JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **25**, No. 3, August 2012

RELATION BETWEEN THE FLOOR BOUND AND THE ORDER BOUND

Seungkook Park*

Abstract. The purpose of this paper is to show that the coset bound can be used to prove the floor bound. Our proof provides a natural relation between the floor bound and the order bound.

1. Introduction

For algebraic geometric codes, it is in general hard to determine the actual minimum distance. The main methods for finding the lower bound for the minimum distance of an algebraic geometric code can be divided into two categories which are Lundell-McCullough floor bound [4] and Beelen order bound [1]. The connection between the two bounds were given in [2, 3]. In [3], ABZ bound for codes and ABZ bound for cosets are formulated. The authors prove that ABZ bound for codes improves the floor bound. Then by showing that the order bound, obtained with the ABZ bound for cosets, is at least the ABZ bound for codes, they prove that the order type bound improves the floor bound. In this paper, we give a direct proof that the floor bound can be obtained by using the decompositions from two different order sequences and merging them into one new sequence. Our proof establishes a natural relation between the floor bound and the order bound. The paper is organized as follows: In Section 2 we give the definition of an algebraic geometric code and recall the method for finding the lower bound for the minimum distance based on the order bound. In Section 3 we prove the Lundell-McCullough floor bound using the order bound, which provides a better understanding of the relation between the two bounds. In

Received December 26, 2011; Accepted July 19, 2012.
2010 Mathematics Subject Classification: Primary 11T71; Secondary 14G50.
Key words and phrases: algebraic-geometric code, floor bound, order bound.
*This research was supported by the Sookmyung Women's University Research Grants 2012.

Section 3, we give an example for finding the minimum distance using the floor bound and the order bound.

2. Algebraic geometric codes and order bound

Let $X/\mathbb{F}$ be an algebraic curve (absolutely irreducible, smooth, projective) of genus g over a finite field $\mathbb{F}$. Let $\mathbb{F}(X)$ be the function field of $X/\mathbb{F}$ and let $\Omega(X)$ be the module of rational differentials of $X/\mathbb{F}$. Given a divisor E on X defined over $\mathbb{F}$, let $L(E) = \{f \in \mathbb{F}(X)\backslash\{0\} : (f) + E \geq 0\} \cup \{0\}$ and let $\Omega(E) = \{\omega \in \Omega(X)\backslash\{0\} : (\omega) \geq E\} \cup \{0\}$. Let K represent the canonical divisor class. For n distinct rational points $P_1, \ldots, P_n$ on X and for disjoint divisors $D = P_1 + \cdots + P_n$ and G, the geometric Goppa codes $C_L(D, G)$ and $C_\Omega(D, G)$ are defined as the images of the maps

$$\begin{aligned} \alpha_L &: L(G) \longrightarrow \mathbb{F}^n,\ f \mapsto (\, f(P_1), \ldots, f(P_n)\,), \\ \alpha_\Omega &: \Omega(G - D) \longrightarrow \mathbb{F}^n,\ \omega \mapsto (\, \mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)\,). \end{aligned}$$

The maps establish isomorphisms $L(G)/L(G - D) \simeq C_L(D, G)$ and $\Omega(G - D)/\Omega(G) \simeq C_\Omega(D, G)$. The codes $C_L(D, G)$ and $C_\Omega(D, G)$ are dual to each other. The Hamming distance between two vectors $x, y \in \mathbb{F}^n$ is $d(x, y) = |\{i : x_i \neq y_i\}|$. The minimum distance of a nontrivial linear code $\mathcal{C}$ is

$$\begin{aligned} d(\mathcal{C}) &= \min\{d(x, y) : x, y \in \mathcal{C}, x \neq y\} \\ &= \min\{d(x, 0) : x \in \mathcal{C}, x \neq 0\}. \end{aligned}$$

The Hamming distance between two nonempty subsets $X, Y \subset \mathbb{F}^n$ is the minimum of $\{d(x, y) : x \in X, y \in Y\}$. For a proper subcode $\mathcal{C}' \subset \mathcal{C}$, the minimum distance of the collection of cosets $\mathcal{C}/\mathcal{C}'$ is

$$\begin{aligned} d(\mathcal{C}/\mathcal{C}') &= \min\{d(x + \mathcal{C}', y + \mathcal{C}') : x, y \in \mathcal{C}, x - y \notin \mathcal{C}'\} \\ &= \min\{d(x, 0) : x \in \mathcal{C}, x \notin \mathcal{C}'\}. \end{aligned}$$

For two vectors $x, y \in \mathbb{F}^n$, let $x * y \in \mathbb{F}^n$ denote the Hadamard or coordinate-wise product of the two vectors. We state the theorem of coset bound from ([3], Theorem 1.2.) without proof.

THEOREM 2.1 (Coset bound). *Let $\mathcal{C}/\mathcal{C}_1$ be an extension of $\mathbb{F}$-linear code with corresponding extension of dual codes $\mathcal{D}_1/\mathcal{D}$ such that* $\dim \mathcal{C}/\mathcal{C}_1 = \dim \mathcal{D}_1/\mathcal{D} = 1$. *If there exist vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such*

that

$$\begin{cases} a_i * b_j \in \mathcal{D} & \text{for } i+j \le w, \\ a_i * b_j \in \mathcal{D}_1 \backslash \mathcal{D} & \text{for } i+j = w+1, \end{cases}$$

then $d(\mathcal{C}/\mathcal{C}_1) \ge w$.

Theorem 2.1 can be used to estimate the minimum distance $d(\mathcal{C}/\mathcal{C}')$ of an extension $\mathcal{C}/\mathcal{C}'$ with $\dim \mathcal{C}/\mathcal{C}' > 1$, after dividing $\mathcal{C}/\mathcal{C}'$ into subextensions.

LEMMA 2.2. *Let $\mathcal{C}/\mathcal{C}'$ be an extension of $\mathbb{F}$-linear code of length n. For $\mathcal{C} \supset \mathcal{C}'' \supset \mathcal{C}'$,*

$$d(\mathcal{C}/\mathcal{C}') = \min\{\, d(\mathcal{C}/\mathcal{C}''),\ d(\mathcal{C}''/\mathcal{C}') \,\}.$$

Proof.

$$\begin{aligned} d(\mathcal{C}/\mathcal{C}') &= \min\{\, d(x,0) : x \in \mathcal{C}, x \notin \mathcal{C}' \} \\ &= \min\{\{d(x,0) : x \in \mathcal{C}, x \notin \mathcal{C}''\} \cup \{d(x,0) : x \in \mathcal{C}'', x \notin \mathcal{C}'\}\} \\ &= \min\{\, d(\mathcal{C}/\mathcal{C}''),\ d(\mathcal{C}''/\mathcal{C}') \,\}. \end{aligned}$$

□

To find the minimum distance of a code $\mathcal{C}$ we use the following lemma:

LEMMA 2.3. *Let $\mathcal{C}/\mathcal{C}'$ be an extension of $\mathbb{F}$-linear codes of length n. Then the minimum distance of the code $\mathcal{C}$ is*

$$d(\mathcal{C}) = \min\{d(\mathcal{C}/\mathcal{C}'), d(\mathcal{C}')\}.$$

Proof.

$$\begin{aligned} d(\mathcal{C}) &= \min\{\, d(x,0) : x \in \mathcal{C}, x \neq 0 \,\} \\ &= \min\{\{d(x,0) : x \in \mathcal{C}, x \notin \mathcal{C}'\} \cup \{d(x,0) : x \in \mathcal{C}', x \neq 0\,\}\} \\ &= \min\{\, d(\mathcal{C}/\mathcal{C}'),\ d(\mathcal{C}') \,\}. \end{aligned}$$

□

The order bound uses a filtration of subcodes of the code obtaining different coset bounds for different subsets of codewords. In general, we obtain an improved bound if for each subset we can find a coset bound better than a uniform bound for all codewords.

3. Proof of floor bound using order bound

We state and prove the Lundell-McCullough floor bound using the order bound.

THEOREM 3.1 (Lundell-McCullough floor bound). *Let $G = A+B+Z$, for $Z \geq 0$ such that $L(A+Z) = L(A)$ and $L(B+Z) = L(B)$. For D with $\mathrm{supp}(D) \cap \mathrm{supp}(Z) = \emptyset$, a nonzero word in $C_\Omega(D, G)$ has weight at least $\deg G - (2g-2) + \deg Z$.*

Proof. Let $G = A + B + Z$. We use the coset bound to show that for each $r \geq 0$, a word in $C_\Omega(D, G+rP)\backslash C_\Omega(D, G+rP+P)$ has weight at least $\deg G - (2g-2) + \deg Z$. Let $\deg A = a$, $\deg B = b$, and $\deg Z = z$. For $i = 0, 1, \ldots, a$,

$$G + rP + P = (A - iP) + (B + Z + rP + iP + P).$$

For $j = 0, 1, \ldots, b$,

$$G + rP + P = (A + Z + rP + jP + P) + (B - jP).$$

We claim that among the $(a+1)+(b+1) = a+b+2$ decompositions of $G + rP + P$ there are at least $a + b + 2 - 2(g - z)$ decompositions that are sums of two nongaps at P.
Since

$$\begin{aligned}
&\dim L(A + Z + rP + bP + P) - \dim L(A + Z + rP) \\
&\quad + \dim L(A) - \dim L(A - aP - P) \\
&\geq \deg(A + Z + rP + bP + P) + 1 - g \\
&\quad - (\dim L(A + Z + rP) - \dim L(A)) \\
&\geq \deg(A + Z + rP + bP + P) + 1 - g \\
&\quad - (\dim L(A+Z+rP) - \dim L(A + Z) + \dim L(A+Z) - \dim L(A)) \\
&\geq (a + z + r + b + 1) + 1 - g - r = a + b + 2 - (g - z),
\end{aligned}$$

there are at most $(g - z)$ gaps at P among

$$\{A - aP, \ldots, A\} \cup \{A + Z + rP + P, \ldots, A + Z + rP + bP + P\}.$$

Similarly, the following inequality

$$\begin{aligned}
&\dim L(B+Z+rP+aP+P) - \dim L(B+Z+rP) \\
&\quad + \dim L(B) - \dim L(B-bP-P) \\
&\geq \deg(B+Z+rP+aP+P) + 1 - g \\
&\quad - (\dim L(B+Z+rP) - \dim L(B)) \\
&\geq \deg(B+Z+rP+aP+P) + 1 - g \\
&\quad - (\dim L(B+Z+rP) - \dim L(B+Z) + \dim L(B+Z) - \dim L(B)) \\
&\geq (b+z+r+a+1) + 1 - g - r = a+b+2-(g-z)
\end{aligned}$$

yields that there are at most $(g-z)$ gaps at P among

$$\{B-bP,\ldots,B\} \cup \{B+Z+rP+P,\ldots,B+Z+rP+aP+P\}.$$

Thus among the $a+b+2$ decompositions of $G+rP+P$ there are at least $a+b+2-2(g-z)$ decompositions such that the decomposition consists of two nongaps at P that sum up to $G+rP+P$. Thus, by Theorem 2.1,

$$d(C_\Omega(D, G+rP)/C_\Omega(D, G+rP+P)) \geq a+b+2-2(g-z) \text{ for } r \geq 0.$$

By applying Lemma 2.2 and Lemma 2.3 repeatedly, we have

$$d(C_\Omega(D,G)) \geq a+b+2-2(g-z) = \deg\, G - (2g-2) + \deg\, Z.$$

□

4. Example of one-point Hermitian codes

We give an example of how to find the lower bound for the minimum distance of one-point Hermitian code. For comparison, we will use both the floor bound and order bound to find the lower bound for the minimum distance.

EXAMPLE 4.1. *Let X be a Hermitian curve defined by $y^4+y=x^5$ over $\mathbb{F}_{16}$. Then X has 65 rational points over $\mathbb{F}_{16}$, denoted by $P_1,\ldots,P_{64},P_\infty$, where P_∞ is the point at infinity of X. The genus is 6. A canonical divisor is $K=10P_\infty$. Let $\mathbb{F}_{16}(X)$ be the function field of X over $\mathbb{F}_{16}$. For $f \in \mathbb{F}_{16}(X)\backslash\{0\}$, let $(f)_\infty$ denote the pole divisor of f and let $(f)_0$ denote the zero divisor of f. Then the divisor of f can be written as $(f)=(f)_0-(f)_\infty$. Consider the Weierstrass semigroup of the point P_∞; that is,*

$$H(P_\infty) = \{n \in \mathbb{N}_0 : \exists\ f \in \mathbb{F}_{16}(X) \text{ with } (f)_\infty = nP_\infty\}.$$

Since $(x)_\infty = 4P_\infty$ *and* $(y)_\infty = 5P_\infty$, *the gap numbers at* P_∞ *are* $\{1,\ 2,\ 3,\ 6,\ 7,\ 11\}$ *and*

$$H(P_\infty) = \langle 4, 5\rangle = \{0,\ 4,\ 5,\ 8,\ 9,\ 10,\ 12,\ 13,\ 14,\ 15,\ 16, \ldots\}.$$

For $G = 17P_\infty$ *and* $D = P_1 + \cdots + P_{64}$, *we show that* $d(C_\Omega(D, G)) \geq 8$.

Floor Bound :

For $G = 17P_\infty = A + B + Z$, *let* $A = 10P_\infty$, $B = 6P_\infty$, *and* $Z = P_\infty$. *Then*

$$L(A + Z) = L(11P_\infty) = L(10P_\infty) = L(A)$$

and

$$L(B + Z) = L(7P_\infty) = L(6P_\infty) = L(B).$$

Then by Theorem 3.1,

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

Order Bound :

To the extension of codes $\mathcal{C}/\mathcal{C}_1 = C_\Omega(D, 17P_\infty)/C_\Omega(D, 18P_\infty)$ *corresponds an extension of dual codes* $\mathcal{D}_1/\mathcal{D} = C_L(D, 18P_\infty)/C_L(D, 17P_\infty)$. *If there exist vectors* $a_1, \ldots, a_w$ *and* $b_1, \ldots, b_w$ *such that*

$$\begin{cases} a_i * b_j \in \mathcal{D} = C_L(D, 17P_\infty) & \text{for } i + j \leq w, \\ a_i * b_j \in \mathcal{D}_1 \backslash \mathcal{D} = C_L(D, 18P_\infty) \backslash C_L(D, 17P_\infty) & \text{for } i + j = w + 1, \end{cases}$$

then $d(\mathcal{C}/\mathcal{C}_1) \geq w$. *In other words, if there exist rational functions* $f_1,\ f_2, \ldots, f_w$ *and* $g_1,\ g_2, \ldots, g_w$ *such that*

$$\begin{cases} f_i g_j \in L(17P_\infty) & \text{for } i + j \leq w, \\ f_i g_j \in L(18P_\infty) \backslash L(17P_\infty) & \text{for } i + j = w + 1, \end{cases}$$

then $d(\mathcal{C}/\mathcal{C}_1) \geq w$. *Note that* $f_i g_j \in L(18P_\infty) \backslash L(17P_\infty)$ *means that* $f_i g_j$ *has a pole only at* P_∞ *with exact pole order 18, that is,* $(f_i g_j)_\infty = 18P_\infty$. *Now we find the rational functions that satisfy the above conditions. Consider the following figure. In the figure, the numbers below and to the right of the functions are the pole order of the functions at* P_∞.
It follows from the figure that

$$\begin{cases} f_i g_j \in L(17P_\infty) & \text{for } i + j \leq 9, \\ f_i g_j \in L(18P_\infty) \backslash L(17P_\infty) & \text{for } i + j = 10. \end{cases}$$

			f_1	f_2	f_3	f_4	f_5	f_6		f_7	f_8				f_9
			1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3	x^4	x^3y	x^2y^2
			0	*4*	*5*	*8*	*9*	*10*	*12*	*13*	*14*	*15*	*16*	*17*	*18*
g_1	1	*0*													*18*
g_2	x	*4*									*18*				
g_3	y	*5*								*18*					
g_4	x^2	*8*						*18*							
g_5	xy	*9*					*18*								
g_6	y^2	*10*				*18*									
	x^3	*12*													
g_7	x^2y	*13*			*18*										
g_8	xy^2	*14*		*18*											
	y^3	*15*													
	x^4	*16*													
	x^3y	*17*													
g_9	x^2y^2	*18*	*18*												

Thus $d(\mathcal{C}/\mathcal{C}_1) \geq 9$. By a careful observation we notice that the problem of finding the rational functions is equivalent to finding pairs of numbers that add up to 18 *with both numbers being nongaps. We illustrate the method below. We write the numbers from* 0 *to* 18 *in the first row. In the second row, we write the numbers from* 18 *to* 0*. Then we cross out the gaps in both rows and count the number pairs that is not crossed out.*

✓				✓	✓			✓	✓	✓			✓	✓				✓
0	~~1~~	~~2~~	~~3~~	4	5	~~6~~	~~7~~	8	9	10	~~11~~	12	13	14	15	16	17	18
18	*17*	*16*	*15*	*14*	*13*	*12*	~~*11*~~	*10*	*9*	*8*	~~*7*~~	~~*6*~~	*5*	*4*	~~*3*~~	~~*2*~~	~~*1*~~	*0*

Applying the same method to $C_\Omega(D, 18P_\infty)/C_\Omega(D, 19P_\infty)$ we have

$$d(C_\Omega(D, 18P_\infty)/C_\Omega(D, 19P_\infty)) \geq 8.$$

By repeated application, we can compute the lower bound for the weights of codewords in the subsets(layers) of the code. Thus we have

≥ 9	$C_\Omega(D, 17P_\infty) \backslash C_\Omega(D, 18P_\infty)$
≥ 8	$C_\Omega(D, 18P_\infty) \backslash C_\Omega(D, 19P_\infty)$
≥ 9	$C_\Omega(D, 19P_\infty) \backslash C_\Omega(D, 20P_\infty)$
≥ 10	$C_\Omega(D, 20P_\infty) \backslash C_\Omega(D, 21P_\infty)$
	$\vdots$

By taking the minimum of the weights of the codewords, we have

$$d(C_\Omega(D, G)) \geq 8.$$

5. Conclusion

In the proof of Theorem 3.1 we use the decompositions from two different order sequences and merge them into one new sequence. Thus floor bound equals merging two order sequences.

References

[1] P. Beelen, *The order bound for general algebraic geometric codes*, Finite Fields Appl. **13** (2007), 665-680.

[2] I. M. Duursma, R. Kirov, and S. Park.*Distance bounds for algebraic geometric codes,* J. Pure Appl. Algebra. **215** (2011), 1863-1878.

[3] I. M. Duursma and S. Park, *Coset bounds for algebraic geometric codes,* Finite Fields Appl. **16** (2010), 36-55.

[4] B. Lundell and J. McCullough, *A generalized floor bound for the minimum distance of geometric Goppa codes,* J. Pure Appl. Algebra. **207** (2006), 155–164.

*

Department of Mathematics
Sookmyung Women's University
Seoul 140-742, Republic of Korea
E-mail: skpark@sm.ac.kr