論文 95-4-4-19

Codes from Some Subfields of the Hermitian Function Field:Abundant Case

Kyeong Cheol Yang* Regular Members

허미션 함수체의 부분체로부터 파생되는 부호:어번던트한 경우

正會員 梁 景 喆*

이 연구는 1994년도 한국과학재단 핵심전문연구과제(과제번호: 941-0900-070-1)에 의한 결과임

ABSTRACT

Geometric Goppa codes (or algebraic geometric codes) are classified into two types according to the injectivity of the evaluation map: *non-abundant* or *abundant* codes. Some subfields of the Hermitian function field are considered in this paper, which are defined by $y^s+y=x^t$ over GF(q^2) where s divides $q+1$. These subfields are also maximal like the Hermitian function field since they have the maximum number of places of degree one permissible by the Hasse-Weil bound. Abundant codes arising from these subfields are studied and their dimension and minimum distance are exactly and completely presented in this paper.

要 約

기하 Goppa 부호 혹은 대수기하부호는 평가사상의 단사성(일대일 성질)에 따라 비어번던트 부호와 어번던트 부호 두가지로 분류된다. 본 논문에서는 허미션 함수체의 부분체를 다루는데, 이는 $GF(q^2)$ 위에서 $y^s+y=x^t$로 정의되며 s는 $q+1$을 나누는 정수이다. 이러한 부분체들은 허미션함수체와 마찬가지로 최대가 되는데, 이는 Hasse-Weil 한계식에 의해 허용되는 최대 갯수의 1차점들을 갖기때문이다. 본 논문에서는 이러한 부분체로 부터 파생되는 어번던트 부호를 연구하여 이들 부호의 차원과 최소거리를 정확 하고 완전하게 구하였다.

*한양대학교 전자통신공학과
Dept. of Electronic Communication Engineering
Hanyang University
論文番號 : 9512-0111
接受日字 : 1994年 1月 11日

Ⅰ. Introduction

Originally, Goppa constructed algebraic geometric codes using differentials of a function field and the residue map, which are now well-known to be the duals of algebraic geometric codes using funtions of a function field and the evaluation map. The presentation here will adopt the function/evauation viewpoint. See [4], [6], [10] for more details.

Let F/K be an algebraic function field of genus g over a finite constant field K (see [1], [6], [10] for example). Let $\{P_i | i=1,2,\cdots,n\}$ be a set of places of degree one in F/K. Let G and D be divisors of F/K such that $D=P_1+P_2+\cdots+P_n$ and $\mathrm{supp}(G)\cap \mathrm{supp}(D)=\varphi$, where $\mathrm{supp}(G)$ and $\mathrm{supp}(D)$ denote the supports of G and D, respectively. Define the vector space $L(G)$ as follows:

$$L(G):=\{f\in F |\ f=0 \text{ or } (f)\geq -G\} \tag{1}$$

where (f) is the principal divisor of f. For a divisor A of F/K, denote by $\dim A$ and $\deg A$ the dimension of $L(A)$ over K and the degree of A, respectively. Now consider the K-linear evaluation map ψ given by

$$\begin{array}{rccc} \psi : & L(G) & \rightarrow & K^n \\ & f & \rightarrow & (f(P_1),\ f(P_2),\ \cdots,\ f(P_n)) \end{array} \tag{2}$$

Then the geometric Goppa code (or algebraic geometric code) associated with two divisors D and G is defined by

$$C_L(D,G) := \text{Image of } \psi = \psi(L(G)) \tag{3}$$

The basic parameters of $C_L(D,G)$ are well-known in the following proposition [4], [10].

Proposition 1 (Goppa) $C_L(D,G)$ is an $[n,k,d]$ code with parameters

$k=\dim G-\dim(G-D)$ and $d\geq n-\deg G$.

Furthermore, if $2g-2<\deg G<n$, then $k=\deg G-g+1$

Geometric Goppa codes may be classified into two types according to the injectivity of ψ in (2): If ψ is not one-to-one, then $\dim(G-D)>0$ and the code is called *abundant*; otherwise, $\dim(G-D)=0$ and the code is said to be *non-abundant*. The number $a:=\dim(G-D)$ is called the *abundance* of the code. Abundant codes have been studied by Pellikaan [7], but note that he has defined $\deg(G-D)$ to be the abundance of the code.

A particularly interesting class of geometric Goppa codes are codes arising from the Hermitian function field. The large length of these codes in comparison with their alphabet size makes them attractive over conventional Reed-Solomon codes having the same alphabet. These codes are called Hermitian codes and their true minimum distances have been determined by Stichtenoth [8], Yang and Kumar [11].

Another interesting class of of geometric Goppa codes are codes arising from some subfields of the Hermitian function field. Like the Hermitian function field, these subfields defined by $y^s+y=x^{s+1}$ over $GF(q^2)$ where s divides $q+1$ are also maximal, having the maximum number of places of degree one permissible by the Hasse-Weil bound. The dimension and minmum distance of these codes in the non-abundant case are known in [13].

In this paper we are interested in the abundant codes arising from some subfields of the Hermitian function field. We provide complete results on the dimension and minimum distance of these codes.

Ⅱ. Some Subfields of Hermitian Function Fields

Let K be a finite field $K=GF(q^2)$(q=a power of some prime p) and $F=K(x,y)$ be the function field defined by

$$F=K(x,y) \text{ with } y^s+y=x^{s+1} \text{ where } s|q+1 \tag{4}$$

(see [2], [3], [8], [10]). If $s=q+1$, then F/K is

called the Hermitian function field over K. If $s<q+1$, then F/K is isomorphic to a subfield of the Hermitian function field and we shall therefore refer to it as a subfield of the *Hermitian function field*. The genus g of the function field F/K is given by $g=(q-1)(s-1)/2$ and the divisor of the differential dx can be shown to be

$$(dx) = (2g-2)Q_\infty \tag{5}$$

where Q_∞ is the common pole of x and y.

The places of degree one of F/K are given as follows: The place Q_∞ is one of them. Let $\alpha \in K$. Note that $T^q+T=\alpha^s$ has a root in K if and only if $\alpha^s \in GF(q)$. For any α with $\alpha^s \in GF(q)$, there are exactly q distinct solutions in K of $T^q + T=\alpha^s$. Let U' be the subgroup of order $(q-1)s$ of the multiplicative group K^* and let $U:=U' \cup \{0\}$. Then for $\alpha \in K$, $\alpha^s \in GF(q)$ if and only if $\alpha \in U$. Hence the number N of places of degree one in F/K is

$$N = q \cdot |U| + 1 = q(1+(q-1)s)+1 \tag{6}$$

Since $N = 1+q^2+2gq = 1+q^2+q(q-1)(s-1)$, F/K achieves the Hasse-Weil bound and is therefore a maximal function field.

We define $P_{\alpha,\beta}$ to be the common zero of $x-\alpha$ and $y-\beta$ whenever $\alpha \in U$ and $\beta \in K$ are such that $\beta^q+\beta=\alpha^s$. Then the divisors of $x-\alpha$ and $y-\beta$ are as follows:

$$(x-\alpha) = \begin{cases} \sum_{\substack{\beta \in K, \\ \beta^q+\beta=\alpha^s}} P_{\alpha,\beta} - qQ_\infty, & \text{if } \alpha \in U, \\ R_\alpha - qQ_\infty, & \text{if } \alpha \in K \setminus U, \end{cases} \tag{7}$$

where R_α is a divisor of degree q in F/K depending on α whose support does not contain any place of degree one and

$$(y-\beta) = \begin{cases} sP_{0,\beta} - sQ_\infty, & \text{if } \beta^q+\beta=0, \\ \sum_{\substack{\alpha \in K, \\ \alpha^s=\beta^q+\beta}} P_{\alpha,\beta} - sQ_\infty, & \text{if } \beta^q+\beta \neq 0, \end{cases} \tag{8}$$

For each integer $m \geq 0$, the set $B(m)$ given by

$$B(m) := \{x^i y^j \mid 0 \leq i,\ 0 \leq j \leq q-1,\ iq+js \leq m\} \tag{9}$$

is a basis of $L(mQ_\infty)$ over K.

Let $st := q+1$. From here on, we will assume that

$$G := mQ_\infty \quad \text{and} \quad G := \sum_{\alpha \in U} \sum_{\substack{\beta \in K \\ \beta^q+\beta=\alpha^s}} P_{\alpha,\beta} \tag{10}$$

Consider the geometric Goppa code $C_L(D,G)$ associated with two divisors D and G. Then $C_L(D,G)$ is a linear code of length $n:=q(1+(q-1)s)$. To simplify notation, let

$$C_m := C_L(D, mQ_\infty) \tag{11}$$

Let $d(C_m)$ denote the minimum distance of the code C_m. Note that C_m is a linear code of length $n=q(1+(q-1)s)$ and that if $m_1 \leq m_2$, then $C_{m1} \subseteq C_{m2}$ and therefore $d(C_{m1}) \geq d(C_{m2})$.

Consider the function u defined by $u:=\prod_{\alpha \in U}(x-\alpha)$. Then we have

$$(u) = D - nQ_\infty$$

and

$$u = x \prod_{\alpha \in U^*}(x-\alpha) = x(x^{(q-1)s}-1) = x^{1+(q-1)s} - x.$$

Let $\omega := dx/u$. Then we get

$$(\omega) = (dx) - (u) = (n+2g-2)Q_\infty - D \tag{12}$$

This implies that $v_P(\omega) = -1$ for any place $P \in \mathrm{supp}(D)$ where $v_P(\cdot)$ denotes the discrete valuation of F/K at P. For any linear code C of length n over K and any n-tuple $\underline{a}:=(a_1, \cdots, a_n)$ where $0 \neq a_i \in K$ for all i, let

$$\underline{a} \cdot C = \{(a_1c_1, \cdots, a_nc_n) \mid (c_1, \cdots, c_n) \in C\} \tag{13}$$

Then we have the following proposition by applying Theorem 2.5 in [9] to our code C_m.

Proposition 2 ([9], Theorem 2.5) For any integer m, the codes C_m and $\underline{a} \cdot C_{n+2g-2-m}$ are dual to each other, where $\underline{a} := (\mathrm{res}_{P_1}\omega, \cdots, \mathrm{res}_{P_n}\omega)$ and res_{P_i} is the residue of ω at P.

Remark 3 (a) The differential $\eta := du/u$ has $v_P(\eta) = -1$ and $\mathrm{res}_P\eta = 1$ for any $P \in \mathrm{supp}(D)$. If $s \equiv 1 \bmod p$, then we have $du = -dx$ and $(\eta) = (n+2g-2)Q_\infty - D$. Hence, C_m and $C_{n+2g-2-m}$ are dual to each other in this case.

(b) The condition $s \equiv 1 \bmod p$ holds for $p=2$ since s and q are relatively prime. It also holds for the Hermitian function field since $s = q+1$.

An integer $i \geq 0$ is called a *gap* number of Q_∞ if there is no function $f \in F$ such that $f \in L(lQ_\infty) \setminus L((l-1)Q_\infty)$. Otherwise, l is called a *pole number* of Q_∞. Let S be the set of all gap numbers of Q_∞. From the above basis of $L(mQ_\infty)$ given in (9), it is easy to check that

$$S = S_1 \cup S_2 \tag{14}$$

where

$$S_1 = \{aq + cs + b \mid 0 \leq a \leq s-2,\ 0 \leq c \leq t-2,\ a+1 \leq b \leq s-1\}$$

and

$$S_2 = \{aq + (t-1)s + b \mid 0 \leq a \leq s-3,\ a+1 \leq b \leq s-2\}.$$

This gap sequence plays a central role in determining the dimension and minimum distance of the code C_m as in the Hermitian case [8], [11].

Remark 4 (a) If t=1(i.e., $s = q+1$) then F/K is the Hermitian function field and $S = \{aq+b \mid 0 \leq a \leq q-2,\ a+1 \leq b \leq q-1\}$. In particular, the length n of the code C_m is $n = q^3$ in this case.

(b) If $t = q+1$(i.e., $s=1$) then F/K is a rational function field since $F = K(x, y) = K(y)$. In this case, Q_∞ does not have a gap number and $n = q^2$.

The dimension of the code C_m is easily determined from the above gap sequence given in (14). Let

$$I(m) := \{l \leq m \mid l = iq + js,\ i \geq 0,\ 0 \leq j \leq q-1. \tag{15}$$

Any integer m can be uniquely expressed as follows:

$$m = aq + cs + b \text{ with } a \geq 0,\ 0 \leq c \leq t-2, \text{ and } 0 \leq b \leq s-1 \tag{16}$$

or

$$m = aq + (t-1)s + b \text{ with } a \geq 0, \text{ and } 0 \leq b \leq s-2 \tag{17}$$

Using this expression and the basis of $L(mQ_\infty)$ in (9), it is easy to calculate $|I(m)|$, that is,

$$|I(m)| = \begin{cases} \dfrac{a(a+1)}{2}t + c(a+1) + \min\{a, b\} \\ \quad + 1, \text{ for } 0 \leq m \leq 2g-2 \\ m + 1 - g, \quad \text{for } m > 2g-2. \end{cases} \tag{18}$$

Proposition 5 Assume that $0 \leq m \leq n+2g-2 = qs^2 - s - 1$. Then the dimension of C_m is given by

$$\dim C_m = \begin{cases} |I(m)| & \text{for } 0 \leq m \leq 2g-2, \\ n - |I(m^\perp)| & \text{for } n \leq m \leq n+2g-2 \end{cases}$$

where $m^\perp := n+2g-2-m = q^2-s-1-m$. For $2g-2 < m < n$, we have

$$\dim C_m = m + 1 - g = m + 1 - \frac{(q-1)(s-1)}{2}.$$

Proof: For $0 \leq m < n$, we have $\dim C_m = \dim L(mQ_\infty) = |I(m)|$. For $n \leq m \leq n+2g-2$, we have by Proposition 2

$$\dim C_m = n - \dim C_m^\perp = n - \dim \underline{a} \cdot C_{n+2g-2-m}$$
$$= n - \dim C_{n+2g-2-m} = n - |I(m^\perp)|$$

where $m^\perp = n+2g-2-m \leq 2g-2 < n$. □

In order to determine the minimum distance of

the code C_m, we focus on the case that $1<s<q+1$ (equivalently, $1<t<q+1$ because $st=q+1$). By the Goppa bound, we have

$$d(C_m)\geq n-m$$

For any nonnegative integer m, let $\tilde{m}$ be the largest pole number of Q_∞ with $\tilde{m}\leq m$. Then it is clear that $L(mQ_\infty)=L(\tilde{m}Q_\infty)$, so we may assume in what follows that m is a pole number of Q_∞.

In the nonabundant case ($0\leq m<n$), we can divide our problem into two cases:

- n-m is a pole number of Q_∞.
- n-m is not a pole number of Q_∞.

From the gap sequence given in (14), it is easily checked that if $n-m$ is not a pole number of Q_∞, we have either

$m=n-aq-cs+b$ with $0\leq a\leq s-2$, $1\leq c\leq t-1$, $1\leq b\leq s-1-a$

or

$m=n-aq-ts+b$ with $0\leq a\leq s-3$, and $2\leq b\leq s-1-a$.

Based on this expression on m, the minimum distance of C_m in the non-abundant case is determined in the following proposition [13].

Proposition 6 (Non-abundant Case) Assume that $0\leq m<n$ and m is a pole number of Q_∞.

(a) If $n-m$ is a pole number of Q_∞, then

$$d(C_m)=n-m.$$

(b) If $m=n-aq-cs+b$ with $0\leq a\leq s-2$, $1\leq c\leq t-1$, and $1\leq b\leq s-1-a$, then

$$d(C_m)=n-m+b=aq+cs$$

(c) If $m=n-aq-ts+b$ with $0\leq a\leq s-3$ and $2\leq b\leq s-1-a$, then

$$d(C_m)=n-m+b-1=aq+ts-1=(a+1)q.$$

Ⅲ. The Minimum Distance of Abundant Codes: $m\geq n$

In this range, $L(mQ_\infty - D)$ is not always {0} since $m-n\geq 0$. Also, Goppa's lower bound $d(C_m)\geq n-\deg G=n-m$ is not useful any more. To simplify notation, let

$$m^\perp:=n+2g-2-m=q^2-s-1-m.$$

By Proposition 2, the dual $C_m^\perp$ of C_m is

$$C_m^\perp:=\underline{a}\cdot C_{m^\perp}$$

where $\underline{a}=(\mathrm{res}_{P_1}\omega, \cdots, \mathrm{res}_{P_n}\omega)$ and $\omega=dx/u$ in (12). If H is a generator matrix for $C_m^\perp$, then a parity check matrix H' for C_m may be written as follows:

$$H' = H\begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_n \end{bmatrix}.$$

Thus C_m and the dual code of $C_{m^\perp}$ have the same dimension, the same minimum distance and the same weight distribution [5]. Therefore, we can determine the minimum distance of C_m by investigating the generator matrix H of $C_{m^\perp}$.

If $m>n+2g-2$, then $m^\perp<0$, so $L(m^\perp Q_\infty)=\{0\}$ and $C_{m^\perp}=\{0\}$. As a result, $C_m=K^n$ and $d(C_m)=1$. We can therefore restrict our attention to $n\leq m\leq n+2g-2$. Then we have $0\leq m^\perp\leq 2g-2=(s-2)q+(q-1-s)$. Hence $m^\perp$ can be uniquely expressed as

$$m^\perp=aq+b \text{ with } 0\leq a\leq s-2 \text{ and} 0\leq b\leq q-1 \qquad (19)$$

The set $B(m^\perp)$ in (9) can be chosen as basis of $L(m^\perp Q_\infty)$. As a first step, we would like to construct a generator matrix H for $C_{m^\perp}$ and show that any $a+1$ columns of H are linearly independent over K.

Consider a submatrix A of H obtained by choosing $a+1$ distinct columns from H arbitrarily. Since each column of H corresponds to a place $P_{\alpha,\beta}$ of degree one, we can rearrange the columns of A in the following order based on β without loss of generality:

$$P_{\alpha_{1,1},\beta_1} \quad P_{\alpha_{1,2},\beta_1} \quad \cdots \quad P_{\alpha_{1,b_1},\beta_1}$$

$$\begin{matrix} P_{\alpha_{1,1},\beta_1} & P_{\alpha_{1,2},\beta_2} & \cdots & P_{\alpha_{1,b_2},\beta_2} \\ \vdots & \vdots & & \vdots \\ P_{\alpha_{\nu,1},\beta_\nu} & P_{\alpha_{\nu,2},\beta_\nu} & \cdots & P_{\alpha_{\nu,b_\nu},\beta_\nu} \end{matrix} \tag{20}$$

where β_j's are pairwise distinct and $b_1+b_2+\cdots+b_\nu = a+1$ with $b_1 \geq b_2 \geq \cdots \geq b_\nu \geq 1$. Clearly, we have $b_j \leq a+2-j$. Consider the element $x^{i_j}y^{j-1}$ with $0 \leq i_j \leq b_j-1$ and $1 \leq j \leq \nu$. Note that

$$\begin{aligned} -v_{Q_\infty}(x^{i_j}y^{j-1}) &= i_j q + (j-1)s \\ &\leq (b_j-1)q + (j-1)s \\ &\leq (a+1-j)q + (j-1)s \\ &= (j-1)(s-q) + aq. \end{aligned}$$

Since $ts=q+1$ and $t>1$, we get $s<q$ and $-v_{Q_\infty}(x^{i_j}y^{j-1}) \leq aq \leq m^{\perp}$. Hence we have the following lemma.

Lemma 7 Assume that $m^{\perp}=aq+b$ with $0 \leq a \leq s-2$ and $0 \leq b \leq q-1$. Let $b_1, \cdots, b_\nu$ be positive integers such that $b_1+b_2+\cdots+b_\nu = a+1$ and $b_1 \geq b_2 \geq \cdots \geq b_\nu \geq 1$. Then

$$x^{i_j}y^{j-1} \in L(m^{\perp}Q_\infty)$$

for any integer i_j and j with $0 \leq i_j \leq b_j-1$ and $1 \leq j \leq \nu$.

Now rewrite these elements in the following order:

$$\begin{matrix} 1, & x, & \cdots & x^{b_1-1} \\ y, & xy, & \cdots & x^{b_2-1}y \\ \vdots & \vdots & & \vdots \\ y^{\nu-1}, & xy^{\nu-1}, & \cdots & x^{b_\nu-1}y^{\nu-1} \end{matrix} \tag{21}$$

Then we can choose an $(a+1)\times(a+1)$ submatrix B of A as follows: (i) Each row corresponds to a function in the order as given in (21). (ii) Each column corresponds to a place of degree one in the order as given in (20). (iii) Each entry of B is obtained by evaluation. That is,

$$B=[B_{i,j}],\ i,j=1,2,\cdots,\nu \tag{22}$$

where $B_{i,j}$ is a $(b_i \times b_j)$ matrix whose (k,l)-th entry is $\beta_j^{i-1}\alpha_{j,l}^{k-1}$, i.e.,

$$B_{i,j} = \beta_j^{i-1}D_{i,j} \tag{23}$$

with

$$D_{i,j} := \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_{j,1} & \alpha_{j,2} & \cdots & \alpha_{j,b_j} \\ \alpha_{j,1}^2 & \alpha_{j,2}^2 & \cdots & \alpha_{j,b_j}^2 \\ \vdots & \vdots & & \vdots \\ \alpha_{j,1}^{b_i-1} & \alpha_{j,2}^{b_i-1} & \cdots & \alpha_{j,b_j}^{b_i-1} \end{bmatrix} \tag{24}$$

Using the Gaussian elimination method and induction, we get

$$\begin{aligned} \det(B) &= \prod_{i=1}^{\nu} \det(\lambda_i D_{i,i}) \\ &= \prod_{i=1}^{\nu} \lambda_i^{b_i} \det(D_{i,i}) \end{aligned} \tag{25}$$

where

$$\lambda_1 := 1 \quad \text{and} \quad \lambda_i := \prod_{\mu=1}^{i-1}(\beta_i-\beta_\mu),$$

$$i = 2, 3, \cdots, \nu.$$

Lemma 8 Assume that $n \leq m \leq n+2g-2$ and write $m^{\perp}=aq+b$ where $0 \leq a \leq s-2$ and $0 \leq b \leq q-1$. Then any $a+1$ columns of the generator matrix H for $C_{m^{\perp}}$ described as above are linearly independent over K.

Proof: Construct a generator matrix H for $C_{m^{\perp}}$ as described before and consider any $a+1$ distinct columns of H. Rearrange these columns according to β of $P_{\alpha,\beta}$ and construct matrices A and B, etc., as described above. It suffices to show that the columns of A are linearly independent over K. Since β_i's are pairwise distinct for i with $1 \leq i \leq \nu$, we have $\lambda_i \neq 0$ for any i with $1 \leq i \leq \nu$. Since $\alpha_{i,\mu}$'s are pairwise distinct for μ with $1 \leq \mu \leq b_i$ and a given i, we get $\det(D_{i,i}) \neq 0$(Note that $D_{i,i}$ is a Vandermonde matrix of order b_i.) Thus $\det(B) \neq 0$ by Equation (25). This means that $a+1=\text{rank}\,(B) \leq \text{rank}(A) \leq a+1=$the number of columns in A, and therefore we have rank $(A)=a+1$. Hence the columns of A are linearly independent over K. □

Note that if $n \le m \le n+2g-2$ then any m can be uniquely expressed as

$m=n-s+aq+b$ with $0 \le a \le s-2$ and $0 \le b \le q-1$.

Using this expression, the minimum distance of C_m in the abundant case is determined in the following theorem.

Theorem 9 Assume that $n \le m \le n+2g-2$ and write $m=n-s+aq+b$ where $0 \le a \le s-2$ and $0 \le b \le q-1$. Then we have $d(C_m)=s-a$.

Proof: Let $V:=\{\alpha \in U \mid \alpha^q \neq 1\}$ and let $z_1 := \prod_{\alpha \in V}(x-\alpha)$. Choose α_i's and β_j's such that $\alpha_i^s=\beta_j^q+\beta_j=1$ for any i and j with $1 \le i \le s$ and $1 \le j \le q$. Let $z_2 := \prod_{i=1}^{a}(y-\beta_i)$ and let $z_3 := \prod_{i=2}^{q}(x-\alpha_i)$. Then $h:=z_1z_2 \in L((n-s)Q_\infty)$ has $n-s$ distinct zeros in supp(D) and $f:=z_1z_2z_3 \in L((n-s+aq)Q_\infty)$ has $n-s+a$ distinct zeros in supp(D). Thus $d(C_m) \le n-(n-s+a)=s-a$.

Let $m^\perp := n+2g-2-m=(s-2-a)q+(q-1-b)$ and let H be the generator matrix for $C_{m^\perp}$ described before. Since any $s-a-1$ columns of H are linearly independent over K by Lemma 8, the minimum distance of the dual code of $C_{m^\perp}$ is at least $s-a$. Note that C_m and the dual code of $C_{m^\perp}$ have the same weight distribution. Thus we have $d(C_m) \ge s-a$. □

Ⅳ. Conclusion

An interesting family of geometric Goppa codes are studied here, which arise from some subfields of the Hermitian function field over GF(q^2) defined by $y^s+y=x^r$ where s divides $q+1$. These codes have the large length $n=q(1+(q-1)s)$ compared with their fixed alphabet size q^2, so they may be more attractive than the conventional Reed-Solomon codes. Their dimension and and minimum distance are explicitly are given in the abundant case: $m>n$ where m is the parameter that governs both dimension and minimum distance of the code.

References

1. C. Chevalley, *Introduction to the Theory of Algebraic Functions of one Variable*, Math. Surveys 6 (AMS, Providence, RI), 1951.
2. A. Garcia and H. Stichtenoth, "Elementary Abelian p-extensions of algebraic function fields," *Manuscripta Math.*, vol. 72, pp.67-79, 1991.
3. A. Garcia and P. Viana, "Weierstrass points on certain non-classical curves," *Arch. Math.* vol. 46, pp.315-322, 1986.
4. J. H. van Lint and van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, DMV Seminar, Band 12, Birkhauser, 1988.
5. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, Amsterdam: North-Holland, 1977.
6. C. J. Moreno, *Algebraic Curves over Finite Fields*, Cambridge University Press, 1991.
7. R. Pellikaan, "On the gonality of curves, abundant codes and decoding," H. Stichtenoth and M. A. Tsfasman (Eds.), *Lecture Notes in Mathematices, vol. 1518, Coding Theory and Algebraic Geometry*, Springer-Verlag, pp.132-144, 1992.
8. H. Stichtenoth, "A note on Hermitian codes over $GF(q^2)$," *IEEE Trans. Inform. Theory*, vol. IT-34, pp.1345-1348, Sept. 1988.
9. H. Stichtenoth, "Self-dual Goppa codes," *J. Pure and Appl. Math.*, vol. 55, pp.199-211, 1988.
10. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Springer-Verlag, 1993.
11. K. Yang and P. V. Kumar, "On the true minimum distance of Hermitian codes," H. Stichtenoth and M. A. Tsfasman (Eds.), *Lecture Notes in Mathematics, vol. 1518, Coding Theory and Algebraic Geometry*, Springer-Verlag, pp.99-107, 1992.
12. K. Yang, P. V. Kumar, and H. Stichtenoth, "On the weight hierarchy of geometric Goppa codes," *IEEE Trans. Inform. Theory*, vol. 40, pp.913-920,

May. 1994.
13. K. Yang, "Algebraic geometric codes and subfields of the Hermitian function field," *Journal of KICS*, vol. 19, no. 3, pp.418-424, March. 1994.

梁 景 喆 (Kyeong Cheol Yang) 정회원

1986년 2월 : 서울대학교 전자공학과 졸업(공학사)
1988년 2월 : 서울대학교 대학원 전자공학과 졸업(공학석사)
1992년 12월 : University of Southern California, 전기공학과 졸업(Ph.D)
1990년 6월~9월 : 미국 Bellcore 연구원
1993년 3월~현재 : 한양대학교 전자통신공학과 교수