88656

CDMA를 위한 최적부호 발생에 관한 연구

윤 기 룡°　　이 정 재

동의대학교 전자통신공학과　동의대학교 전자통신공학과

The Construction of the families of the sequences with optimal Hamming correlation properties

Kee Lyong YOON　　Jeong Jae LEE

Dept. of Electronic Communication Dongeui University

ABSTRACT　In this paper, we consider the construction of the families of sequences with optimal Hamming correlation properties, consisting of σ_2 (v) - transform and σ_3 (v)-transform of the ternary M - sequence X respectively.

1. 서론

MA(Multiple Access)통신은 여러 이용자들이 동일매체를 분담하여 사용하는 모든 통신시스템을 말한다. 가장 일반적인 방법은 FDMA(Frequency Division Multiple Access)와 TDMA(Time Division Multiple Access)이며 세번째의 방법이 부호를 이용한 분리방법으서 CDMA(Code Division Multiple Access)이다. 이 시스템의 신호들은 여러 이용자들이 각각 고유한 부호에 의하여 확산된 신호를 모든 대역폭에 송신하게 되어 대역확산 다중통신 (SSMA:Spread Sprectrum Multiple Access)이라고도 한다. CDMA 시스템은 크게 대별하여 DS-CDMA (Direct Sequence -CDMA)와 FH-CDMA(Frequency Hopped -CDMA)의 두 종류로 분류할 수 있으며 DS-CDMA에 사용되는 분할을 위한 부호는 서로 다른 이용자의 고유부호 상호간에 상호상관 특성이 적은 부호가 사용되여야 하며 이를 위해 m-sequence를 조합 또는 변형하여 만든 Gold부호,Kasami부호 등이 있다. 반면 FH-CDMA를 위한 부호는 DS-CDMA와는 달리 각 이용자들이 사용하는 각 각의 부호상호간에 해밍(Hamming)거리가 큰 특성을 갖어야만 수신측에서 복조가 용이하게 된다.[1] 이를 위한 대표적인 부호는 Read-Solomon 부호를 이용한 유한번지부호 (Finite Address Codes)[2] ,소수부호(Primitive Codes)[3] 와 m-sequence를 이용한 최적부호가 있다. 본 연구는 최적부호의 발생에 따른 ABRAHAM Lempel과 Hain Greenberger[4] 에 의해 제안된 최적부호의 발생에 따른 알고리즘 및 구성에 대하여 연구하였다.

2. 본론

2.1 최적 부호

일반적인 상관함수와는 달리 두부호계열 X = {x(j)}, Y = {y(j)} 사이의 해밍메트릭을 이용한 해밍상관함수

$$H_{XY}(\tau)=\sum_{j=0}^{q-1} h[x(j),y(j+\tau)] \ , \ 0\le\tau<q \qquad (1)$$

여기서 q : 부호의 길이

$$h[x,y]=\begin{cases} 0 \ , \ \text{if } x\neq y \\ 1 \ , \ \text{if } x=y \end{cases} \qquad (2)$$

S를 길이 q의 모든 부호계열의 집합이라 하면 X, Y∈S 에 대하여

$$H(X)=\max_{0<\tau<q}\{H_{XX}(\tau)\} \qquad (3)$$

$$H(X,Y)=\max_{0\le\tau<q}\{H_{XY}(\tau)\} \qquad (4)$$

그리고

$$M(X,Y)=\max\{H(X),H(Y),H(X,Y)\} \qquad (5)$$

라 하면, 다음 판별에 의하여 최적이 결정된다.

i) X∈S는 만약 H(X)≤H(X'), X'∈S 최적
ii) X,Y∈S는 만약 M(X,Y)≤M(X',Y'), X',Y'∈S 최적짝
iii)F⊂S는 만약 F에 속하는 벌개의 짝이 최적 짝이면 최적집단

2.2 최적부호 설계

최적부호는 GF(P)에 대한 m-sequence를 이용하여 발생시킨다. 주기 $q=p^n-1$ 이고 GF(P)에 대하여 차수 n의 m-sequence

$$B=\{b(j)\} \qquad (6)$$

i) 각 소수 p 와 각 정수 n에 대하여 $q=p^n-1$의 m-sequence가 GF(p)에서 존재
ii) W를 GF(p)에서 영(zero) n-tuple을 제외한 모든 집합이라 하면 각 w∈W 에 대하여 범위 $0\le j<q$ 에서 유일한 j가 존재하여
W = b(j),b(j+1),- - - ,b(j+n-1)
의 관계를 갖는다.

$$\sum_{i=0}^{n} f_i\, b(j-i) = 0 \qquad (7)$$

여기서 순환계수 f_i 는 원시다항식

$$f(z) = \sum_{i=0}^{n} f_i Z^i$$ 로부터 이루어지며 $f_i \in GF(p)$

이다.

$$P = \{0,1, - - - ,p-1\} \quad (8)$$

$$P_k = \{0,1, - - - ,p^k -1\} \quad (9)$$

P^k : P에서 길이 k(k-tuples)인 모든 부호어들의 집합

$$P^k \xrightarrow{\sigma} P_k$$

σ: P^k 에서 P_k 로 mapping 하는 변환

$$W = (w_0 ,w_1 , - -- , w_{k-1}) \in P^k \quad (10)$$

일 때

$$w\sigma = \sum_{i=0}^{k-1} w_i P^i \in P_k \quad (11)$$

P에서 길이 q의 계열
X = { x(j) }
X(j,k) : X에서 j번째 k-tuple

$$\{x(j),x(j+1), - - - , x(j+k-1)\} \quad (12)$$

μ_x (W) : X안에서 $0 \le j < q$ 인 범계의 위치 j의 수 즉 W의 배수

$$w = X(j,k) \in P^k \quad (13)$$

X에서 x(0)는 x(q-1) 다음에 온다.
Y = {y(j)}
P_k 에서 길이 q의 계열
X의 연속적인 k-tuples에서 mapping σ 를 적용하면

$$Y(j) = X(j,k)\sigma = \sum_{i=0}^{k-1} x(j+i)P^i \ , \ 0 \le j < q \quad (14)$$

$$Y = X\sigma_k$$

$$X \xrightarrow{\sigma_k} Y$$

이라 할 때 X를 GF(p)에 대한 길이 $q = p^n -1$의 m-sequence라고 하면 각 k에 대하여 X의 σ_k 변환은 P_k 에서 길이 q의 최적계열이 되며, 각 $j \in P_v$, $v \in P_k$, $1 \le k < n$ 에 대하여

X_v (j,k) : X의 j번째 k-tuple과 σ에 대하여 v에 mapping되는 k-tuple $v\sigma^{-1} \in P^k$ 와의 mod-p

$$X_v (j,k) = X(j,k) + v\sigma^{-1}$$

Y_v = { y_v (j) } : P_k 에서 길이 $P^n -1$의 계열

j번째 항

$$y_v (j) = X_v (j,k)\sigma$$

$$X \xrightarrow{\sigma_k (v)} Y_v$$

$$Y_v = X\sigma_k (v)$$

이라 하면 $Y_v = X\sigma_k (v)$ 는 최적이다.[4)]

2.3. 최적부호 발생

최적부호는 P가 소수일 때 발생시 킬 수 있으며 P=3인 경우 주기는 $P^n -1 = 3^3 -1 = 26$, 원시다항식은 $Z^3 + Z^2 + 2$ 이므로

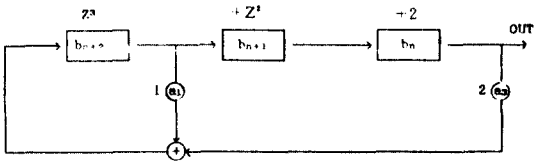

Fig.1. Nonbinary M-sequence Generator GF(3)

Table 1. The States of M-sequence over GF(3)

n	b_{n+2}	b_{n+1}	b_n	X
0	1	0	0	0
1	1	1	0	0
2	1	1	1	1
3	0	1	1	1
4	2	0	1	1
5	1	2	0	0
6	1	1	2	2
7	2	1	1	1
8	1	2	1	1
9	0	1	2	2
10	1	0	1	1
11	0	1	0	0
12	0	0	1	1
13	2	0	0	0
14	2	2	0	0
15	2	2	2	2
16	0	2	2	2
17	1	0	2	2
18	2	1	0	0
19	2	2	1	1
20	1	2	2	2
21	2	1	2	2
22	0	2	1	1
23	2	0	2	2
24	0	2	0	0
25	0	0	2	2
26	1	0	0	0

에 의해 발생된

x = (0,0,1,1,1,0,2,1,1,2,1,0,1,0,0,2,2,2,0,1,2,2,1,2,0,2)

σ_k (v) 변환에서 k-tuple 을 2로 하면 σ_2 (v)변환은

$$X \xrightarrow{\sigma_2 (v)} Y_v$$

$$Y_v = X\sigma_2 (v) = X_v (j,2)\sigma = [X(j,2) \oplus v\sigma^{-1}]\sigma \quad (15)$$

$v \in P_k = 3^2 -1 = 8$

Table 2. The 9-number family F consting of the σ_2 (v) - transforms of the ternary M-sequence X.

x(j)	X(j+1)	Y_0	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8
0	0	0	1	2	3	4	5	6	7	8
0	1	3	4	5	6	7	8	0	1	2
1	1	4	5	3	7	8	6	1	2	0
1	1	4	5	3	7	8	6	1	2	0
1	0	1	2	0	4	5	3	7	8	6
0	2	6	7	8	0	1	2	3	4	5
2	1	5	3	4	8	6	7	2	0	1
1	1	4	5	3	7	8	6	1	2	0
1	2	7	8	6	1	2	0	4	5	3
2	1	5	3	4	8	6	7	2	0	1
1	0	1	2	0	4	5	3	7	8	6
0	1	3	4	5	6	7	8	0	1	2
1	0	1	2	0	4	5	3	7	8	6
0	0	0	1	2	3	4	5	6	7	8
0	2	6	7	8	0	1	2	3	4	5
2	2	8	6	7	2	0	1	5	3	4
2	2	8	6	7	2	0	1	5	3	4
2	0	2	0	1	5	3	4	8	6	7
0	1	3	4	5	6	7	8	0	1	2
1	2	7	8	6	1	2	0	4	5	3
2	2	8	6	7	2	0	1	5	3	4
2	1	5	3	4	8	6	7	2	0	1
1	2	7	8	6	1	2	0	4	5	3
2	0	2	0	1	5	3	4	8	6	7
0	2	6	7	8	0	1	2	3	4	5
2	0	2	0	1	5	3	4	8	6	7

$$X \xrightarrow{\sigma_3 (v)} Y_v$$

$$\begin{aligned} Y_v &= X\sigma_3 (v) \\ &= X_v (j,3)\sigma \\ &= [X(j,3) \oplus v\sigma^{-1}]\sigma \end{aligned} \qquad (16)$$

$$v \in P_k = 3^3 - 1 = 26$$

식(15)와 (16)에 의해 발생된 최적부호는 Table 2., Table 3.와 같다.

3. 결론

본문에서는 LEMPEL과 GREENBERGER에 의해 제안된 최적부호의 발생알고리즘및 σ_k (v)-변환에서 k=2와 k=3인 때 부호를 발생시키고 특성을 확인하였다. 본 발생부호는 Hamming 상관함수특성이 좋기때문에 FH/CDMA 용의 부호로 적절하게 이용할 수 있을 것이다.

참 고 문 헌

(1) Marvin K.Simon,Jim K.Omura, Spread-Spectrum C-ommunications,Vol.I,Computer Science press,Inc .1985

(2) G.Einarsson,"Address Assignment for a time fr-equency coded,Spread-Spectrum System",B,S,T,J, Vol.59,NO.7,pp.1241-1255,Sep.1980

(3) Timothy J.Healy,"Coding and Decoding for code Division Multiplier User Communication System" ,IEEE Trans.COMM.Vol.COM-33, pp.310-315, April 1985

(4) Abraham Lempel and Haim Greenberger, "Families of Sequences with Optimal Hamming Correlation Properties",Vol.it 20,No.1, pp.90-94, January, 1974.

Table 3. The 27-number Family F consting of the σ_3 (v) - transforms of the ternary M-sequence X.

x(j)	x(j+1)	X(j+2)	Y_0	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}	Y_{17}	Y_{18}	Y_{19}	Y_{20}	Y_{21}	Y_{22}	Y_{23}	Y_{24}	Y_{25}	Y_{26}
0	0	1	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8
0	1	1	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2
1	1	1	13	14	12	16	17	15	10	11	9	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0
1	1	0	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	9	22	23	21	25	26	24	19	20	18
1	0	2	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15
0	2	1	15	16	17	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5
2	1	1	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1
1	1	2	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	9
1	2	1	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21	7	8	6	1	2	0	4	5	3
2	1	0	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19
1	0	1	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6
0	1	0	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20
1	0	0	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24
0	0	2	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	2	2	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14
2	2	2	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13
2	2	0	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22
2	0	1	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22	26	24	25	2	0	1	5	3	4	8	6	7
0	1	2	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11
1	2	2	25	26	24	19	20	18	22	23	21	7	8	6	1	2	0	4	5	3	16	17	15	10	11	9	13	14	12
2	2	1	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4
2	1	2	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10
1	2	0	7	8	6	1	2	0	4	5	3	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21
2	0	2	20	18	19	23	21	22	26	24	25	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16
0	2	0	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23
2	0	0	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22	26	24	25