

# 대역확산 통신시스템을 위한 非二元 GMW 부호계열 발생 및 특성에 관한 연구

正會員 李 正 宰\* 正會員 韓 榮 烈\*\*

## A Study on the Generation and Characteristics of Non-Binary GMW Code Sequences for Spread Spectrum Communication System.

Jeong Jae LEE\*, Young Yeul HAN\*\* *Regular Members*

**要 約** Trace 사상을 이용하여 GF(2)에서 GF(p),  $p > 2$ 로 기본장을 확장한 非二元 GMW 부호계열을 발생시킬 수 있는 알고리즘을 제시하고 GF(3)와 GF(5)에서 부호계열을 각각 발생시켜 이들 부호계열은 m-계열과 같은 해밍자기상관함수 특성을 갖고 선형성에 대한 단점을 보완하며 평형특성을 갖게 됨을 보였다.

**ABSTRACT** Using the trace mapping, we suggest the generating algorithm of non-binary GMW code sequences, to expand the ground field GF(2) into GF(p),  $p > 2$ . And constructing non-binary GMW code sequences over GF(3) and GF(5), respectively, it is shown that they have the Hamming autocorrelation functions identical to m-sequences, non-linearity to improve the disadvantages of linearity, and balance properties.

### I. 서 론

Gordon, Mills와 Welch는 GF(2)에서 GMW 부호계열을 발생시킬 수 있는 알고리즘을 제안하였

으며 R.A. Scholtz와 Lloyd R. Welch 의해 대역 확산통신에 적용하기 위한 연구가 진행되었다. (1) GMW 부호계열은 m-계열과 같은 우수한 주기적인 자기상관함수 특성을 갖으며 비선형적으로 발생되어 m-계열의 선형성이 갖는 부호계열의 보안성에 대한 단점을 보완할 수 있다. 또한 한주기 동안 발생된 부호계열의 서로 다른 심볼의 갯수는 발생빈도가 한개 이상의 차이가 발생하지 않는 평형특성을 갖는다. 지금까지는 기본장을 GF(2)로 갖는 장에서 연구되어 직접대

\*東義大學校 電子通信工學科  
Dept. of Electronic Communication Engineering,  
Dongyeui Univ.

\*\*漢陽大學校 電子通信工學科  
Dept. of Electronic Communication Engineering  
Han Yang University  
論文番號 : 90-06(接受1989. 10. 2)

역확산통신(direct sequence : DS)에만 적용이 가능하며 주파수도약(frequency hopping : FH)을 위한 패턴에는 사용할 수 없었다. 본문에서는 기본장을 GF(p), p>2로 확장하여 주파수도약패턴에 적용이 가능한 非二元 GMW 부호계열을 발생시킬 수 있는 발생알고리즘을 제시하고 발생된 부호계열의 특성을 분석하였다.

### II. m-계열의 Trace 함수표현

Trace 함수는 아래와 같이 정의 되며 n이 m으로 나누어질때 GF(p<sup>n</sup>)의 원 α를 GF(p<sup>m</sup>)으로 사상시킬 수 있는 함수이다.

$$\text{tr}_m^n(\alpha) = \sum_{i=0}^{(n/m)-1} \alpha^{p^{mi}} \quad (1)$$

Trace 함수는 다음과 같은 수학적 특성을 갖는다.<sup>(2)</sup>

a).  $\text{tr}_m^n(\alpha) = \text{tr}_m^n(\alpha^{p^m}),$

$$\alpha \in \text{GF}(p^n), 0 \leq i \leq (n/m)-1 \quad (2a)$$

b).  $\text{tr}_m^n(a\alpha + b\beta) = a \text{tr}_m^n(\alpha) + b \text{tr}_m^n(\beta),$

$$a, b \in \text{GF}(p^m), \alpha, \beta \in \text{GF}(p^n) \quad (2b)$$

c).  $\text{tr}_m^n(\alpha) = b, b \in \text{GF}(p^m)$ 을 만족하는 해는  $\alpha \in \text{GF}(p^n)$  때 정확하게 p<sup>n-m</sup>개의 해를 갖는다.

$$(2c)$$

d).  $\text{tr}_1^n(\alpha) = \text{tr}_1^m(\text{tr}_m^n(\alpha), \alpha \in \text{GF}(p^n)) \quad (2d)$

m-계열 {b<sub>n</sub>}을 발생시킬 수 있는 원시다항식은 다음과 같다.

$$m_\alpha(x) = x^n + \sum_{i=1}^n m_i x^{n-i}, m_i \in \text{GF}(p) \quad (3)$$

α를 GF(p<sup>n</sup>)의 원시원이라 하면 계열 {b<sub>n</sub>}은 Trace 함수와 다음과 같은 관계를 갖는다.

$$b_n = \text{tr}_1^n(\alpha^n) \quad (4)$$

m-계열 발생에 사용된 쉬프트 레지스터의 초기조건에 따라 b<sub>n</sub>과 Trace 함수와 일치하지 않고 일정한 간격으로 지연될 수 있으나 순환적이므로 같은 개념이 된다.

### III. 非二元 GMW 부호계열 발생 알고리즘

非二元 GMW 부호계열 {c<sub>j</sub>}은 GF(p)에서 다음과 같이 정의된다.

$$c_j = \text{tr}_1^m([\text{tr}_m^n(\alpha^j)]^r) \quad (5)$$

여기서 α는 GF(p<sup>n</sup>)의 원시원이며 r은 p<sup>m</sup>-1과 상대적으로 소수인 정수로서 0 < r ≤ p<sup>m</sup>-1이다. r=1이면 (2d)에서 GF(p)에서의 m-계열의 특성을 갖게 된다.

T를 GF(p<sup>m</sup>)의 원소로서 α의 가장 적은 거듭제곱이라 하면 T=(p<sup>n</sup>-1)/(p<sup>m</sup>-1)로서 정의되며 다음 단계에 의하여 非二元 GMW 부호계열이 발생된다.

단계 1 : GF(p<sup>n</sup>)의 원시원을 α라 하고 0을 제외한 모든 원을 n차 m-계열발생기를 이용하여 GF(p)에서 n 차원 벡터로 표현한다.

단계 2 : GF(p<sup>n</sup>)의 0을 제외한 모든 원을 n/m 차 m-계열발생기를 이용하여 GF(p<sup>n</sup>)에서 n/m 차원 벡터로 표현하여 tr<sub>m</sub><sup>n</sup>(α<sup>j</sup>)를 구한다.

단계 3 : tr<sub>m</sub><sup>n</sup>(α<sup>j</sup>)로 표현된 GF(p<sup>m</sup>) 상의 주기 p<sup>n</sup>-1인 모든 원을 r승으로 변환한뒤 Trace 변환을 통하여 GF(p) 상의 원으로 변환시킨다.

#### IV. 非二元 GMW 부호계열 특성

##### 1. 해밍자기상관함수 특성

非二元 GMW 계열  $\{c_j\}$ 의 해밍자기상관함수는 다음과 같이 정의된다.

$$P_{cc}(\tau) = \sum_{j=0}^{p^n-2} h[c_j, c_{j+\tau}] \quad (6)$$

여기서

$$h[c_j, c_{j+\tau}] = \begin{cases} 1, & c_j = c_{j+\tau} \\ 0, & c_j \neq c_{j+\tau} \end{cases} \quad (7)$$

이다. 따라서  $0 \leq j < p^n - 1$ 인 범위에서  $c_j - c_{j+\tau} = 0$ 이 되는 회수를 계수하면 된다.

Trace 함수의 선형성을 이용하면

$$\begin{aligned} c_j - c_{j+\tau} &= \text{tr}_1^m \left( \left[ \text{tr}_m^n (\alpha^j) \right]^r \right. \\ &\quad \left. - \text{tr}_1^m \left( \left[ \text{tr}_m^n (\alpha^{j+\tau}) \right]^r \right) \right) \\ &= \text{tr}_1^m \left( \left[ \text{tr}_m^n (\alpha^j) \right]^r - \left[ \text{tr}_m^n (\alpha^{j+\tau}) \right]^r \right) \end{aligned} \quad (8)$$

$$\delta(j, \tau) = \left[ \text{tr}_m^n (\alpha^j) \right]^r - \left[ \text{tr}_m^n (\alpha^{j+\tau}) \right]^r = 0 \quad (9)$$

을 만족하는 경우의 수는  $r$ 의 값과 무관하므로

$$\text{tr}_m^n (\alpha^j) - \text{tr}_m^n (\alpha^{j+\tau}) = \text{tr}_m^n (\alpha^j(1 - \alpha^\tau)) = 0 \quad (10)$$

$\tau=0$ 면  $j$ 의 값에 관계없이 항상 성립한다. 따라서  $P_{cc}(\tau) = p^n - 1$ 이다.

$\tau \neq 0$ 면  $\text{tr}_m^n (\alpha^j(1 - \alpha^\tau)) = 0$ 을 만족하는 경우는 (2c)에서  $p^{n-m}$ 개가 발생한다. 같은 방법으로  $\text{tr}_1^m (\delta(j, \tau)) = 0$ 을 만족하는 경우는  $p^{m-1}$ 개가 발생되므로  $j$ 의 변화에 따른 총 경우의 수는

$(p^{n-m})(p^{m-1}) = p^{n-1}$ 개가 발생되며 원이 0인 경우는 다른 원에 비하여 쉬프트 레지스터의 내용이 전부 0인 상태로 되지 않기 때문에 1개가 부족하게 된다. 따라서 이를 종합하여 표현하면 해밍자기상관함수는

$$P_{cc}(\tau) = \begin{cases} p^n - 1, & \tau = 0 \\ p^{n-1} - 1, & \tau \neq 0 \end{cases} \quad (11)$$

이 된다.

##### 2. 평형특성

$\text{tr}_m^n (\alpha^j)$ 은  $m$ -계열로서 선형스펜은  $n/m$ 이며 이 계열의 한주기에서  $k$ -tuples  $c'_1, c'_2, \dots, c'_k$ 이  $N_{c'}$ 회 발생한다면  $m$ -계열의 평형특성에서<sup>2)</sup>

$$N_{c'} = \begin{cases} p^{m(n-m-k)}, & c' \neq 0, 1 \leq k \leq n/m \\ p^{m(n-m-k)} - 1, & c' = 0, 1 \leq k \leq n/m \end{cases}$$

이 되며  $r$ 이  $p^m - 1$ 과 상대적으로 소수이기 때문에  $\left[ \text{tr}_m^n (\alpha^j) \right]^r$ 의  $r$ 승은 1:1로 자신의 장에 사상한다.  $Sc'$ 를  $GF(p^m)$ 에 대한  $k$ -tuples  $c'$ 의 집합이라 하고  $c$ 로 Trace 사상한다고 하면

$$c_i = \text{tr}_1^m (c'_i), \quad i=1, 2, \dots, k$$

의 관계를 갖는다. 전부 0인  $k$ -tuple은 그 자신으로 사상하고  $\{c_i\}$ 의 한주기에서  $c$ 의 발생회수는

$$N_c = \sum_{c' \in S_{c'}} N_{c'}$$

로 주어진다.

$c_i$ 로 사상하는  $GF(p^m)$ 의 원의 수는  $p^{m-1}$ 이며  $k$ -tuples  $c'$ 에 대하여

$$Sc' = (p^{m-1})^k$$

가 된다.  $c \neq 0$  즉,  $0 \notin Sc'$ 이면

$$Nc = |Sc'| p^{m(n-m)k} = (p^{m-1})^k p^{n-mk} = p^{n-k}, \underline{c} \neq \underline{0}$$

그리고

$$Nc = -1 + \sum_{\underline{c}' \neq \underline{0}} Nc' = p^{n-k} - 1, \underline{c} = \underline{0}$$

으로 되며 이를 종합하면

$$Nc = \begin{cases} p^{n-k}, \underline{c}' \neq \underline{0}, 1 \leq k \leq n/m \\ p^{n-k} - 1, \underline{c}' = \underline{0}, 1 \leq k \leq n/m \end{cases} \quad (12)$$

이다.

### 3. 非二元 GMW 부호계열군

Ngmw를 발생될 수 있는 부호계열의 군이라 하면 주어진 n과 m에 의하여

$$Ngmw = Np(n) Np(m) \quad (13)$$

로 주어지며 여기서 N(d)는 GF(p)에서 차수 d인 원시다항식의 수를 나타낸다.

### V. 非二元 GWM 부호계열 발생

非二元 GMW 부호계열 모델로 p=3, 5, n=4, m=2인 경우를 택하고 GF(3)에서의 원시다항식을  $x^4+x^3+2$ , GF(5)에 대한 원시다항식을  $x^4+x^3+x+3$ 이라 하고(3),(4)이들의 원시원을 각각  $\alpha$ ,  $\beta$ 라 하면 두 경우에 대한 非二元 GMW 부호계열은

$$\begin{aligned} \{a_j\} &= \text{tr}_1^m \{ [\text{tr}_m^n (\alpha^j)] \} \\ &= \text{tr}_1^2 \{ [\text{tr}_2^4 (\alpha^j)] \} \end{aligned} \quad (14)$$

$$\{b_j\} = \text{tr}_1^m \{ [\text{tr}_m^n (\beta^j)] \}$$

$$\text{tr}_1^2 \{ [\text{tr}_2^4 (\beta^j)] \} \quad (15)$$

로 나타낼 수 있다. 그림 1은 GF(3)에서 GF(3<sup>4</sup>)의 m-계열 발생기이며 그림 2는 GF(5)에서 GF(5<sup>4</sup>)의 m-계열 발생기를 나타내고 있다. 그림 1로부터 발생되는 GF(3<sup>4</sup>)의 원으로 표현되는 GF(3<sup>2</sup>)에서의 원시다항식  $x^2+\alpha^{70}+\alpha^{50}$ 을 이용하고 그림 2로부터 발생되는 GF(5<sup>4</sup>)의 원으로 표현되는 GF(5<sup>2</sup>)에서의 원시다항식  $x^2+\beta^{234}+\beta^{338}$ 을 이용하여  $\text{tr}_2^4 (\alpha^j)$ 과  $\text{tr}_2^4 (\beta^j)$ 를 발생한다. 그림 3, 그림 5는 이들의 관계를 보여주고 있다.

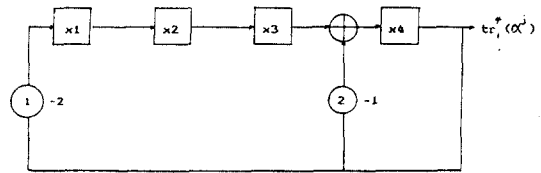


그림 1. GF(3)에서 GF(3<sup>4</sup>)의 m-계열발생기  
M-sequence generator of GF(3<sup>4</sup>) over GF(3).

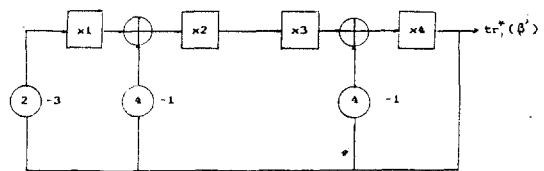


그림 2. GF(5)에서 GF(5<sup>4</sup>)의 m-계열발생기  
M-sequence generator of GF(5<sup>4</sup>) over GF(5).

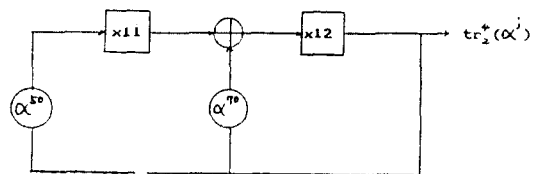


그림 3. GF(3)에서 GF(3<sup>4</sup>)의 m-계열발생기  
M-sequence generator of GF(3<sup>4</sup>) over GF(3<sup>2</sup>)

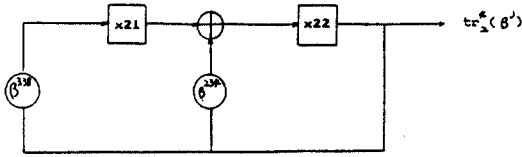


그림 4. GF(5<sup>2</sup>)에서 GF(5<sup>4</sup>)의 m-계열발생기  
M-sequence generator of GF(5<sup>4</sup>) over GF(5<sup>2</sup>)

그림 3에 의해 발생된  $tr_2^4(\alpha^i)$ 는 GF(3<sup>4</sup>)에서 GF(3<sup>2</sup>)으로 사상하며 GF(3<sup>2</sup>)은 0을 포함하여 9개의 원을 갖게 되며  $T = (3^4 - 1) / (3^2 - 1) =$

표 1. GF(3<sup>2</sup>)의 원  $\mu$ 에 대한 GF(3)의 4차원 벡터표현과  $tr_1^2(\mu^i)$ 의 관계

The relation between vector representation of elements of GF(3<sup>2</sup>),  $\mu$ , over GF(3) and  $tr_1^2(\mu^i)$

GF(3 <sup>2</sup> )의 원 $\mu$	x1 x2 x3 x4	$tr_1^2(\mu)$	$tr_1^2(\mu^2)$	$tr_1^2(\mu^3)$	$tr_1^2(\mu^4)$
0	0 0 0 0	0	0	0	0
1	1 0 0 0	2	2	2	2
$\alpha^{10}$	1 0 2 1	1	1	2	2
$\alpha^{20}$	2 0 2 1	0	0	0	0
$\alpha^{30}$	0 0 1 2	1	1	2	2
$\alpha^{40}$	2 0 0 0	1	1	1	1
$\alpha^{50}$	2 0 1 2	2	2	1	1
$\alpha^{60}$	1 0 1 2	0	9	0	0
$\alpha^{70}$	0 0 2 1	2	2	1	1

표 2. GF(5<sup>2</sup>)의 원  $\xi$ 에 대한 GF(5)의 4차원 벡터표현과  $tr_1^2(\xi^i)$ 의 관계

The relation between vector representation of elements of GF(5<sup>2</sup>),  $\xi$ , over GF(5) and  $tr_1^2(\xi^i)$ .

GF(5 <sup>2</sup> )의 원 $\xi$	y1 y2 y3 y4	$tr_1^2(\xi)$	$tr_1^2(\xi^2)$	$tr_1^2(\xi^3)$	$tr_1^2(\xi^4)$
0	0 0 0 0	0	0	0	0
1	1 0 0 0	4	4	4	4
$\beta^{26}$	2 2 1 3	3	1	2	4
$\beta^{52}$	1 3 4 2	4	1	4	1
$\beta^{78}$	0 3 4 2	0	0	0	0
$\beta^{104}$	3 1 3 4	2	2	2	2
$\beta^{130}$	2 3 4 2	3	1	2	4
$\beta^{156}$	2 0 0 0	3	2	3	2
$\beta^{182}$	4 4 2 1	1	3	4	2
$\beta^{208}$	2 1 3 4	3	3	3	3
$\beta^{234}$	0 1 3 4	0	0	0	0
$\beta^{260}$	1 2 1 3	4	1	4	1
$\beta^{286}$	4 1 3 4	1	3	4	2
$\beta^{312}$	4 0 0 0	1	1	1	1
$\beta^{338}$	3 3 4 2	2	4	3	1
$\beta^{364}$	4 2 1 3	1	4	1	4
$\beta^{390}$	0 2 1 3	0	0	0	0
$\beta^{416}$	2 4 2 1	3	3	3	3
$\beta^{442}$	3 2 1 3	2	4	3	1
$\beta^{468}$	3 0 0 0	2	3	3	3
$\beta^{494}$	1 1 3 4	4	2	1	3
$\beta^{520}$	3 4 2 1	2	2	2	2
$\beta^{546}$	0 4 2 1	0	0	0	0
$\beta^{572}$	4 3 4 2	1	4	1	4
$\beta^{598}$	1 4 2 1	4	2	1	3

10의 배수를  $\alpha$ 의 거듭제곱으로 갖는다. 즉  $\{\alpha^{10^i} \mid i=0, 1, 2, \dots, 7\}$ 이 되며 이를 원으로 하여 주기  $3^4-1=80$ 인 계열을 발생한다. 한편 그림 4에 의해 발생된  $\text{tr}_2^4(\beta^i)$ 은  $\text{GF}(5^4)$ 에서  $\text{GF}(5^2)$ 으로 사상하며  $\text{GF}(5^2)$ 은 0을 포함하여 26개의 원을 갖으며 그 중 25개의 원은  $T=(5^4-1)/(5^2-1)=26$ 의 배수를 각각  $\beta$ 의 거듭제곱으로  $\{\beta^{26^i} \mid i=0, 1, 2, \dots, 24\}$ 의 원들을 갖게 되며 주기  $5^4-1=624$ 의 주기를 갖는 계열이 된다. 표1,

표2는 이들 원들과  $\text{GF}(p^2)$ 에서  $\text{GF}(p)$ 로 사상하는 Trace 변환과의 관계를 나타낸다. 표1에서  $r$ 은  $3^2-1=8$ 과 상대적으로 소수인 정수로서  $0 < r < 8$ 인 범위에서 구할 수 있으며 1, 3, 5, 7 중에서 택할 수 있으나 표1에서 알 수 있는 바와 같이  $r=1, r=3$  일때와  $r=5, r=7$ 일 경우 동일한 계열을 발생하게 된다. 따라서  $r=1$  과  $r=5$ 인 두 경우에 발생된 非二元 GMW 부호계열은 표3과 같다.

표 3.  $\text{GF}(3)$ 에서 非二元 GMW 부호계열( $r=1, r=5$ )  
Non-binary GMW code sequences for  $r=1$  and  $r=5$  over  $\text{GF}(3)$

$r=1$ :	1212201112222020211201021002212022002000
	2121102221111010122102012001121011001000
$r=5$ :	1111101221121020111202012001121012001000
	2222202112212010222101021002212021002000

표 4.  $\text{GF}(5)$ 에서 非二元 GMW 부호계열( $r=17$ )  
Non-binary GMW code sequence for  $r=17$  over  $\text{GF}(5)$

$r=17$ :	40433 02303 40404 33121 323120 42222 34423 11100 41203 411342
	14200 12442 02003 43143 413324 02344 32120 21201 13132 143222
	22033 33024 41403 02440 002032 43144 20233 24203 20044 230403
	20244 01404 20202 44313 414310 21111 42214 33300 23104 233421
	32100 31221 01004 24324 234412 01422 41310 13103 34341 324111
	11044 44012 23204 01220 001041 24322 10144 12104 10022 140104
	10122 03202 10101 22434 232430 13333 21132 44400 14302 144213
	41300 43113 03002 12412 142231 03211 23430 34304 42423 412333
	33022 22031 14102 03110 003023 12411 30322 31302 30011 320102
	30311 04101 30303 11242 141240 34444 13341 22200 32401 322134
	23400 24334 04001 31231 321143 04133 14240 42402 21214 231444
	44011 11043 32301 04330 004014 31233 40411 43401 40033 410301

표 2에서  $r$ 은  $5^2-1=24$ 와 상대적으로 소수인 정수로서  $0 < r < 24$ 인 범위에서 구하며 1, 5, 7, 11, 13, 17, 19, 23 중에서 택할 수 있으나  $r=1$ 과  $r=5, r=7$ 과  $r=11, r=13,$ 과  $r=17, r=19$ 와

$r=23$ 은 동일계열을 발생하며 각각 서로 다른 부호계열 4종류를 발생시킬 수 있으나 그중  $r=17$ 을 택하여 발생된 非二元 GMW 부호계열은 표 4와 같다.

표 5. 주기 80인 非二元 GMW 부호계열의 k-tuple 분포 (r=5)  
 K-tuple statistics for the non-binary GMW code sequence of length 80 for r=5

k	k-tuple: 발생빈도
1	(0:26), (1:27), (2:27)
2	(00:8), (01:9), (02:9), (10:9), (11:9), (12:9), (20:9), (21:9) (22:9)
3	(000:2), (001:3), (002:3), (010:3), (011:3), (012:3), (020:3) (021:3), (022:3), (100:3), (101:3), (102:3), (110:1), (111:4) (112:4), (120:5), (121:2), (122:2), (200:3), (201:3), (202:3) (210:5), (211:2), (212:2), (220:1), (221:4), (222:4)

표 6. 주기 624인 非二元 GMW 부호계열의 k-tuple 분포 (r=17)  
 K-tuple statistics for the non-binary GMW code sequence of length 624 for r=17.

k	k-tuple: 발생빈도
1	(0:124), (1:125), (2:125), (3:125), (4:125)
2	(00:24), (01:25), (02:25), (03:25), (04:25), (10:25), (11:25), (12:25) (13:25), (14:25), (20:25), (21:25), (22:25), (23:25), (24:25), (30:25) (31:25), (32:25), (33:25), (34:25), (40:25), (41:25), (42:25), (43:25) (44:25)
3	(000:4), (001:5), (002:5), (003:5), (004:5), (010:5), (011:5), (012:9) (013:1), -----

표 5, 표 6에서와 같이 발생된 계열은 1-tuple  
 과 2-tuple에서 평형특성을 갖는다. 그림 5a와

그림 5b는 두 경우의 정규화된 해밍자기상관함  
 수  $P_{cc}(\tau) / (p^n - 1)$ 를 나타낸다.

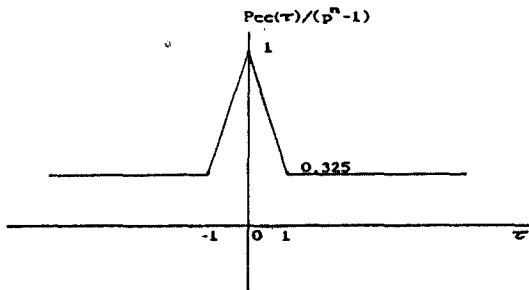


그림 5a. GF(3)에서 非二元 GMW 부호계열의 해밍자기상관  
 함수 특성  
 Hamming autocorrelation characteristics  
 of non-binary GMW code sequence over GF(3).

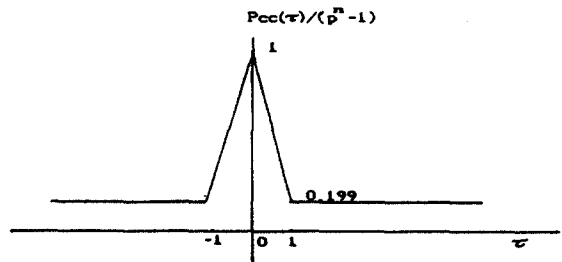


그림 5b. GF(5)에서 非二元 GMW 부호계열의 해밍자기상관  
 함수 특성  
 Hamming autocorrelation characteristics  
 of non-binary GMW code sequence over GF(5).

각 그림에서  $\tau=0$  때 1과  $\tau \neq 0$  경우  $r$ 의 값과 관계없이 그림 5a에서 0.325, 그림 5b에서 0.199 값을 갖게 되어  $m$ -계열의 특성과 일치하고 주기가 길어지면 해밍자기상관함수 값이 줄어 들게 됨을 알 수 있다. 이 해밍자기상관함수 값은 Kumar<sup>(6)</sup>에 의해 제안된 부호계열의 해밍자기상관함수  $(p^{n-1}+p^{n-2}-p^{n-2-1}) / (p^{n-1})$  값 0.425와 0.232에 비하여 특성이 좋다. 발생될 수 있는 계열군은 GF(3)에서 차수 4와 2인 원시다항식 숫자는 각각  $N_p(4)=8$ ,  $N_p(2)=2$ 로서  $Ngmw=16$ 개를 발생시킬 수 있고 GF(5)에서는  $N_p(4)=48$ ,  $N_p(2)=4$ 로서  $Ngmw=192$ 개를 발생시킬 수 있다.

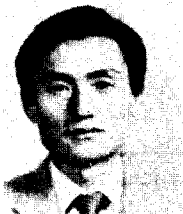
## VI. 결 론

본 논문에서는 GF(p),  $p>2$ 에서 발생될 수 있는 비二元 GMW 부호계열에 대한 발생 알고리즘을 제시하고, GF(3)와 GF(5)에서 발생된 부호계열이 평형특성을 갖고 해밍자기상관함수가  $m$ -계열과 같은 우수한 특성을 갖으며, 비선형적으로 발생되므로  $m$ -계열이 갖는 선형성에 대한 단점을 보완할 수 있음을 보였다. 한편 비二元 GMW 부호계열은  $\tau \neq 0$ 을 제외한 해밍자기상관함수 특성이 Kumar에 의해 제안된 부호

계열과 비교하여 우수하나 해밍상호상관함수 특성이 뒤떨어지며, 부호계열을 발생시키기 위해서는 관련된 원시다항식이 적절히 선택되어 사용되어야 한다.

## 參 考 文 獻

1. R.A. Scholtz and L.R. Welch, "GMW sequences", IEEE Trans. Inform. Theory, IT-30, pp. 548~553, May 1984.
2. Marvin K. Simon and Jim K. Omura, Spread Spectrum communications, Vol. I, Computer science press, Inc. 1985.
3. William W. Wu, Elements of Digital Satellite Communication, Vol. II, Computer science press, Inc. 1984.
4. F.J. Mac Williams and N.J.A. Sloane, The theory of Error-Correcting Codes, north-holland publishing co., 1977.
5. Kumar, P.V., "On Bent Sequences and Generalized Bent Functions", Ph. D. Dissertation in Electrical Engineering, University of Southern California, August 1983.



李 正 宰 (Jeong Jae LEE) 正會員  
 1950年 6月30日生  
 1973年 2月: 西江大學校 電子通信工學科 卒業  
 1984年 2月: 漢陽大 産業大學院 電子工學科 卒業(工學碩士)  
 1987年 2月: 漢陽大 大學院 電子通信工學科 博士課程 修了  
 1979年 2月~1984年11月: 韓國機械研究所 研究員  
 1986年 9月~1987年 2月: 三星綜合技術院 先任研究員

1987年 3月~現在: 東義大學校 電子通信工學科 專任講師



韓 榮 烈 (Young Yeul HAN) 正會員  
 1938年 6月10日生  
 1960年 2月: 서울大學校 電子工學科 卒業  
 1976年 5月: 美利주리大學校(工學碩士)  
 1979年 5月: 美利주리大學校(工學博士)  
 1961年 8月~64年 8月: 西獨Siemens社 勤務  
 1969年 8月~70年 9月: KAIST 勤務  
 1980年 1月~80年 9月: ADD 勤務

IEEE Senior member, member of sigma Xi

現在: 漢陽大學校 電子通信工學科 教授