通信情報保護學會誌
第2卷 第2號, 1992. 3

코드분할 다중통신용 코드의 상호상관 특성

Crosscorrelation Properties of Sequences for Code Division Multiple Access Communication

김 철 기*

1. 서 론

코드분할 다중통신(Code Division Multiple Access Communication)은 Spread Spectrum 통신의 발전된 형태로서 군사목적상 이동 무선통신(Combat Multiple Communication)을 위해서 최근들어 급속도로 중요시 되고 있다. 잘 알려진 바와 같이 두가지 가장 일반적인 다중통신 방식은 주파수 분할 다중통신방식과 시분할 다중통신방식이다. 주파수 분할 다중통신방식에서는 모든 사용자가 각각 다른 주파수를 사용하여 동시에 신호를 보내고 시분할 다중통신방식에서는 같은 주파수를 사용하되 시간대를 달리하고 있다. 이 두가지 방식을 결합하여 모든 사용자가 같은 시각과 같은 주파수를 공유하여 통신을 가능케 할 수 있는 방식이 코드분할 다중통신이다. 여기에서 사용자는 각각 고유한 코드(수열)를 부여받는다. 따라서 CDMA통신 시스템에 사용되는 수열(코드, sequences)들은 양호한 동기 특성(synchronization properties)과 다른 수열(sequence)과 쉽게 구별되는 것이 요구된다. 동기(synchronization) 특성을 위해서는 동기가 맞을 때는 큰 자기상관(autocorrelation) 값을 갖고 동기가 안 맞을 때는 0에 가까운 자기 상관(autocorrelation) 값을 갖는 것이 요구된다. 이것은 최대 길이 수열(maximal-length sequence(m-sequence))을 이용하면 되며 상호상관(cross-correlation)값이 작으면 더욱 좋다. 작은 상호 상관(cross-correlation)값은 우선쌍(preferred pair)이라고 불리는 특정한 m-sequence 간에 얻을 수 있다. 그러나 대부분의 경우 CDMA 통신 시스템에 사용하기 위한 같은 길이의 우선쌍(perfrred pair) 숫자는 충분치 못하기 때문에, 낮은 상호 상관(cross-correlation)값을 갖는 Gold code를 사용하게 된다[3].

본고에서는 최대 길이 수열(maximal length sequence)과 우선쌍(preferred pair), 그리고 Gold code에 대해서 알아보고, 이러한 코드가 CDMA에 사용되는 실예를 제시한다.

2. Maximal Length Sequence

최대 길이 수열(maximal length sequence)의 또 다른 이름은 Pseudo-Noise sequence 또는 Pseudo-random sequence로서 주기 $N = p^n - 1$(p는 소수)를 갖는 GF(p)상에서의 최대 길이 수열(maximal

* 陸軍 3士官學校

length sequence)은 차수(degree) n의 원시다항식(primitive polynomial)에 의해 생성된다.

A = $a_0 a_1 a_2$……가 GF(p)상의 최대 길이 수열(m-seq.)라고 정의하자. a_i는 0, 1, 2,……, p−1 [GF(p)상의 정수]

만약 p=2 이면 0과 1을 갖는 2진 최대 길이 수열(m-seq.)이 된다. **A**를 생성하는 원시다항식(primitive polynomial)을

$$p(x) = x^n - c_{n-1}x \cdots - c_1 x - c_0 \qquad (1)$$

라 하자. 여기서 c_i는 GF(p)상의 원소이다. 최대 길이 수열(m-seq.) **A** = $a_0 a_1 a_2$……는 다음의 반복관계(recursion relationship)를 만족한다[1),2)].

$$a_r = \sum_{i=1}^{n} c_{n-i}\, a_{r-i} \qquad (2)$$

예를 들면, GF(2)상에서의 원시 다항식(primitive polynomial) $p(x) = x^5 + x^3 + 1$은 $a_r = a_{r-2} + a_{r-5}$의 반복관계(recursion relationship)을 만족시킨다. 이는 길이 $N = 2^5 - 1 = 31$을 갖는 최대 길이 수열(m-seq.)

A = 1010111011000111110011010010000(반복)를 생성한다.

길이 $N = p^n - 1$을 갖는 최대 길이 수열(m-seq.) **A**의 자기 상관(autocorrelation)함수는 다음과 같다.

$$R_A(\tau) = \sum_{i=0}^{N-1} \theta(a_i)\,[\theta(a_{i+\tau})]^* \qquad (3)$$

여기서 *는 복소공액(complex conjugation)을 나타낸다. 사상(mapping) θ는 최대 길이 수열(m-seq.) 각 원소를 단위원으로 1대 1 대응한다. 즉,

$$\theta(a_i) = \exp\left[\frac{j\,2\pi\,a_i}{p}\right],\ j = \sqrt{-1} \qquad (4)$$

이러한 사상(mapping)은 다음의 2가지의 자기상관 (autocorrelation) 값을 갖는다.

$$R_A(\tau) = \begin{cases} p^n - 1, & \tau = k(p^n - 1),\ k \text{ 정수} \\ -1, & \text{그밖(otherwise)} \end{cases} \qquad (5)$$

이 값은 τ = 0(동기가 맞을 때)에서 큰 최대값을 갖으며 그렇지 않을 때는 아주 작은 값(−1)을 갖으며 이는 최대값과 비교할 때 무시할 수 있는 정도의 값이다. 따라서 동기(synchronization)를 맞추기 위한 요구조건은 충족된다.

p=2이면, (4)의 사상(mapping) θ는 θ(0) = 1과 θ(1) = −1로 축약된다. 예를 들면,

p=2, n=5일때

A = 1010111011000111110011010010000(반복)

코드는 다음의 값을 갖는다.

$$R_A(\tau) = \begin{cases} 31, & \tau = 31,\ k \text{ 정수} \\ -1, & \text{그밖(otherwise)} \end{cases} \qquad (6)$$

이러한 최대 길이 수열(m-seq.)들 내에서 적당한 쌍의 최대 길이 수열(m-seq.)은 다른 쌍의 최대 길이 수열(m-seq.)보다 낮은 상호상관(cross-correlation) 값을 갖는다[3)]. 이러한 최대 길이 수열(m-seq.)들은 3종류의 상호 상관(cross-correlation) 값($n \not\equiv 0$ mod 4일때)이거나 4종류의 상호 상관(cross-correlation) 값(n=0 mod 4일때)을 갖는다.

B = $b_0 b_1 b_2$…… 이 **A** = $a_0 a_1 a_2$……의 k번째 decimation으로 구성되고,

B = **A**[k]로 기술하자. 즉 **B** = $a_0 a_k a_{2k} a_{3k}$…….

만약 **A**가 차수(degree) n을 갖는 원시다항식 g(x)로 생성된 m-seq.라 하면, **A**의 주기는 $N = p^n - 1$. 여기서 N이 k로 나누어지면 **B** = **A**[k]의 주기는 N/k이고, N과 k가 서로 소(relatively prime)일때, 최대주기 N을 갖는다. 따라서 같은 주기를 갖는 모든 최대 길이 수열(m-seq.) 셋은 한가지 최대 길이 수열(m-seq.)을 이용해 적당한 decimation에 의해서 구성될 수 있다. 예를 들면,

k = 3,

B = **A**[3] = 1011010100011101111100100110000 (반복)

여기서 3과 31은 서로 소(relatively prime)이다. 또한 **B**는 $g_B(x) = x^5 + x^3 + x^2 + x + 1$에 의해서 반복관계(recursion relationship) $b_r = b_{r-2} + b_{r-3} + b_{r-4} + b_{r-5}$에 의해서 생성될 수도 있다.

3. Preferred Pairs와 Gold Codes

두 코드 A와 B사이의 상호 상관 값은[4)]

$$R_{AB}(\tau) = \sum_{i=0}^{N-1} \theta(a_i)\,[\theta(a_{i+\tau})]^* \qquad (7)$$

(4)의 사상(mapping)을 사용하면,

$$R_{AB}(\tau) = \begin{cases} t(n)-2, & \text{또는} \\ -1, & \text{또는} \\ -t(n) \end{cases} \qquad (8)$$

여기서 $t(n)=p^{(n+e)/2}+1$이고 n이 홀수 일때 e=1과 n=2 mod 4일때 e=2의 값을 갖는다. 이러한 우선쌍(preferred pair)를 위한 충분조건은 **B**=**A**[d]일때,

$$d=p^{2k}-p^k+1 \text{ 또는},$$
$$d=2^k+1,\ p=2\ ;\ d=(p^{2k}+1)/2,\ p\neq 2 \qquad (9)$$

여기서 n이 홀수이면 (n,k)=1 (서로 소)이어야 하고 n=2 mod 4이면, gcd(n,k)=2 (최대 공약수)이어야 한다.

일반적으로 볼때 우선쌍(preferred pairs)들을 사용하지 않으면, 최대 상호 상관 값은 커진다. 따라서 큰 최대 상호 상관(cross-correlation)값으로는 동시에 같은 주파수 band내에서 다른 수열(sequence)을 분리해 내기 위한 낮은 최대 상호상관(cross-correlation)값의 조건을 만족시키기가 어렵게 되는 것이다. 예를 들면,

A = 1010111011000111110011010010000 ……과
B = **A**[3] = 1011010100011101111100100110011 … 에서 (n=5, p=2, d=3, k=1)이다. (n,k)=1 이므로 **A**와 **B**는 우선쌍(perferred pair)이다.
(8)을 사용해서 ($\theta(0)=1$과 $\theta(1)=-1$의 사상 이용)

$$R_{AB}(\tau) = \begin{cases} 7, & \text{또는} \\ -1, & \text{또는} \\ -9 \end{cases}$$

예를 들면, p=2, n=7 일 때 최대 상호상관값은 우선쌍(preferred pair)일때 17이고 그렇지 않을때 41이고, n=11일 때는 우선쌍(preferred pair)일때 65이고 그렇지 않을 때 383이다(5.9배 큰 값이다). 또한 n=0 mod 4인 우선쌍(preferred pair)일 때는 4단계 상호상관(cross-correlation)값을 갖는다. 예를 들면, **A** and **B** = **A**[$2p^{n/2}-1$]일때

$$R_{AB}(\tau) = \begin{cases} 2p^{n/2}-1, & \text{또는} \\ p^{n/2}-1, & \text{또는} \\ -1, & \text{또는} \\ -p^{n/2}-1 \end{cases} \qquad (10)$$

4. Gold Code

Gold코드는 항상 3단계 상호상관값을 갖으며 다음과 같이 표시된다[3)].

$$\mathbf{G}=\{\mathbf{A}, \mathbf{B}, \mathbf{A}+\mathbf{B}, \mathbf{A}+\mathbf{B}_1, \cdots\cdots, \mathbf{A}+\mathbf{B}_{N-1}\} \qquad (11)$$

$\mathbf{B}_i$ 는 최대 길이 수열(m-seq.) **B**의 i만큼의 왼쪽으로의 위상변화이며 **A**와 **B**는 우선쌍(preferred pair)이다. 따라서 $N+2=p^n+1$개의 코드(수열)셋이 형성되며 각각은 주기 $N=p^n-1$을 갖는다. 주의할 점은 **A**, **B**를 제외한 나머지 Gold코드(수열)는 최대 길이 수열(m-seq.)이 아닌 것이다. **A**와 **B** = **A**[3]를 사용한 Gold Code의 예는 표 1.에 있다. 이 코드는 N+2 = 33개 코드로 구성되며 N = 31이다. 이 코드셀내의 어떤 쌍에 대해서도 상호 상관(cross-correlation)값은 7, −1, −9이며 최대 자기상관(m-seq.)값은 31이다. 다른 예로 GF(3)에서 차수 3인 원시다항식 $g(x)=x^3+2x+1$을 고려하자. 반복관계 $a_r=a_{r-2}+2a_{r-3}$ 로 부터, 주기 $N=3^3-1=26$인 최대 길이 수열(m-seq.) **A** = 10121120111002021221022200 …… 를 생성한다. (9)로부터 d=5(k=1)는 **A**와 우선쌍(preferred pair)을 만족한다. **B**=**A**[5]=11120011010212221002202012 …… 는 우선쌍(preferred pair)이다. 또한 **B**는 $g_B(x)=x^3+2x^2+x+1$ 로 부터 직접 구해질 수도 있으며 반복관계 $b_r=b_{r-1}+2b_{r-2}+2b_{r-3}$ 를 만족한다. (4)으로부터 ($\theta(0)=1$, $\theta(1)=e^{j2\pi/3}$, $\theta(2)=e^{j4\pi/3}$이고 자기 상관계수

표 1. GF(2)에서 $g(x)=x^5+x^3+1$인 Gold 코드셀 (A, B=A[3])

A	1010111011000111110011010010000
B	1011010100011101111100100110000
$A+B$	0001101111011010001111110100000
$A+DB$	1111010001001001001101000001000
$A+D^2B$	1000001110000000101100011011100
$A+D^3B$	1011100001100100011100110110110
$A+D^4B$	1010010110010110000100100000011
$A+D^5B$	0010101101101111001000101011001
$A+D^6B$	0110110000010011101110101110100
$A+D^7B$	1100111110101101111101101100010
$A+D^8B$	1001111001110010110100001101001
$A+D^9B$	0011011010011101010000111101100
$A+D^{10}B$	1110001011101010100010100101110
$A+D^{11}B$	1000100011010001011011101001111
$A+D^{12}B$	0011110111001100100111001111111
$A+D^{13}B$	0110011101000010011001011100111
$A+D^{14}B$	0100101000000101000110010101011
$A+D^{15}B$	0101110010100110101001110001101
$A+D^{16}B$	0101011111110111011110000011110
$A+D^{17}B$	1101001001011111100101111010111
$A+D^{18}B$	0001000010001011111000000110011
$A+D^{19}B$	0111000111100001110110111000001
$A+D^{20}B$	0100000101010100110001100111000
$A+D^{21}B$	1101100100001110010010001000100
$A+D^{22}B$	1001010100100011000011111111010
$A+D^{23}B$	1011001100110101101011000100101
$A+D^{24}B$	0010000000111110111111011001010
$A+D^{25}B$	1110100110111011010101010111101
$A+D^{26}B$	0000110101111001100000010000110
$A+D^{27}B$	1111111100011000111010110011011
$A+D^{28}B$	0000011000101000010111100010101
$A+D^{29}B$	0111101010110000000001001010010
$A+D^{30}B$	1100010011111100001010011110001

표 2. GF(3)에서 $g(x)=x^3+2x+1$인 Gold 코드셀 (A, B=A[5])

A	10121120111002021221022200
B	11120011010212221002202012
$A+B$	21211101121211212220221212
$A+DB$	21021200210121201210012021
$A+D^2B$	22122221102221121111220111
$A+D^3B$	00102100020220020120001211
$A+D^4B$	10201222200212010211110012
$A+D^5B$	11222111000102211122200020
$A+D^6B$	21101002002001220200100100
$A+D^7B$	20220212021021011012101201
$A+D^8B$	11112012211222222102112211
$A+D^9B$	20000011110201000002222010
$A+D^{10}B$	12210000100022111000020001
$A+D^{11}B$	01010220001200202011000210
$A+D^{12}B$	22012122010011102121102002
$A+D^{13}B$	02001112101120100222120221
$A+D^{14}B$	02221010012210111202002112
$A+D^{15}B$	01120022120110221001121022
$A+D^{16}B$	20110110202111022022010122
$A+D^{17}B$	10011021022122002201201121
$A+D^{18}B$	12020102222202101020111110
$A+D^{19}B$	02111211220000122212211000
$A+D^{20}B$	00022001201010001100210202
$A+D^{21}B$	12100201011112120010202222
$A+D^{22}B$	00212202112100012110122120
$A+D^{23}B$	11002210122012200112021102
$A+D^{24}B$	22202020221101110101011220
$A+D^{25}B$	01200121212020210021212101

(autocorrelation)은 아래와 같으며,

$$R_A(\tau) = \begin{cases} 26, & \tau=26k \quad k=\text{정수} \\ -1, & \text{그밖(otherwise)} \end{cases}$$

A와 **B**의 상호 상관(cross-correlation)값은 3가지 값을 갖는다.

$$R_{AB}(\tau) = \begin{cases} 8, & \text{또는} \\ -1, & \text{또는} \\ -10 & \end{cases}$$

A와 **B**를 이용한 다진 Gold code의 예는 표 2.에 있다. 이 코드들은 $N+2 = 3^3+1=28$개로 구성되며 각각의 주기는 N=26이다. 이 코드 셀 내의 어떤 쌍도 상호 상관값은 8 또는 −1 또는 −10이다.

5. CDMA의 예

11 사용자를 가진 CDMA의 예가 표 3.에 보여진다. 첫번째 사용자는 첫번째 행의 코드를 사용하고 이때, 보내는 정보는 맨 오른쪽의 0이다. 두번째 사용자는 두번째 행의 코드를 사용하고 보내는 정보는 맨 오른쪽의 1이다. 따라서, 전체 11 사용자의 전체정보는 01100010011이다.(맨 오른쪽 열).

사상(mapping) $\theta(0)=1$과 $\theta(1)= -1$을 사용해서 각 행과 정보 01100010011을 1 −1 −1 1 1 1 −1 1 1 −1 −1로 바꾸고, 각 행의 코드와 맨 오른쪽의 정보 비트를 곱한 뒤 11개의 코드를 다 합한 값이 송수신

값 1 -1 -5 3 -1 3 1 5 3 -3 1 7 3 1 1 -3 1 3 -3 3 -1 1 3 -3 -1 5 -7 -3 -5 3 3이다. 계산하기 쉬운 방법은 1열의 값 11011110011과 정보 01100010011이 일치하는 bit수는 6개고 불일치하는 것은 5개이므로 6 × 1 + 5 × (−1) = 1 (가운데 송수신 첫번째 값)이다. 수신측에서는 송수신값에 자기의 고유코드의 사상(mapping)값을 다시 곱해서 합하면 최종 결정신호 31 -25 -33 23 31 23 -41 31 23 -41 -33(11 사용자)를 얻는다. 각 값이 0보다 크면 0으로 결정하고 0보다 작으면 1로 결정하므로 (θ(0) =1, θ(1)= −1이므로) 01100010011의 원래의 송신신호를 각각 얻는다. (여기서의 예는 잡음이 없을 때를 가정한 것임).

표 3. 표 1.의 Gold 코드셋을 이용한 11사용자를 갖는 CDMA

1 0 1 0 1 1 1 0 1 1 0 0 0 1 1 1 1 1 0 0 1 1 0 1 0 0 1 0 0 0 0	0
1 0 1 1 0 1 0 1 0 0 0 1 1 1 0 1 1 1 1 1 0 0 1 0 0 1 1 0 0 0 0	1
0 0 0 1 1 0 1 1 1 1 0 1 1 0 1 0 0 0 1 1 1 1 1 1 0 1 0 0 0 0 0	1
1 1 1 1 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 1 0 1 0 0 0 0 0 1 0 0 0	0
1 0 0 0 0 0 1 1 1 0 0 0 0 0 0 1 0 1 1 0 0 0 1 1 0 1 1 1 1 0 0	0
1 0 1 1 1 0 0 0 0 1 1 0 0 1 0 0 0 1 1 1 0 0 1 1 0 1 1 0 1 1 0	0
1 0 1 0 0 1 0 1 1 0 0 1 0 1 1 0 0 0 0 1 0 0 1 0 0 0 0 0 0 1 1	1
0 0 1 0 1 0 1 1 0 1 1 0 1 1 1 1 0 0 1 0 0 0 1 0 1 0 1 1 0 0 1	0
0 1 1 0 1 1 0 0 0 0 0 1 0 0 1 1 1 0 1 1 1 0 1 0 1 1 1 0 1 0 0	0
1 1 0 0 1 1 1 1 1 0 1 0 1 1 0 1 1 1 1 1 0 1 1 0 1 1 0 0 0 1 0	1
1 0 0 1 1 1 1 0 0 1 1 1 0 0 1 0 1 1 0 1 0 0 0 0 1 1 0 1 0 0 1	1
1-1-5 3-1 3 1 5 3-3 1 7 3 1 1-3 1 3-3 3-1 1 3-3-1 5-7-3-5 3 3	
-1-1 5 3 1-3-1 5-3 3 1 7 3-1-1 3-1-3-3 3 1-1 3 3-1 5 7-3-5 3 3	31
-1-1 5-3-1-3 1-5 3-3 1-7-3-1 1 3-1-3 3-3-1 1-3-3-1-5 7-3-5 3 3	-25
1-1-5-3 1 3-1-5-3 3 1-7-3 1-1-3 1 3 3-3 1-1-3 3-1-5-7-3-5 3 3	-33
-1 1 5-3-1-3 1 5 3 3 1 7-3 1 1 3 1 3 3-3-1-1 3-3-1 5-7 3-5 3 3	23
-1-1-5 3-1-3-1-5-3-3 1 7 3 1 1-3-1 3 3-3-1 1 3 3 1 5 7 3 5 3 3	31
-1-1 5 3 1 3 1 5 3 3-1 7 3-1 1-3 1-3 3-3-1 1-3 3-1-5 7-3 5-3 3	23
-1-1 5-3-1-3 1-5-3-3 1-7 5-1-1-3 1 3-3-3-1 1-3-3-1 5-7-3-5-3-3	-41
1-1 5 3 1 3-1-5 3 3-1 7-3-1-1 3 1 3 3 3-1 1-3-3 1 5 7 3-5 3-3	31
1 1 5 3 1-3 1 5 3-3 1-7 3 1-1 3-1 3 3-3 1 1-3-3 1-5 7-3 5 3 3	23
-1 1-5 3 1-3-1-5-3-3-1 7-3-1 1 3-1-3 3-3-1-1-3-3 1-5-7-3-5-3 3	-41
-1-1-5-3 1-3-1 5 3 3-1-7 3 1-1-3-1-3-3-3-1 1 3-3 1-5-7 3-5 3-3	-33

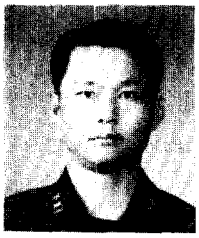
6. 결 론

CDMA 통신의 장점은 통신망의 동기화(synchronization)를 필요로하지 않는 것 즉 비동기 통신방식으로 이용할 수 있으며, 시스템상에 새로운 가입자를 증가시키기가 대단히 쉽다는 점이다. 그러나 가장 큰 이익은 자기의 고유코드가 부여되므로 정보의 노출이 쉽지 않다는 점이다. 따라서 군통신에서의 이동통신에 아주 적합하며 상업용 이동통신에서도 장차 주도적인 통신방식으로 사용될 것이다. 특히 보안이 요구되는 무선통신에 있어서는 코드길이를 길게 하고 2진코드가 아닌 다진코드를 사용함에 의해서 가입자의 증가는 물론 적의 도청이나 방해의 가능성을 줄일 수 있게 된다. 이러한 보안코드들은 어느 국가나 고유개발하여야 하므로, 국가기밀 사항에 대한 무선통신 사항, 군 상급지휘관의 무선이동통신을 위한 우리 고유의 시스템과 고유코드의 개발을 위한 연구가 필요할 것이라 생각되며, 또한 상업용 이동통신 시스템용 독자코드의 개발을 위한 연구가 진행되어야 할 것이다.

참 고 문 헌

1. R.J. McEliece, Finite Fields for Computer Scientists and Engineers. Boston, MA : Kluwer, 1987.
2. R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications. New York : Cambridge University Press, 1986.
3. R. Gold, "Maximum recursive sequences with 3-valued recursive cross-correlation functions," IEEE. Trans. Inform. Theory, vol.IT-14, pp.154-156, Jan. 1986.
4. D.V. Sarwate, "Cross-correlation Properties of Pseudorandom and Related Sequences," Proceedings of the IEEE, vol.68, No.5, May 1980.
5. S.W. Golomb, "Shift Register Sequences," Holden-Day, 1967.
6. Jong-seon No and P.V. Kumar, "A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span," IEEE Trans. On Information Theory, vol.35, No.2, Mar. 1989.
7. M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications. vol.1, Rockville, MD : Computer Science Press, 1985.

□ 著者紹介



김 철 기

1978년	육군 사관학교 졸업
1982년	연세 대학원 전자공학과(석사)
1982년~1983년	육군 사관학교 전자공학과 강사
1983년~1987년	육군 3사관학교 전자공학과 전임강사
1987년~1991년	미 Clemson University
현 재	육군 3사관학교 조교수