論文 94-19-3-3

Algebraic Geometric Codes and Subfields of Hermitian Function Field

Kyeong Cheol Yang* *Regular Member*

대수기하부호와 Hermitian 함수체의 부분체

正會員 梁 景 喆*

ABSTRACT

Lke the Hermitian function field over $GF(q^2)$, those subfields defined by $y^q+y=x^s$ where s divides $q+1$ are also maximal, having the maximum number of places of degree one permissible by the Hasse-Weil bound. Geometric Goppa codes(or algebraic geometric codes) arising from these subfields of the Hermitian function field are studied in this paper. Their dimension and minimum distance are explicilty and completely presented for any m with $m<n$ where n is the length and m is a parameter that governs both dimension and minimum distance of the code.

요 약

GF(q^2) 위의 Hermitian 함수체와 마찬가지로, $q+1$을 나누는 정수 s에 대해 $y^q+y=x^s$로 정의되는 부분체들도 Hasse-Weil 한계식에 의해 허용되는 최대수의 1차 점들을 가지므로 최상이 된다. 본 논문에서는 Hermitian 함수체의 이러한 부분체들로부터 생성되는 기하 Goppa 부호(혹은 대수기하부호)를 연구한다. n을 부호장, m을 이들 부호의 차원과 최소거리를 결정하는 패러미터라 할때, n보다 작은 임의의 m에 대해 차원과 최소거리가 명확하면서도 완전하게 주어진다.

Ⅰ. Introduction

In a series of papers ([5]-[8]), Goppa discovered an amazing connection between the theory of algebraic curves over a finite field $GF(q)$ and the theory of error-correcting block codes' over $GF(q)$. His idea generalizes the well-known construction of Reed-Solomon and classical Goppa codes. Following his idea, Tsfasman, Vladut, and Zink [14] used modular and Shimura curves when q is a perfect square, and showed in a landmark result that there is a sequence of codes which exceed the Gilbert-Varshamov bound for $q\geq 49$. Thereafter, these codes are called geometric Goppa codes or algebraic geometric codes (AGC).

A particularly interesting class of geometric

*漢陽大學校 電子通信工學科
Dept. of Electronic Communication Engineering Han Yang University

論文番號：93139
接受日字：1993年 8月 2日

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. Tiersma [13] studied these codes in more detail and provided a clear description of their dual codes.

Stichtenoth [11] generalized and simplified the results of Tiersma by working with an isomorphic curve having only one point at infinity. Codes of length $n=q^3$ and any dimension k with $0 \le k \le q^3$ over $GF(q^2)$ were considered by him. In particular, the exact minimum distance of these codes in the range that $0 \le m \le q^3-q^2$ or $m \equiv 0(\mathrm{mod}\ q)$ with $m < q^3$(where m is a parameter that governs both dimension and minimum distance of the code) was determined in his paper. The true minimum distance for ranges of the parameter m not covered in [11] was completely determined by Yang and Kumar [15]. The generalized Hamming weights of these codes were also studied by Yang, Kumar, and Stichtenoth [16].

Like the Hermitian function field, those subfields defined by $y^q+y=x^s$ where s divides $q+1$ are also maximal, having the maximum number of places of degree one permissible by the Hasse-Weil bound. Some partial results on minimum distance of codes arising from these subfields were obtained by Garcia, Kim and Lax [12] using consecutive Weierstrass gaps.

In this paper we provide complete results on the dimension and minimum distance of these codes with $m < n$, where n is the length and m is a parameter that governs both dimension and minimum distance of the code

II. Geometric Goppa Codes

Origianlly, Goppa constructed algebraic geometric codes using differentials of a fuction field and the residue map, which are now well-known to be the duals of algebraic geometric codes using functions of a fuction field and the evaluation map. The presentation here will adopt the function/evaluation viewpoint. See [9], [10], [12] for more details.

Let F/K be an algebraic function filed of genus g over a finite constant field K (see [1], [10], [12] for example). Let $\{P_i \mid i=1,2,\cdots,n\}$ 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 $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \phi$ where $\mathrm{supp}(G)$ and $\mathrm{supp}(D)$ denote the supports of G and D respectively. Define the vector space $\mathcal{L}(G)$ as follows :

$$\mathcal{L}(G) := \{f \in F \mid (f) \ge -G \text{ or } f=0\},$$

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 $\mathcal{L}(A)$ over K and the degree of A respectively. Now conssider the K-linear evaluation map φ given by

$$\begin{aligned} \varphi : \mathcal{L}(G) &\to K^n \\ f &\to (f(P_1), f(P_2), \cdots, f(P_n)). \end{aligned} \qquad (1)$$

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

$$C_{\mathcal{L}}(D, G) := \text{Image of } \varphi = \varphi(\mathcal{L}(G)). \qquad (2)$$

Here we assume that $\deg G < n$ for simplicity. The following proposition is well-known [9], [12].

Proposition 1 *$C_{\mathcal{L}}(D, G)$ is an $[n, k, d]$ code with parameters*

$k=\dim G$ *and* $d \ge n-\deg G$.

Furthermore, if $\deg G > 2g-2$, *then* $k=\deg G+1-g$.

III. 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

$$F=K(x, y) \text{ with } y^q+y=x^s \text{ and } s \mid q+1 \qquad (3)$$

(see [3], [4], [11], [12]). If $s=q+1$, then F/K

is called the Hermitian function field over K. If $s \langle q+1$, 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

$$(dx)=(2g-2)Q_\infty \tag{4}$$

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

$$N=q \cdot |U|+1=q(1+(q-1)s)+1. \tag{5}$$

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 :

$$(x-\alpha)=\begin{cases} \displaystyle\sum_{\substack{\beta \in K,\\ \beta^q+\beta=\alpha^s}} P_{\alpha,\beta}-qQ_\infty & \text{if } \alpha \in U, \\ R_\alpha-qQ_\infty & \text{if } \alpha \in K \setminus U \end{cases} \tag{6}$$

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

$$(y-\beta)=\begin{cases} sP_{0,\beta}-sQ_\infty, & \text{if } \beta^q+\beta=0, \\ \displaystyle\sum_{\substack{\alpha \in K,\\ \alpha^s=\beta^q+\beta}} P_{\alpha,\beta}-sQ_\infty & \text{if } \beta^q+\beta \neq 0. \end{cases} \tag{7}$$

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

$$B(m):=\{x^i y^j \mid 0 \leq i,\ 0 \leq j \leq q-1,\ iq+js \leq m\} \tag{8}$$

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

Let $s \cdot t:=q+1$. From here on, we will assume that

$$G:=mQ_\infty \text{ and } D:=\sum_{\alpha \in U} \sum_{\substack{\beta \in K,\\ \beta^q+\beta=\alpha^s}} P_{\alpha,\beta}. \tag{9}$$

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

$$C_m:=C_{\mathcal{L}}(D, mQ_\infty). \tag{10}$$

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

$$(u)=D-nQ_\infty \tag{11}$$

and

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

An integer $l \geq 0$ is called a gap number of Q_∞ if there is no function $f \in F$ such that $f \in \mathcal{L}(lQ_\infty) \setminus \mathcal{L}((l-1)Q_\infty)$. 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 $\mathcal{L}(mQ_\infty)$ given in (8), it is easy to check that

$$S=S_1 \cup S_2 \tag{12}$$

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

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

This gap sequence plays a central role in determining the dimension and minimum distance of the ocd C_m as in the Hermitian case [11], [15].

Remark 2 (a) If $t=1(i.e.,\ s=q+1)$ then F/K is the Hermitian function field and $S=\{aq+b|0\leq a\leq q-2, a+1\leq b\leq q-1\}$. 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 (12). Let

$$I(m):=\{l\leq m|l=iq+js, i\geq 0, 0\leq j\leq q-1\}. \quad (13)$$

Any integer m can be uniquely expressed as follows :

$$m=aq+cs+b \text{ with } a\geq 0, 0\leq c\leq t-2, \text{ and } 0\leq b\leq s-1 \quad (14)$$

or

$$m=aq+(t-1)s+b \text{ with } a\geq 0, \text{ and } 0\leq b\leq s-2. \quad (15)$$

Using this expression and the basis of $\mathfrak{L}(mQ_\infty)$ in (8), it is easy to calculate $|I(m)|$, that is,

$$|I(m)|=\begin{cases}\dfrac{a(a+1)}{2}t+c(a+1)+\min\{a,\ b\}+1 & \text{for } 0\leq m\leq 2g-2,\\ m+1-g & \text{for } m\rangle 2g-2.\end{cases} \quad (16)$$

Proposition 3 *Assume that* $0\leq m\langle n=q((q-1)s+1)$. *Then the dimension of* C_m *is given by*

$$\dim C_m=|I(m)|.$$

Proof. It is obvious because

$$\dim C_m=\dim\mathfrak{L}(mQ_\infty)=|I(m)|$$

for $0\leq m\langle n$. □

Ⅳ. Minimum Distance of the Code C_m

In this section, we will completely determine the ture minimum distance of the code C_m defined in (10) for any $m(\langle n)$. In the case of Hermitian code, Stichtenoth [11] determined the exact minimum distance of C_m for $0\leq m\leq q^3-q^2$. Yang and Kumar [15] determined it for any m with $q^3-q^2\leq m\leq q^3+q^2-q-2$. If $s=1$, then F/K is a rational function field over K, and C_m is therefore MDS(maximum distance separable).

From here on, we focus on the case that $1\langle s\langle q+1$(equivalently, $1\langle t\langle q+1$ since $st=q+1$). Since $n=q(1+(q-1)s)$, we have $q^2\langle n\langle q^3$ in our case. By Goppa's lower bound, we have

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

For any integer $m\geq 0$, let $\tilde{m}$ be the largest pole number of Q_∞ with $\tilde{m}\leq m$. Clearly, $\mathfrak{L}(mQ_\infty)=\mathfrak{L}(\tilde{m}Q_\infty)$. Therefore, we can assume in what follows that m is a pole number of Q_∞ without loss of generality.

Theorem 4 *Assume that* $0\leq m\langle n=q(1+(q-1)s)$ *and that is a pole number of* Q_∞. *If* $n-m$ *is a pole number of* Q_∞ *then*

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

Proof. We divide our region into three cases.

Case (a). $m=n-(s-1)q=q((q-2)s+2)$: Choose $i:=(q-2)s+2$ distinct elements $\alpha_1,\cdots,\alpha_i\in U$. Then the function

$$f:=\prod_{\nu=1}^{i}(x-\alpha_\nu)\in\mathfrak{L}(mQ_\infty)$$

has exactly $iq=m$ distinct zeros in supp(D). This implies that $d(C_m)\leq n-m$, so we are done.

Case (b). $m\langle n-(s-1)q=q((q-2)s+2)$: Since m is a pole number of Q_∞, we write $m=iq+js$ with $i\geq 0$ and $0\leq j\leq q-1$. Thus $i\leq (q-2)s+1=(q-1)s+1-s$. Let $A:=\{\alpha\in K\mid\alpha^s\neq 1\}$. Then $|A|=(q-1)s+1-s\geq i$, and we can choose $\alpha_1,\cdots,\alpha_i\in A$. The element

$$z_1:=\prod_{\nu=1}^{i}(x-\alpha_\nu)$$

has iq distinct zeros in supp(D). Next we choose j distinct elements $\beta_1,\cdots,\beta_j\in K$ such that $\beta^q+\beta=1$ and let

$$z_2:=\prod_{\mu=1}^{j}(y-\beta_\mu).$$

Note that z_2 has js distinct zeros in supp(D). Then $z:=z_1z_2\in\mathfrak{L}(mQ_\infty)$ has exactly m distinct zeros in supp(D).

Case(c). $n-(s-1)q\langle m\langle n$: Wehave $0\langle n-m\langle(s-1)q\langle q((q-2)s+2)$. Since $n-m$ is a pole number of Q_∞ by assumption, there exists an element $z\in\mathfrak{L}((n-m)Q_\infty)$with the divisor $(z)=E-(n-m)Q_\infty$ where $0\leq E\leq D$ and deg$E=n-m$. The element $u:=x^{(q-1)s+1}-x\in F$ has the divisor $(u)=D-nQ_\infty$, hence

$$(u/z)=(D-E)-mQ_\infty.$$

Hence, the codeword corresponding to $u/z\in\mathfrak{L}(mQ_\infty)$ has weight $n-m$. □

Using the gap sequence in (12), it is easy to check that $n-m$ is not a pole number of Q_∞ if and only if

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

or

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

where $ts=q+1$.

In the case that $n-m$ is not a pole number of Q_∞, the minimum distance of C_m is given in the following two theorems.

Theorem 5 *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*

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

Proof. Note that $m\rangle n-aq-cs$ and that both $n-aq-cs$ and $aq+cs$ are pole numbers of Q_∞. By Theorem 4 we have

$$d(C_m)\leq d(C_{n-aq-cs})=aq+cs.$$

In order to prove the equality, it suffices to show that any element $f\in\mathfrak{L}(mQ_\infty)$ has at most $m-b=n-aq-cs$ distinct zeros in supp(D). Suppose there is an element $f\in\mathfrak{L}(mQ_\infty)$ such that f has m' distinct zeros in supp(D) where $n-aq-cs+1\leq m'\leq n-aq-cs+b=m$. Then there exisits an integer m'' with $m'\leq m''$ such that

$$(f)=E+J-m''Q_\infty$$

with $0\leq E\leq D$, $\deg(E)=m'$, $J\geq 0$, supp$(J)\cap$ supp$(D)\subseteq$ supp(E), $Q_\infty\notin$ supp(J), and $j:=\deg(J)=\deg(J)=m''-m'$. Let $u:=x^{(q-1)s+1}-x$. Then

$$\begin{aligned}(u/f)&=D-nQ_\infty-E-J+m''Q_\infty\\&=(D-E)-J-(n-m'')Q_\infty.\end{aligned}$$

Now let $\bar{K}$ be the algebraic closure of $K=GF(q^2)$ and consider the constant field extension $F'=F\bar{K}$ of F/K. Then $F'/\bar{K}$ has the same genus and the same gap sequence at Q_∞. The degree of any divisor in F/K is preserved in $F'/\bar{K}$ (see [12]). Our aim is to show that even in the extension field F', such a function u/f with the divisor as given above does not exist. In $F'/\bar{K}$, all places (except Q_∞) are of degree one and correspond to points (α,β) with coordinates in $\bar{K}$. Given a place of degree one (a point) $P_{\alpha,\beta}$ contained in the support of J, we consider the the function $y-\beta$

having $P_{\alpha,\beta}$ as a zero. Since $(y-\beta)=P_{\alpha,\beta}+I-sQ_\infty$ where $\beta^q+\beta=\alpha^s$, $I\geq 0$ and $Q_\infty\notin \mathrm{supp}(I)$, we get $P_{\alpha,\beta}\sim -I+sQ_\infty$. Replacing each place of degree one in the support of J with an equivalent divisor in this way, we get

$$J\sim -R+jsQ_\infty$$

where $R\geq 0$ and $Q_\infty\notin \mathrm{supp}(R)$. Thus

$$(u/f)\sim D-E+R-(n-m''+js)Q_\infty,$$

where $D-E+R\geq 0$ and $Q_\infty\notin \mathrm{supp}(D-E)\cup \mathrm{supp}(R)$. Let $m'':=n-aq-cs+b''$ and $m':=n-aq-cs+b'$ where $1\leq b'\leq b''\leq b$. Then

$$\begin{aligned}n-m''+js&=aq+cs-b''+js\\&=aq+(c+j-1)s+s-b''.\end{aligned}$$

write $c+j-1:=kt+l$ with $0\leq l\leq t-1$ and $k\geq 0$. Note that $j\geq k$ since $t>1$ and $1\leq c\leq t-1$. Thus

$$\begin{aligned}n-m''+js&=aq+kts+ls+s-b''\\&=(k+a)+ls+(s-b''+k).\end{aligned}$$

Here we have

$$s-b''+k\geq s-(s-1-a)+k=k+a+1>k+a$$

and

$$s-b''+k=s-b'-(j-k)\leq s-b'\leq s-1.$$

In particular, if $l=t-1$, then $j>k$ and

$$k+a<s-b''+k\leq s-b'-1\leq s-2.$$

This implies that $n-m''+js$ is a gap number of Q_∞, and we get a contradiction to our equivalence of (u/f). Hence, there is no function $f\in \mathcal{L}(mQ_\infty)$ such that f has exactly m' distinct zeros in supp(D) with $n-aq-cs+1\leq m'\leq m$. □

Theorem 6 *If* $m=n-ts-aq+b$ *with* $0\leq a\leq s-3$, *and* $2\leq b\leq s-1-a$, *then*

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

Proof. The same arguments in the Proof of Theorem 5 holds except that

$$n-aq-ts+2\leq m'\leq m''\leq m=n-aq-ts+b$$

where $2\leq b\leq s-1-a$ and $0\leq a\leq s-3$. Then

$$\begin{aligned}n-m''+js&=aq+ts-b''+js\\&=aq+(j+t-1)s+(s-b'').\end{aligned}$$

If $j=0$ then $s-2\geq s-b''\geq s-(s-1-a)=a+1>a$, and therefore $n-m''+js$ is a gap number of Q_∞. If $j\geq 1$ then write $j+t-1:=kt+l$ with $0\leq l\leq t-1$ and $k\geq 0$. Then we have

$$n-m''+js=aq+kts+ls+s-b''=(a+k)q+ls+(s-b''+k).$$

Here

$$s-b''+k\geq s-(s-a-1)+k=a+k+1>a+k$$

and

$$s-b''+k=s-b'-(j-k)\leq s-b'\leq s-2$$

since $j\geq k$. This implies that $n-m''+js$ is a gap number of Q_∞. Hence, we have a contradiction. □

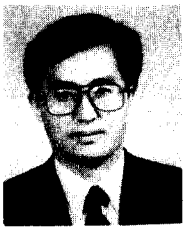
V. Conclusion

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 $y^q+y=x^s$ where s divides $q+1$. These codes have large length $n=q((q-1)s+1)$ compared with their alphabet size q^2, so they may be more attractive than the conventional Reed-Solomon codes. Their dimension and minimum distance are explicitly and completely given for any $m<n$ where m is a 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, S. J. Kim, and R. F. Lax, "Consecutive Weistrass gaps and minimum distance of Goppa codes," To appear in *J. Pure and Applied Algebra*.
3. A. Garcia and H. Stichtenoth, "Elementary Abelian p-extensions of algebraic function fields," *manuscripta math*, vol. 72, pp. 67-79, 1991.
4. A. Garcia and P. Viana, "Weierstrass points on certain non-classical curves," Arch. Math. vol. 46, pp. 315-322, 1986.
5. V. D. Goppa, "Codes associated with divisors," *Probl. Inform. Transmission*, vol. 13, pp. 22-27, 1977.
6. V. D. Goppa, "Codes on algebraic curves," *Soviet Math. Dokl.*, vol. 24, no. 1, pp. 170-172, 1981.
7. V. D. Goppa, "Algebraico-geometric codes," *Math. USSR Izvestiya*, vol. 21, no. 1, pp. 75-91, 1983.
8. V. D. Goppa, "Codes and information," *Russian Math. Surveys*, 39 : 1, pp. 87-141, 1984.
9. J. H. van Lint and van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, DMV Seminar, Band 12, Birkhauser, 1988.
10. C. J. Moreno, *Algebraic Curves over Finite Fields*, Cambridge University Press, 1991.
11. H. Stichtenoth, "A note on Hermitian codes over $GF(q^2)$," *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 1345-1348, Sept. 1988.
12. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Springer-Verlag, 1993.
13. H. J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 605-609, July 1987.
14. M. A. Tsfasman, S. G. Vladut, and Th. Zink, "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound," *Math. Nachr.*, vol. 109, pp. 21-28, 1982.
15. K. Yang and P. V. Kumar, "On the true minimum distance of Hermitian codes," H. Stichtenoth and M. A. Tsfasman (Eds.), *Lotes in Mathematices. vol. 1518, Coding Theory and Algebraic Geometry*, Springer-Verlag, pp. 99-107, 1992.
16. K. Yang, P. V. Kumar, and H. Stichtenoth, "On the weight hierarchy of geometric Goppa codes," to appear in the *IEEE Trans. Inform. Theory*, *May* 1994.



梁 景 喆(Kyeong Cheol Yang) 정회원
1986년 2월 : 서울대학교 전자공학과(공학사)
1988년 2월 : 서울대학교 전자공학과(공학석사)
1992년 12월 : University of Southern California, 전기공학과(Ph.D)
1990년 6월 ~ 9월 : 미국 Bellcore 연구원
1993년 3월 ~ 현재 : 한양대학교 전자통신공학과 교수
※주관심분야 : 부호이론, 암호학, 통신이론