G)$ with $i(G)$ by Serre's duality ([16, Theorem I.5.14]) which provides an isomorphism between the spaces $\Omega(G)$ and $\mathcal{L}(W - G)$.

Let Q be any place of F. A nonnegative integer α is called a *pole number* for Q if there exists $f \in F$ whose pole divisor $(f)_\infty$ is αQ. Otherwise, α is called a *gap*

number for Q. By Weierstrass Gap Theorem ([16, Theorem I.6.7]), a rational place Q has exactly g gaps. Moreover, the set of nongaps (i.e. the complement of the gap set in $\{0, 1, \cdots\} = \mathbb{N}_0$) forms a semigroup which is called the *Weierstrass semigroup at* Q.

If a divisor $A \in \mathrm{Div}(F)$ is written as $A = A_0 - A_\infty$, where both A_0 and A_∞ are positive with disjoint support, then we call A_0 (resp. A_∞) the *zero* (resp. the *pole*) *part of* A. The gap concept can be generalized as follows ([6, 12]):

Definition 1.1.1. *Let G be a divisor and Q be a rational place of F. Then $\alpha \geq -\deg(G)$ is called a $G-$nongap at Q if there exists $f \in F$ such that*

$$((f) + G)_\infty = \alpha Q.$$

Otherwise, α is called a $G-$gap at Q.

For $A, B \in \mathrm{Div}(F)$, we define their *greatest common divisor* as

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

Lemma 1.1.2. *We have $\mathcal{L}(\gcd(A, B)) = \mathcal{L}(A) \cap \mathcal{L}(B)$.*

Proof. Since $\gcd(A, B)$ is less than or equal to both A and B, the inclusion from left to right is clear. Let $z \in F$ be the element of the intersection. Then we have

$$v_P(z) \geq \max\{-v_P(A), -v_P(B)\} = -\min\{v_P(A), v_P(B)\} = -v_P(\gcd(A, B))$$

for any place P. Hence, $z \in \mathcal{L}(\gcd(A, B))$. □

Next, we introduce the notion of the *floor* of a divisor.

Proposition 1.1.3. *If G is a divisor with $\ell(G) > 0$, then there exists a unique divisor $\lfloor G \rfloor$ (called the floor of G) of minimal degree such that*
(i) $\mathcal{L}(G) = \mathcal{L}(\lfloor G \rfloor)$,
(ii) $\lfloor G \rfloor \leq \tilde{G}$ *for all* $\tilde{G} \in \mathrm{Div}(F)$ *with* $\mathcal{L}(\tilde{G}) = \mathcal{L}(G)$.

Proof. Since $\ell(G) > 0$, any divisor A with $\mathcal{L}(A) = \mathcal{L}(G)$ satisfies $\deg(A) \geq 0$. Let H be the divisor of the least degree such that $\mathcal{L}(H) = \mathcal{L}(G)$. For any $\tilde{G} \in \mathrm{Div}(F)$ with $\mathcal{L}(\tilde{G}) = \mathcal{L}(G)$, we have

$$\deg(H) \leq \deg(\tilde{G}) \tag{1.1}$$

by the minimality of the degree of H. On the other hand,

$$\gcd(\tilde{G}, H) \leq H. \tag{1.2}$$

Since $\mathcal{L}(\gcd(\tilde{G}, H)) = \mathcal{L}(\tilde{G}) \cap \mathcal{L}(H)$ (cf. Lemma 1.1.2), (1.1) and (1.2) imply that $\gcd(\tilde{G}, H) = H$. Hence, $H \leq \tilde{G}$ and (ii) is proved. We set $\lfloor G \rfloor = H$ and call it the floor of G.

Suppose H and $\tilde{H}$ are two divisors of the same least degree such that $\mathcal{L}(H) = \mathcal{L}(\tilde{H}) = \mathcal{L}(G)$. Then, by part (ii) that we've just proved, we obtain $H \leq \tilde{H}$ and $\tilde{H} \leq H$. Hence the floor is uniquely determined. □

Corollary 1.1.4. *If $G \geq 0$, then $\lfloor G \rfloor \geq 0$. In this case we have* $\mathrm{supp}(\lfloor G \rfloor) \subseteq \mathrm{supp}(G)$.

Proof. If $G \geq 0$ then it is easy to see that

$$\mathcal{L}(0) = \mathbb{F}_q \subseteqq \mathcal{L}(G) = \mathcal{L}(\lfloor G \rfloor).$$

This means $(c) = 0 \geq -\lfloor G \rfloor$ for all $c \in \mathbb{F}_q \setminus \{0\}$. Consequently, $\lfloor G \rfloor$ is effective. □

The dual notion to the floor of a divisor is called the *ceiling of a divisor* G. Namely, the ceiling $\lceil G \rceil$ of G (with $i(G) > 0$) is the unique divisor of maximum degree such that $\Omega_F(\lceil G \rceil) = \Omega_F(G)$. One can show that $G \leq \lceil G \rceil$ (see [15]). For a canonical divisor W, we have

$$W - \lceil G \rceil = \lfloor W - G \rfloor \quad \text{and} \quad W - \lfloor G \rfloor = \lceil W - G \rceil \quad \text{(cf. [15, Theorem 11])}. \tag{1.3}$$

These essentially follow from the isomorphism between $\Omega(G)$ and $\mathcal{L}(W - G)$ (cf. [16, Theorem I.5.14]).

We now define the codes of interest in this thesis. Assume that $P_1, P_2, \cdots, P_n$ are pairwise distinct rational places of $F/\mathbb{F}_q$ and let $D = P_1 + P_2 + \cdots + P_n$. Choose a divisor G whose support does not contain P_i, for any $1 \leq i \leq n$. Then the *Algebraic Geometry* (AG) codes associated with D and G are defined by

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

and

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

The codes $C_{\mathcal{L}}$ and C_{Ω} are also called the *functional* and the *residual* codes, respectively. The dimension and the minimum distance of these codes satisfy

$$k(C_{\mathcal{L}}) = \ell(G) - \ell(G-D), \qquad d(C_{\mathcal{L}}) \geq n - \deg G,$$
$$k(C_{\Omega}) = i(G-D) - i(G), \qquad d(C_{\Omega}) \geq \deg G - (2g-2). \tag{1.4}$$

The lower bounds in (1.4) are called the *designed distances*. Moreover, the functional and residual codes are dual to each other ([16, Proposition II.2.10]). We have,

$$C_{\Omega}(D,G) = C_{\mathcal{L}}(D, W+D-G)$$

where $W = (\omega)$ such that ω is a Weil differential with $v_{P_i}(\omega) = -1$ and $\omega_{P_i}(1) = 1$ for $i = 1, \cdots, n$.

Let us finish this section by fixing some notation which will be used throughout.

- F is an algebraic function field of genus g with full constant field $\mathbb{F}_q$.
- $P_1, ..., P_n$ are pairwise distinct places of $F/\mathbb{F}_q$ of degree 1.
- $D = P_1 + ... + P_n$.
- G is a divisor of $F/\mathbb{F}_q$ such that $\text{supp}(G) \bigcap \text{supp}(D) = \varnothing$.

1.2 Earlier Improvements on $d(C_{\Omega})$

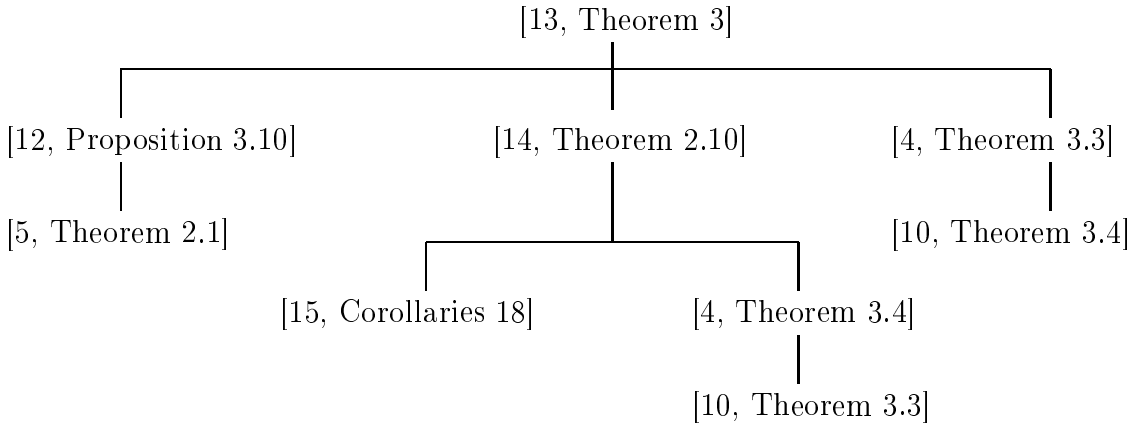
The main purpose of this thesis is to improve the designed distance of C_{Ω} codes in (1.4). In this section, we present earlier efforts to achieve this goal.

Several authors have attempted to sharpen Goppa's general estimate on $d(C_{\Omega})$ by making assumptions on the divisor G. In [4, 5, 6, 10, 12], the main idea is to choose a divisor G with certain assumptions on the Weierstrass gap set of the points in $\text{supp}(G)$ and then use this to obtain better estimates than the designed distance of C_{Ω}. More recently, Maharaj et al. [14] introduced the notion of the *floor of a divisor*, which yielded further improvements and extended some of the earlier works. Finally in [13], Lundell and McCullough generalize the results of Maharaj et al. Except for [6, Theorem 4], all of the results on $d(C_{\Omega})$ in the articles mentioned so far can be recovered from the theorem of Lundell-Mccullough ([13, Theorem 3.3]). Thus, we state the main result of Lundell and McCullough first.

Theorem 1.2.1. *([13, Theorem 3.3]) Let A, B and $Z \geq 0$ be divisors of F such that $\mathcal{L}(A) = \mathcal{L}(A - Z)$, $\mathcal{L}(B) = \mathcal{L}(B + Z)$. Set $G = A + B$. Then the minimum distance d of the code $C_\Omega(D, G)$ satisfies*

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g - 2) + \deg(Z).$$

Theorem 1.2.1 implies many other results on the improvement of Goppa bound on C_Ω codes. These implications are indicated in the next diagram. We will show how these implications follow in the remaining part of this section.



Theorem 1.2.2. *([12, Proposition 3.10]) Suppose that the integers $\alpha, \alpha+1, \cdots, \alpha+t$ are A-gaps at Q and $\beta, \beta-1, \cdots, \beta-t$ are B-gaps at Q. Let $G = A+B+(\alpha+\beta-1)Q$. Then, the minimum distance of the code $C_\Omega(D, G)$ satisfies*

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g - 2) + t + 1.$$

Proof. Let $\tilde{A} = A + (\alpha + t)Q$, $\tilde{B} = B - (\beta - t - 1)Q$ and $Z = (t + 1)Q$. Hence, we have $G = \tilde{A} + \tilde{B}$. Since $\alpha, \alpha + 1, \cdots \alpha + t$ are A-gaps at Q, $\mathcal{L}(\tilde{A}) = \mathcal{L}(\tilde{A} - Z)$. Similarly, $\mathcal{L}(\tilde{B}) = \mathcal{L}(\tilde{B} + Z)$ as $\beta, \beta - 1, \cdots \beta - t$ are B-gaps at Q. Therefore, the designed distance of $C_\Omega(D, G)$ is improved as much as $\deg(Z) = t + 1$ by Theorem 1.2.1. □

If we let $t = 0$ and $A = B$ in Theorem 1.2.2, we obtain the following result of Garcia and Lax.

Theorem 1.2.3. *([5, Theorem 2.1]) Suppose α and β are A-gaps at some rational place Q and let $G = (\alpha + \beta - 1)Q + 2A$. Then the minimum distance d of the code $C_\Omega(D, G)$ satisfies*

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g - 2) + 1.$$

Another effort to improve the designed distance of the residue codes is due to Maharaj, Matthews, Pirsic ([14]). They use the notion of the floor of a divisor for this purpose. We will see that this also follows from the Theorem 1.2.1.

Theorem 1.2.4. *([14, Theorem 2.10]) Let $G = A + \lfloor A \rfloor$ be a divisor of F, where $A > 0$. Then the minimum distance of the code $C_\Omega(D, G)$ satisfies*

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g-2) + \deg(A - \lfloor A \rfloor).$$

Proof. Set $B = \lfloor A \rfloor$ and $Z = A - \lfloor A \rfloor$. Then $\mathcal{L}(A) = \mathcal{L}(A - Z) = \mathcal{L}(\lfloor A \rfloor)$ and $\mathcal{L}(B) = \mathcal{L}(B + Z) = \mathcal{L}(A)$. Thus,

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g-2) + \deg(A - \lfloor A \rfloor)$$

by Theorem 1.2.1.

□

Let $B \in \mathrm{Div}(F)$ be such that $\lfloor A \rfloor \leq B \leq A$. Slightly modifying Theorem 1.2.4, let $G = A+B$ and $Z = A-B$. This yields the following result of Maharaj-Matthews.

Corollary 1.2.5. *([15, Corollary 18]) Let $G = A+B$ be a divisor of F where $A > 0$ and $\lfloor A \rfloor \leq B \leq A$. Then the minimum distance of the code $C_\Omega(D, G)$ satisfies*

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g-2) + \deg(A - B).$$

Let $Q_1, \cdots, Q_t$ be rational places of F. A t-tuple of positive integers $(\alpha_1, \cdots, \alpha_t)$ is called a *pure gap* at $(Q_1, \cdots, Q_t)$ if and only if

$$\mathcal{L}(\sum_{i=1}^{t} (\alpha_i - 1)Q_i) = \mathcal{L}(\sum_{i=1}^{t} \alpha_i Q_i).$$

The following result of Carvalho-Torres can also be obtained through the idea of the floor.

Theorem 1.2.6. *([4, Theorem 3.4]) Suppose that $(\alpha_1, \cdots, \alpha_t)$ and $(\beta_1, \cdots, \beta_t)$ are pure gaps at $(Q_1, \cdots, Q_t)$ where $\alpha_i \leq \beta_i$ for all $i = 1, ..., t$. Assume that for all $(\gamma_1, \cdots, \gamma_t)$ with $\alpha_i \leq \gamma_i \leq \beta_i$ (for all $i = 1, ..., t$), the tuple $(\gamma_1, \cdots, \gamma_t)$ is also a pure gap at $(Q_1, ..., Q_t)$. Then*

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g-2) + t + \sum_{i=1}^{t} (\beta_i - \alpha_i).$$

Proof. Note that by assumption

$$\mathcal{L}(\sum_{i=1}^{t} \beta_i Q_i) = \mathcal{L}(\sum_{i=1}^{t} (\alpha_i - 1) Q_i) \tag{1.5}$$

If $A = \sum_{i=1}^{t} \beta_i Q_i$ then $B = \sum_{i=1}^{t} (\alpha_i - 1) Q_i \geq \lfloor A \rfloor$ by (1.5). Hence, as in Corollary 1.2.5, we have

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g-2) + \deg(A-B) = \deg(G) - (2g-2) + t + \sum_{i=1}^{t} (\beta_i - \alpha_i).$$

□

The case $t = 2$ of Theorem 1.2.6 is an earlier result of Homma and Kim.

Theorem 1.2.7. *([10, Theorem 3.3]) Let (α_1, α_2) and (β_1, β_2) be pure gaps at (Q_1, Q_2) where $\alpha_i \leq \beta_i$ for $i = 1, 2$. Assume that for all (γ_1, γ_2) with $\alpha_i \leq \gamma_i \leq \beta_i$ (for $i = 1, 2$), the tuple (γ_1, γ_2) is also a pure gap at (Q_1, Q_2). Then*

$$d_{C_\Omega(D,G)} \geq deg(G) - (2g-2) + 2 + \sum_{i=1}^{2} (\beta_i - \alpha_i).$$

The following result of Carvalho-Torres has weaker assumptions than Theorem 1.2.6 and it follows from Theorem 1.2.1.

Theorem 1.2.8. *([4, Theorem 3.3]) Let $(\alpha_1, \cdots, \alpha_t)$ and $(\beta_1, \cdots, \beta_t)$ be two pure gaps at $(Q_1, \cdots, Q_t)$. If $G = \sum_{i=1}^{t} (\alpha_i + \beta_i - 1) Q_i$, then*

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g-2) + t.$$

Proof. Let $A = \sum_{i=1}^{t} \alpha_i Q_i$, $B = \sum_{i=1}^{t} (\beta_i - 1) Q_i$ and $Z = \sum_{i=1}^{t} Q_i$ in Theorem 1.2.1. □

We simply note that [10, Theorem 3.4] is a special case of the Theorem 1.2.8 by taking $t = 2$.

As seen so far, the results in the implication diagram all follow from the theorem of Lundell-Mccullough (Theorem 1.2.1) very easily. There is, however, another improved bound on $d(C_\Omega)$ which is independent of Theorem 1.2.1. This is due to Garcia-Kim-Lax.

Theorem 1.2.9. *([6, Theorem 4]) Let each of the integers $\alpha, \alpha+1, \cdots, \alpha+t$ and $\beta-(t-1), \beta-(t-2), \cdots, \beta$ be an A-gap at Q where $\alpha+t \leq \beta$. If $G = 2A + (\alpha+\beta-1)Q$, then*

$$d_{C_\Omega(D,G)} \geq \deg(G) - (2g-2) + t + 1.$$

Remark 1.2.10. Writing $G = (A + (\alpha+t-1)Q) + (A + (\beta-t)Q)$, and letting $Z = tQ$ Theorem 1.2.1 can only yield an improvement of $t = \deg Z$ in Theorem 1.2.9. However, if we make the further assumptions that $\beta - t \leq \alpha + t \leq \beta$ in Theorem 1.2.9, then we have

$$\mathcal{L}(A + \beta Q) = \mathcal{L}(A + (\alpha-1)Q).$$

In this case Theorem 1.2.1 yields a much stronger improvement of

$$\deg(A + \beta Q) - \deg(A + (\alpha-1)Q) = \beta - \alpha + 1 \geq t + 1.$$

Let us finish this section by noting a recent work of Beelen ([2]) on improving the bound for $d(C_\Omega)$. He generalizes the order bound for one point AG codes ([11]) to multi point AG codes. In Chapter 2, we will compare our results' performance against Beelen's bound.

1.3 Earlier Improvements on $d(C_\mathcal{L})$ and the Ceiling of a Divisor

In this section we have two goals. The first is to discuss the improvements on the Goppa bound for $C_\mathcal{L}$ codes, and the second is to point out that the notion of ceiling of a divisor is not needed for the existing improvements on the Goppa bound for C_Ω codes.

Results on improving the Goppa bound on the functional AG codes are scarce compared to residue codes. There are only two results known to us: [6, Theorem 3] and [14, Theorem 2.9]. However the former is implied by the latter, hence there is only one improved bound for $C_\mathcal{L}$ codes. Let G be a divisor such that $\ell(G) > 0$ with $P_i \notin \mathrm{supp}(\lfloor G \rfloor)$ for $1 \leq i \leq n$. Then, [14, Theorem 2.9] states that

$$d\left(C_\mathcal{L}(D,G)\right) \geq n - \deg\lfloor G \rfloor. \tag{1.6}$$

Note that $\mathcal{L}(G) = \mathcal{L}(\lfloor G \rfloor)$ by definition of the floor, hence $C_\mathcal{L}(D,G) = C_\mathcal{L}(D, \lfloor G \rfloor)$. Applying the Goppa bound (1.4) on the floor divisor, one gets (1.6).

We finish by commenting on the role of the ceiling of a divisor on the minimum distance estimates of AG codes. Maharaj and Matthews use the ceiling of a divisor to obtain bounds on some residue codes. Their proofs are based on the idea of the proof of (1.6), i.e. use the Goppa bound on the ceiling rather than the original divisor. Using the duality between floor and ceiling (cf. (1.3)), we now show that these results can be proved using the notion of floor.

Proposition 1.3.1. *([15, Theorem 16, Proposition 20])* (i) *If G is such that $P_i \notin supp\,(\lceil G - D\rceil + D)$ for $1 \leq i \leq n$, then*

$$d\,(C_\Omega(D,G)) \geq \deg G - (2g-2) + \deg\left((W - G + D) - \lfloor W - G + D\rfloor\right),$$

where W is a canonical divisor.
(ii) *If G is such that $P_i \notin supp\,(\lceil G\rceil)$ for $1 \leq i \leq n$, then*

$$d\,(C_\Omega(D,\lceil G\rceil)) \geq \deg G - (2g-2) + \deg\left(\lceil G\rceil - G\right).$$

Proof. (i) We know that $C_\Omega(D,G) = C_{\mathcal{L}}(D, W-(G-D))$ for a canonical divisor W with $v_{P_i}(W) = -1$ for each i (cf. [16, Proposition 2.2.10]). By assumption, we also have $v_{P_i}(\lceil G - D\rceil) = -1$ for $1 \leq i \leq n$. Using (1.3), we have

$$v_{P_i}(\lfloor W-(G-D)\rfloor) = v_{P_i}(W - \lceil G - D\rceil) = 0, \quad \text{for } 1 \leq i \leq n.$$

Therefore, the code $C_{\mathcal{L}}(D, \lfloor W-(G-D)\rfloor)$ exists. Since $C_{\mathcal{L}}(D, \lfloor W-(G-D)\rfloor) = C_{\mathcal{L}}(D, W-(G-D)) = C_\Omega(D,G)$ and using (1.6), we have

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

(ii) We know that $C_\Omega(D,\lceil G\rceil) = C_{\mathcal{L}}(D, W-(\lceil G\rceil - D))$ for a canonical divisor W. From Goppa's bound (1.4), we conclude

$$\begin{aligned} d\,(C_\Omega(D,\lceil G\rceil)) &\geq n - \deg(W-(\lceil G\rceil - D)) \\ &= \deg\lceil G\rceil - (2g-2) \\ &= \deg G - (2g-2) + \deg\left(\lceil G\rceil - G\right). \end{aligned}$$

□

CHAPTER 2

NEW IMPROVEMENTS ON THE DESIGNED DISTANCE OF AG CODES

Our goal in this chapter is to obtain two different improvements on the Goppa bound by extending the results of [6, 13]. Let us assume that $D = P_1 + \cdots + P_n$ as in the previous chapter where $P_1, \cdots P_n$ are rational places of F. We note that the MAGMA software ([3]) has been used for our numerical computations (cf. Example 2.1.6, Table 2.1, etc.)

2.1 The First Lower Bound on $d(C_\Omega)$

We start with a useful observation.

Lemma 2.1.1. *Let A, B, H be divisors with the following properties:*
(i) $\mathcal{L}(A) \subseteq \mathcal{L}(B)$,
(ii) $H \geq 0$,
(iii) $v_P(A) = v_P(B)$ *for all* $P \in \mathrm{supp}(H)$.
Then we have $\mathcal{L}(A - H) \subseteq \mathcal{L}(B - H)$.

Proof. Let $f \in \mathcal{L}(A - H)$. Then $f \in \mathcal{L}(B)$ since $\mathcal{L}(A - H) \subseteq \mathcal{L}(A) \subseteq \mathcal{L}(B)$ by (i) and (ii). For $P \notin \mathrm{supp}(H)$, we have

$$v_P(f) \geq -v_P(B) = -v_P(B - H).$$

For $P \in \mathrm{supp}(H)$,

$$v_P(f) \geq -v_P(A - H) = -v_P(B - H)$$

by (iii). Hence, $f \in \mathcal{L}(B - H)$. □

The following is an immediate consequence of Lemma 2.1.1 and it generalizes [10, Lemma 3.1].

Corollary 2.1.2. *Let A, B be divisors with $\mathcal{L}(A) = \mathcal{L}(B)$. Let $H \geq 0$ be a divisor with $v_P(A) = v_P(B)$ for all $P \in \mathrm{supp}(H)$. Then $\mathcal{L}(A - H) = \mathcal{L}(B - H)$.*

Remark 2.1.3. Condition (iii) in Lemma 2.1.1 is essential. To see this, let $A = P$ be a place with $\ell(A) = 1$. Let $B = 0$ and $H = P$. Then, $\mathcal{L}(A) = \mathcal{L}(B) = \mathbb{F}_q$. However, $\mathcal{L}(A - H) = \mathbb{F}_q$ and $\mathcal{L}(B - H) = \mathcal{L}(-P) = \{0\}$. So, $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ but $\mathcal{L}(A - H) \not\subseteq \mathcal{L}(B - H)$.

We are ready to state our first improvement on Goppa's bound for residue codes.

Theorem 2.1.4. *Suppose that $A, B, C, Z \in Div(F)$ satisfy the following conditions:*
(i) $\Big(\mathrm{supp}(A) \cup \mathrm{supp}(B) \cup \mathrm{supp}(C) \cup \mathrm{supp}(Z)\Big) \bigcap \mathrm{supp}(D) = \emptyset$,
(ii) $\mathcal{L}(A) = \mathcal{L}(A - Z)$ *and* $\mathcal{L}(B) = \mathcal{L}(B + Z)$,
(iii) $\mathcal{L}(C) = \mathcal{L}(B)$.
If $G = A + B$, then the minimum distance d of the code $C_\Omega(D, G)$ satisfies

$$d \geq \deg G - (2g - 2) + \deg Z + (i(A) - i(G - C)). \tag{2.1}$$

Proof. Let $\omega \in \Omega(G - D)$ be a differential such that the codeword

$$c = (\omega_{P_1}(1), \ldots, \omega_{P_n}(1))$$

of $C_\Omega(D, G)$ has the minimal weight d. Assume without loss of generality that $\omega_{P_i}(1) \neq 0$ for $1 \leq i \leq d$. If we set

$$D' = P_1 + \cdots + P_d,$$

then $(\omega) \geq G - D'$. The canonical divisor $W = (\omega)$ can be written as

$$W = G - D' + E, \tag{2.2}$$

with $E \geq 0$ and $\mathrm{supp}(E) \cap \mathrm{supp}(D') = \emptyset$. Since $\deg W = 2g - 2$, it follows from (2.2) that

$$d = \deg D' = \deg G - (2g - 2) + \deg E. \tag{2.3}$$

We want to give a lower bound on $\deg E$. By the Riemann-Roch theorem we have

$$\begin{aligned} \ell(A + E) &= \deg(A + E) + 1 - g + i(A + E) \\ \ell(A) &= \deg A + 1 - g + i(A), \end{aligned}$$

and hence

$$\deg E = (\ell(A+E) - \ell(A)) + (i(A) - i(A+E))\,. \tag{2.4}$$

Terms on the right-hand side of (2.4) can be rewritten as follows:

$$\begin{aligned}
\ell(A+E) - \ell(A) &= \ell(A+E) - \ell(A-Z) && \text{(by (ii))}\\
&\geq \ell(A+E) - \ell((A-Z)+E) && \text{(as } E \geq 0\text{)}\\
&= \deg Z + \ell(W-A-E) - \ell(W-(A-Z)-E) && \text{(by Riemann -Roch thm.)}\\
&= \deg Z + \ell(B-D') - \ell((B+Z)-D') && \text{(by (2.2)}\\
&= \deg Z && \text{(by (i,ii) and Cor. 2.1.2)}
\end{aligned}$$

On the other hand,

$$\begin{aligned}
i(A+E) &= \ell(W-A-E)\\
&= \ell(B-D') && \text{(by (2.2) and defn. of } G\text{)}\\
&= \ell(C-D') && \text{(by (i,iii) and Cor. 2.1.2)}\\
&\leq \ell(C-D'+E) && \text{(since } E \geq 0\text{)}\\
&= i(G-C) && \text{(by (2.2))}
\end{aligned}$$

Combining these two inequalities with Equation (2.4), we get

$$\deg E \geq \deg Z + (i(A) - i(G-C))\,.$$

Putting this in (2.3), we finish the proof of Theorem 2.1.4. □

Remark 2.1.5. Note that we can assume that $i(A) - i(G-C) \geq 0$ since by letting $C = B$, we have $G - C = G - B = A$.

The bound of Lundell-McCullough (Theorem 1.2.1), and hence all of the other results that it implies (cf. the diagram in Section 1.2), is obviously a special case of Theorem 2.1.4.

Example 2.1.6. Consider the Suzuki function field $F = \mathbb{F}_8(x,y)/\mathbb{F}_8$ defined by the equation $y^8 - y = x^{10} - x^3$. This function field has 65 rational places and its genus is 14. Let P_∞ denote the unique (rational) place at infinity and $P_{0,0}$ be the rational place corresponding to $x = y = 0$. Let D be the sum of the remaining rational places. We consider the two-point AG code $C_\Omega(D,G)$ with $G = 17P_\infty + 11P_{0,0}$. Let

$$A = 15P_\infty + 3P_{0,0}, \quad B = 2P_\infty + 8P_{0,0}, \quad C = 8P_{0,0}, \quad \text{and} \quad Z = 2P_\infty.$$

Since

$$\mathcal{L}(13P_\infty+3P_{0,0}) = \mathcal{L}(15P_\infty+3P_{0,0}) \text{ and } \mathcal{L}(8P_{0,0}) = \mathcal{L}(2P_\infty+8P_{0,0}) = \mathcal{L}(4P_\infty+8P_{0,0}),$$

the hypotheses of Theorem 2.1.4 are satisfied. We have $i(A)-i(G-C) = 1$. Hence, the Goppa bound on the minimum distance is improved by 3 to obtain

$$d_{C_\Omega(D,G)} \geq 28 - 26 + 2 + 1 = 5.$$

We note that the improvement on this code obtained by Lundell-McCullough only comes from $\deg Z$ and it is equal to 2 (cf. [13, Table 2]).

Similary, we improve the Lundell-McCullough bound by 1 for the codes in Table 2.1, i.e. one more improvement over $\deg Z$. For simplicity, we write $aP_\infty + bP_{0,0}$ as (a, b) in the table. Note that $d_G, d_{LM}, \tilde{d}_1$ represent the bounds of Goppa, Lundell-McCullough and Theorem 2.1.4, respectively.

G	A	B	C	Z	d_G	d_{LM}	$\tilde{d}_1$
$(17, 9)$	$(15, 1)$	$(2, 8)$	$(0, 8)$	$(2, 1)$	0	3	4
$(17, 11)$	$(15, 3)$	$(2, 8)$	$(0, 8)$	$(2, 0)$	2	4	5
$(18, 8)$	$(15, 2)$	$(3, 6)$	$(0, 0)$	$(2, 1)$	0	3	4
$(21, 5)$	$(15, 2)$	$(6, 3)$	$(0, 0)$	$(1, 2)$	0	3	4
$(24, 6)$	$(16, 2)$	$(8, 4)$	$(0, 8)$	$(0, 2)$	4	6	7

Table 2.1: Improvements on codes over the Suzuki function field over $\mathbb{F}_8$ via Theorem 2.1.4

Remark 2.1.7. Aside from the removal of positivity condition on divisor Z, the main contribution of Theorem 2.1.4 over Theorem 1.2.1 is the difference of indices of speciality (cf. Inequality 2.1 and Example 2.1.6).

Remark 2.1.8. Since $\mathcal{L}(A) = \mathcal{L}(A - Z)$, we have $\deg Z = i(A - Z) - i(A)$ by Riemann-Roch theorem. Hence, maximum possible contribution by (2.1) over the Goppa bound is

$$\deg Z + i(A) - i(G - C) = i(A - Z) - i(G - C) \leq i(A - Z).$$

2.2 The Second Lower Bound on $d(C_\Omega)$

In this section, our aim is to obtain a second improvement on the Goppa bound by generalizing the result of Garcia-Kim-Lax in [6]. For this purpose we define a useful function. If $E \geq 0$ is an effective divisor, define

$$h_E(A) := \ell(A+E) - \ell(A) \geq 0, \qquad \text{for any } A \in \mathrm{Div}(F).$$

We need some lemmas related to the function h_E. Note that these lemmas are generalizations of the Lemma on page 203 of [6].

Lemma 2.2.1. *If $Z \geq 0$ is a divisor with $\mathrm{supp}(Z) \cap \mathrm{supp}(E) = \emptyset$, then $h_E(B) \leq h_E(B+Z)$ for any divisor $B \in \mathrm{Div}(F)$.*

Proof. Define the linear map

$$\begin{array}{rccc} \varphi: & \mathcal{L}(B+Z) & \longrightarrow & \mathcal{L}(B+Z+E)/\mathcal{L}(B+E) \\ & z & \mapsto & z \mod \mathcal{L}(B+E). \end{array}$$

Note that the kernel of φ is

$$\ker(\varphi) = \mathcal{L}(B+Z) \cap \mathcal{L}(B+E) = \mathcal{L}(B)$$

by Lemma 1.1.2 and the assumption that $\mathrm{supp}(Z) \cap \mathrm{supp}(E) = \emptyset$. Therefore φ induces an embedding of $\mathcal{L}(B+Z)/\mathcal{L}(B)$ into $\mathcal{L}(B+Z+E)/\mathcal{L}(B+E)$, which implies that the difference

$$h_E(B+Z) - h_E(B) = \big(\ell(B+Z+E) - \ell(B+E)\big) - \big(\ell(B+Z) - \ell(B)\big)$$

is nonnegative. Hence, $h_E(B) \leq h_E(B+Z)$. □

Lemma 2.2.2. *Let A, B, D', E, Z be divisors with the following properties:*
(i) *$Z \geq 0$, $\mathcal{L}(A) = \mathcal{L}(A-Z)$ and $\mathcal{L}(B) = \mathcal{L}(B+Z)$,*
(ii) *$D' \geq 0$ and $\mathrm{supp}(Z) \cap \mathrm{supp}(D') = \emptyset$,*
(iii) *$E = W - A - B + D' \geq 0$ for a canonical divisor W.*
Then, $h_E(A) = h_E(A-Z) + \deg Z$ and $h_E(B+Z) = h_E(B) + \deg Z$.

Proof. The first equality follows from the following:

$$\begin{array}{rcll} h_E(A) - h_E(A-Z) & = & \ell(A+E) - \ell(A-Z+E) & \text{(by (i))} \\ & = & \deg Z + \ell(W-A-E) - \ell(W-A+Z-E) & \text{(by R,R)} \\ & = & \deg Z + \ell(B-D') - \ell(B+Z-D') & \text{(by (iii))} \\ & = & \deg Z & \text{(by (i,ii))} \end{array}$$

The other equality is proved similarly. □

The following is our second improvement over Goppa's bound.

Theorem 2.2.3. *Suppose that $A, B, Z \in \mathrm{Div}(F)$ satisfy the following properties:*
(i) $\Big(\mathrm{supp}(A) \cup \mathrm{supp}(B) \cup \mathrm{supp}(Z)\Big) \bigcap \mathrm{supp}(D) = \emptyset$,
(ii) $\mathrm{supp}(A - B) \subseteq \mathrm{supp}(Z)$,
(iii) $Z \geq 0$, $\mathcal{L}(A) = \mathcal{L}(A - Z)$ *and* $\mathcal{L}(B) = \mathcal{L}(B + Z + Q)$ *for all* $Q \in \mathrm{supp}(Z)$,
(iv) $B + Z + P \leq A$ *for some* $P \in \mathrm{supp}(Z)$.
If $G = A + B$, then the minimum distance d of the code $C_\Omega(D, G)$ satisfies

$$d \geq \deg G - (2g - 2) + \deg Z + 1. \tag{2.5}$$

Proof. By Theorem 2.1.4, we know that $d \geq \deg G - (2g-2) + \deg Z$. Suppose that the equality holds and let $\omega \in \Omega(G - D)$ be a differential yielding a codeword of weight $\deg G - (2g - 2) + \deg Z$. Proceeding as in the proof of Theorem 2.1.4, we can assume that $\omega \in \Omega(G - D')$ for $D' = P_1 + \cdots + P_d$. Then, there exists a positive divisor E with $\deg E = \deg Z$ such that

$$(\omega) = G - D' + E.$$

We claim that $\mathrm{supp}(E) \cap \mathrm{supp}(Z) = \emptyset$. Suppose not and let Q be a place in the supports of both divisors. Then we can write

$$(\omega) = G + Q - D' + E'$$

with $E' \geq 0$. Hence $\omega \in \Omega(G + Q - D)$. Note that if we view $G + Q = A + (B + Q)$, then Theorem 2.1.4 applies to the code $C_\Omega(D, G + Q)$ to yield

$$d(C_\Omega(D, G + Q)) \geq \deg(G + Q) - (2g - 2) + \deg Z.$$

This means that the weight of the codeword $(\omega_{P_1}(1), \cdots, \omega_{P_n}(1))$ is different from $\deg G - (2g - 2) + \deg Z$, which is a contradiction. Hence,

$$\mathrm{supp}(E) \cap \mathrm{supp}(Z) = \emptyset. \tag{2.6}$$

We clearly have

$$h_E(A) = \ell(A + E) - \ell(A) \leq \deg E = \deg Z. \tag{2.7}$$

If P is the place in (iv), then

$$\begin{aligned} h_E(A) &= h_E(A-P)+\deg P && \text{(by Lemma 2.2.2)} \\ &\geq h_E(B+Z)+\deg P && \text{(by (ii), (iv), (2.6) \& Lemma 2.2.1)} \quad (2.8) \\ &\geq h_E(B)+\deg Z+\deg P && \text{(by Lemma 2.2.2)} \end{aligned}$$

However, (2.7) and (2.8) contradict each other. Therefore, our initial assumption is wrong, i.e. $d \geq \deg G - (2g-2) + \deg Z + 1$. □

Remark 2.2.4. By choosing $\tilde{A} = A + \beta Q$, $\tilde{B} = A + (\alpha - 1)Q$ in Theorem 1.2.9 and applying Theorem 2.2.3 to the divisor $G = \tilde{A} + \tilde{B}$, we recover the result of Garcia-Kim-Lax.

Remark 2.2.5. Assume that a hypothesis stronger than (iv) in Theorem 2.2.3 holds:

"There exists $P \in \mathrm{supp}(Z)$ with $A - Z \leq B + Z + P \leq A$"

Note that this assumption is analogous to the assumption we made in Remark 1.2.10. That is, this amounts to changing (iii) in Theorem 1.2.9 to $\beta - t \leq \alpha + t \leq \beta$. In this case, we have $\mathcal{L}(B) = \mathcal{L}(A-Z) = \mathcal{L}(B+Z+P) = \mathcal{L}(A)$ and Theorem 2.2.3 is a special case of Theorem 2.1.4. In fact, Theorem 2.1.4 yields a better improvement for the same code $C_\Omega(D, A+B)$:

$$\deg A - \deg B = \deg Z + \deg(A - Z - B) \geq \deg Z + 1.$$

Example 2.2.6. Consider the Suzuki function field F over $\mathbb{F}_8$ as in Example 2.1.6. Let $G = 27P_\infty + 6P_{0,0}$ and D be the sum of the remaining rational places. Let us decompose G as $A+B$, where $A = 14P_\infty + 6P_{0,0}$, $B = 13P_\infty$, and let $Z = P_\infty + P_{0,0}$. Then, assumptions (i,ii) in Theorem 2.2.3 are satisfied. Moreover, we have

$$\mathcal{L}(13P_\infty + 5P_{0,0}) = \mathcal{L}(14P_\infty + 6P_{0,0}),$$

$$\mathcal{L}(13P_\infty) = \mathcal{L}(14P_\infty + P_{0,0}) = \mathcal{L}(15P_\infty + P_{0,0}) = \mathcal{L}(14P_\infty + 2P_{0,0}).$$

Hence, assumptions (iii,iv) of Theorem 2.2.3 are also satisfied. Therefore, the improvement over the Goppa bound via Theorem 2.2.3 is $\deg Z + 1 = 3$. In [13], the improvement for the same code is 2 (see [13, Table 2]).

Similarly, we increase the Lundell-McCullough improvement over Goppa bound from 2 to 3 for the codes in Table 2.2 over the Suzuki function field. We use the same notation as in Table 2.1. We denote the bound obtained from Theorem 2.2.3 by $\tilde{d_2}$. Also, $(a,b) = (c,d)$ means that the Riemann-Roch spaces of the associated divisors are the same. Note that among the codes in Tables 2.1 and 2.2, only $C_\Omega(D, 17P_\infty + 11P_{0,0})$ is common, i.e. both Theorem 2.1.4 and Theorem 2.2.3 apply and yield the same improvement on this code.

$G,\ \ A,\ \ B,\ \ Z$	$\mathcal{L}$ space equalities	d_G	d_{LM}	$\tilde{d_2}$
$(16,11)\ (14,6)\ (2,5)\ (1,1)$	$(13,5) = (14,6)$ $(2,5) = (3,6) = (3,7) = (4,6)$	1	3	4
$(17,11)\ (14,6)\ (3,5)\ (1,1)$	$(13,5) = (14,6)$ $(3,5) = (4,6) = (4,7) = (5,6)$	2	4	5
$(18,11)\ (14,6)\ (4,5)\ (1,1)$	$(13,5) = (14,6)$ $(4,5) = (5,6) = (5,7) = (6,6)$	3	5	6
$(19,11)\ (14,6)\ (5,5)\ (1,1)$	$(13,5) = (14,6)$ $(5,5) = (6,6) = (6,7) = (7,6)$	4	6	7
$(27,4)\ (14,4)\ (13,0)\ (1,1)$	$(13,3) = (14,4)$ $(13,0) = (14,1) = (14,2) = (15,1)$	5	7	8
$(27,6)\ (14,6)\ (13,0)\ (1,1)$	$(13,5) = (14,6)$ $(13,0) = (14,1) = (14,2) = (15,1)$	7	9	10
$(30,1)\ (17,1)\ (13,0)\ (1,1)$	$(16,0) = (17,1)$ $(13,0) = (14,1) = (14,2) = (15,1)$	5	7	8
$(32,1)\ (19,1)\ (13,0)\ (1,1)$	$(18,0) = (19,1)$ $(13,0) = (14,1) = (14,2) = (15,1)$	7	9	10

Table 2.2: Improvements on the Suzuki function field over $\mathbb{F}_8$ via Theorem 2.2.3

2.3 Refinements of the Second Bound

In this section, our goal will be to obtain further improvements over Theorems 2.1.4 and 2.2.3. This is possible if the Riemann-Roch spaces involved satisfy extra conditions, which are listed in the following Lemma.

Lemma 2.3.1. *Let A, B, D', E, Z be divisors which satisfy*

(iv) $\mathrm{supp}(A - Z - B) \cap \mathrm{supp}(E) = \emptyset$,

in addition to the hypothesis (i),(ii) *and* (iii) *in Lemma 2.2.2. Let $G = A + B$, $P \in \mathrm{supp}(Z) \backslash \mathrm{supp}(E)$ and*

$$A_0 := B,\ A_1, \ldots, A_{n-2},\ A_{n-1} := A - Z,\ A_n := A$$

be a sequence of divisors satisfying

(v)$\mathcal{L}(A_i) = \mathcal{L}(A_i + P)$, *for all* $i = 0, 1, \ldots, n-1$,

(vi) $\mathcal{L}(G - A_i) = \mathcal{L}(G - A_i - P)$, *for all* $i = 0, 1, \ldots, n-1$,

(vii) $A_i + P \leq A_{i+1}$, *for all* $i = 0, 1, \ldots, n-1$.

Then, $h_E(A) \geq (n-1)\deg P + \deg Z$.

Proof. We give a sketch since analogous arguments have already been used in the proofs of earlier results. First, we prove that

$$h_E(A_i + P) - h_E(A_i) = \deg P, \quad \text{for all } i = 0, 1, \ldots, n-1. \tag{2.9}$$

The proof is very similar to the proof of Lemma 2.2.2. We use (v), Riemann-Roch Theorem, (iii), (vi) and Corollary 2.1.2. Then, we see that

$$h_E(A_{i+1}) \geq h_E(A_i + P), \quad \text{for all } i = 0, 1, \ldots, n-1. \tag{2.10}$$

We use the assumptions (iv) and (vii) in order to employ Lemma 2.2.1 here. Using Equations 2.9 and 2.10, we conclude that

$$\begin{aligned} h_E(A - Z) = h_E(A_{n-1}) &\geq h_E(A_{n-2} + P) \\ &= h_E(A_{n-2}) + \deg P \\ &\vdots \qquad\qquad \vdots \\ &\geq h_E(A_0) + (n-1)\deg P \geq (n-1)\deg P. \end{aligned}$$

By Lemma 2.2.2 we have $h_E(A) = h_E(A - Z) + \deg Z$. Hence, the proof is finished. □

Example 2.3.2. Let F be the Suzuki function field over $\mathbb{F}_8$ as in the previous examples. Let $G = 27P_\infty$ and D be the sum of the remaining 64 $\mathbb{F}_8$-rational places. The gap sequence at P_∞ is

$$1, 2, \ldots, 7, 9, 11, 14, 15, 17, 19, 27. \tag{2.11}$$

Hence, by choosing $A = 27P_\infty$, $B = 0$ and $Z = P_\infty$ in Theorem 2.2.3, we improve the Goppa bound by 2 and obtain

$$d \geq 27 - 26 + 2 = 3.$$

Note that the result of Garcia-Kim-Lax is also applicable here since the code is a one-point code (let $A = 0$ in Theorem 1.2.9). The improvement for the same code $C_\Omega(D, G)$ is 1 in [13, Table 2].

Now, we would like to improve the lower bound further by using Lemma 2.3.1. Assume that $d = 3$. Let $(\omega) = W = G - D' + E$ be a canonical divisor, where $\omega \in \Omega(G - D)$ is a differential yielding a weight 3 codeword, $D' \leq D$ is of degree 3 and $E \geq 0$ with $\deg E = 2$. We proceed as in the proof of Theorem 2.2.3 to conclude that $P_\infty \notin \text{supp}(E)$. Namely, assuming the opposite we can construct the code $C_\Omega(D, 28P_\infty)$ which contains the codeword produced by ω and whose minimum distance is at least $28 - 26 + 2 = 4$, by Theorem 2.1.4 via tha gap sequence (2.11). This is a contradiction.

Consider the sequence of divisors:
$A_0 = 0$, $A_1 = 8P_\infty$, $A_2 = 10P_\infty$, $A_3 = 13P_\infty$, $A_4 = 16P_\infty$, $A_5 = 18P_\infty$, $A_6 = 26P_\infty$, $A_7 = 27P_\infty$. By the gap sequence (2.11) and the fact that $P_\infty \notin \text{supp}(E)$, this sequence satisfies the hypotheses of Lemma 2.3.1. Hence, $h_E(27P_\infty) \geq 6 + 1 = 7$. However, we also have $h_E(27P_\infty) \leq \deg E = 2$, by definition of h_E. This contradiction implies that $d(C_\Omega(D, 27P_\infty) \geq 4$ and we improve the Goppa bound by 3.

Example 2.3.3. We continue working with the Suzuki function field $F/\mathbb{F}_8$. Let $G = 27P_\infty + 2P_{0,0}$ and D be the sum of the remaining rational places. Let $A = 17P_\infty + 2P_{0,0}$, $B = 10P_\infty$ and $Z = P_\infty + 2P_{0,0}$. Using the equalities

$$\mathcal{L}(17P_\infty + 2P_{0,0}) = \mathcal{L}(16P_\infty) \text{ and } \mathcal{L}(10P_\infty) = \mathcal{L}(11P_\infty + 2P_{0,0}),$$

we improve the Goppa bound by $\deg Z = 3$ to conclude that $d(C_\Omega(D, G)) \geq 6$ (cf. Theorem 2.1.4). This is the same as the improvement of Lundell-McCullough ([13, Table 2]).

Assume that $d = 6$ and proceed as in Example 2.3.2. Let $(\omega) = W = G - D' + E$ be a canonical divisor, where $\omega \in \Omega(G - D)$ is a differential yielding a weight 6

codeword, $D' \leq D$ is of degree 6 and $E \geq 0$ with $\deg E = 3$. If we assume that $P_\infty \in \text{supp}(E)$, then we can construct the code $C_\Omega(D, G + P_\infty) = C_\Omega(D, 28P_\infty + 2P_{0,0})$ which contains the weight 6 codeword produced by ω. However, the minimum distance of $C_\Omega(D, 28P_\infty + 2P_{0,0})$ is at least $30-26+(17-13) = 8$, since $28P_\infty + 2P_{0,0} = (15P_\infty + 2P_{0,0}) + (13P_\infty)$ and we have $\mathcal{L}(15P_\infty + 2P_{0,0}) = \mathcal{L}(13P_\infty)$ (cf. Theorem 2.1.4). This is a contradiction and hence, $P_\infty \notin \text{supp}(E)$.

Due to the fact that $P_\infty \notin \text{supp}(E)$ and the properties of the relevant Riemann-Roch spaces, the following sequence satisfies the hypotheses of Lemma 2.3.1:

$$A_0 = 10P_\infty,\ A_1 = 13P_\infty,\ A_2 = 16P_\infty,\ A_3 = 17P_\infty + 2P_{0,0}.$$

Hence, $h_E(17P_\infty + 2P_{0,0}) \geq 2 + 3 = 5$. However, we also have $h_E(17P_\infty + 2P_{0,0}) \leq \deg E = 3$, by definition of h_E. This contradiction implies that $d(C_\Omega(D, 27P_\infty + 2P_{0,0})) \geq 7$ and we improve the Goppa bound by 4. In fact, a similar argument can be carried out one more time to further improve the estimate to $d(C_\Omega(D, 27P_\infty + 2P_{0,0})) \geq 8$.

(i, j)	d_G	d_{LM}	d_B	$\tilde{d}_3$
$(27, 1)$	2	4	7	6
$(29, 1)$	3	6	8	8
$(30, 1)$	4	7	8	8
$(31, 1)$	5	8	9	9
$(32, 1)$	6	9	10	10
$(33, 1)$	7	10	11	11
$(24, 2)$	0	3	4	4
$(27, 2)$	3	6	7	8
$(28, 2)$	4	8	7	8
$(30, 2)$	6	9	9	10

Table 2.3: Comparison of the bounds for $C_{i,j} = C_\Omega(D, iP_\infty + jP_{0,0})$

In [2], Beelen obtained improved minimum distance estimates for codes of the form $C_{i,j} = C_\Omega(D, iP_\infty + jP_{0,0})$ $(j = 1, 2,\ i + j \geq 26)$ on the Suzuki function field over $\mathbb{F}_8$ by using the concept of the generalized order bound. Here, D is the sum of the remaining 63 rational places of the function field, as in Example 2.3.3. For

many $C_{i,j}$'s his bound coincides with that of Lundell-McCullough (cf. [2, page 674]). Therefore, our bounds in Theorems 2.1.4 and 2.2.3 perform at least as good as the estimate of Beelen in those cases. In Table 2.3, we list some examples where our results yield a better estimate than one of the two bounds mentioned above. Except for one case ($(i,j) = (30,1)$, cf. Table 2.2), we use arguments as in Examples 2.3.2 and 2.3.3 to obtain these improvements. We denote Lundell-McCullough, Beelen and our bounds by $d_{LM}, d_B, \tilde{d_3}$ respectively.

CHAPTER 3

A NEW EQUIVALENCE RELATION ON THE DIVISOR GROUP

The results of Section 2.1 motivate the study of the following relation on $\mathrm{Div}(F)$:

$$M \approx N \iff \mathcal{L}(M) = \mathcal{L}(N) \tag{3.1}$$

In this case we call the divisors M and N *equivalent*. Clearly, this is an equivalence relation on $\mathrm{Div}(F)$ and we denote the class of a divisor M by $c(M)$. Note that this relation is different from the usual notion of linear equivalence of divisors (cf. [16, page 16]).

For a divisor M with $\ell(M) > 0$, it is clear that $\lfloor M \rfloor \in c(M)$. Note that Theorems 2.1.4 and 2.2.3 demand divisors M whose class with respect to the new equivalence is nontrivial, i.e. $c(M) \supsetneq \{M\}$. Clearly, if $c(M) = \{M\}$ then $M = \lfloor M \rfloor$. The converse of this is not true in general.

We start with a lemma that contains an observation to be used in this chapter.

Lemma 3.1. *If M is nonspecial (i.e. $\ell(M) = \deg M + 1 - g$), then there exists no $N > M$ such that $\mathcal{L}(N) = \mathcal{L}(M)$.*

Proof. Since M is nonspecial, any divisor $N \geq M$ is also nonspecial. If $N \neq M$, then

$$\ell(N) = \deg N + 1 - g > \deg M + 1 - g = \ell(M).$$

Hence, $\mathcal{L}(N) \supsetneq \mathcal{L}(M)$. □

Proposition 3.2. *If $\deg M \geq 2g$, then $c(M) = \{M\}$.*

Proof. Since M is nonspecial, there exists no divisor $N > M$ in $c(M)$ by Lemma 3.1. Hence, if we can show that $\lfloor M \rfloor = M$ the proof will be finished.

Suppose $\lfloor M \rfloor < M$. If $\deg \lfloor M \rfloor > 2g - 2$, then

$$\ell(\lfloor M \rfloor) = \deg \lfloor M \rfloor + 1 - g < \deg M + 1 - g = \ell(M).$$

Since $\lfloor M \rfloor \in c(M)$, this is a contradiction. Therefore, we have $\deg \lfloor M \rfloor \leq 2g-2$. Then by Clifford's Theorem ([16, Theorem 1.6.11]), we have

$$\ell(\lfloor M \rfloor) \leq 1 + \frac{\deg \lfloor M \rfloor}{2} \leq g.$$

However, $\ell(M) = \deg M + 1 - g \geq g+1$ by hypothesis. This is a contradiction and hence, $\lfloor M \rfloor = M$. □

Proposition 3.2 shows that the divisor $G = A + B$ in Theorems 2.1.4 and 2.2.3 must satisfy $\deg G < 4g$, since we would like both of the divisors A and B to have nontrivial classes $c(A)$ and $c(B)$.

The following observation shows that the lower bound on $\deg M$ in Proposition 3.2 is sharp.

Proposition 3.3. *Let M be a divisor of degree $\deg M = 2g-1$. Then, either $c(M) = \{M\}$ or $M = W + P$ for a canonical divisor W and a rational place P. In the latter case, we have $\lfloor M \rfloor = W$ and*

$$c(M) = \{W\} \cup \{W + Q : Q \text{ is a rational place}\}.$$

Proof. Assume that $c(M) \neq \{M\}$. By Riemann-Roch theorem, we have $\ell(M) = g$. Note that a divisor $N > M$ cannot be in $c(M)$, since $\ell(N) > g$ for such N. Assume that $N \in c(M)$ and $N < M$. If $\deg N < 2g-2$, then $\ell(N) < g$ by Clifford's bound. So, $\deg N = 2g-2$. Moreover, $\ell(N) = \ell(M) = g$ and hence, $N = W$ is a canonical divisor. Since $W < M$, we must have $M = W + P$ for a rational place P. Note that there is no divisor smaller than W in $c(M)$ and for any rational place Q, $\ell(W+Q) = g$. Hence, $\lfloor M \rfloor = W$ and $W + Q \in c(M)$ for any rational place Q. □

The next result shows that among the divisors of interest with respect to Proposition 3.2, those meeting the Clifford bound are equal to their floor.

Proposition 3.4. *If $0 \leq \deg M \leq 2g-2$ and $\ell(M) = 1 + (\deg M)/2$, then $M = \lfloor M \rfloor$.*

Proof. If $\deg M = 0$, then $\ell(M) = 1$. Note that $\ell(M - P) = 0$ for any place P since $\deg(M-P) < 0$. Therefore, $M = \lfloor M \rfloor$ in this case.

For a divisor M with $0 < \deg M \leq 2g-2$ that meet the Clifford bound, assume that $\lfloor M \rfloor \neq M$. Then, $\mathcal{L}(M) = \mathcal{L}(M-P)$ for some place P. On one hand

$$\ell(M-P) = \ell(M) = 1 + \frac{\deg M}{2},$$

and on the other hand

$$\ell(M-P) \leq 1 + \frac{\deg(M-P)}{2} \quad (\text{ by Clifford's Theorem}).$$

This yields a contradiction, hence $\lfloor M \rfloor = M$. □

Remark 3.5. By Proposition 3.4 we have $W = \lfloor W \rfloor$ for any canonical divisor.

Our discussion on the triviality of the class of a divisor will end with a result that relates this to the index of speciality of its floor (cf. Corollary 3.7). For this purpose we need the following lemma which is a slight generalization of [16, Proposition 1.6.10]. We will denote the set of rational places of the function field F by $\mathbb{P}_F^{(1)}$.

Lemma 3.6. *Let M be a special divisor of F and assume that F has at least $2g-1-\deg M$ rational places. Then, there exists a rational place $P \in \mathbb{P}_F^{(1)}$ such that $\mathcal{L}(M) = \mathcal{L}(M+P)$.*

Proof. Suppose that $\mathcal{L}(M+P) \neq \mathcal{L}(M)$ for any rational place P. This implies that

$$\ell(M+P) = \ell(M) + 1 \quad \text{and} \quad i(M+P) = i(M),$$

for any $P \in \mathbb{P}_F^{(1)}$. Hence, $\mathcal{L}(W-M-P) = \mathcal{L}(W-M)$ for a canonical divisor W of F and for any $P \in \mathbb{P}_F^{(1)}$. Then we have

$$\begin{aligned}
\mathcal{L}(W-M) &= \bigcap_{P \in \mathbb{P}_F^{(1)}} \mathcal{L}(W-M-P) \\
&= \mathcal{L}\Big(\gcd\big(\{W-M-P : P \in \mathbb{P}_F^{(1)}\}\big)\Big) \qquad (\text{by Lemma 1.1.2 }) \\
&= \mathcal{L}\left(W-M-\sum_{P \in \mathbb{P}_F^{(1)}} P\right).
\end{aligned}$$

By assumption $\ell(W-M) = i(M) > 0$ whereas the dimension of the last divisor is 0, since its degree is negative. So, there must exist a rational place P with $\mathcal{L}(M) = \mathcal{L}(M+P)$. □

Corollary 3.7. *Let M be a divisor of F with $\ell(M) \geq 1$.*
(i) *If $\lfloor M \rfloor$ is nonspecial, then $\lfloor M \rfloor = M$ and $c(M) = \{M\}$.*
(ii) *Assume that F has at least $2g - 1 - \deg M$ many rational places. Then the converse of part (i) is true, i.e. if $c(M) = \{M\}$, then $\lfloor M \rfloor$ is nonspecial.*

Proof. (i) By Lemma 3.1, there exists no divisor in $c(M)$ that is greater than $\lfloor M \rfloor$. From the minimality of the floor, we reach the conclusion.
(ii) Assume that $\lfloor M \rfloor$ is special. Then, Lemma 3.6 implies that $\mathcal{L}(\lfloor M \rfloor + P) = \mathcal{L}(\lfloor M \rfloor)$ for some rational place P. Hence $\lfloor M \rfloor + P \in c(M)$, which is a contradiction to triviality of the class of M. □

For a divisor M with $\ell(M) \geq 1$, define the *height* of its class $c(M)$ as

$$ht(c(M)) := \max\{\deg N - \deg L : N, L \in c(M)\}.$$

Since the floor of divisors in the same class are the same, the height of any two such divisors are also the same. In the rest of this section, we are interested in the maximum possible height for a given class.

Proposition 3.8. *Let M be such that $\ell(M) \geq 1$. Then,*

$$\begin{aligned} ht(c(M)) &\leq i(\lfloor M \rfloor) && (3.2)\\ &\leq g + 1 - \ell(M) && (3.3)\\ &\leq g && (3.4) \end{aligned}$$

Proof. If $\deg M \geq 2g$ or $i(\lfloor M \rfloor) = 0$, we know by Proposition 3.2 and Corollary 3.7 that $c(M) = \{M\}$, which is not interesting. Therefore we assume that $\deg M \leq 2g - 1$ and $i(\lfloor M \rfloor) > 0$. Let N be a divisor in $c(M)$. Since $\ell(N) = \ell(\lfloor M \rfloor)$, from Riemann-Roch theorem we have

$$\deg N - \deg \lfloor M \rfloor = i(\lfloor M \rfloor) - i(N) \leq i(\lfloor M \rfloor).$$

This proves (3.2). Let W be a canonical divisor of the function field. Since we assumed that $i(\lfloor M \rfloor) = \ell(W - \lfloor M \rfloor) > 0$ and $\ell(\lfloor M \rfloor) = \ell(M) \geq 1$, by [16, Lemma 1.6.12] we have that

$$\ell(W - \lfloor M \rfloor) = \ell(W - \lfloor M \rfloor) + \ell(\lfloor M \rfloor) - \ell(\lfloor M \rfloor) \leq 1 + \ell(W) - \ell(M) = g + 1 - \ell(M).$$

This proves (3.3). Note that the last inequality is trivial. □

The bound (3.2) on the size of $ht(c(M))$ is sharp under a mild assumption as the following theorem shows.

Theorem 3.9. *Assume that a function field F has at least $2g-1-\deg\lfloor M\rfloor$ rational places, where M is a divisor with $\ell(M) \geq 1$ and $i(\lfloor M\rfloor) \geq 1$. Then for any $1 \leq i \leq i(\lfloor M\rfloor)$, there exists $N_i \in c(M)$ such that $\deg N_i - \deg\lfloor M\rfloor = i$. In particular, $ht(c(M)) = i(\lfloor M\rfloor)$.*

Proof. By Lemma 3.6, there exists a divisor $N_1 \in c(\lfloor M\rfloor) = c(M)$ with $\deg N_1 - \deg\lfloor M\rfloor = 1$. If N_1 is nonspecial, then

$$\ell(\lfloor M\rfloor) = \ell(N_1) = \deg N_1 + 1 - g = \deg\lfloor M\rfloor + 1 - g + 1.$$

Hence, $i(\lfloor M\rfloor) = 1$ and this shows the sharpness of the bound (3.2). If N_1 is special, then apply Lemma 3.6 to N_1 to construct $N_2 \in c(N_1) = c(\lfloor M\rfloor)$ with $\deg N_2 = \deg N_1 + 1$. Continuing this way, we can construct divisors $N_1, \ldots, N_{i(\lfloor M\rfloor)} \in c(\lfloor M\rfloor)$ such that

$$\deg N_i - \deg\lfloor M\rfloor = i, \quad \text{for each } 1 \leq i \leq i(\lfloor M\rfloor).$$

□

Remark 3.10. By [1, Proposition 9], most function fields $F/\mathbb{F}_q$ of genus $g \geq 2$ have an effective nonspecial divisor of degree g. The dimension of such a divisor M satisfies

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

Hence, $\mathcal{L}(M) = \mathbb{F}_q = \mathcal{L}(0)$. Therefore, the bound 3.4 is reached by some pair of divisors for many function fields, regardless of the number of rational places.

Bibliography

[1] Ballet, S., Le Brigand, D., "On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$", *J. Number Theory*, vol. **116**, no. 2, pp. 293-3100, 2006.

[2] Beelen, P., "The order bound for general algebraic geometric codes", *Finite Fields Appl.*, vol. **13**, no. 3, pp. 665-680, 2007.

[3] Bosma, W., Cannon, J., Playoust, C., "The Magma algebra system I: the user language", *J. Symb. Comp.*, vol. **24**, pp. 235-265, 1997.

[4] Carvalho, C., Torres, F., "On Goppa codes and Weierstrass gaps at several points", *Des. Codes Cryptogr.*, vol. **35**, no. 2, pp. 211-225, 2005.

[5] Garcia, A., Lax, R.F., "Goppa codes and Weierstrass gaps", *Coding Theory and Algebraic Geometry (Luminy, 1991)*, Lecture Notes in Math. vol. **1518**, pp. 33-42, 1992.

[6] Garcia, A., Kim, S.J., Lax, R.F., "Consecutive Weierstrass gaps and minimum distance of Goppa codes", *J. Pure Appl. Algebra*, vol. **84**, no. 2, pp. 199-207, 1993.

[7] Goppa, V.D., "Codes on algebraic curves", *Soviet Math. Dokl.*, vol. **24**, no. 1, pp. 170-172, 1981.

[8] Goppa, V.D., *Algebraico-geometric Codes*, Math. Ussr-Izv, Vol. **21** 75-91, 1983.

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

[10] Homma, M., Kim, S.J., "Goppa codes with Weierstrass pairs", *J. Pure Appl. Algebra*, vol. **162**, no. 2-3, pp. 273-290, 2001.

[11] Høholdt, T., van Lint, J.H., Pellikaan, R., in V.S. Pless, W.C. Huffman (Eds.) *Handbook of Coding Theory*, vol. I, chapter 10, 1998.

[12] Kirfel, C., Pellikaan, R., "The minimum distance of codes in an array coming from telescopic semigroups", *IEEE Trans. Inform. Theory*, vol. **41**, no. 6, pp. 1720-1732, 1995.

[13] Lundell, B., McCullough, J., "A generalized floor bound for the minimum distance of geometric Goppa codes", *J. Pure Appl. Algebra*, vol. **207**, no. 1, pp. 155-164, 2006.

[14] Maharaj, H., Matthews, G.L., Pirsic, G., "Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low discrepancy sequences", *J. Pure Appl. Algebra*, vol. **195**, no. 3, pp. 261-280, 2005.

[15] Maharaj, H., Matthews, G.L., "On the floor and the ceiling of a divisor", *Finite Fields Appl.*, vol. **12**, pp. 38-55, 2006.

[16] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.