FURTHER IMPROVEMENTS ON THE DESIGNED MINIMUM DISTANCE OF ALGEBRAIC GEOMETRY CODES

Cem Güneri[a,*] Henning Stichtenoth[a] İhsan Taşkın[a,b]

[a] Sabancı University, FENS, 34956 İstanbul, Turkey
[b] Tübitak UEKAE, 41470 Kocaeli, Turkey

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 article is to show that most of these improvements can be obtained in a unified way from one (rather simple) theorem. Our result does not only simplify previous results but it also improves them further.

1. Introduction

Let F be an algebraic function field of genus g with full constant field $\mathbb{F}_q$, where q is a prime power. Let G and D be two divisors of F such that $D = P_1 + \cdots P_n$ is the sum of n distinct rational places of F and $P_i \notin \text{supp}(G)$ for any i. With these data, Goppa constructed two types of linear codes (see [7]), which are now called *Algebraic Geometry (AG) codes*. These are:

$$\begin{aligned} C_{\mathcal{L}} = C_{\mathcal{L}}(D,G) &= \{(f(P_1),\ldots,f(P_n)) : f \in \mathcal{L}(G)\} \\ C_{\Omega} = C_{\Omega}(D,G) &= \{(\text{res}_{P_1}(\omega),\ldots,\text{res}_{P_n}(\omega)) : \omega \in \Omega(G-D)\} \end{aligned}$$

The codes $C_{\mathcal{L}}$ and C_{Ω} are also called the *functional* and the *residue* codes, respectively.

The theory of function fields gives us tools to estimate the parameters of AG codes. It is clear that the length of both codes is n. For the dimension and the minimum distance, we have

$$k(C_{\mathcal{L}}) = \ell(G) - \ell(G-D), \qquad d(C_{\mathcal{L}}) \geq n - \deg G,$$

(1.1)

$$k(C_{\Omega}) = i(G-D) - i(G), \qquad d(C_{\Omega}) \geq \deg G - (2g-2).$$

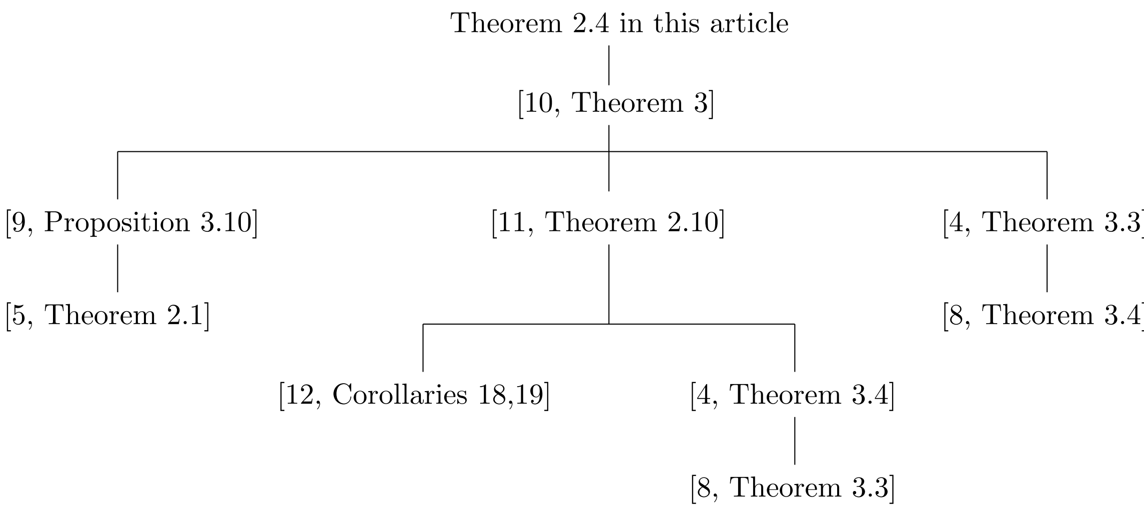
Here, as usual, $\ell(G)$ stands for the dimension of the space $\mathcal{L}(G)$ and $i(G)$ is the index of speciality of G, which is also equal to $\ell(W-G)$ for a canonical divisor W of F.

The lower bounds of Goppa on the minimum distances of AG codes in (1.1) are called the *designed minimum distances* of $C_{\mathcal{L}}$ and C_{Ω}. 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, 8, 9], the main idea is to choose a divisor G with certain assumptions on the Weierstrass gap set of the points

*Corresponding author. E-mail: guneri@sabanciuniv.edu ; Tel: +90 216 483 9521 ; Fax: +90 216 483 9550

in supp(G) and then use this to obtain better estimates than the designed distance of C_Ω. More recently, Maharaj et al. [11] introduced the notion of the *floor of a divisor*, which yielded further improvements and extended some of the earlier works. Finally in [10], Lundell and McCullough obtained a result that generalizes 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 [10, Theorem 3].

In this article we obtain two new results that improve the designed distances of residue codes further. One of these (Theorem 2.4) extends and improves the bound of Lundell-McCullough. The diagram below indicates the implications between various results on the subject.



Our second result (Theorem 2.12) generalizes the bound of Garcia-Kim-Lax ([6, Theorem 4]), which is not implied by any other result mentioned above, hence missing in the diagram. These theorems, together with related examples, are provided in Section 2. Our examples are generated on the Suzuki function field over the finite field $\mathbb{F}_8$. We present examples of codes for which [10, Theorem 3] or [6, Theorem 4] are not applicable or they yield weaker improvements. We also compare our bounds' performance against the recent generalized order bound of Beelen ([2]).

In all of the works mentioned above, and also in Section 2, a major role is played by divisors whose Riemann-Roch spaces are invariant under "growing" or "shrinking" by certain effective divisors. This leads us to define and study a new equivalence relation on the group $Div(F)$ of divisors of F in Section 3.

In the final section, we address two issues. The first is the improvements on the Goppa bound for *functional codes* in the literature. Such results are scarce and they follow rather easily. Secondly, we prove that the notion of the *ceiling of a divisor* introduced in [12] is not needed for the purpose of obtaining improved minimum distance estimates on AG codes, since related results in [12] can be obtained from the floor notion if Serre's duality is used.

Notation used througout will be rather standard and is the same as that used in [13]. Unless otherwise stated, we assume that the divisor D is

$$D = P_1 + P_2 \cdots + P_n, \tag{1.2}$$

where the P_i's are distinct rational places of the function field $F/\mathbb{F}_q$. In our examples, we used Magma [3] to compute dimensions of Riemann-Roch spaces.

2. New Lower Bounds for $d(C_\Omega)$

Our goal in this section is to obtain two different improvements on the Goppa bound by extending the results of [6, 10]. We start with a useful observation.

Lemma 2.1. *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* $P \in \operatorname{supp}(H)$.

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 $P \notin \operatorname{supp}(H)$, we have

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

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

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

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

The following is an immediate consequence of Lemma 2.1 and it generalizes [8, Lemma 3.1].

Corollary 2.2. *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 $P \in \operatorname{supp}(H)$. Then $\mathcal{L}(A-H) = \mathcal{L}(B-H)$.*

Remark 2.3. Condition (iii) in Lemma 2.1 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 $\mathcal{L}(A-H) \nsubseteq \mathcal{L}(B-H)$.

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

Theorem 2.4. *Let D be as in (1.2) and suppose that $A, B, C, Z \in Div(F)$ satisfy the following conditions:*

(i) $\Big(\operatorname{supp}(A) \cup \operatorname{supp}(B) \cup \operatorname{supp}(C) \cup \operatorname{supp}(Z)\Big) \bigcap \operatorname{supp}(D) = \emptyset$,

(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 $c = (\operatorname{res}_{P_1}(\omega), \ldots, \operatorname{res}_{P_n}(\omega))$ of $C_\Omega(D, G)$ has the minimal weight d. Assume without loss of generality that $\operatorname{res}_{P_i}(\omega) \neq 0$ 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 $\text{supp}(E) \cap \text{supp}(D') = \emptyset$. 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:

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

On the other hand,

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

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 2.4. □

Remark 2.5. 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, and hence all of the other results that it implies (cf. the diagram in Section 1), is a straightforward consequence of Theorem 2.4.

Corollary 2.6. *(*[10, Theorem 3]*) Let D be as in (1.2) and suppose that $A, B, Z \in Div(F)$ satisfy the following conditions:*

(i) $\big(\text{supp}(A) \cup \text{supp}(B) \cup \text{supp}(Z)\big) \bigcap \text{supp}(D) = \emptyset$,
(ii) $Z \geq 0$, $\mathcal{L}(A) = \mathcal{L}(A - Z)$ *and* $\mathcal{L}(B) = \mathcal{L}(B + Z)$.

If $G = A + B$, then the minimum distance d of the code $C_\Omega(D, G)$ satisfies

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

Example 2.7. 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 2.4 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. [10, Table 2]).

Similary, we improve the Lundell-McCullough bound by 1 for the codes in Table 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}, d_{GST} represent the bounds of Goppa, Lundell-McCullough and Theorem 2.4, respectively.

G	A	B	C	Z	d_G	d_{LM}	d_{GST}
$(17,9)$	$(15,1)$	$(2,8)$	$(0,8)$	$(2,1)$	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 1. Improvements on the Suzuki function field over $\mathbb{F}_8$ via Theorem 2.4

Remark 2.8. Aside from the removal of positivity condition on divisor Z, the main contribution of Theorem 2.4 over Corollary 2.6 is the difference of indices of speciality (cf. Inequality 2.1 and Example 2.7).

Remark 2.9. 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

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

Our next goal 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

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

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

Proof. Define the linear map

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

Note that the kernel of φ is

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

by Lemma 3.1(i) and the assumption that $\operatorname{supp}(Z) \cap \operatorname{supp}(E) = \emptyset$. Therefore φ induces an embedding, 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 2.11. *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 $\operatorname{supp}(Z) \cap \operatorname{supp}(D') = \emptyset$,*
(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:

$$\begin{array}{rcll} h_E(A) - h_E(A-Z) & = & \ell(A+E) - \ell(A-Z+E) & \text{(by (i))} \\ & = & \deg Z + \ell(W-A-E) - \ell(W-A+Z-E) & \text{(by Riemann-Roch)} \\ & = & \deg Z + \ell(B-D') - \ell(B+Z-D') & \text{(by (iii))} \\ & = & \deg Z & \text{(by (i,ii) \& Cor. 2.2)} \end{array}$$

The other equality is proved similarly. □

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

Theorem 2.12. *Let D be as in (1.2) and suppose that $A, B, Z \in Div(F)$ satisfy the following properties:*

(i) $\Big(\operatorname{supp}(A) \cup \operatorname{supp}(B) \cup \operatorname{supp}(Z)\Big) \bigcap \operatorname{supp}(D) = \emptyset$,
(ii) $\operatorname{supp}(A-B) \subseteq \operatorname{supp}(Z)$,
(iii) *$Z \geq 0$, $\mathcal{L}(A) = \mathcal{L}(A-Z)$ and $\mathcal{L}(B) = \mathcal{L}(B+Z+Q)$ for all $Q \in \operatorname{supp}(Z)$,*

(iv) $B+Z+P \leq A$ *for some* $P \in \operatorname{supp}(Z)$.

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 2.4, 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 2.4, 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 $\operatorname{supp}(E) \cap \operatorname{supp}(Z) = \emptyset$. 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 2.4 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 ω cannot yield a vector of weight $\deg G - (2g-2) + \deg Z$, which is a contradiction. Hence,

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

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

$$\begin{aligned} h_E(A) &= h_E(A-P) + \deg P && \text{(by Lemma 2.11)} \\ &\geq h_E(B+Z) + \deg P && \text{(by (ii), (iv), (2.6) \& Lemma 2.10)} \\ &\geq h_E(B) + \deg Z + \deg P && \text{(by Lemma 2.11)} \end{aligned} \tag{2.8}$$

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

The following is the main result of Garcia-Kim-Lax in [6] which gives an improvement over the Goppa bound for certain residue codes. Theorem 2.12 generalizes this result.

Corollary 2.13. *(*[6, Theorem 4]*) Let* D *be as in (1.2),* H *be a divisor and* P *be a rational place that satisfy the following conditions:*

(i) $\left(\operatorname{supp}(H) \cup \{P\}\right) \bigcap \operatorname{supp}(D) = \emptyset$,

(ii) *the integers* $\alpha, \alpha+1, \ldots, \alpha+t$ *and* $\beta-(t-1), \ldots, \beta-1, \beta$ *are* H*-gaps at* P,

(iii) $\alpha + t \leq \beta$ *and* $t \geq 1$.

If $G = (\alpha + \beta - 1)P + 2H$*, then the minimum distance* d *of the code* $C_\Omega(D, G)$ *satisfies*

$$d \geq \deg G - (2g - 2) + (t + 1).$$

Proof. By definition of H-gaps ([9, Remark 3.2]), (ii) is equivalent to the following equalities of Riemann-Roch spaces:

$$\mathcal{L}((\beta - t)P + H) = \cdots = \mathcal{L}((\beta - 1)P + H) = \mathcal{L}(\beta P + H),$$

$$\mathcal{L}((\alpha - 1)P + H) = \mathcal{L}(\alpha P + H) = \cdots = \mathcal{L}((\alpha + t)P + H).$$

Letting $A = \beta P + H$, $B = (\alpha - 1)P + H$ and $Z = tP$, the hypotheses of Theorem 2.12 are satisfied and the result follows. □

Remark 2.14. Assume that a hypothesis stronger than (iv) in Theorem 2.12 holds:

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

Note that this amounts to changing (iii) in Corollary 2.13 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 2.12 is a special case of Theorem 2.4. In fact, Theorem 2.4 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 2.15. Consider the Suzuki function field F over $\mathbb{F}_8$ as in Example 2.7. 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 2.12 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 2.12 are also satisfied. Therefore, the improvement over the Goppa bound via Theorem 2.12 is $\deg Z + 1 = 3$. In [10], the improvement for the same code is 2 (see [10, Table 2]).

Similarly, we increase the Lundell-McCullough improvement over Goppa bound from 2 to 3 for the codes in Table 2 over the Suzuki function field. We use the same notation as in Table 1. We denote the bound obtained from Theorem 2.12 by d_{GST2}. 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 1 and 2, only $C_\Omega(D, 17P_\infty + 11P_{0,0})$ is common, i.e. both Theorem 2.4 and Theorem 2.12 apply and yield the same improvement on this code.

In the remaining examples, our goal will be to obtain further improvements over Theorems 2.4 and 2.12. This is possible if the Riemann-Roch spaces involved satisfy extra conditions, which are listed in the following Lemma.

Lemma 2.16. *Let* A, B, D', E, Z *be divisors which satisfy*

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

G	A	B	Z	$\mathcal{L}$ space equalities	d_G	d_{LM}	d_{GST2}
$(16,11)$	$(14,6)$	$(2,5)$	$(1,1)$	$(13,5)=(14,6)$ $(2,5)=(3,6)=(3,7)=(4,6)$	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. Improvements on the Suzuki function field over $\mathbb{F}_8$ via Theorem 2.12

in addition to the hypothesis (i,ii,iii) in Lemma 2.11. Let $G = A + B$, $P \in \operatorname{supp}(Z)\backslash\operatorname{supp}(E)$ 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 of the article. 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 2.11. We use (v), Riemann-Roch Theorem, (iii), (vi) and Corollary 2.2. 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 2.10 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 2.11 we have $h_E(A) = h_E(A-Z) + \deg Z$. Hence, the proof is finished. □

Example 2.17. 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 2.12, 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 $H = 0$ in Corollary 2.13). The improvement for the same code $C_\Omega(D, G)$ is 1 in [10, Table 2].

Now, we would like to improve the lower bound further by using Lemma 2.16. 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 2.12 to conclude that $P_\infty \notin \mathrm{supp}(E)$. 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 2.4 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 $P_\infty \notin \mathrm{supp}(E)$, this sequence satisfies the hypotheses of Lemma 2.16. 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 2.18. 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 2.4). This is the same as the improvement of Lundell-McCullough ([10, Table 2]).

Assume that $d = 6$ and proceed as in Example 2.17. 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 $P_\infty \in \mathrm{supp}(E)$, 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 2.4). This is a contradiction and hence, $P_\infty \notin \mathrm{supp}(E)$.

Due to the fact that $P_\infty \notin \mathrm{supp}(E)$ and the properties of the relevant Riemann-Roch spaces, the following sequence satisfies the hypotheses of Lemma 2.16:

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

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 $d(C_\Omega(D, 27P_\infty + 2P_{0,0})) \geq 8$.

In [2], Beelen introduced the generalized order bound and 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 $\mathbb{F}_8$. Here, D is the sum of the remaining 63 rational places of the function field, as in Example 2.18. For many $C_{i,j}$'s his bound coincides with that of Lundell-McCullough (cf. [2, page 674]). Therefore, our bounds in Theorems 2.4 and 2.12 perform at least as good as the estimate of Beelen in those cases. In Table 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), we use arguments as in Examples 2.17 and 2.18 to obtain these improvements. We denote Lundell-McCullough, Beelen and our bounds by $d_{LM}, d_B, \tilde{d}$ respectively.

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

TABLE 3. Comparison of the bounds for $C_{i,j} = C_\Omega(D, iP_\infty + jP_{0,0})$

3. A New Equivalence Relation on $Div(F)$

Results of Section 2 motivates the study of the following relation on $Div(F)$:

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

In this case we call the divisors M and N *equivalent*. Clearly, this is an equivalence relation on $Div(F)$ 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. [13, page 16]).

Let us recall the definition of a closely related concept: floor of a divisor. For a divisor M with $\ell(M) > 0$, the floor of M is defined to be the unique divisor $\lfloor M \rfloor$ of the least degree such that $\mathcal{L}(M) = \mathcal{L}(\lfloor M \rfloor)$ (see [11]). In particular, $\lfloor M \rfloor \in c(M)$. Note that Theorems 2.4 and 2.12 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 some observations to be used in this section. For two divisors M and N, set

$$\gcd(M, N) := \sum_P \min\{v_P(M), v_P(N)\}P.$$

Lemma 3.1. *(i)* $\mathcal{L}(\gcd(M, N)) = \mathcal{L}(M) \cap \mathcal{L}(N)$. *Hence, if* $M \approx N$, *then* $\gcd(M, N) \in c(M)$.

(ii) If $M = \lfloor M \rfloor$, *then* $N \geq M$ *for any* $N \in c(M)$.

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

$$v_P(z) \geq \max\{-v_P(M), -v_P(N)\} = -\min\{v_P(M), v_P(N)\} = -v_P(\gcd(M, N))$$

for any place P. Hence, $z \in \mathcal{L}(\gcd(M, N))$.

(ii) Since $M = \lfloor M \rfloor$ is the unique divisor of the least degree in $c(M)$, for any $N \in c(M)$ we have $\gcd(M, N) = M$ by (i). This implies $M \leq N$.

(iii) 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(iii). 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 ([13, 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 2.4 and 2.12 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 [13, 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

$$\begin{aligned}
\mathcal{L}(W-M) &= \bigcap_{P \in \mathbb{P}_F^{(1)}} \mathcal{L}(W-M-P) \\
&= \mathcal{L}\Big(\gcd\big(\{W-M-P : P \in \mathbb{P}_F^{(1)}\}\big)\Big) \qquad \text{(by Lemma 3.1)} \\
&= \mathcal{L}\left(W - M - \sum_{P \in \mathbb{P}_F^{(1)}} P\right).
\end{aligned}$$

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(iii), 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,*

$$ht(c(M)) \leq i(\lfloor M \rfloor) \tag{3.2}$$

$$\leq g + 1 - \ell(M) \tag{3.3}$$

$$\leq g \tag{3.4}$$

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 [13, 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.

4. Concluding Remarks

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 is scarce compared to residue codes. Among the articles mentioned in Section 1, there are only two results known to us: [6, Theorem 3] and [11, Theorem 2.9]. However the former is implied by the latter, hence there is only one improved bound for $C_{\mathcal{L}}$ codes. Let D be as in (1.2) and G be such that $P_i \notin \operatorname{supp}(\lfloor G \rfloor)$ for $1 \leq i \leq n$. Then, [11, Theorem 2.9] states that

$$d\left(C_{\mathcal{L}}(D, G)\right) \geq n - \deg\lfloor G \rfloor. \tag{4.1}$$

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 (1.1) on the floor divisor, one gets (4.1).

We finish by commenting on the role of the ceiling of a divisor on the minimum distance estimates of AG codes. For a divisor M with $i(M) > 0$, the *ceiling* is defined to be the unique divisor $\lceil M \rceil$ of the largest degree such that $\Omega(M) = \Omega(\lceil M \rceil)$ (see [12]). For a canonical divisor W, we have

$$W - \lceil M \rceil = \lfloor W - M \rfloor \quad \text{and} \quad W - \lfloor M \rfloor = \lceil W - M \rceil \qquad \text{(cf. [12, Theorem 11]).} \tag{4.2}$$

These essentially follow from the isomorphism between $\Omega(M)$ and $\mathcal{L}(W - M)$ (cf. [13, Theorem I.5.14]).

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 (4.1), i.e. use the Goppa bound on the ceiling rather than the original divisor. Using the duality between floor and ceiling (cf. (4.2)), we now show that these results can be proved using the notion of floor.

Proposition 4.1. *(*[12, Theorem 16, Proposition 20]*) Let D be as in (1.2).*

(i) *If G is such that $P_i \notin supp\,(\lceil G - D \rceil + D)$ for $1 \le i \le n$, then*

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

where W is a canonical divisor.

(ii) *If G is such that $P_i \notin supp\,(\lceil G \rceil)$ for $1 \le i \le n$, then*

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

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. [13, Proposition 2.2.10]). By assumption, we also have $v_{P_i}(\lceil G - D \rceil) = -1$ for $1 \le i \le n$. Using (4.2), we have

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

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 (4.1), we have

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

(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 (1.1), we conclude

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

∎

References

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

[9] 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.

[10] 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

[11] 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.

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

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