論文 97-22-5-19

Z_4위의 Preparata 부호의 연쇄조건

正會員 임 두 루*, 양 경 철*

On the Chain Condition for Preparata Codes over Z_4

Dooroo Lim*, Kyeongcheol Yang* *Regular Members*

※이 논문은 정보통신연구관리단 대학기초연구지원사업(과제관리번호 : 96174-CT-12)에 의한 결과임.

요 약

길이가 8인 Z_4위의 Preparata 부호는 연쇄조건을 만족하는 반면에, 길이가 16 또는 32인 경우 Z_4위의 Preparata 부호는 연쇄조건을 만족하지 않는다. 본 논문에서는 Z_4위의 Preparata 부호의 무게체계와 연쇄조건과의 관계를 조사함으로써 길이가 2^m인 Z_4위의 Preparata 부호가 $m=4, 5, 6$과 8에 대해 연쇄조건을 만족하지 않음을 보였다.

ABSTRACT

Though the Preparata code of length 8 over Z_4 satisfies the chain condition, the Preparata code of length 16 or 32 over Z_4 does not satisfy the chain condition. In this paper we show that the Preparata code of length 2^m over Z_4 does not satisfy the chain condition for $m=4$, 5, 6, and 8 by investigating relations between weight hierarchy and chain condition.

Ⅰ. 서 론

Nordstrom-Robinson 부호, Kerdock 부호, Preparata 부호, Goethals 부호, Delsarte-Goethals 부호들은 주어진 길이와 최소거리에 대해 지금까지 알려진 어떠한 이진선형부호보다 더 많은 부호어를 가지는 비선형부호들이다. 예를 들면 Preparata 부호는 확장된 이중오류정정(extended double-error correcting) BCH 부호보다 두배의 부호어를 가진다. 이러한 부호들은 비선형이기 때문에 구현이 어려웠으나, Hammons, Kumar, Calderbank, Sloane과 Solé는 Z_4위에서 적절히 정의하면 선형부호가 됨을 보였다[2].

일반화된 Hamming 무게(generalized Hamming weights)와 무게체계(weight hierarchy)는 부호를 암호시스템에 응용하는 과정에서 도입된 개념으로서 II형 도청채널(wire-tap channel)에서의 부호의 성능을 결정한다. 또한 격자도를 이용하여 연판정(soft decision)

*한양대학교 전자통신공학과
論文番號:97122-0401
接受日字:1997年 4月 1日

으로 블럭부호를 복호할 때 상태복잡도를 결정하는 요소이다. 이진부호에 비해 Z_4위의 선형부호에 대한 일반화된 Hamming 무게는 많이 알려져 있지 않으며, Kerdock, Preparata, Goethals 부호들에 대해서는 Yang과 Helleseth 등에 의해 부분적인 결과가 알려져 있다[6], [7], [8].

연쇄조건(chain condition)은 승산부호(product code)의 일반화된 Hamming 무게를 연구하는 과정에서 도입된 개념이다[5]. 옥타부호(octacode)라 부르는 길이가 8인 Z_4위의 Preparata 부호는 연쇄조건을 만족하는 반면에 길이가 16 또는 32인 경우에는 연쇄조건을 만족하지 않는다[9], [10]. 본 논문에서는 무게체계와 연쇄조건과의 관계를 조사함으로써 일반적인 방법으로 길이가 2^m인 Z_4위의 Preparata 부호가 $m=4, 5, 6$과 8에 대해 연쇄조건을 만족하지 않음을 보인다.

Ⅱ. Z_4위의 Preparata 부호

이진선형부호를 유한체(Galois fields 또는 finite fields)에서 다루듯이 Z_4위의 선형부호에 대한 접근은 Galois 환(Galois rings)에서 이루어진다.

Z를 정수들의 집합이라 하자. Z_n이란 n으로 모듈로(modulo)를 취한 정수들의 집합을 의미하며, $Z_n[x]$란 Z_n의 원소들을 계수로 가지는 다항식을 말한다. $\mu : Z_4 \rightarrow Z_2$를 Z_4의 원소들에 대해 2로 모듈로를 취하는 축약사상(reduction map)이라 정의하자. $Z_4[x]$에 속하는 m차의 다항식 $f(x)=a_0+a_1x+\cdots+a_mx^m$에 대해 μ를 적용하면, $Z_4[x]$에서 $Z_2[x]$로의 축약사상은

$$\mu(f(x))=\mu(a_0)+\mu(a_1)x+\cdots+\mu(a_m)x^m$$

과 같다. $f(x)\in Z_4[x]$에 대해 $\mu(f(x))$가 Z_2위에서 인수분해가 되지 않으면, $f(x)$를 기약다항식(basic irreducible polynomial)이라 한다. 유한체의 경우 m차의 인수분해가 되지 않는 다항식 $h(x)\in Z_2[x]$에 의해 GF(2)에서 GF(2^m)으로의 확장(extension)이 이루어진다. 즉 유한체 GF(2^m)은 GF(2^m)$\cong Z_2[x]/(h(x))$로 정의된다. 이와 유사하게 m차의 기약다항식 $f(x)\in Z_4[x]$를 이용하여 Galois 환 $R_m=$GR(4, m)은 확장된 환 $Z_4[x]/(f(x))$로 자연스럽게 정의된다.

Galois 환과 유한체의 가장 큰 차이점은 Galois 환이 0의 젯수(zero divisor)를 원소로 가지고 있다는 점이다. R_m은 0의 젯수들의 집합, 즉 $2R_m$을 유일한 최대 아이디얼(maximal ideal)로 가지는 국소가환환(local commutative ring)이다. 아이디얼 이외의 원소들은 곱셈에 대해 역원을 가지며, 이들 원소들로 구성된 승산군(multiplicative group) R_m^*은 아래의 구조를 가진다:

$$R_m^*\cong Z_{2^{m-1}}\times Z_2\times Z_2\times\cdots\times Z_2.$$

여기서 $Z_2\times\cdots\times Z_2$는 m개의 Z_2의 데카르트곱(Cartesian product)이고, $Z_{2^{m-1}}$은 주기가 2^m-1인 순회군(cyclic group)이다. $h(x)\in Z_2[x]$를 최고차항의 계수가 1이고 인수분해가 되지 않는 m차의 원시다항식(primitive polynomial)이라 하면, 최고차항의 계수가 1이며 $\mu(g(x))\equiv h(x)$을 만족하고 $x^{2^m-1}-1 \pmod 4$를 나누는 m차의 다항식 $g(x)\in Z_4[x]$가 유일하게 존재하며, 이를 원시기약다항식(primitive basic irreducible polynomial)이라 부른다. β를 $g(x)$의 근이라 하면 β는 $Z_{2^{m-1}}$의 생성자(generator)가 된다. S_m을 $S_m=\{0, 1, \beta, \beta^2, \beta^{2^m-2}\}$로 정의하면 R_m에 속하는 임의의 원소 γ를 아래와 같이 유일하게 표현 할 수 있다:

$$\gamma=A+2B,\qquad A, B\in S_m.$$

여기서 $\alpha=\mu(\beta)$는 m차의 원시다항식 $\mu(g(x))$의 근이 되고, $\mu(S_m)=\{0, 1, \alpha, \alpha^2, \alpha^{2^m-2}\}$는 유한체 GF($2^m$)이 된다.

길이가 n인 Z_4위의 선형부호 C는 가산군(additive group) Z_4^n의 부분군(subgroup)으로 정의된다. Z_4위의 선형부호의 성능을 결정하는 가장 중요한 요소중 하나는 최소 Lee 무게(minimum Lee weight)이다. Z_4에 속하는 0, 1, 2, 3의 Lee 무게는 각각 0, 1, 2, 1이 되고, Z_4^n에 속하는 벡터 $a=(a_1, a_2, \cdots, a_n)$의 Lee 무게는 각 원소들의 Lee 무게의 합이 된다.

부호길이가 2^m인 Z_4위의 Preparata 부호 P_m은 아래의 행렬 H를 검사행렬로 가지는 부호이다:

$$H=\begin{bmatrix}1 & 1 & 1 & 1 & \cdots & 1\\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{2^m-2}\end{bmatrix}$$

즉 P_m의 임의의 부호어 $(u_x)_{x\in S_m}$에 대해

$$\sum_{X\in S_m} u_X = 0, \qquad \sum_{X\in S_m} u_X X = 0$$

이 만족된다.

보조정리 2.1 ([2]) Z_4위의 Preparata 부호는 아래의 비선형 순열변환들로 구성된 이중추이군(doubly transitive group)에 대해 불변의 성질을 갖는다:

$$X \to (AX+B)^{2^m}.$$

여기서 $A, B \in S_m$이고 $A \neq 0$이다.

보조정리 2.2 ([3]) Z_4위의 벡터 $e=(e_X)_{X\in S_m}$가 주어질 때 $j=0, 1, 2, 3$에 대해 $E_j=\{X|e_X=j\}$라 하면, 다음의 수식

$$\sum_{X\in S_m} e_X X = A+2B, \quad A, B\in S_m, \quad e_X \in Z_4$$

은 아래 두 개의 수식과 등가이다:

$$a=\sum_{X\in E_1\cup E_3} x,$$

$$b^2=\sum_{X\in E_2\cup E_3} x^2+\sum_{\substack{X,Y\in E_1\cup E_3\\ X<Y}} xy.$$

여기서 a, b, x와 y는 각각 $\mu(A)$, $\mu(B)$, $\mu(X)$와 $\mu(Y)$를 의미하며, '<'는 S_m의 원소들에 대한 어떤 순서(ordering)를 뜻한다.

위의 보조정리를 이용하여 R_m위에서 정의된 하나의 수식을 GF(2^m)위에서 정의된 두 개의 수식으로 변환할 수 있다.

Ⅲ. 무게체계와 연쇄조건

D를 4^k개의 부호어를 가지는 Z_4위의 선형부호 C의 부분모듈(submodule)이라 하자. $\chi(D)$로 표시되는 D의 받침대(support)는 D에 속하는 부호어들의 성분들 중에서 0이 아닌 성분에 대한 좌표들의 집합이다. 즉 아래와 같이 정의된다:

$$\chi(D)=\{i: \exists\ (x_1, x_2, \cdots, x_n)\in D, \quad x_i\neq 0\}.$$

$2r$이 정수가 되는 0과 k사이의 r에 대해 C의 r차의 일반화된 Hamming 무게 $d_r(C)$는 C의 부분모듈 중에서 차원이 r이며 최소의 받침대 크기를 가지는 부분모듈의 받침대 크기로 정의된다. 즉

$$d_r(C)=\min\{|\chi(D)|: D\text{는 } 4^r\text{개의 원소를 가지는 부분모듈}\}.$$

예를 들어 $C=\langle(1, 1, 2, 0, 0), (0, 0, 0, 1, 3)\rangle$를 Z_4위의 선형부호라 하면 $\langle(1, 1, 2, 0, 0)\rangle$과 $\langle(0, 0, 0, 1, 3)\rangle$이 1차원의 부분모듈에 해당한다. 각각의 받침대 크기는 3과 2이므로 $d_1(C)=2$이다. 또한 $2r=3$, 즉 $r=1.5$이면 $\langle(1, 1, 2, 0, 0), (0, 0, 0, 2, 2)\rangle$와 $\langle(2, 2, 0, 0, 0), (0, 0, 0, 1, 3)\rangle$이 1.5차원의 부분모듈에 해당한다. 각각의 받침대 크기는 5와 4이므로 $d_{1.5}(C)=4$이다. 관례적으로 d_0는 0으로 가정한다. 특히 $d_1(C)$는 C의 최소 Hamming 거리(minimum Hamming distance)를 의미한다. C의 일반화된 Hamming 무게들의 수열 $\{d_r(C)|0.5\leq r\leq k\}$를 C의 무게체계(weight hierarchy)라 한다. 위의 예에서 무게체계는 {2, 2, 4, 5}이다.

다음의 성질을 가지는 C의 부분모듈 $\{D_r|0.5\leq r\leq k\}$이 존재할 때 C가 연쇄조건(chain condition)을 만족한다고 정의한다:

i) D_r은 4^r개의 부호어를 가지며 받침대의 크기가 $d_r(C)$이다.

ii) $2r$이 정수가 되는 임의의 r에 대해 $D_r\subset D_{r+0.5}$를 만족한다. 즉 $D_{0.5}\subset D_1\subset D_{1.5}\subset\cdots\subset D_k$이 성립한다.

예를 들어 $C_1=\langle(1, 1, 1, 1, 0, 0), (1, 3, 0, 2, 1, 1)\rangle$를 Z_4위의 선형부호라 하면 C_1의 무게체계는 {4, 4, 6, 6}이다. C_1의 부분모듈을 아래와 같이 선택하자:

$$D_{0.5}=\langle(2, 2, 2, 2, 0, 0)\rangle,$$
$$D_1=\langle(1, 1, 1, 1, 0, 0)\rangle,$$
$$D_{1.5}=\langle(1, 1, 1, 1, 0, 0), (2, 2, 0, 0, 2, 2)\rangle,$$
$$D_2=\langle(1, 1, 1, 1, 0, 0), (1, 3, 0, 2, 1, 1)\rangle.$$

그러면 $D_{0.5}\subset D_1\subset D_{1.5}\subset D_2$이므로 C_1은 연쇄조건을 만족한다.

한편 $C_2=\langle(1, 2, 2, 0, 0), (0, 0, 0, 1, 1)\rangle$인 경우 C_2의 무게체계는 {1, 2, 3, 5}이고 받침대의 크기가 $d_r(C_2)$인 각각의 부분모듈은

$D_{0.5}=\langle(2,0,0,0,0)\rangle$,
$D_1=\langle(0,0,0,1,1)\rangle$,
$D_{1.5}=\langle(2,0,0,0,0),(0,0,0,1,1)\rangle$,
$D_2=\langle(1,2,2,0,0),(0,0,0,1,1)\rangle$

로 선택할 수 있다. 그러나 $D_{0.5}$는 D_1의 부분집합이 아니므로 C_2는 연쇄조건을 만족하지 않는다.

Ⅳ. Z_4위의 Preparata 부호의 연쇄조건

길이가 2^m인 Preparata 부호 P_m의 r차의 일반화된 Hamming 무게를 편의상 $d_r(m)$이라 둔다.

옥타부호(octacode)라 부르는 길이가 8인 Z_4위의 Preparata 부호 P_3의 무게체계는 다음과 같다 [1]:

{4, 5, 6, 6, 7, 7, 8, 8}.

β를 3차의 원시기약다항식 $x^3+3x^3+2x+3=0$의 근이라 하면 P_3의 검사행렬 H를 아래와 같이 구성할 수 있다:

$$H=\begin{bmatrix}c_4\\c_3\\c_2\\c_1\end{bmatrix}=\begin{bmatrix}1&1&1&1&1&1&1&1\\0&1&0&0&1&1&3&2\\0&0&1&0&2&3&3&3\\0&0&0&1&1&3&2&1\end{bmatrix}$$

P_3는 자기쌍대부호(self-dual code)이므로 생성행렬과 검사행렬이 동일하다. 따라서 c_i를 생성행렬의 i번째 행이라고 하면 P_3의 r차원의 부분모듈 D_r을 아래와 같이 정의할 수 있다:

$$D_r=\begin{cases}\langle c_1,c_2,\cdots,c_r\rangle, & 2r\text{이 짝수일 때,}\\ \langle c_1,c_2,\cdots,c_{r-0.5},2c_{r+0.5}\rangle, & 2r\text{이 홀수일 때.}\end{cases}$$

예를 들어 $r=1.5$이면

$D_{1.5}=\langle(0,0,0,1,1,3,2,1),(0,0,2,0,0,2,2,2)\rangle$

이고, $r=2$이면

$D_2=\langle(0,0,0,1,1,3,2,1),(0,0,1,0,2,3,3,3)\rangle$

이다. D_r의 반침대 크기는 $d_r(3)$과 같고, $D_r\subset D_{r+0.5}$이므로 P_3는 연쇄조건을 만족함을 알 수 있다.

$m=3$과 달리 $m=4$와 5에 대해 Z_4위의 Preparata 부호는 연쇄조건을 만족하지 않는다. 연쇄조건을 만족하지 않는 두 부호 P_4와 P_5의 무게체계로부터 아래의 사실을 유도할 수 있다.

정리 4.1 $2r$이 홀수일 때 부분모듈의 차원이 $r-1$, $r-0.5$와 r인 경우 각각의 일반화된 Hamming 무게가

$$d_{r-1}(m)=l,\quad d_{r-0.5}(m)=l+1,\quad d_r(m)=l+1$$

과 같이 주어지면, Z_4위의 Preparata 부호 P_m은 연쇄조건을 만족하지 않는다.

(증명) Preparata 부호 P_m이 연쇄조건을 만족한다고 가정하자. $2r$이 홀수가 되는 r에 대해 D_r을 반침대의 크기가 $d_r(m)$인 P_m의 r차원의 부분모듈로서

$$D_r=\langle c_1,c_2,\cdots,c_{r-0.5},2c_{r+0.5}\rangle$$

와 같이 정의하자. G를 $D_{r-1.5}$의 생성행렬이라 하면, 보조정리 2.1로부터 일반성을 잃지 않고 D_r의 생성행렬을 아래와 같이 쓸 수 있다:

$$\begin{bmatrix}c_1\\c_2\\\cdot\\\cdot\\c_{r-1.5}\\c_{r-0.5}\\2c_{r+0.5}\end{bmatrix}=\begin{bmatrix}&&&&0&0\\&&&&0&0\\&&G&&\cdot&\cdot\\&&&&\cdot&\cdot\\&&&&0&0\\*&\cdots&*&1&2\\*&\cdots&*&0&2\end{bmatrix}$$

$D_{r-0.5}=\langle c_1,c_2,\cdots,c_{r-0.5}\rangle$의 반침대를 $\{X_1,X_2,\cdots,X_{l+1}\}$이라 하면, 또다른 $r-0.5$ 차원의 부분모듈 $D'=\langle c_1,\cdots,c_{r-0.5}+2c_{r+0.5}\rangle$는 $\{X_1,X_2,\cdots,X_l\}$를 반침대로 가진다. 이는 $d_{r-0.5}(m)=l+1$에 위배되므로 P_m은 연쇄조건을 만족하지 않는다. □

정리 4.2 ([7]) 길이가 16인 Z_4위의 Preparata 부호의 무게체계는 아래와 같다:

{4, 4, 6, 6, 7, 8, 8, 9, 10, 10, 11, 11, 12, 12, 13, 13, 14, 14, 15, 15, 16, 16}.

따름정리 4.3 길이가 16인 Z_4위의 Preparata 부호는 연쇄조건을 만족하지 않는다.

(증명) 정리 4.2로부터 $d_{2.5}(4)=7$, $d_3(4)=8$이고 $d_{3.5}(4)=8$이므로 P_4는 연쇄조건을 만족하지 않는다. □

정리 4.4 ([7]) 길이가 32인 Z_4위의 Preparata 부호의 무게체계는 아래와 같다:

{4, 5, 6, 7, 8, 8, 9, 9, 10, 10, 11, 12, 12, 13, 13, 14, 14, 15, 15, 16, 16, 17, 18, 18, 19, 19, 20, 20, 21, 21, 22, 22, 23, 23, 24, 24, 25, 25, 26, 26, 27, 27, 28, 28, 29, 29, 30, 30, 31, 31, 32, 32}.

따름정리 4.5 길이가 32인 Z_4위의 Preparata 부호는 연쇄조건을 만족하지 않는다:

(증명) 정리 4.4로부터 $d_{5.5}(5)=11$, $d_6(5)=12$이고 $d_{6.5}(5)=12$이므로 P_5는 연쇄조건을 만족하지 않는다. □

정리 4.6 ([7]) 길이가 64인 Z_4위의 Preparata 부호의 무게체계는 아래와 같다:

{4, 4, 6, 6, 7, 7, 8, 8, 10, 10, 11, 12, 12, 13, 14, 14, 15, 15, 16, 16, 17, 17, 18, 18, 19, 19, 20, 20, 21, 22, 23, 23, 24, 24, 25, 25, 26, 26, 27, 27, 28, 28, 29, 29, 30, 30, 31, 31, 32, 32, 33, 34, 34, 35, 35, 36, 36, 37, 37, 38, 38, 39, 39, 40, 40, 41, 41, 42, 42, 43, 43, 44, 44, 45, 45, 46, 46, 47, 47, 48, 48, 49, 49, 50, 50, 51, 51, 52, 52, 53, 53, 54, 54, 55, 55, 56, 57, 57, 58, 58, 59, 59, 60, 60, 61, 61, 62, 62, 63, 63, 64, 64}.

따름정리 4.7 길이가 64인 Z_4위의 Preparata 부호는 연쇄조건을 만족하지 않는다.

(증명) 정리 4.6으로부터 $d_{5.5}(6)=11$, $d_6(6)=12$이고 $d_{6.5}(6)=12$이므로 P_6은 연쇄조건을 만족하지 않는다. □

길이가 256인 Z_4위의 Preparata 부호 P_8의 무게체계에 대해서는 부분적인 결과만이 알려져 있다[7]. 그러나 $d_{2.5}(8)=7$, $d_3(8)=8$과 $d_{3.5}(8)=8$로부터 P_8도 연쇄조건을 만족하지 않음을 알 수 있다.

V. 결 론

길이가 8인 Z_4위의 Preparata 부호 P_3는 연쇄조건을 만족하는 반면에, $m=4$, 5, 6과 8인 경우 Z_4위의 Preparata 부호는 연쇄조건을 만족하지 않는다. 본 논문에서는 무게체계와 연쇄조건과의 관계를 조사함으로써 길이가 2^m인 Z_4위의 Preparata 부호가 $m=4$, 5, 6과 8인 경우에 대해 연쇄조건을 만족하지 않음을 보였다.

참 고 문 헌

1. A. E. Ashikhmin, "Generalized Hamming weights for Z_4-linear codes," *Proc. IEEE Int. Symp. Inform. Theory*, p. 306, Trondheim, Norway, June 1994.
2. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301-319, Mar. 1994.
3. T. Helleseth and P. V. Kumar, "The algebraic decoding of the Z_4-linear Goethals code," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2040-2048, Nov. 1995.
4. V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1412-1418, Sept. 1991.
5. V. K. Wei and K. Yang, "On the generalized Hamming weights of product codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1709-1713, Sept. 1993.
6. K. Yang, T. Helleseth, P. V. Kumar, and A. Shanbhag, "On the weight hierarchy of Kerdock codes over Z_4," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1587-1593, Sept. 1996.
7. K. Yang and T. Helleseth, "On the weight hierarchy of Preparata codes over Z_4," to appear in *IEEE Trans. Inform. Theory*, 1997.
8. K. Yang and T. Helleseth, "On the weight hierarchy of Goethals codes over Z_4," submitted to

IEEE Trans. Inform. Theory, November 1996.

9. 양경철, 임두루, "길이가 16인 Z_4위의 Preparata 부호는 연쇄조건을 만족하지 않는다," *한국통신정보보호학회 종합학술발표회 논문집*, vol 6, No. 1, pp. 286-294, 동국대학교, 1996년 11월.
10. 임두루, 양경철, "길이가 32인 Z_4위의 Preparata 부호의 연쇄조건," *제7회 통신정보합동학술대회 (JCCI'97) 논문집*, pp. 71-74, 1997년 4월.

林 두 루(Dooroo Lim) 정회원

1996년 2월 : 한양대학교 전파공학과 졸업(공학사)

1996년 3월~현재 : 한양대학교 대학원 전자통신공학과 석사과정

※주관심분야 : 부호 및 정보이론, 이동통신

梁 景 喆(Kyeongcheol 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 : Bellcore 연구원(미국 New Jersey 주, Morristown 소재)

1993년 3월~현재 : 한양대학교 전자통신공학과 조교수

※주관심분야 : 부호 및 정보이론, 암호이론, 이산수학의 응용