논문 00-25-2A-11 한국통신학회논문지 '00-2 Vol.25 No.2A

최소거리가 5 또는 7인 새로운 이진 순회부호

정회원 노 종 선*, 김 영 제**

New Binary Cyclic Codes with Minimum Distance 5 or 7

Jong-Seon No*, Young-Je Kim** *Regular Members*

요 약

순회부호는 선형부호 중에서 가장 중요한 부호이지만 그의 체계적인 생성방법이 알려진 이진부호로는 Hamming 부호, BCH 부호, Golay 부호, quadratic residue 부호, simplex 부호 등 그리 많지 않은 편이다. 본 논문에서는 부호길이가 2^n-1이며 최소거리가 5 또는 7인 새로운 이진 순회부호를 컴퓨터 search를 통하여 발견하고 이들의 새로운 순회부호를 conjecture들로서 제안하였다.

ABSTRACT

It is well-known that cyclic code is an important subclass of linear codes, but a few cyclic codes such as Hamming codes, BCH codes, Golay codes, quadratic residue codes and simplex codes are already found. In this paper, we find some new binary cyclic codes with minimum distance 5 or 7 of length 2^n-1 by computer search, and formulate these new cyclic codes as conjectures.

Ⅰ. 서 론

선형부호 C에 있는 모든 부호어(codeword)를 cyclic shift한 부호어도 부호 C에 있는 부호어 일 때 이를 순회부호(cyclic code)라 한다. 순회부호는 모든 선형부호 중에서 가장 중요하게 연구되어지고 있는 부호로서 부호기의 구현 및 신드롬 계산기의 구현이 용이하고 구현 가능한 복호 알고리즘의 개발이 용이하며 연집오류에 강한 특징을 갖고 있는 매우 중요한 부호이다.

유한필드(finite field) F_2의 원시원(primitive element)을 α라하고, 필드 F_2상에서 α^i의 최소다항식(minimal polynomial)을 $m_i(x)$라 하자. 그리고 부호길이 $N=2^n-1$인 $[N, N-a\times n]$ 이진 순회부호 C의 생성다항식(generator polynomial)을 다음의 식과 같이 정의하자.

$$g(x)=m_{i_1}(x)m_{i_2}(x)\cdots m_{i_a}(x), \quad 1\le i_1<i_2<\cdots<i_a\le 2^n-2 \tag{1}$$

여기서 $i_1, i_2, \cdots, i_a$들은 어떠한 것들도 modulo 2^n-1로 계산되는 동일한 cyclotomic coset에 속하지 않는다고 가정하자. 그리고 위와 같은 순회부호의 생성다항식을 그를 구성하는 a개의 최소다항식들의 순서쌍 $(i_1, i_2, \cdots, i_a)$으로 표현하자.

일반적으로 부호에 있어서 최소거리는 가장 중요한 성질 중의 하나이다. 그러나 $[N, N-a\times n]$ 순회부호에서 a가 2 또는 3과 같이 작은 값을 갖는 경우는 부호어의 개수가 매우 많아서 이러한 부호의 최소거리를 구한다는 것은 매우 어려운 일이다. 이러한 경우 이 부호의 쌍대부호(dual code)인 $[N, a\times n]$ 이진 순회부호의 weight 분포를 구하는 것은 비교적 쉽기 때문에 이 부호의 weight 분포를

* 서울대학교 전기공학부 (jsno@snu.ac.kr)
** (주) NSI Technology (youngjoy@nsit.co.kr)
논문번호 : 98296-0715, 접수일자 : 1998년 7월 15일
※ 본 연구는 정보통신연구관리단(과제번호: 96003-RT-I1)의 연구비지원에 의한 연구결과임.

먼저 구하고 MacWilliams identity를 이용하면 원래 구하고자 하는 이진 순회부호의 weight 분포 및 최소거리를 구할 수 있다. MacWilliams identity는 다음과 같이 주어진다.[1]

$$W_{C^\perp}(x,y)=\frac{1}{|C|}W_C(x+y,x-y) \tag{2}$$

여기서 $|C|$는 부호어의 개수이고 $W_C(x,y)$와 $W_{C^\perp}(x,y)$를 weight enumerator라 하며 다음 식으로 주어진다.

$$W_C(x,y)=\sum_{i=0}^{N}A_i x^{N-i}y^i \tag{3}$$

$$W_{C^\perp}(x,y)=\sum_{i=0}^{N}A_i' x^{N-i}y^i \tag{4}$$

위 식에서 A_i, A_i'는 부호 C와 그의 쌍대부호 $C^\perp$의 Hamming weight가 i 인 부호어의 개수이고 이 식을 이용하면 식(2)는 아래의 식과 같이 전개된다.

$$\sum_{k=0}^{N}A_k' x^{N-k}y^k=\frac{1}{|C|}\sum_{i=0}^{N}A_i(x+y)^{N-i}(x-y)^i \tag{5}$$

여기서 A_i와 A_i'의 관계를 구하기 위해 위 식의 우변에 있는 항을 다음과 같은 식으로 표현하자.

$$(x+y)^{N-i}(x-y)^i=\sum_{k=0}^{N}P_k(i)x^{N-k}y^k \tag{6}$$

여기서 $P_k(i)$는 Krawtchouk 다항식으로 다음과 같이 정의된다.

$$P_k(i)=\sum_{j=0}^{k}(-1)^j\binom{i}{j}\binom{N-i}{k-j},\quad k=0,1,2,\cdots \tag{7}$$

위의 식들을 이용하면 A_i와 A_i'의 관계는 아래의 식으로 주어진다.

$$A_k'=\frac{1}{|C|}\sum_{i=0}^{N}A_iP_k(i) \tag{8}$$

위의 관계식을 이용하면 쌍대부호의 weight 분포로부터 원하는 부호의 weight 분포를 구할 수 있다. 순회부호는 선형부호 중에서 가장 중요한 부호이지만 그의 체계적인 생성방법이 알려진 이진순회부호로는 Hamming 부호, BCH 부호, Golay 부호, quadratic residue 부호, simplex 부호 등 그리 많지 않은 편이다. 최근 들어서 최소거리가 5인 새로운 이진 순회부호가 발견되었다.[1][7][8][9] 이러한 순회부호들은 그의 쌍대부호인 Gold 부호 및 Gold-like 부호를 이용하여 생성할 수 있었다.

본 논문에서는 최소거리가 7인 새로운 이진 순회부호를 컴퓨터 search를 통하여 발견하였다. II장에서는 최근에 발견된 최소거리가 5인 이진 순회부호에 대하여 설명하였고 또한 최소거리가 5인 새로 발견된 이진 순회부호를 기술하였다. III장에서는 부호길이가 2^n-1인 $[2^n-1,\ 3n]$ 이진 순회부호를 컴퓨터 search를 통하여 발견하고 MacWilliams identity를 이용하여 쌍대부호의 weight 분포를 구하고 최소거리가 7인 새로운 $[2^n-1,2^n-1-3n]$ 이진 순회부호를 conjecture로 제안하였다.

II. 최소거리가 5인 이진 순회부호

서로 다른 두 시퀀스 x_m과 y_m의 상호상관(crosscorrelation) 함수는 다음의 식으로 정의된다.[2]

$$\theta_{x,y}(\tau)=\sum_{m=0}^{N-1}x_m\,y_{m+\tau} \tag{9}$$

Gold 부호는 주기 2^n-1의 두 시퀀스 x_m과 y_m으로 구성되며 3개의 상호상관값을 갖는다. 여기서, x_m을 주기 $N=2^n-1$의 m-시퀀스라 할 때, y_m은 $\gcd(2^n-1,q)=1$인 q로 decimation한 m-시퀀스이다. 양의 정수 k에 대하여 아래의 식은 Gold 부호를 만족하는 q값이다.[2][3] 그리고 Gold 부호의 특성다항식(characteristic polynomial)은 $m_1(x)\,m_q(x)$가 된다.

$$\begin{aligned}&q=2^k+1 \text{ 또는 } q=2^{2k}-2^k+1,\\ &\text{여기서 } \gcd(n,k)=\begin{cases}1, & n \text{ odd}\\ 2, & n=2 \bmod 4\end{cases}\end{aligned} \tag{10}$$

Gold-like 부호는 n이 짝수일 때, 두 시퀀스 중에서 y_m의 주기가 $N/3$인 시퀀스로서 $\gcd(2^n-1,q)=3$인 q로 decimation 한 시퀀스이다.[3]

Gold 부호는 3개의 상호상관값을 갖으며 k가 양의 정수이고 $e=\gcd(n,k)$ 일 때 n/e가 홀수이면, 상호상관 함수 $\theta_{x,y}(\tau)$는 다음 식의 발생분포를 갖는다.[5]

$$\theta_{x,y}(\tau)=\begin{cases}-1+2^{(n+e)/2}\,;\,2^{n-e-1}+2^{(n-e-2)/2} \text{ 발생}\\ -1\qquad\qquad\;;\,2^n-2^{n-e}-1 \text{ 발생}\\ -1-2^{(n+e)/2}\,;\,2^{n-e-1}-2^{(n-e-2)/2} \text{ 발생}\end{cases} \tag{11}$$

이진 순회부호 $[2^n-1, 2^n-1-2n]$의 생성다항식은 다음 식으로 정의된다.

$$g(x)=m_{i_1}(x)m_{i_2}(x) \tag{12}$$

위의 생성다항식 $g(x)$를 (i_1, i_2)로 표현하자. 이에 의해 생성되는 최소거리가 5인 순회부호는 많은 사람들에 의해 연구되었다. 아래의 식 (13), (14), 및 conjecture 1, 2와 3의 생성다항식들은 부호길이가 $N=2^n-1$이고 최소거리가 5인 이진 순회부호의 생성다항식들이다.[1][4][7][8][9]

$$(1, 2^k+1) \text{ 또는 } (1, 2^{2k}-2^k+1), \quad \text{여기서 } \gcd(n, k)=1 \tag{13}$$

만일 $k=1$이면 최소거리가 5인 BCH 부호이다.[1]

위 식은 식(10)과 비교하여 볼 때, n이 홀수인 경우 Gold 부호의 쌍대부호는 최소거리가 5인 순회부호임을 알 수 있다. 그러나 $n=2 \bmod 4$인 경우에는 3개의 상호상관값을 가지나 그의 쌍대부호는 최소거리가 5 미만인 부호들이다. 즉, n이 짝수인 경우에 최소거리가 5인 순회부호는 주기 $N/3$인 시퀀스로 구성되는 Gold-like 부호와 쌍대부호의 관계이다. 그리고 다음의 생성다항식을 갖는 부호길이가 2^n-1인 순회부호는 최소거리가 5인 순회부호이나 그의 쌍대부호는 Hamming weight의 종류가 세 개 이상인 순회부호이다.

$$(1, 2^{n-1}-1), \quad \text{여기서 } n=2k+1 \tag{14}$$

Conjecture 1

부호길이가 $N=2^n-1$이고 k는 양의 정수이며 $n=2k+1$일 때, 생성다항식이 $(1, 2^k+3)$인 선형부호는 최소거리가 5인 $[N, N-2n]$ 순회부호이다. ■

위 conjecture의 쌍대부호는 Welch[5]에 의해 세 개의 weight를 갖는 부호라고 알려져 있으며 위 conjecture에 의해 주어진 순회부호는 컴퓨터 시뮬레이션을 통해 $n\leq 15$에 대해 최소거리가 5인 순회부호임을 확인하였다.

Conjecture 2

부호길이 $N=2^n-1$이고 k는 양의 정수이며 $n=2k+1$일 때, 다음의 q를 만족하는 생성다항식이 $(1, q)$인 순회부호는 최소거리가 5인 $[N, N-2n]$ 순회부호이다.

$q = 2^k+2^{k/2}-1$, k가 짝수일 때

$q = 2^{k+(k+1)/2}-2^{(k+1)/2}+1$, k가 홀수일 때 ■

위의 conjecture의 쌍대부호는 Niho[5]가 발견한 세 개의 상호상관값을 갖는 시퀀스이며 Niho의 conjecture를 coset leader의 q값을 갖도록 변형시켰다. 위 conjecture에 의해 주어진 순회부호는 컴퓨터 시뮬레이션을 통해 $n\leq 17$에 대해 최소거리가 5인 순회부호임을 확인하였다.

Conjecture 3

부호길이가 $N=2^n-1$이고 k는 양의 정수이며 $n=5k$일때, 생성다항식이 $(1, 2^{4k}-2^{3k}+2^{2k}-2^k+1)$인 선형부호는 최소거리가 5인 $[N, N-2n]$ 순회부호이다. ■

위 conjecture는 본 논문을 통해 새롭게 발견된 것으로 컴퓨터 시뮬레이션을 통해 $n\leq 15$에 대해서 최소거리가 5인 순회부호임을 확인하였고 이를 만족하는 순회부호의 생성다항식은 아래와 같다. 이의 쌍대부호는 Hamming weight의 종류가 세 개 이상인 부호이다. 지금까지 알려진 최소거리가 5인 이진 순회부호가 Gold와 Gold-like부호를 이용하여 생성된 반면 이 부호의 쌍대부호는 다른 형태의 weight 분포를 갖는 부호이다.

$N=31$ 일 때, $(1, 15)$
$N=1023$ 일 때, $(1, 213)$
$N=32767$ 일 때, $(1, 3657)$

Ⅲ. 최소거리가 7인 이진 순회부호

순회부호에서 부호어의 개수가 매우 많은 경우에는 부호의 최소거리를 구한다는 것은 매우 어려운 일이다. 이러한 경우 이 부호의 쌍대부호인 $[2^n-1, 3\times n]$ 이진 순회부호의 weight 분포를 구하고 MacWilliams identity를 이용하면 원래 구하고자 하는 이진 순회부호의 weight 분포 및 최소거리를 구할 수 있다.

$[2^n-1, 2^n-1-3n]$ 이진 순회부호의 생성다항식을 다음 식과 같이 정의하자.

$$g(x)=m_{i_1}(x)m_{i_2}(x)m_{i_3}(x) \tag{15}$$

여기서 위의 생성다항식을 다음의 순서쌍

(i_1, i_2, i_3)으로 표현하자.

본 장에서는 $[2^n-1, 3\times n]$ 이진 순회부호를 컴퓨터 search를 통하여 모두 구하고 MacWilliams identity를 이용하여 그의 쌍대부호인 새로운 $[2^n-1, 2^n-1-3n]$ 이진 순회부호의 weight 분포 및 최소거리를 구하였다. 위의 부호 중에서 최소거리가 7인 $[2^n-1, 2^n-1-3n]$ 이진 순회부호들을 구하고 이 부호들을 다음의 conjecture들로 제시하였다.

이미 잘 알려진 것과 같이 모든 정수 n에 대해 부호길이가 $N=2^n-1$ 일 때, $(i_1, i_2, i_3)=(1,3,5)$를 생성다항식으로 갖는 $[N, N-3n]$ 순회부호는 최소거리가 7인 BCH 부호이다.

Conjecture 4

부호길이 $N=2^n-1$ 이고 k는 양의 정수이며 $n=2k+1$일 때, (1, 3, 11)과 (1, 3, 13)을 생성다항식으로 갖는 $[N, N-3n]$ 이진 순회부호는 최소거리가 7이다. ■

이의 쌍대부호의 weight 분포는 다음 표 1과 같으며 이는 또한 n이 홀수일 때 최소거리가 7인 BCH 부호의 쌍대부호의 weight 분포와 동일하다.[6]

Conjecture 5

부호길이가 $N=2^n-1$ 이고 k는 양의 정수이며 $n=2k$일 때, (1, $2^{k-2}+1$, $2^{k-1}+1$)을 생성다항식으로 갖는 $[N, N-3n]$ 이진 순회부호는 최소거리가 7이다. ■

표 1. $[N,3n]$ 부호의 Weight 분포(n:홀수)

weight, i	weight i를 갖는 부호어의 개수
0	1
$2^{n-1}-2^{(n+1)/2}$	$2^{(n-5)/2}[2^{(n-3)/2}+1](2^{n-1}-1)(2^n-1)/3$
$2^{n-1}-2^{(n-1)/2}$	$2^{(n-3)/2}[2^{(n-1)/2}+1](5\cdot 2^{n-1}+4)(2^n-1)/3$
2^{n-1}	$(9\cdot 2^{2n-4}+3\cdot 2^{n-3}+1)(2^n-1)$
$2^{n-1}+2^{(n-1)/2}$	$2^{(n-3)/2}[2^{(n-1)/2}+1](5\cdot 2^{n-1}+4)(2^n-1)/3$
$2^{n-1}+2^{(n+1)/2}$	$2^{(n-5)/2}[2^{(n-3)/2}-1](2^{n-1}-1)(2^n-1)/3$

위 conjecture를 만족하는 순회부호의 생성다항식은 아래와 같이 주어지며 그의 쌍대부호의 weight 분포는 표 2와 같다.

$N=63$ 일 때, (1, 3, 5)
$N=255$ 일 때, (1, 5, 9)
$N=1023$ 일 때, (1, 9, 17)

표 2. $[N, 3n]$ 부호의 Weight 분포(n:짝수)

weight, i	weight i를 갖는 부호어의 개수
0	1
$2^{n-1}-2^{(n+4)/2-1}$	$[2^{n-1}+2^{(n+4)/2-1}](2^n-4)(2^n-1)/960$
$2^{n-1}-2^{(n+2)/2-1}$	$7[2^{n-1}+2^{(n+2)/2-1}]2^n(2^n-1)/48$
$2^{n-1}-2^{n/2-1}$	$2(2^{n-1}+2^{n/2-1})(3\cdot 2^n+8)(2^n-1)/15$
2^{n-1}	$(29\cdot 2^{2n}-4\cdot 2^n+64)(2^n-1)/64$
$2^{n-1}+2^{n/2-1}$	$2(2^{n-1}-2^{n/2-1})(3\cdot 2^n+8)(2^n-1)/15$
$2^{n-1}+2^{(n+2)/2-1}$	$7[2^{n-1}-2^{(n+2)/2-1}]2^n(2^n-1)/48$
$2^{n-1}+2^{(n+4)/2-1}$	$[2^{n-1}-2^{(n+4)/2-1}](2^n-4)(2^n-1)/960$

위 표는 n이 짝수일 때 앞서 언급한 최소거리가 7인 BCH 부호의 쌍대부호의 weight 분포[6]와 동일하다.

Conjecture 6

부호길이가 $N=2^n-1$ 이고 k는 양의 정수이며 $n=2k+1$ 일 때, (1, $2^{k_1}+1$, $2^{k_2}+1$)을 생성다항식으로 갖는 $[N, N-3n]$ 이진 순회부호는 최소거리가 7이다. 여기서 $1\le k_1<k_2\le k$이다.

■

위의 conjecture를 만족하는 순회부호의 생성다항식은 아래와 같고 쌍대부호의 weight 분포는 앞의 표 1과 같다. 특별히 $k_1=k-1$ 이고 $k_2=k$ 일 경우는 Roos Bound에 의해 최소거리가 7임이 증명되었다.[11]

$N=127$ 일 때, (1, 3, 5),(1, 3, 9),(1, 5, 9)
$N=511$ 일 때, (1, 3, 5), (1, 3, 9), (1, 3, 17), (1, 5, 9), (1, 5, 17), (1, 9, 17)
$N=2047$ 일 때, (1, 3, 5), (1, 3, 9), (1, 3, 17), (1, 3, 33), (1, 5, 9), (1, 5, 17), (1, 5, 33), (1, 9, 17), (1, 9, 33), (1, 17, 33)

Theorem 7

부호길이가 $N=2^n-1$ 이고 k는 양의 정수이며 $n=2k+1$ 일 때, $(1, 2^k+1, 2^k+2^{k-1}+1)$을 생성다항식으로 갖는 $[N, N-3n]$ 이진 순회부호는 최소거리가 7 이상이다. ■

위의 부호는 최근 Anjung Chang에 의해 최소거리가 7이상인 순회부호임이 증명되었고 이 부호의 쌍대부호로서 아래와 같이 정의되는 외사불규칙시퀀

스(pseudorandom sequence)는 이상적인 자기상관특성(ideal autocorrelation)을 갖는 3-trace 시퀀스로 알려져 있다.[10]

$$s(t)=tr_1^n\{a^t\}+tr_1^n\{a^{(2^{\frac{n}{2}}+1)t}\}+tr_1^n\{a^{(2^{\frac{n}{2}}+2^{\frac{n}{4}}+1)t}\} \quad (16)$$

Miscellaneous Pairs

다음은 앞에서 제시한 conjecture 4, 5, 6과 theorem 7에 포함되지 않는 최소거리가 7인 순회부호의 생성다항식들이다. 이들은 $n\leq 10$에 대하여 컴퓨터 search를 통해 full-search한 결과이며, $n=11$에 대해서는 표 1의 weight 분포를 갖는 경우이다. 그리고 1)과 2)의 경우는 표 1과 표 2의 weight 분포와 다른 weight 분포를 갖는 특이한 경우이다.

1) $N=2^6-1$ 일 때, (1, 3, 31)
2) $N=2^7-1$ 일 때, (1, 3, 63)
3) $N=2^9-1$ 일 때, (1, 3, 43), (1, 13, 109)
4) $N=2^{11}-1$ 일 때, (1, 11, 171), (1, 43, 171), (1, 57, 235), (1, 95, 221)

Ⅳ. 결 론

$[N, N-2n]$ 이진순회부호에서 $n\leq 15$에 대해 full-search 하였으며 최소거리가 5인 부호는 본 논문에 기술한 부호 외에는 없다. 최소거리가 5인 이진 순회부호에서 쌍대부호가 Gold 부호와 다른 weight 분포를 갖는 식(14)와 conjecture 3)외의 부호들의 쌍대부호는 모두 Sidelnikov 하한식 근처에서 최적의 상관특성을 갖으며 n이 홀수인 경우 세 개의 상호상관값을 갖고 n이 짝수인 경우에 다섯 개의 상호상관값을 갖는다.

그리고 부호길이가 $N=2^n-1$이며 최소거리가 7인 새로운 $[N, N-3n]$ 이진 순회부호를 컴퓨터 search를 통하여 발견하고 이들의 새로운 순회부호를 conjecture들로서 제안하였다. 또한 이들의 쌍대부호인 $[N, 3n]$ 이진 순회부호의 weight 분포가 표 1과 표 2에 주어진 분포를 갖는다는 것을 발견하였다. 그러나 최소거리가 7인 순회부호 중에서 $N=63$일 때 생성다항식 (1, 3, 31)과 $N=127$일 때 생성다항식 (1, 3, 63)인 경우는 최소거리가 7임에도 불구하고 표 1과 표 2의 weight 분포를 갖지 않는다는 것을 발견하였다. 앞으로 연구할 내용은 본 논문에서 주어진 conjecture들을 증명하는 것이 될 것이다.

참 고 문 헌

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, New York, 1986.

[2] D. V. Sarwarte and M. B. Pursley, "Cross-correlation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp.593-620, May 1980.

[3] R. E. Ziemer and R. L. Perterson, *Digital Communications and Spread Spectrum Systems*, Macmillan, New York, 1985.

[4] P. Charpin, A. Tietäväinen and V. Zinoviev, "On The Minimum Distance of Certain Cyclic Codes," *IEEE ISIT* 1997, p. 505, Ulm, Germany, June 29- July 4, 1997.

[5] Y. Niho, "Multi-valued Cross-correlation Functions between Two Maximal linear Recursive Sequences," Ph.D. dissertion, Dept. Elec. Eng., Univ. Southern California (also USC EE Rep. 409), 1972.

[6] S. Lin and D. J. Costello, Jr., *Error Control Coding, Prentice-Hall*, New Jersey, 1983.

[7] H. Janwa and R. M. Wilson, "Hyperplane Sections of Fermat Varieties in p^3 in Chap. 2 and Some Applications to Cyclic Codes," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings AAECC-10, Lecture Notes in Computer Science*, vol. 673, Springer-Verlag, New York-Berlin, pp. 180-194, 1993.

[8] T. Kasami, "The weight enumerators for several classes of subcodes of 2nd order binary Reed-Muller codes," *Info. and Control* 18 (1971), pp. 369-394.

[9] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Transactions in Information Theory*, vol. 32, pp. 23-40, January 1986.

[10] 노종선, 이환근, "이상적인 자기상관특성을 갖는 주기가 2^n-1인 새로운 이진 의사불규칙 시퀀스," 한국통신학회논문지, 1996년 12월호.

[11] Cornelis Roos, "A New Lower Bound for the Minimum Distance of a Cyclic Code," *IEEE*

Transactions in Information Theory, vol. IT-29, pp. 330-332, May 1983.

노 종 선(Jong-Seon No) 종신회원

1981년 2월 : 서울대학교 전자공학과 졸업(공학사)
1984년 2월 : 서울대학교 대학원 전자공학과 졸업 (공학석사)
1988년 5월 : University of Southern California, Dept. of EE. (공학박사)
1988년 2월~1990년 7월 : Hughes Network Systems, Senior MTS
1990년 9월~1999년 7월 : 건국대학교 전자공학과 부교수
1999년 8월~현재 : 서울대학교 전기공학부 조교수
<주관심 분야> 오류정정부호, PN 시퀀스, 암호학, 이동통신

김 영 제(Young-Je Kim) 정회원

1997년 2월 : 건국대학교 전자공학과 졸업(공학사)
1999년 2월 : 건국대학교 대학원 전자공학과 졸업(공학석사)
1999년 3월~현재 : NSI Technology 연구소 근무
<주관심 분야> 오류정정부호, 이동통신