

Pseudonoise Code의 상관 특성에 관한 연구

이상근, 김원후

한국항공대학 항공전자공학과

A Study on Correlation Property of Pseudonoise Code

Sang Keun Lee, Won Hoo Kim

Dept. of Avionic Eng., Hankuk Aviation College

Abstract

In the case of Spread Spectrum multiple access, the interference between the PN codes must be small.

In this paper, decimation coset of maximal sequence is applied in preferred pair m-sequence, and correlation relation of preferred pair m-sequence is showed in a diagram form.

1. 서론

주파수 대역을 세분하여 사용하는 기존의 통신방식과는 반대로 전송신호를 주파수축 위에서 되도록 넓게 확산시켜 통신하는 방식인 Spread Spectrum(이하 SS)의 장점이라하면 정보의 은닉성, 비화성, 고정밀도의 거리측정, 동일 주파수대의 공용, 멀티풀 액세스, 개별 번지화, 방해간섭의 영향을 받지 않음, 과부화 통신의 가능 등을 들수있다.

이러한 SS 방식의 특색이라하면 송신측에서 고속의 Pseudo Noise Generator을 이용하여 전송신호를 주파수 대역에 매우넓게 확산시키고 수신측에서 송신측에서 사용된것과 같은 PN code를 이용하여 동기시키는 것이다. 이러한 PN code는 SS 시스템의 성능에 큰 영향을 미친다.

효율적인 PN 코드인 maximal 계열 코드의 경우 자기 상관치가 위상천이가 0 일때는 $N=2^n-1$ (n : stage 수),

0이 아닐때는 -1을 갖는다. 하지만 상호상관치는 불투명하게 어떤 값 이하로 제한이 되지 않으므로 선별적인 사용이 요구된다.

이러한 선별된 maximal 계열을 preferred m-계열, 특수 m-계열이라한다. 본 논문에서는 이러한 preferred m-계열과, 특수 m-계열을 decimation coset 이론과 컴퓨터를 이용하여 실용화 되고있는 stage 10 까지 도식화 하였다.

2. Maximal 계열의 특성

Maximal 계열 코드 (이하 m-계열)는 PN 코드의 가장 일반적인 코드이다.

m-계열의 일반적인 특성은 다음과 같다.

여기서 u는 m-계열에 속하고

n : shift register 의 수

T: 위상 천이

$Wt(u)$: u 코드의 Hamming Weight

Θ_{uv} : u 와 v 의 상호 상관함수

i, j, k: 임의의 정수

N: 주기

$$i) N = 2^n - 1$$

$$ii) T^i u + T^j u = T^k u$$

$$iii) \text{wt}(u) = 2^{n-1} = 1/2(N+1)$$

$$iv) \Theta_{uv}(l) = N \quad \text{if } l \equiv 0 \pmod{N}$$

$$\quad \quad \quad -1 \quad \text{if } l \not\equiv 0 \pmod{N}$$

v) $\tilde{u}[i] = \tilde{u}[i] \cdot (\tilde{u}:u \text{의 특성 phase})$

vi) $u[x]$ 의 주기는 $N/\text{gcd}(N, x)$ 이며 그것의 primitive 다항식의 근은 u 계열의 primitive 다항식 근의 n 번 째 데시메이션이다

vii) 계열의 종류수 = $\phi(2^n - 1)/n$
($\phi(\cdot)$: 오일러 함수)

3. Decimation Coset

m -계열의 특성 v 를 이용하여 $n=6$ 인 경우를 고찰하면 그 자체의 계열 u 의 decimation 수를 c_0 라 하면

$$c_0: 1, 2, 4, 8, 16, 32, \pmod{N=2^6-1}$$

decimation 2와 4사이의 3에 대해 c_a 를 구성하면

$$c_a: 3, 6, 12, 24, 48, 33 \pmod{N=2^6-1}$$

i) 경우는 주기 $p=63/\text{gcd}(63, 3)=21$ 이 되어 nonmaximal 하며 특성 방정식은 nonprimitive 하다.

이와 같은 방법으로 $n=6$ 일 때의 coset 를 구성하면 다음과 같다. ($n=7, 8, 9, 10$ 은 생략)

c 아래의 숫자는 primitive 다항식, 문자는 nonprimitive 다항식을 나타낸다.

$$n=6 \quad N=2^6 - 1 = 63$$

$$C_0 \quad 1 \quad 2 \quad 4 \quad 8 \quad 16 \quad 32$$

$$C_1 \quad 5 \quad 10 \quad 20 \quad 40 \quad 17 \quad 34$$

$$C_2 \quad 11 \quad 22 \quad 44 \quad 25 \quad 50 \quad 37$$

$$C_3 \quad 13 \quad 26 \quad 52 \quad 41 \quad 19 \quad 38$$

$$C_4 \quad 23 \quad 46 \quad 29 \quad 58 \quad 53 \quad 43$$

$$C_5 \quad 31 \quad 62 \quad 61 \quad 59 \quad 55 \quad 37$$

$$C_6 \quad 3 \quad 6 \quad 12 \quad 24 \quad 48 \quad 33$$

$$C_7 \quad 7 \quad 14 \quad 28 \quad 56 \quad 49 \quad 35$$

$$C_8 \quad 9 \quad 18 \quad 36$$

$$C_9 \quad 15 \quad 30 \quad 60 \quad 57 \quad 51 \quad 39$$

$n=6$ 의 coset 를 고찰하면 primitive 다항식 $h(x)$

는 6개로 $\phi(2^6 - 1)/6 = 6$ 과 일치한다.

여기서 $C_0-C_5, C_1-C_4, C_2-C_3$ 등은 $1+62=63, 5+58=63$ 등이 되어 서로 역순의 계열이다.

$n=6$ 의 coset 의 decimation 관계를 도식화 하면 그림 1과 같이 된다. 안의 숫자는 각 계열 특성 방정식의 3진법 표기이다.

ex) 155 = 001101101

$$h(x) = x^9 + x^6 + x^4 + x^3 + x + 1$$

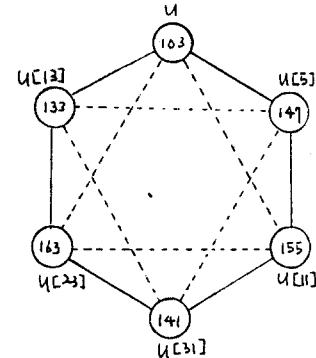


그림 1 : $n=6$ 의 decimation 관계로 대각선은 역순의 계열, 시계방향은 5, 시계 반 방향 13, 접선의 시계방향 11, 시계 반 방향 23 decimation 을 나타낸다.

4. 제한된 상호 상관치를 갖는 m -계열

PN 코드의 상호 상관함수 고찰에 있어서 모든 위상천이 l 에 대한 $\Theta_{uv}(l)$ 값 보다는 $\Theta_{uv}(l)$ 의 값의 종류와 빈도를 나타내는 스펙트럼 만으로 충분하다.

이러한 상호상관 스펙트럼은 그 자신의 계열에 의하는 것이 아니라 decimation 수에 따른다.

즉 $u=v[x]$ 이고 $x=v[a]$ 라면 $\Theta_{uv}(l)$ 의 스펙트럼은 $\Theta_{vv}(l)$ 의 스펙트럼과 같다.

a 가 $2^k + 1, 2^{2k} - 2^k + 1, 2^{3k} + 2^k + 1, 1 + 2^{\frac{k(n+2k-1)}{2}}$

등의 형식을 갖는 수 일 때 $\Theta_{uv}(l)$ 의 스펙트럼은

다음과 같이 나타난다.

(단 k 는 $n/\gcd(n, k)$ 가 홀수 이기 위한 수,

$\lfloor a \rfloor$ 는 a 의 정수부분, $e = \gcd(n, k)$)

$-1+2^{\frac{(n+e)/2}{2}}$ 가 $2^{\frac{n-e-1}{2}} + 2^{\frac{(n-e-2)/2}{2}}$ 번

-1 가 $2^{\frac{n-2}{2}-1}$ 번

$-1-2^{\frac{(n+e)/2}{2}}$ 가 $2^{\frac{n-e-1}{2}} - 2^{\frac{(n-e-2)/2}{2}}$ 번

발생한다.

n 이 4의 배수가 아니고 위와 같은 스펙트럼을 갖는 maximal 계열을 preferred pair m-계열이라 한다.

n 이 4의 배수이고 a 가 $-1+2^{\frac{(n+2)/2}{2}}$ 일 때

$\theta_{uv}(L)$ 의 스펙트럼은 다음과 같다.

$-1+2^{\frac{(n+2)/2}{2}}$ 가 $(2^{\frac{n-1}{2}} - 2^{\frac{(n-2)/2}{2}})/3$ 번

$-1+2^{\frac{n}{2}}$ 가 $2^{\frac{n}{2}}$ 번

-1 가 $2^{\frac{n-1}{2}} - 2^{\frac{(n-2)/2}{2}-1}$ 번

$-1-2^{\frac{n}{2}}$ 가 $(2^{\frac{n-1}{2}} - 2^{\frac{n}{2}})/3$ 번 발생

이와 같은 스펙트럼을 갖는 maximal 계열을 특수

m-계열이라 한다. 위의 decimation 을 만족하는

수를 $n=5\sim 10$ 에 대하여 나열하면 표 1 과 같다.

n	a
5	3, 5, 7, 11
6	5, 13
7	3, 5, 9, 11, 13, 15, 23, 27, 29, 43
8	31, 91
9	3, 5, 13, 19, 27, 47, 103, 171
10	5, 13, 17, 25, 41, 49, 79, 107, 181, 205

표 1: $n=5\sim 10$ 의 proper decimation

$n=6$ 일 때 그림 1에서 표 1의 proper decimation 수 5, 13에 대해 preferred pair를 구성 하면

133-103, 103-147 등과 같이 인접한 두개의 계열이다

$n=7$ 에서는 그림 2에서와 같이 구성되어 동시에 사용

할 수 있는 preferred pair m-계열의 수 (QMP)

6 개가 된다. 즉 7 개 이상의 시스템을 멀티풀 액세

스 하면 최대 크기가 41 까지 나타나는 바람직 하지

않은 상호 삼관함수를 나타나게 된다. (표 2 참조)

같은 방법으로 $n=8, 9, 10$ 에 대하여 preferred

m-계열과 특수 m-계열을 그림 3, 4, 5에 나타내었다.

decimation	value	frequency
3, 5, 9, 11	15	36
13, 27, 29	-1	63
43, 15, 23	-17	28
	23	7
	15	14
	7	28
7, 19, 55	-1	35
31, 63, 47	-9	28
21	-17	14
	-41	1

표 2: $n=7$ 의 crosscorrelation spectrum

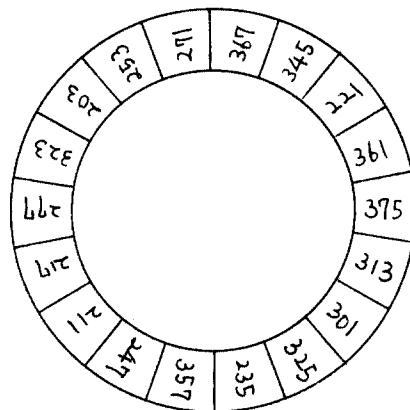


그림 2: $n=7$ 의 preferred pair m-계열

(인접한 6개의 계열), 반대편은 서로 reciprocal

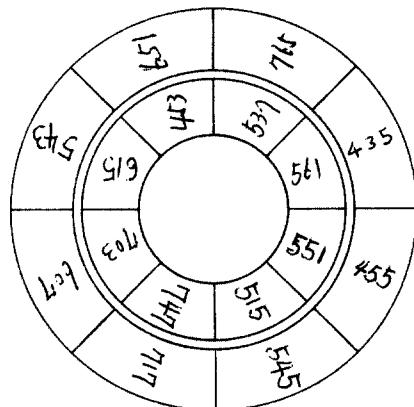


그림 3: $n=8$ 의 특수m-계열 (인접한 2개의 계열)

안과 바깥은 서로 reciprocal

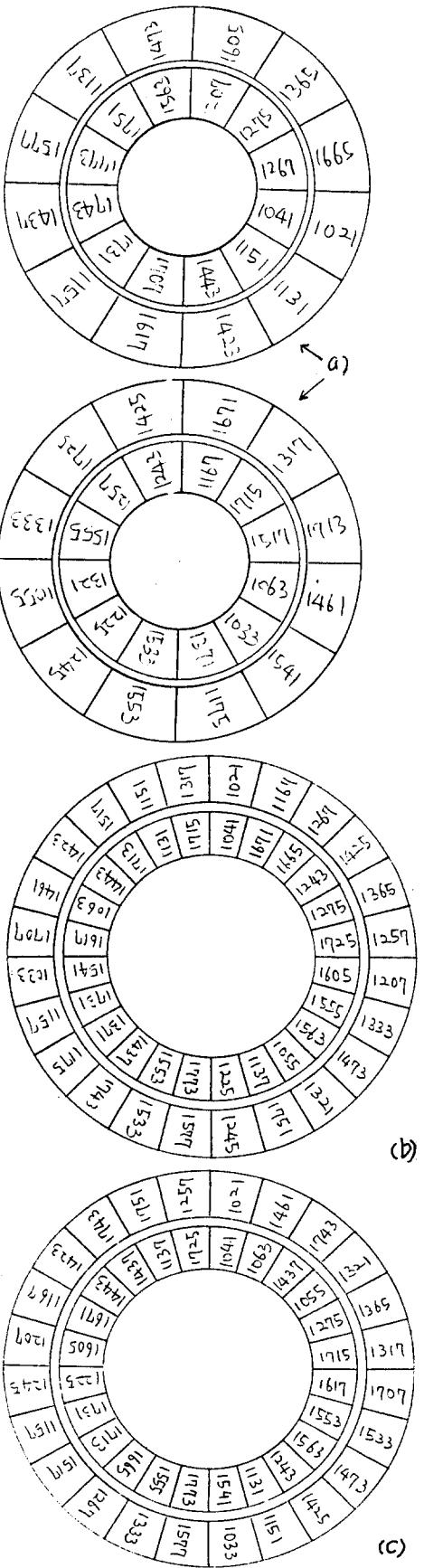
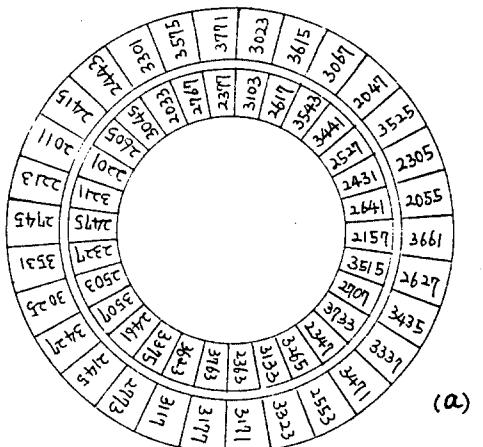
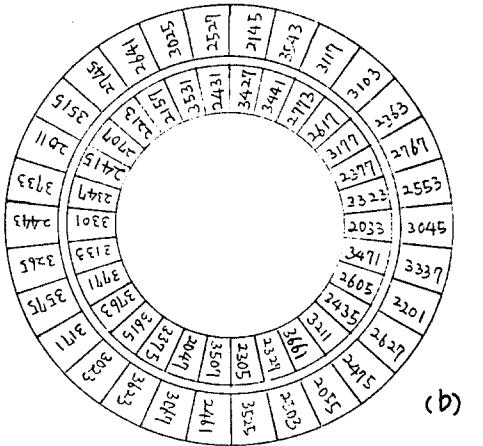


그림 4: $n=9$ 의 preferred pair m -계열, 안과
바깥은 서로 reciprocal

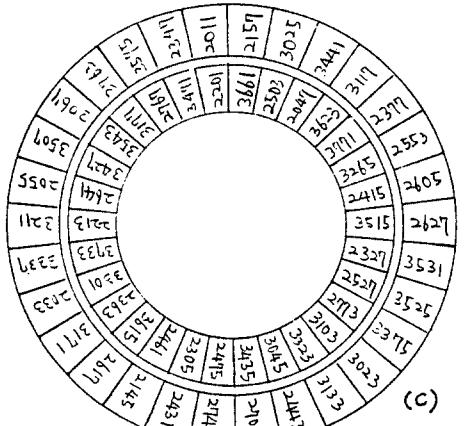
- a) 인접한 두개의 계열과 세번째 위치한 두개의 계열
- b), c) 인접한 두개의 계열



(a)



(b)



(c)

그림 5: $n=10$ 의 preferred pair m-계열

- a) 인접한 세개의 계열과 열번째 위치한 세개의 계열 (Ex: 3117-2443-2025)
안과 바깥은 서로 reciprocal
- b) 인접한 세개의 계열, 안과 바깥은 서로 reciprocal
- c) 인접한 두개의 계열, 반대면은 서로 reciprocal

5. 결 론

그림 4. a) 에서 컴퓨터에 의해 계산한 proper decimation 관계가 아닌 1021 과 1423 의 θ_m 은 65 이고 1021 과 1715 의 θ_m 은 113 이다.

$n=8$ 에서 reciprocal 계열의 θ_m 은 θ_{mp} 와 같고 $n=10$ 에서 reciprocal 계열의 θ_m 은 θ_{mp} 보다 오히려 작아 (63) 좋은 상관 특성을 나타낸다. 그러므로 $n=8$ 과 $n=10$ 에서 reciprocal 계열로도 상관 특성이 우수한 Gold 나 Kasami 코드 등을 구성 할 수 있다.

이러한 proper decimation 관계를 SS 에서 실용화 되고 있는 stage 인 $n=10$ 까지 정리함으로써 PN 코드의 효율적인 이용과 편리함을 기할수 있

도록 하였다.

참고문헌

1. W. W. Peterson and E. J. Weldon, Jr., "Error-correcting Codes", 2nd ed. Cambridge, MA: MIT Press 1972
2. Jack K. Holmes, "Coherent Spread Spectrum Systems", A Wiley-Interscience Publication, 1982
3. R. C. Dixon, "Spread Spectrum Systems", New York Wiley, 1976
4. Golomb, S. W., "Shift Register Sequence", Holden-day, 1967
5. R. Gold, "Optimal Binary Sequence for Spread Spectrum Multiplexing", IEEE Trans. Infor. Oct. 1967
6. "스펙트럼 확산 통신 방식과 그 응용분야" 전편, 전자과학, 3월호. 1984
7. Dennis A. Shedo and Dilip V. Sarwate, "Construction of Sequences with Good Correlation Properties", IEEE Trans. Inform. Jan. 1979