Z_4상에서 정의된 Delsarte-Goethals 부호의 완전 무게 분포

정회원 신 동 준*

Complete Weight Enumerator of the Delsarte-Goethals Code over Z_4

Dong-Joon Shin* *Regular Member*

요 약

이 논문에서 Z_4 상에서 정의된 Delsarte-Goethals 부호의 완전 무게 분포를 구하였다. 이 부호의 부호어를 3가지 경우로 나눠서 각각의 완전 무게 분포를 구하였으며, 이때 이미 알려진 이 부호의 부분 부호의 지수합 분포 및 이진 무게 분포를 이용하였다. 이 결과와 MacWilliams 항등식을 이용하여 Z_4 상에서 정의된 Goethals 부호의 완전 무게 분포를 쉽게 구할 수 있다. 또한 이 결과는 Goethals 부호와 Delsarte-Goethals 부호에서 3-design을 찾는데 이용되었다.

Key Words : complete weight enumerator; Delsarte-Goethals code over Z_4.

ABSTRACT

In this paper, the complete weight enumerator of the Delsarte-Goethals code over Z_4 is obtained. This code is divided into 3 cases and the complete weight enumerator of each case is calculated. During this weight enumeration, the known distribution of exponential sums and binary weight distribution of the sub-codes are used. By combining this result and MacWilliams identity, the complete weight enumerator of the Goethals code over Z_4 can be easily obtained. This result is also used for finding 3-designs from the Goethals and Delsarte-Goethals codes over Z_4.

I. 서 론

부호(특히 선형부호)의 오류 정정 및 탐지 성능에 대한 정확한 분석을 위해서는 부호의 무게 분포를 알아야 한다. 또한 선형 (또는 비선형) 부호의 무게 분포를 이용하여 MacWilliams 항등식을 사용한 dual 부호의 무게 분포 계산, 부호로부터 t-design 발견 등의 다양한 수학적 성질을 규명할 수 있다. 따라서 부호의 무게 분포를 찾는데 오랫동안 많은 연구가 이루어졌으나 현재 알려진 부호들 중 일부분에 대한 무게 분포만 알려져 있다. 예를 들면, 골레이 부호, 일중, 또는 이중 오류 정정 이진 원시 BCH 부호 (binary primitive BCH code), Reed-Solomon 부호, Reed-Muller 부호 일부분에 대한 무게 분포는 알려져 있다 [4]. Z_4 상에서 정의된 선형부호에 대한 연구는 1996년에 Hammons, Kumar, Calderbank, Sloane, Sole의 논문[2]이 발표된 이후에 더욱 활발해졌다. 현재 Z_4 상에서 정의된 선형부호가 3세대 이동

* 한양대학교 전자전기컴퓨터 공학부 (djshin@hanyang.ac.kr),
논문번호 : 020536-1217, 접수일자 : 2002년 12월 18일
※ 이 논문은 2000년 한양대학교 교내연구비 지원으로 연구되었음.

통신 표준인 W-CDMA의 스크램블링 부호로 채택되었으며 사용자 수를 증가시키기 위해서는 미래의 표준에서도 이 부호들을 사용하여야 하는 상황이다. Z_4 상에서 정의된 선형부호 중에서는 Kerdock부호와 Preparata 부호 등의 무게 분포가 알려져 있다. Kerdock부호가 Delsarte-Goethals 부호의 부분 부호 (subcode)이므로 Delsarte-Goethals 부호와Goethals 부호의 무게 분포를 알아보는 것이 당연한 연구 주제이다. 이를 이용하여 이 부호들의 정확한 성능 평가를 하고 이 부호에서 3-design을 찾을 수 있다. 이 논문에서는 길이가 2^m인(m은 홀수) Delsarte-Goethals 부호의 완전 무게 분포를 구하였다. Goethals 부호의 완전 무게 분포는 MacWilliams 항등식을 이용하여 쉽게 구할 수 있다 [2].

II. Z_4 상에서 정의된 선형 부호

Z_4 상에서 정의된 선형부호에 대해서 기본적인 개념을 알아본 후 Delsarte-Goethals 부호와 Goethals 부호에 대하여 알아본다. 4^m 개의 원소를 갖는 Z_4의 확장인 갈루와 환(Galois ring)을 $GR(4,m)$로 표기하고 $q=2^m$개의 원소를 갖는 유한체를 F_q로 표기한다. $GR(4,m)$에는 차수(order)가 2^m-1인 단위원소 β가 존재하고 이를 이용하여 *Teichmuller* 집합 T = $\{0,1,\beta,\beta^2,\cdots,\beta^{2^m-2}\}$ 를 만든다. 이때, $\alpha=\beta \bmod 2$ 이면 *Teichmuller* 집합은 T mod $2=\{0,1,\alpha,\alpha^2,\cdots,\alpha^{q-2}\}\cong F_q$의 관계를 가진다. $GR(4,m)$의 모든 원소 X는 2진 형태인 $X=A+2B, A,B\in$T로 유일하게 표현되며, $GR(4,m)$에서는 Frobenius map, $\sigma(X)=A^2+2B^2$ 에 의해 생성되는 m차의 순회 갈루와 그룹(Galois group)을 가진다.

$GR(4,m)$의 원소 X 를 Z_4의 원소로 맵핑시키는 트레이스 함수 $T(X)$ 는 다음과 같이 정의된다.

$$T(X)=\sum_{i=0}^{m-1}\sigma^i(X)$$

여기서 σ^i는 σ를 i 번 결합시킨 것을 의미한다. F_{2^m}에서 Z_2로 가는 유한체 상에서의 일반적인 트레이스 함수는 tr(x)로 표기한다. 이 논문에서 우리는 m은 항상 홀수라고 가정하며 더 많은 정보를 위해서는 [2]번 논문을 참조하기 바란다.

$c=\{c_1,c_2,\cdots,c_n\}$는 Z_4상에서 정의된 선형 부호 C의 부호어이고 c에서 i 의 발생 빈도수를 $n_i(c)=|\{k|c_k=i, 1\le k\le n\}|$라 표기한다. 이때 c의 완전 무게는 $W^{n_0(c)}X^{n_1(c)}Y^{n_2(c)}Z^{n_3(c)}$로 정의된다. c의 대칭 무게는 $W^{n_0(c)}X^{n_1(c)+n_3(c)}Y^{n_2(c)}$로 정의되며, 해밍 무게는 $W^{n_0(c)}X^{n_1(c)+n_2(c)+n_3(c)}$로 정의된다. 이를 이용하여 부호 C에 대해 다음과 같이 다양한 무게 분포를 정의한다. C의 완전 무게 분포(CWE)는 $cwe_C(W,X,Y,Z)=\sum_{c\in C}W^{n_0(c)}X^{n_1(c)}Y^{n_2(c)}Z^{n_3(c)}$로 정의되고, C의 대칭 무게 분포(SWE)는 $swe_C(W,X,Y)=\sum_{c\in C}W^{n_0(c)}X^{n_1(c)+n_3(c)}Y^{n_2(c)}$로 정의된다. C의 해밍 무게 분포(HWE)는 $hwe_C(W,X)=\sum_{c\in C}W^{n_0(c)}X^{n_1(c)+n_2(c)+n_3(c)}$로 정의된다.

Z_4 상에서 정의된 길이가 $q=2^m$ 인 Goethals 부호 G는 다음과 같은 검사 행렬 H_g를 가진 선형 부호이며, Delsarte-Goethals 부호 DG는 Z_4상에서의 G의 dual 형태이다.

$$H_g=\begin{pmatrix}1 & 1 & 1 & 1 & \cdot & 1\\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{q-2}\\ 0 & 2 & 2\beta^3 & 2\beta^6 & \cdots & 2\beta^{3(q-2)}\end{pmatrix}$$

여기서 β는 $GR(4,m)$에서 차수가 q-1인 단위원소이다.

H_g의 두 번째 열에서 알 수 있듯이 우리는 G의 부호어 좌표를 정의하기 위해 T 또는 F_q를 이용하여 $c=(c_X)_{X\in F_q}$와 같이 표기한다.

지금부터 우리는 다음과 같은 간단한 표기법을 사용할 것이다.

Z_4 상에서 정의된 Goethals 부호: G

Z_4 상에서 정의된 Delsarte-Goethals 부호: DG

III. DG 부호의 완전 무게 분포(CWE)

우리는 트레이스 함수를 이용해서 다음과 같이 DG를 정의한다.

$$\{(T([A_0+2A_1]X+2BX^3)+K)_{X\in T}$$
$$|A_0, A_1, B\in T, K\in Z_4\}$$

우리는 DG를 다음의 3가지 경우로 나누고 각각의 경우에 대해 완전 무게 분포를 구할 것이다.

(1): B=0일 경우

(2): B≠0 이고 A_0=0일 경우

(3): B≠0 이고 A_0≠0일 경우

C를 길이가 q 인 Z_4상에서 정의된 선형부호라고 하면 부호어 $c=\{c_1,\cdots,c_q\}$의 지수합은 다음과 같이 정의된다.

$$\mathrm{Exp}(c)=\sum_{j=1}^{q} i^{c_j}=$$
$$n_0(c)-n_2(c)+i(n_1(c)-n_3(c))$$
$$\text{where } i=\sqrt{-1}$$

우리는 DG의 CWE를 알아내기 위해 다음의 식을 이용한다.

$$n_0(c)+n_1(c)+n_2(c)+n_3(c)=q$$
$$(n_0(c)-n_2(c))+i\cdot(n_1(c)-n_3(c))=$$
$$Re(\mathrm{Exp}(c))+i\cdot Im(\mathrm{Exp}(c))$$
$$n_1(c)+n_3(c)=Hw(c)$$

위에서 세 번째 식은 부호어 c에 modulo 2 연산을 한 후에 얻은 해밍 무게를 이용하여 만든 식이다. 첫 번째 식은 이미 알려져 있으므로 우리는 두 번째와 세 번째 식만 알아내면 된다. 그러면 우리는 다음과 같은 관계를 이용해서 c의 완전 무게를 계산해 낼 수 있다.

$$\begin{pmatrix} n_0(c)\\ n_1(c)\\ n_2(c)\\ n_3(c)\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1&1&0&-1\\0&0&1&1\\1&-1&0&-1\\0&0&-1&1\end{pmatrix}\begin{pmatrix}q\\ Re(c)\\ Im(c)\\ Hw(c)\end{pmatrix}\cdots(*)$$

DG의 지수합의 분포는 [3]번 논문의 결과를 이용해서 유도할 수 있으며 유사한 방법을 사용하여 설명할 것이다. 먼저 아래처럼, DG를 좌표 0에서 축약시킨(shortened) DG^s을 고려한다.

$$DG^s=\{(T(AX+2BX^3))_{X\in T}\cdot|$$
$$A\in GR(4,m), B\in T\}$$

DG의 부호어인 $(T(AX+2BX^3))_{X\in T}$ 의 지수합은 다음과 같이 표현할 수 있다.

$$\xi(A,B)=\sum_{X\in T} i^{T(AX)+2T(BX^3)},\ i=\sqrt{-1}$$

그러면 $\sum_{X\in T^*} i^{T(AX)+2T(BX^3)}=-1+\xi(A,B)$

임을 쉽게 알 수 있다. 우리는 DG^s을 다음의 4가지 경우로 나누어서 지수합의 분포를 구할 것이다. 이때, R = $GR(4,m)$이다.

(i): $A=B=0$일 경우

(ii): $A\in 2R\setminus\{0\}$ 이고 $B=0$일 경우

(iii): $A\in 2R$이고 $B\in T^*$일 경우

(iv): $A\in R\setminus 2R$이고 $B\in T$일 경우

DG^s에서의 부호어의 순회 천이(cyclic shift)가 지수합의 값을 바꾸지 않기 때문에 (i), (ii)와 (iii)의 경우에 대해서 우리는 q-1의 순회 천이를 해도 같은 지수합 값을 얻을 수 있다. 그러므로 DG^s에서의 지수합의 분포는 표 1처럼 요약될 수 있다.

(i): $\xi(0,0)=q$ 임을 쉽게 알 수 있다.

(ii): 이 경우는 이진 m-수열의 지수합과 일치한다. 그러므로 $\xi(2,0)$=0을 알 수 있다.

표 1. DG^s의 지수합의 분포

	지수합	빈도수
(i)	$-1+\xi(0,0)=q-1$	1
(ii)	$-1+\xi(2,0)=-1$	$q-1$
(iii)	$-1+\xi(2A,1)$	$q-1$ for $A\in$T
(iv)	$1+\xi(1+2A,B)$	$q-1$ for A, $B\in$T

(iii): 이 경우의 부호어는 확장된 이진 이중 오류정정 BCH 부호의 dual 부호와 밀접한 연관이 있다. 이를 이용하여 A ∈T에 대해서 다음과 같은 지수합의 분포를 구할 수 있다.

$$\xi(2A,1)=\begin{cases}0, & \frac{q}{2}\ times\\ \sqrt{2q}, & \frac{q}{4}+\sqrt{\frac{q}{8}}\ times\\ -\sqrt{2q}, & \frac{q}{4}-\sqrt{\frac{q}{8}}\ times\end{cases}$$

(iv): 이 경우의 지수합의 분포는 [3, pp. 587-589]에서 발견할 수 있으며 이를 표 2에 정리하였다.

위의 결과를 종합하여 우리는 DG^s의 지수합의 분포를 얻을 수 있으며, 좌표 0에서 0을 가지는 부호어로 구성된 DG의 부분집합의 지수합의 분포는 DG^s에서 구한 각각의 지수합에 1을 더함으로써 얻을 수 있다. 그러면 DG의 지수합의 분포는 위에서 구한 DG의 부분집합의 지수합에 1, i, -1, $-i$를 곱함으로써 얻을 수 있다. 그 결과를 표 3에 정리하였다.

(1): 이 경우는 Z_4 상에서 정의된 Kerdock 부호에 해당한다. 이 부호의 CWE는 이미 알려져 있으며 표 4에서 주어졌다 [1].

(2): 이는 다음의 경우에 해당한다.
$\{(2T(A_1X+BX^3)+K)_{x\in T} | A_1\in T, B\in T^*, K\in Z_4\}$
만일 우리가 좌표 0에서 (2) 의 부호어를 축약한다면, $(2T(A_1X+BX^3))_{X\in T^*}$를 얻을 수 있으며 이를 다음과 같이 표현할 수 있다.
$2T(A_1X+BX^3))_{X\in T^*}=2\cdot(tr(a_1x+bx^3))_{x\in F_q^*}$
여기서 a_1, b 와 x는 A_1, B와 X에 modulo 2 연산을 하여 얻은 값이다. 이 식의 오른쪽 표현에 해당하는 무게 분포는 이중 오류 정정 이진 BCH 부호의 dual 부호의 무게 분포에서 유도되며 이는 이미 널리 알려져 있다 [4, p.451]. 축약된 (2)의 경우의 CWE는 표 5에 주어졌다. 이때 $b\neq 0$ 이라는 사실에 주의한다. (2)의 경우에 해당하는 부호어는 축약된 (2)의 경우의 부호어에 0을 추가하고 이에 길이가 q인 상수 벡터를 더함으로써 쉽게 얻을 수 있다. (2)의 경우에 해당하는 CWE는 표 6에 주어졌다.

(3): 표 3, 4, 6을 사용해서 (3)의 경우에 해당하는 지수합의 분포를 구할 수 있으며 이를 표 7에 정리하였다. 또한, (3)의 경우의 부호어에 modulo 2 연산을 취한 후에 이에 해당하는 해밍 무게를 계산해야 한다. (3)의 경우의 부호어에 modulo 2 연산을 취하면 아래와 같은 식을 얻을 수 있다.
$\{((T([A_0+2A_1]X+2BX^3)+K)_{X\in T}\mathrm{mod}2 =$
$(tr(a_0x)+k)_{x\in F_q}\}$.
여기서 a_0, x, k는 A_0, X, K에 modulo 2 연산을 하여 얻은 값들이다. $A_0\neq 0$이므로 $a_0\neq 0$이며 이때 $(tr(a_0x)+k)_{x\in F_q}$는 $q/2$개의 0과 $q/2$개의 1을 가진다. 그러므로 (3)의 경우에 속한 모든 부호어 c에 대하여 $n_1(c)+n_3(c)=\frac{q}{2}$가 성립한다. 이 결과를 가지고 (*)번 식과 표 7을 이용하면, 우리는 (3)의 경우의 CWE를 구할 수 있다.

위에서 구한 세 경우 (1), (2), (3)의 결과를 종합하여 홀수 $m\geq 3$에 대하여 길이가 $q=2^m$인 DG의 CWE를 얻을 수 있으며 이 결과를 표 8에 정리하였다.

Ⅳ. 결 론

이 논문에서 길이가 2^m인 (m은 홀수) Delsarte-Goethals 부호와 Goethals 부호의 완전 무게 분포를 구하였다. m이 짝수인 경우는 홀수인 경우와 비슷한 방법으로 구할 수 있으리라 예상되나 이때 사용되는 부분 부호들에 대한 지수합 분포 및 무게 분포는 다른 값들을 사용하여야 한다. Delsarte-Goethals 부호와 Goethals 부호가 차세대 이동통신에서 스크램블링 부호나 사용자 ID용 부호로 사용될 수 있으므로 이 부호들에 대한 완전 무게 분포가 성능 평가에 사용된다는 측면에서 실용적인 의의가 있다고 하겠다. 향후 무게 분포에 대한 연구 주제로 Z_4 상에서 정의된 선형부호로는 우선 m이 짝수인 경우의 Delsarte-Goethals 부호와 Goethals 부호의 완전 무게 분포를 구하는 것, S(m) 부호의 무게 분포를 구하는 것을 들 수 있다 [3].

V. 그림과 표

표 2. (iv) 경우의 지수합의 분포

지수합	빈도수
-1	$\left(\frac{3q}{4}\right)\left(\frac{q-2}{2}\right)$
$-1+\sqrt{q}\left(\frac{1\pm i}{\sqrt{2}}\right)$	$\left(\frac{q+4}{3}\right)\left(\frac{q}{4}+\sqrt{\frac{q}{8}}\right)each$
$-1+\sqrt{q}\left(\frac{-1\pm i}{\sqrt{2}}\right)$	$\left(\frac{q+4}{3}\right)\left(\frac{q}{4}-\sqrt{\frac{q}{8}}\right)each$
$-1\pm i\sqrt{2q}$	$\left(\frac{q-2}{2}\right)\left(\frac{q}{8}-\sqrt{\frac{q}{8}}\right)$
$-1\pm i\sqrt{2q}$	$\left(\frac{q-2}{2}\right)\left(\frac{q}{8}\right)each$
$-1-\sqrt{2q}$	$\left(\frac{q-2}{2}\right)\left(\frac{q}{8}-\sqrt{\frac{q}{8}}\right)$
$-1+2\sqrt{q}\left(\frac{1\pm i}{\sqrt{2}}\right)$	$\left(\frac{q-2}{6}\right)\left(\frac{q}{16}+\sqrt{\frac{q}{32}}\right)each$
$-1+2\sqrt{q}\left(\frac{-1\pm i}{\sqrt{2}}\right)$	$\left(\frac{q-2}{6}\right)\left(\frac{q}{16}-\sqrt{\frac{q}{32}}\right)each$

표 3. Delsarte-Goethals 부호의 지수합의 분포

지수합	빈도수
-1	$\left(\frac{3q}{4}\right)\left(\frac{q-2}{2}\right)$
$-1+\sqrt{q}\left(\frac{1\pm i}{\sqrt{2}}\right)$	$\left(\frac{q+4}{3}\right)\left(\frac{q}{4}+\sqrt{\frac{q}{8}}\right)each$
$-1+\sqrt{q}\left(\frac{-1\pm i}{\sqrt{2}}\right)$	$\left(\frac{q+4}{3}\right)\left(\frac{q}{4}-\sqrt{\frac{q}{8}}\right)each$
$-1\pm\sqrt{2q}$	$\left(\frac{q-2}{2}\right)\left(\frac{q}{8}-\sqrt{\frac{q}{8}}\right)$
$-1\pm i\sqrt{2q}$	$\left(\frac{q-2}{2}\right)\left(\frac{q}{8}\right)each$
$-1-\sqrt{2q}$	$\left(\frac{q-2}{2}\right)\left(\frac{q}{8}-\sqrt{\frac{q}{8}}\right)$
$-1+2\sqrt{q}\left(\frac{1\pm i}{\sqrt{2}}\right)$	$\left(\frac{q-2}{6}\right)\left(\frac{q}{16}+\sqrt{\frac{q}{32}}\right)each$
$-1+2\sqrt{q}\left(\frac{-1\pm i}{\sqrt{2}}\right)$	$\left(\frac{q-2}{6}\right)\left(\frac{q}{16}-\sqrt{\frac{q}{32}}\right)each$

표 4. 길이가 $q=2^m$ 인 Z_4 상에서 정의된 Kerdock 부호의 CWE (m은 3 이상인 홀수)

n_0	n_1	n_2	n_3	빈도수
q	0	0	0	1
0	q	0	0	1
0	0	q	0	1
0	0	0	q	1
$\frac{q}{2}$	0	$\frac{q}{2}$	0	$2(q-1)$
0	$\frac{q}{2}$	0	$\frac{q}{2}$	$2(q-1)$
$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$q(q-1)$
$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$q(q-1)$
$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$q(q-1)$
$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$q(q-1)$

표 5. 축약된 (2) 경우의 CWE

$(a=\frac{q}{2}+\sqrt{\frac{q}{2}},\ b=\frac{q}{2}-\sqrt{\frac{q}{2}})$

n_0	n_1	n_2	n_3	빈도수
$\frac{q}{2}-1$	0	$\frac{q}{2}$	0	$\frac{q}{2}(q-1)$
$a-1$	0	b	0	$(q-1)(\frac{q}{4}+\sqrt{\frac{q}{8}})$
$b-1$	0	a	0	$(q-1)(\frac{q}{4}-\sqrt{\frac{q}{8}})$

표 6. (2) 경우의 CWE

n_0	n_1	n_2	n_3	빈도수
$\frac{q}{2}$	0	$\frac{q}{2}$	0	q
0	$\frac{q}{2}$	0	$\frac{q}{2}$	$q(q-1)$
a	0	b	0	$\frac{q}{2}(q-1)$
0	a	0	b	$\frac{q}{2}(q-1)$
b	0	a	0	$\frac{q}{2}(q-1)$
0	b	0	a	$\frac{q}{2}(q-1)$

$(a=\frac{q}{2}+\sqrt{\frac{q}{2}},\ b=\frac{q}{2}-\sqrt{\frac{q}{2}})$

표 7. (3) 경우의 지수합의 분포

지수합	빈도수
0	$(q-1)(\frac{3}{2}q^2-3q)$
$\sqrt{q}\left(\frac{\pm 1 \pm i\sqrt{2q}}{\sqrt{2}}\right)$	$q(q-1)(\frac{q+1}{3})(each)$
$\pm\sqrt{2q}\pm i\sqrt{2q}$	$\frac{q}{2}(q-1)(\frac{q}{2}-1)(each)$
$2\sqrt{q}\left(\frac{\pm 1 \pm i}{\sqrt{2}}\right)$	$\frac{q}{4}(q-1)(\frac{q-2}{6})(each)$

표 8. *DG* 부호의 CWE ($q = 2^m$, m은 홀수)

n_0	n_1	n_2	n_3	빈도수
q	0	0	0	1
0	q	0	0	1
0	0	q	0	1
0	0	0	q	1
$\frac{q}{2}$	0	$\frac{q}{2}$	0	$(q+2)(q-1)$
0	$\frac{q}{2}$	0	$\frac{q}{2}$	$(q+2)(q-1)$
$\frac{q}{2}+\sqrt{\frac{q}{2}}$	0	$\frac{q}{2}-\sqrt{\frac{q}{2}}$	0	$\frac{q}{2}(q-1)$
$\frac{q}{2}-\sqrt{\frac{q}{2}}$	0	$\frac{q}{2}+\sqrt{\frac{q}{2}}$	0	$\frac{q}{2}(q-1)$
0	$\frac{q}{2}+\sqrt{\frac{q}{2}}$	0	$\frac{q}{2}-\sqrt{\frac{q}{2}}$	$\frac{q}{2}(q-1)$
0	$\frac{q}{2}-\sqrt{\frac{q}{2}}$	0	$\frac{q}{2}+\sqrt{\frac{q}{2}}$	$\frac{q}{2}(q-1)$
$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$q(q-1)(\frac{q+4}{3})$
$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$q(q-1)(\frac{q+4}{3})$
$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$q(q-1)(\frac{q+4}{3})$
$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}-\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$\frac{q}{4}+\sqrt{\frac{q}{8}}$	$q(q-1)(\frac{q+4}{3})$
$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}$	$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}$	$\frac{q}{2}(q-1)(\frac{q}{2}-1)$
$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}$	$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}$	$\frac{q}{2}(q-1)(\frac{q}{2}-1)$
$\frac{q}{4}$	$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}$	$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{2}(q-1)(\frac{q}{2}-1)$
$\frac{q}{4}$	$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}$	$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{2}(q-1)(\frac{q}{2}-1)$
$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}(q-1)(\frac{q-2}{6})$
$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}(q-1)(\frac{q-2}{6})$
$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}(q-1)(\frac{q-2}{6})$
$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}-\sqrt{\frac{q}{2}}$	$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}+\sqrt{\frac{q}{2}}$	$\frac{q}{4}(q-1)(\frac{q-2}{6})$
$\frac{q}{4}$	$\frac{q}{4}$	$\frac{q}{4}$	$\frac{q}{4}$	$(q-1)(\frac{3}{2}q^2-3q)$

참 고 문 헌

[1] A. Bonnecaze and I. M. Duursma, "Translates of linear codes over Z_4," IEEE Trans. on Inform. Theory, Vol. 43, No. 4, pp. 1218-1230, July 1997.

[2] A. R. Hammons, P. V. Kumar, A. R. Calderbank and N. J. A. Sloane, and P. Solé, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," IEEE Trans. on Inform. Theory, Vol 40, No. 2, pp. 301-319, March 1994.

[3] P. V. Kumar, T. Helleseth, A. R. Calderbank and A. R. Hammons, Jr., "Large families of quaternary sequences with low correlation," IEEE Trans. on Inform. Theory, Vol. 42, No. 2, pp. 579-592, March 1996.

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1977.

신 동 준(Dong-Joon Shin) 정회원

1990년 2월 : 서울대학교 전자공학과 공학사

1991년 12월 : Northwestern University, 전기공학과 공학석사

1998년 12월 :University of Southern California, 전기공학과 공학박사

1999년 1월~1999년 4월 : Research Associate at USC

1999 년 4월~2000년 8월 : Hughes Network Systems, MTS

2000년 9월~현재 : 한양대학교 전자전기컴퓨터공학부 조교수

<주관심분야> 디지털통신, 시퀀스, 오류 정정 부호