論 文

# 多元接續(MA)通信시스템을 爲한 複合符號系列 發生 및 特性에 關한 硏究

正會員 李 正 宰*

# A Study on the Composite Code Sequence for CDMA Communication systems

Jeong Jae Lee* *Regular Member*


## 要 約

多重의 非線形性을 위한 변환을 시행하여 발생되는 符號系列로서 Kasami 符號系列, GMW 符號系列, 그리고 No-Kumar 符號系列의 構造的인 특성을 複合的으로 가질 수 있는 複合符號系列을 제시한다. 본 논문에서 제시된 符號系列은 간단한 變數의 변경으로 旣存 符號系列의 發生알고리듬으로 쉽게 변형될 수 있는 특성을 갖고 있다.

컴퓨터 시뮬레이션과 實驗을 통하여 複合符號系列은 쉬프트레지스터 段數 n=0(mod 4)에서 發生週期 $2^n-1$, 發生群 $2^{n/2}$, 最大相關函數 $2^{n/2}+1$을 가지며 複雜度(linear span)의 改善效果를 期待할 수 있음을 보였다.

## ABSTRACT

The composite code sequence generating algorithm based on multiple nonlinear transformation is to be presented. The algorithm suggested here can reproduce, through composite structured characteristics, the other code sequence generating algorithms such as Kasami, GMW, and No-Kumar code sequence by changes of few simple parameters inherent to the multiple nonlinear transformation.

Computer simulations and experiments show that the above composite code sequence presented has a characteristic of period $2^n-1$, family $2^{n/2}$, and maximum correlation function $2^{n/2}+1$ at shift register stage n=0(mod 4) and can be expected to improve the effect of linear span.


## Ⅰ. 서 론

符號分割多元接續(code division multiple access :CDMA) 통신시스템은 帶域擴散의 방법으로 각 이용자가 수신기에서 정보신호를 분리하여 추출할 수 있는 고유 擴散符號系列을 할당 받아 대역을 확산시킨다. 그러므로 이용자간의 시간적 제약을 받지않고 동시에 여러 이용자의 교신이 가능한 시스템이다. 따라서 통신대역을 확산하기 위한 固有擴散符號

*東義大學校 電子通信工學科
Dept. of Electronic Communication Engineering, Dongeui Univ.
論文番號 : 93-28

系列의 발생은 CDMA 통신시스템의 핵심과제로 되어있다.[1-5]

帶域擴散을 위한 擴散符號系列로 自己相關函數 특성이 우수한 M-계열이 오래동안 이용되어 왔으나 DS-CDMA에서는 自己相關函數 특성 못지않게 相互相關函數특성이 중요시 되고 있다. 이를 위해 M-계열발생기를 조합 또는 변형하여 만든 대표적인 부호로서 Gold 符號系列, Kasami 符號系列 등이 있으나[6][7], 이들 線形符號系列의 보안성 증가를 위하여 複雜度가 큰 非線形符號系列에 대한 연구가 계속되고 있으며 발생된 符號系列의 複雜度는 線形스팬(linear span)으로 측정된다[8-13].

Gole, Kasami, OSW[14], No-Kumar[15], GMW[16], 符號系列 그리고 Kasami와 OSW符號系列을 결합한 Kasami-OSW 符號系列[17]은 주어진 週期 N과 發生群 V로부터 Welch 한계[6]를 만족하는 相關函數 특성을 갖는 符號系列들이다. OSW符號系列, No-Kumar 符號系列 그리고 Kasami-OSW 符號系列은 非線形的으로 방어 능력이 뛰어나다. N과 V가 주어진 상태에서 相關函數 最大値가 적절한 값을 갖고 다중의 복잡성을 위한 非線形結合을 통하여 새로운 非線形符號系列인 複合符號系列을 형성할 수 있다.[10]

본 論文을 통하여 제 Ⅱ장에서는 複合符號系列의 발생알고리듬 제시와 특성에 대하여 검토하여 제 Ⅲ장에서는 複合符號系列 발생을 위한 발생기를 구성하고 실험을 통하여 이론적인 분석의 타당성을 확인한다.

## Ⅱ. 複合符號系列의 발생알고리듬

$F_2=GF(2^m)$, $F_3=GF(2^{2m})$이 각각 有限場 $F_0=GF(2)$의 m과 2m의 擴大場이고 $Tr_{2m,m}(x)=x+x^{2^m}$를 元 x의 $F_3$에서 $F_2$로 寫像하는 函數라 하자. 또한 $\alpha$와 $\beta=\alpha^{2^m}+1$을 각각 有限長 $F_3$와 $F_2$의 原始元이라면 非線形符號系列의 발생알고리듬은 다음과 같은 형태로 정의된다.

$$s_z(t)=e(Tr_{m_1,1}(Tr_{m,m_1}(\beta_z\alpha^{(2m+1)t}+Tr_{2m,m}(\alpha^{2t}))^r)^{r_1}) \quad (1)$$

여기서 매개변수 m은 두개의 자연수 $m_1$과 $m_2$의 곱, 즉 $m=m_1m_2$이다.

$F_1=GF(2^{m_1})$, $Tr_{m,m_1}(x)$는 x를 $F_2$에서 $F_1$으로 寫像시키고 또한 $Tr_{m_1,1}(x)$는 $F_1$上의 x를 $F_0$로 寫像시키는 函數다. $r_1$은 자연수로서 $1\leq r_1<2^{m_1}-1$, $(r_1, 2^{m_1}-1)=1$을 만족한다. 또 r은 $0\leq r<2^m-1$, $(r, 2^m-1)=1$로 한다.

$Tr_{m,1}(Tr_{2m,m}(x))=Tr_{2m,1}(x)$는 $x\in F_3$에서 $F_0$로의 寫像이다. $e(\cdot)$는 $F_0$의 중요하지 않는 성질이며 $e(0)=1$, $e(1)=-1$이다. 그리고

$Tr_{m_1,1}(x)=\sum_{j=0}^{m_1-1} x^{2^j}$는 $x\in F_2$를 $F_0$로 寫像시키는 函數로 정의한다.

符號語 $c(a_1, a_2)$, $a_1\in F_2$, $a_2\in F_3$의 원소들 $c_t(a_1, a_2)$를 아래와 같이 정의할때,

$$c_t(a_1, a_2)=\phi[a_1\alpha^{(2m+1)t}+Tr_{2m,m}(a_2\alpha^{2t})^r], \quad t=0, 1, \cdots, 2^{2m}-2 \quad (2)$$

여기서 r은 $2^m-1$과는 서로 素, 즉 $(r, 2^m-1)=1$이다. $F_2$에서 $F_0$로 寫像시킬 수 있는 $\phi$를 이용하여 다음과 같은 관계를 갖는 식을 정의 할 수 있다[10].

$$\sum e(\phi(h_x)+\phi(t_x))=\begin{cases}-1, & h\neq t,\\ 2^m-1, & h=t_x\in F_2-\{0\}\end{cases} \quad (3)$$

여기서 h, $t\in F_2$다. 두벡터 $s(a_1, a_2)$와 $s(b_1, b_2)$를 아래와 같이 정의하면

$$s(b_1, b_2)=(e(c_0(b_1, b_2)), e(c_1(b_1, b_2)), \cdots, e(c_{2^{2m}-2}(b_1, b_2))),$$
$$s(a_1, a_2)=e(c_0(a_1, a_2)), e(c_1(a_1, a_2)), \cdots, e(c_{2^{2m}-2}(a_1, a_2))),$$

여기서 $c_t((\cdot), (\cdot))$, $t=0, 1, \cdots\cdots, 2^{2m}-2$는 (2)로 부터 얻어진다.

$s(a_1, a_2)$와 $s(b_1, b_2)$의 相互相關函數 $R(a_1, a_2;b_1, b_2)$는 다음과 같다.

$$R(a_1, a_2;b_1, b_2)=\sum_{t=0}^{2^{2m}-2} e(\phi[(a_1\alpha^{(2m+1)t}+Tr_{2m,m}(a_2\alpha^{2t}))^r]+\phi[(b_1\alpha^{(2m+1)t}+Tr_{2m,m}(b_2\alpha^{2t}))^r]). \quad (4)$$

$R(a_1, a_2;b_1, b_2)$를 구하기 위하여 아래와 같이 t를

정의한다.

$$t=(2^m+1)t_1+t_2,\ t_1=0,\ 1,\ \cdots,\ 2^m-2,\ t_2=0,\ 1,\ \cdots\cdots,\ 2^m \quad (5)$$

이된다. 임의의 $d\in F_2$, $x\in F_3$에서 $\alpha^{2^m+1}=\beta\in F_2$, $Tr_{2m/m}(dx)=dTr_{2m/m}(x)$의 관계를 고려하면 다음과 같이 된다.

$$R(a_1, a_2; b_1, b_2)$$
$$=\sum_{t_1}^{2^m-2}\sum_{t_1}^{2^m} e\{\phi[\beta^{2rt}{}_1(a_1\beta^{t}{}_2+Tr_{2m/m}a_2\alpha^{2t}{}_2))^r]$$
$$+\phi[\beta^{2rt}{}_1(b_1\beta^{t}{}_2+Tr_{2m/m}(b_2\alpha^{2t}{}_2))^r]\}. \quad (6)$$

$\phi$가 (3)에서 주어진 함수에 속하고 $t_1$이 0부터 $2^m-2$까지 변할때 有限長 $F_2$의 모든 곱요소 $\beta^{2rt}{}_1$을 변화시키면 다음과 같은 결과를 얻는다.

$$R(a_1, a_2; b_1, b_2)=-1-2^m+2^m\sum_{t_2=0}^{2^m}\delta$$
$$[(a_1\beta^{t}{}_2Tr_{2m/m}(a_2\alpha^{2t}{}_2))^r-(b_1\beta^{t}{}_2Tr_{2m/m}(b_2\alpha^{2t}{}_2))^r], \quad (7)$$

여기서 $\delta(x)$는 有限場 $F_3$에서 다음과 같이 정의된다.

$$\delta(x)=\begin{cases}1, & x=0\\ 0, & x\neq 0\end{cases} \quad (8)$$

(7)에서 $t_2$에 대하여 계산하면 $\delta(x)$가 값을 갖을 조건은

$$(a_1\beta^{t}{}_2+Tr_{2m/m}(a_2\alpha^{2t}{}_2))^r=(b_1\beta^{t}{}_2+Tr_{2m/m}(b_2\alpha^{2t}))^r, \quad (9)$$

그러나 $(r, 2^m-1)=1$이기 때문에 아래와 같은 관계가 성립한다.

$$a_1\beta^{t}{}_2+Tr_{2m/m}(a_2\alpha^{2t}{}_2)=b_1\beta^{t}{}_2+Tr_{2m/m}(b_2\alpha^{2t}{}_2) \quad (10)$$

(7)은 다음과 같이 簡略化 된다.

$$R(a_1, a_2; b_1, b_2)=-1-2m+2m\sum_{t_2=0}^{2^m}\delta[(a_1-b_1)\beta^{t}{}_2+Tr_{2m/m}(a_2-b_2)\alpha^{2t}{}_2] \quad (11)$$

따라서 $\phi$가 (3)에 屬하고 $(r, 2^m-1)=1$인 조건에서 두 벡터 $s(a_1, a_2)$와 $s(b_1, b_2)$의 相互相關函數 $R(a_1, a_2; b_1, b_2)$는 媒介變數 r의 변화에 의하여 변화하지 않음을 (11)에서 알 수 있다. $2^m-1$과 서로 表인 변수 r과 임의의 함수 $\phi$에 의해 결정되는 相關函數의 최대값 $r_{max}$는 (11)로부터 $2^m+1$이다. OSW 符號系列 $\{s_z(t)\}$의 모든 경우에서 非線形構造를 만들 수 있는 식은 아래와 같이 정의된다[14].

$$s_z(t)=e\{\phi[(\beta_z\alpha^{(2m+1)t}+Tr_{2m/m}(\alpha^{2t}))^r]\} \quad (12)$$

여기서 $\beta_z\in F_2$는 서로 다른 符號系列을 형성하게 한다. 즉 $2^m$개의 符號系列을 발생시킬 수 있다. 여기서 $\phi(x)$는 다음과 같이 정의 된다.

$$\phi(x)=e(Tr_{m1/1}(Tr_{m/m1}(x))^{r1}, \ x\in F \quad (13)$$

임의의 t에서 $r=2^t \bmod(2^m-1)$이면 (12)는 Kasami 符號系列의 發生構造를 나타내고 $r=2^t \bmod(2^m-1)$는 非線形符號系列을 형성한다. 여기서 $r_1$은 자연수로서 $(r_1, 2^m-1)=1$을 만족한다. 이러한 조건에서 (13)은 多重의 複合符號系列을 형성하고 다음의 조건을 만족한다. 複合符號系列에서 $r=1$, $r_1=1$, $\beta_z=0$의 특별한 경우를 택하여 符號系列의 發生週期를 검토하여도 일반성을 잃지않는다. 따라서

$$s_z(t)=e(Tr_{m1/1}(Tr_{m/m1}Tr_{2m/m}(\alpha^{2t})))$$
$$=e(Tr_{2m/1}(\alpha^{2t})) \quad (14)$$

로 되며 (14)는 t의 변화에 따라 주기 $2^{2m}-1$의 符號系列을 발생한다. 線形스팬의 정확한 계산은 매우 복잡한 계산을 요구하므로 GMW 符號系列[16]과 No-Kumar 符號系列의 線形스팬과 비교검토하는 수준에서 複合符號系列의 線形스팬이 크게될 수 있음을 확인한다. GMW 符號系列 발생알고리듬은

$$b_n=Tr_{J,1}\{[Tr_{M,J}(\alpha^n)]^r\} \quad (15)$$

이며 線形스팬 $L=J(M/J)^w$이며 여기서 W는 r의 2진 表現에서 1의 수이다. 한편 No-Kumar 符號系列

의 선형스팬은 GMW 부호계열에서 M=2J일 경우 L>J(2)$^{w}$이다[15]. 線形스팬은 非線形을 이루는 r의 영향을 크게 받는다. 따라서 多重의 非線形을 갖는 複合符號系列의 線形스팬이 증가됨을 알 수 있다. 이들의 특성을 정리하면

- 週期 : $N=2^{2m}-1$ (16a)
- 發生群 : $V=\sqrt{N+1}$ (16b)
- 最大相關函數 : $R_{max}=2^{m}+1$ (16c)

로서 특성은 Kasami 符號系列과 OSW 符號系列과 완전히 특성을 같이한다. 그러나 非線形的으로 발생된다는 점에서 Kasami 符號系列과 다르며 모든 자연수 m에서도 발생될 수 있다는 점이 m이 짝수에서만 발생할 수 있는 OSW 符號系列과 다른 점이다. 그림 1은 複合符號系列과 각 符號系列과의 관계를 系列발생알고리듬의 基本式을 중심으로 나타낸 것이다.

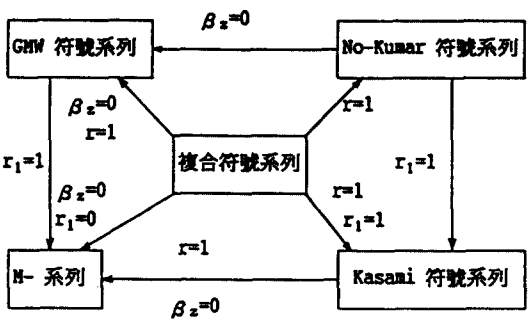


그림 1. 複合符號系列과 각 符號系列과의 關係
Fig. 1. The relations of composite code sequence with various code sequences.

## Ⅲ. 複合符號系列 發生器 構成

(1)의 複合符號系列의 생성식을 다시쓰면

$$s_z(t)=e(Tr_{m,1}(Tr_{m,m}(\beta_z\alpha^{(2m+1)t}+Tr_{2m,m}(\alpha^{2t}))^r)^{r_1}) \quad (17)$$

로 되며 符號系列의 발생은 두 종류의 $2^m$개인 符號系列의 형성으로 이루어진다. $\{Tr_{2m,m}(\alpha^{2t})\}$은 有限場 $F_2$위에서 $\alpha^2$을 原始元으로 하는 最小多項式을 기본으로 발생되는 M-系列이며 또 다른 系列은 $\{\alpha^{(2m+1)t}\}$가 있다. 따라서 複合符號系列은 두 종류의 系列과 $e(Tr_{m,1}(Tr_{m,m}(x)))^{r_1}$, $x\in F_2$의 기능을 통하여 발생될 수 있으므로 그림 2와 같은 구조를 갖는 발생기를 구성할 수 있다.

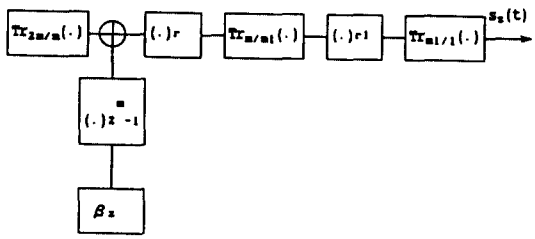


그림 2. 複合符號系列發生器의 概略圖
Fig. 2. The block diagram of composite code sequence generator.

複合符號系列의 발생모델로 簡略化가 가능하도록 m=4, $m_1$=2로 택하면 발생 알고리듬은 다음식으로 변경된다. 이는 복합부호계열의 특별한 경우의 하나로 일반성을 잃지 않는다.

$$s_z(t)=e(Tr_{2,1}(Tr_{4,2}(\alpha^{8}\beta^{(t+z)}+Tr_{8,4}(\alpha^{t}))^{r})^{r_1}) \quad (18)$$

段階 1 : $Tr_{8,1}(\alpha^t)$를 발생시킬 수 있는 8段의 쉬프트 레지스터의 내용 벡터 $(x_0, x_1, \cdots, x_7)$을 $\alpha^t$, t=0, 1, ⋯, $2^{2m}-2$와 대응시킨다.

段階 2 : GF($2^8$)에서 GF($2^4$)로 寫像하기 爲한 $Tr_{8,4}(x)$ 發生器를 構成한다.

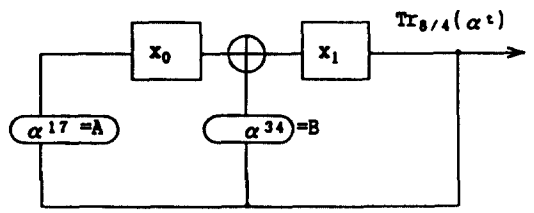


그림 3. $Tr_{8,4}(\alpha^t)$의 發生器
Fig. 3. The generator of $Tr_{8,4}(\alpha^t)$.

| $x_0$ | $x_1$ | $Tr_{8/4}(\alpha^t)$ | 비 고 |
|---|---|---|---|
| 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| A | B | B | $\alpha^{34}=\beta^2$ |
| AB | $A+B^2$ | $A+B^2$ | $A+\alpha^{68}=1$ |

$$\begin{array}{r} 1 : 10000000 \\ +)\ \alpha^{68} : 10011001 \\ \hline A=\alpha^{17}=00011001 \end{array}$$

그림 3의 發生器를 구성할 수 있는 $\alpha$를 原始元으로 하는 原始多項式은

$$m_\alpha(x)=x^2+\alpha^{34}x+\alpha^{17}=x^2+\beta^2x+\beta \qquad (19)$$

로 된다.
위 式의 妥當性을 검토하기 위하여 $\alpha$를 위 式에 대입하면

$$\begin{array}{r} \alpha^2 : 00100000 \\ \alpha^{35} : 00111001 \\ +)\ \alpha^{17} : 00011001 \\ \hline 00000000 \end{array}$$

따라서 原始多項式이 된다.

段階 3 : $Tr_{8/4}(\alpha^t)$로 발생되는 符號系列은 0을 제외한 GF($2^4$)의 모든 元 $\beta^t=\alpha^{17t}$, t=0, 1, ……14로 구성되며 이는 $\beta^t=\nu_0+\nu_1\beta+\nu_2\beta^2+\nu_3\beta^3$로 대응 시킬 수 있다. 여기서 $(\nu_0, \nu_1, \nu_2, \nu_3)$는 $x^4+x+1$로 부터 발생될 수 있는 쉬프트레지스터의 내용이다. 表 1은 이들 관계를 보여준다.

표 1. $\beta^t$의 벡터표현
Table 1. The vector representation of $\beta^t$.

| $\beta^t$ | $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $x_7$ | $\nu_0$ | $\nu_1$ | $\nu_2$ | $\nu_3$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| $\beta=\alpha^{17}$ | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| $\beta^2=\alpha^{34}$ | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| $\beta^3=\alpha^{51}$ | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| $\beta^4=\alpha^{68}$ | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| $\beta^5=\alpha^{85}$ | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| $\beta^6=\alpha^{102}$ | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| $\beta^7=\alpha^{119}$ | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| $\beta^8=\alpha^{136}$ | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| $\beta^9=\alpha^{153}$ | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| $\beta^{10}=\alpha^{170}$ | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| $\beta^{11}=\alpha^{187}$ | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 |
| $\beta^{12}=\alpha^{204}$ | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| $\beta^{13}=\alpha^{221}$ | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| $\beta^{14}=\alpha^{238}$ | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |

$$\begin{aligned} \beta^t\cdot\beta^2&=(\nu_0+\nu_1\beta+\nu_2\beta^2+\nu_3\beta^3)\cdot\beta^2 \\ &=\nu_0\beta^2+\nu_1\beta^3+\nu_2\beta^4+\nu_3\beta^5 \\ &=\nu_0\beta^2+\nu_1\beta^3+\nu_2(1+\beta)+\nu_3(\beta+\beta^2) \\ &=\nu_2\cdot 1+(\nu_2+\nu_3)\beta+(\nu_0+\nu_3)\beta^2+\nu_1\beta^3 \qquad (20) \end{aligned}$$

$$\begin{aligned} \beta^t\cdot\beta&=(\nu_0+\nu_1\beta+\nu_2\beta^2+\nu_3\beta^3)\cdot\beta \\ &=\nu_0\beta+\nu_1\beta^2+\nu_2\beta^3+\nu_3\beta^4 \\ &=\nu_3\cdot 1+(\nu_0+\nu_3)\cdot\beta+\nu_1\beta^2+\nu_2\beta^3 \qquad (21) \end{aligned}$$

(20)과 (21)의 관계를 이용하여 $Tr_{8/4}(\alpha^t)$ 發生器를 그림 4와 같이 구성할 수 있다.

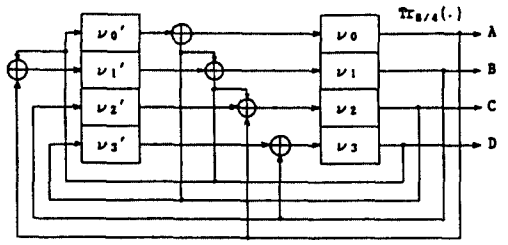


그림 4. $Tr_{8/4}(\alpha^t)$의 等價的인 發生器
Fig. 4. The equivalent generator of $Tr_{8/4}(\alpha^t)$.

段階 4 : $Tr_{8/4}(\cdot)$의 출력에 $(\beta^t)^8$을 더하기 위한 係數發生器 構成

$$\begin{aligned} (\beta^t)^8&=(\nu_0+\nu_1\beta+\nu_2\beta^2+\nu_3\beta^3)^8 \\ &=\nu_0+\nu_1\beta^8+\nu_2\beta+\nu_3\beta^9 \\ &=(\nu_0+\nu_1)+(\nu_2+\nu_3)\beta+\nu_1\beta^2+\nu_3\beta^3 \qquad (22) \end{aligned}$$

이 係數들은 아래 그림 5로부터 구할 수 있다.

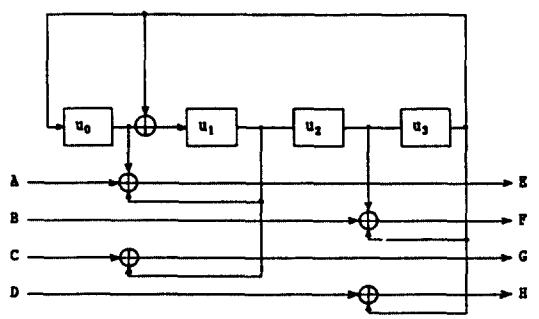


그림 5. $Tr_{8/4}(\cdot)$의 출력에 $(\beta^t)$을 더하기 위한 係數發生器
Fig. 5. The coeficient generator for adding $(\beta^t)^8$ to the output of $Tr_{8/4}(\cdot)$.

段階 5 : 非線形符號系列을 만들기 위하여 E, F, G, H의 출력 $\beta^t$를 r乘한다. $1 \leqq r < 2^4-1=15$, $(r,15)=1$의 조건을 만족해야 하므로 r=7로 택한다.

$$(\beta^t)^7=(\nu_0+\nu_1\beta+\nu_2\beta^2+\nu_3\beta^3)^7$$
$$=u_0\cdot 1+u_1\beta+u_2\beta^2+u_3\beta^3 \qquad (23)$$

여기서 係數

$$u_0=\nu_0+\nu_1+\nu_2+\nu_0\nu_1+\nu_1\nu_3+\nu_0\nu_1\nu_3+\nu_1\nu_2\nu_3+\nu_0\nu_1\nu_2$$
$$u_1=\nu_1+\nu_0\nu_1+\nu_1\nu_3+\nu_0\nu_2+\nu_2\nu_3+\nu_0\nu_2\nu_3+\nu_1\nu_2\nu_3$$
$$u_2=\nu_3+\nu_0\nu_1+\nu_1\nu_2+\nu_1\nu_3+\nu_0\nu_2+\nu_0\nu_1\nu_3$$
$$u_3=\nu_1+\nu_2+\nu_3+\nu_0\nu_3+\nu_1\nu_3+\nu_2\nu_3+\nu_1\nu_2\nu_3$$

로 정리된다. 이 係數들의 결합으로 부터 알 수 있는 바와 같이 합뿐만 아니라 곱도 포함하고 있어 非線形으로 이루어 짐을 단적으로 알 수 있다. (23)의 발생을 위한 구성은 그림 6과 같이 이루어 진다.

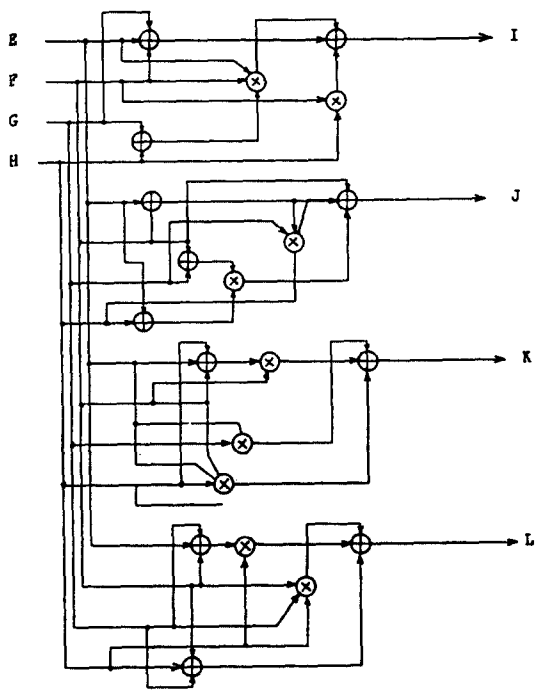


그림 6. 非線形性을 갖는 $(\beta^t)^7$의 構成圖
Fig. 6. The schematic diagram of $(\beta^t)^7$ with nonlinearity.

段階 6 : $Tr_{4,2}(\cdot)$의 變換을 수행하기 위하여 I, J, K, L로 이루어지는 $\beta^t$의 變換은 다음과 같이 單純化 된다.

$$Tr_{4,2}(\beta^t)=\beta^t+\beta^{4t}$$
$$=\nu_0+\nu_1\beta+\nu_2\beta^2+\nu_3\beta^3+\nu_0+\nu_1(1+\beta)$$
$$+\nu_2(1+\beta^2)+\nu_3(1+\beta+\beta^2+\beta^3)$$
$$=(\nu_1+\nu_2+\nu_3)+\nu_3\beta+\nu_3\beta^2 \qquad (24)$$

이 變換課程을 그림 7로 표현하였다.

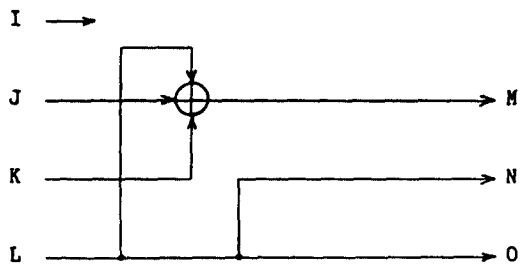


그림 7. $Tr_{4,2}(\beta^t)$ 變換器
Fig. 7. The transformer of $Tr_{4,2}(\beta^t)$

段階 7 : 複合符號系列을 발생 시키기 위한 $1 \leqq r < 3$, $(r,3)=1$ 조건을 만족하는 r은 1, 2뿐이다. r=2로 택하면 M, N, O로부터 출력된

$$(Tr_{4,2}(\beta^t))^2=(\nu_1+\nu_2)+\nu_3\beta+\nu_3\beta^2 \qquad (25)$$

로서 이 모델의 경우 r=2로 택하였기 때문에 非線形性에 기여하지 못함을 알 수 있으나 이는 구성을 간단히 하기위한 모델선정으로 基本的으로 複雜性의 증가에 대한 이론에 벗어나지는 않는다.

段階 8 : 마지막 段階로 $Tr_{2,1}(\cdot)$의 段階를 複合符號系列의 발생이 이루어진다. (25)로부터

$$Tr_{2,1}((\nu_1+\nu_2)+\nu_3\beta+\nu_3\beta^2)=(\nu_1+\nu_2)+\nu_3\beta+\nu_3\beta^2+(\nu_1+\nu_2)+\nu_3\beta^2+\nu_3\beta^4=\nu_3 \qquad (26)$$

이와 같은 8段階의 과정을 거쳐 複合符號系列이 발생된다. 表 2는 구성된 符號系列發生器의 각 出力段으로 부터 발생되는 出力系列중 그림 5의 U=

$(u_0, u_1, u_2, u_3)$ 변화에 따른 4가지 경우를 보여준다.

표 2. $U=(u_0, u_1, u_2, u_3)$의 變換으로 부터 발생된 代表的인 複合符號系列 $s_z(t)$.

Table 2. The composite code sequences $s_z(t)$ to be generated by the change of $U=(u_0, u_1, u_2, u_3)$.

```
U=(1,0,0,0)
00101111011001100101010010110111001011011010111111100
01010000101100100011111100111111010010110010100000100
01000001110111000000100010110111000110111110001000001
01000011101100101000000100110111010001001100000000001
01111100000100000001111111010001010011110111001100 0

U=(0,1,0,0)
10010111101000111111100001010110111010011010101011 1
01010101011011001110000101100111100011001011000101
10010100110010010110000011010010110000001101101010 1
00110001000010000101001011100000100110010001100100 1
01100111000011100010101100000011001111001111000011 0

U=(0,1,1,1)
11100011110101111011011000001111001001010101111111 1
11101100010101011000011111000001000110001110011100 0
11110110111000111000110101011011000001010100110100 0
01110110101010000100000000100101111001101011111101 1
10001111110010011111110010110000110111100100101010 0

U=(1,1,1,1)
00101000110100100000011000010010000000101011101100 1
11111101101000011110101010111001111101100101010111 1
11010011101110110001011000011010111111011011010010
00100010001111101111100011000010111101111110011111 0
00100100111101100000001101100100011111011010011010
```

그림 8은 表 2에서 U=(1, 0, 0, 0)에서 발생된 複合符號系列(0은 1에 그리고 1은 −1에 대응)의 自己相關函數 특성을 보인다. 그림 9는 U=(1, 0, 0, 0)와 U=(0, 1, 1, 1)에서 발생된 複合符號系列간의 相互相

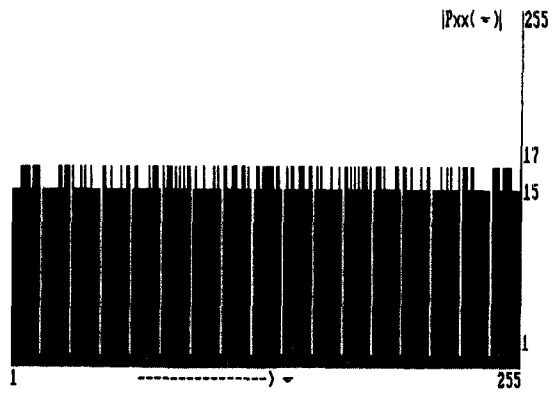


그림 8. U=(1, 0, 0, 0)인 조건에서 발생된 複合符號系列의 自己相關函數.

Fig. 8. The auto-correlation of composite code sequence for U=(1, 0, 0, 0).

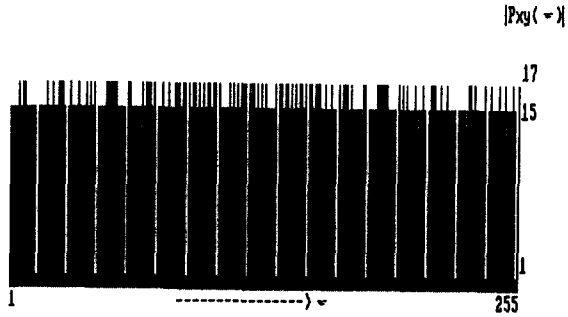


그림 9. U=(1, 0, 0, 0)와 U=(1, 1, 1, 1)에서 발생된 複合符號系列간의 相互相關函數.

Fig. 9. The cross-correlation of composite code sequencel for U=(1, 0, 0, 0) and composite code sequence2 U=(1, 1, 1, 1).

표 3. 代表的 符號系列間의 特性比較.

Table 3. Characteristic comparision of various code sequences.

| 符號系列 | 系列長 | 레지스터 段 n | 發生群 | 最大相關函數 | 線形스팬 |
|---|---|---|---|---|---|
| Gold | $2^n-1$ | odd | $2^n+1$ | $1+2^{(n+1)/2}$ | 2n |
| | $2^n-1$ | 2(mod 4) | $2^n+1$ | $1+2^{(n+2)/2}$ | 2n |
| Kasami(S) | $2^n-1$ | even | $2^m$ | $1+2^m$ | $\leqq 3n/2$ |
| OSW | $2^n-1$ | 0(mod 4) | $2^m$ | $1+2^m$ | $n/2$ $\geqq n/4\ 2^{n/4}$ |
| No-Kumar | $2^n-1$ | even | $2^m$ | $1+2^m$ | $\geqq m.2^{m-1}$ |
| Kasami-OSW | $2^n-1$ | 0(mod 4) | $2.2^m-1$ | $1+2^m$ | − |
| 複合符號 | $2^n-1$ | 0(mod 4) | $2^m$ | $1+2^m$ | − |

關函數특성을 보인다. 각각의 그림에서 알 수 있는 바와 같이 自己相關函數에서 $\tau=0(\mathrm{mod}\ 255)$을 제외한 모든 경우의 相關函數 최대값이 17로서 $2^{m}+1$, m=4를 만족함을 알 수 있다.

表 3은 代表的인 符號系列間의 特性을 나타낸다 OSW, No-Kumar, 複合符號系列은 Kasami 符號系列과 符號群 그리고 相關函數 특성이 같다. No-Kumar와 Kasami 符號系列은 n=0 (mod 2)인 境遇에 發生되나 OSW, Kasami-OSW 그리고 複合符號系列은 n=0 (mod 4)에서 發生되므로 Kasami 符號系列에 比하여 選擇할 수 있는 機會가 적게된다. 한편 Gold 符號系列과 Kasami-OSW 符號系列은 다른 符號系列에 비하여 보다 큰 發生群을 갖는다. 그러나 OSW 符號系列을 제외한 다른 符號系列은 서로 다른 符號系列을 발생시키기 위해 初期化의 문제가 대두된다. 複雜度를 나타내는 線形스팬은 간단한 경우로 n=8로 할 경우 Gold 符號系列은 16, Kasami 符號系列은 12, OSW 符號系列은 24, No-Kumar 符號系列은 32, 그리고 Kasami-OSW 符號系列의 線形스팬은 발생구조에서 알 수 있는 바와 같이 OSW 符號系列보다 클 수 없다. 複合符號系列의 線形스팬은 수학적인 완전한 분석은 이루어 지지 않았으나 二重의 非線形 구조를 갖기 때문에 單一 非線形 구조를 갖는 No-Kumar 符號系列에 비하여 크게됨을 알 수 있다.

그림 4, 그림 5, 그림 6, 그리고 그림 7을 결합하여 複合符號系列發生器를 回路로 構成하였다. 그림 10은 複合符號系列發生器의 각 중요 지점에서의 출력 $u_0$, $u_1$, $u_2$, $u_3$, E, F, G, H 그리고 複合符號系列 $s_z(t)$에 대한 Tecktronix社 PRISM 3002의 출력화면을 나타낸다. 출력표기에서 1은 −1, 그리고 0은 1에 대응되어 실제 複合符號系列이 발생된다.

발생된 複合符號系列의 發生週期는 $2^8-1=255$이며 發生群은 No-Kumar 符號系列에서와 같이 $\beta^{t+z}$를 위한 쉬프트레지스터의 初期化에 의하여 이루어진다. 이는 Gold와 Kasami 符號系列의 경우와 같다. 發生器 구조의 변동없이 GF($2^8$)의 原始元을 기본으로 하는 複合符號系列은 GF($2^4$)의 元의 수 16개의 符號系列을 발생시킬 수 있다. 實驗을 통한 결과와 컴퓨터 시뮬레이션 結果와 一致하여 발생알고리듬의 妥當性이 입증되었다.

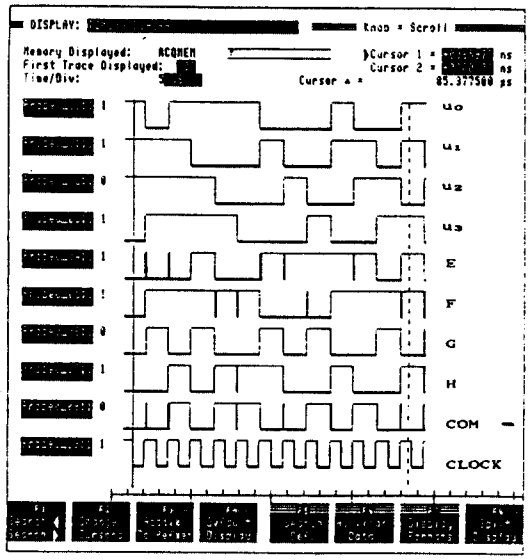


그림 10. a) $Tr_{8,4}(\alpha^k)$의 發生器 出力에 $(\beta^{t+z})^8$을 합하기 위한 係數發生器 출력 $u_0$, $u_1$, $u_2$, $u_3$, E, F, G, H.

b) 複合符號系列 $s_z(t)$

Fig. 10. a) The coefficient generator output $u_0$, $u_1$, $u_2$, $u_3$, E, F, G, H for adding $(\beta^{t+z})^8$ to the output of $Tr_{8,4}(\alpha^k)$ generator.

b) The composite code sequence $s_z(t)$.

{00101110110011001010100101101110010110110101111110001010000101100100011111100111111010010110010100010001000001110111000000100010110111000011001000101000011101100101000000100110111010000100110000000001000000111111010001010011110110011000}

## Ⅳ. 結　論

本 論文에서는 GMW 符號系列, No-Kumar 符號系列과 달리 多重의 非線形을 위한 곱을 수행하여 발생됨으로써 線形스팬을 크게 할 수 있는 複合符號系列發生알고리듬을 提示分析하였다. 複合符號系列의 發生알고리듬은 變數($r$, $r_1$, $\beta_z$)를 변경하여 쉽게 Kasami 符號系列, GMW 符號系列, No-Kumar 符號系列의 發生알고리듬으로 변환될 수 있는 構造的 장점이 있다. 제반 특성이 Kasami 符號系列과 유사하며 線形的으로 발생되는 Kasami 符號系列에서 缺如된 정보의 保安性을 複合符號系列에서는 얻을 수 있다.

컴퓨터시뮬레이션과 實驗을 통하여 Trace 函數에 基礎를 둔 非線形符號系列의 發生알고리듬을 完全히

分析하고 實際的인 符號系列의 發生과 特性分析을 遂行함으로써 理論的이고 數式的인 槪念을 具體化 시켰다. 最近 帶域擴散 通信 시스템을 利用한 民生用 機器의 硏究가 活潑히 進行되고 있어 符號分割多重接近 通信시스템의 核心課題인 擴散符號系列에 對한 硏究結果는 關聯分野 發展에 기여할 것으로 기대된다.

## 참 고 문 헌


1. R. M. Gagliardi, *Satellite Communications*, Van Nostrand Reinhold, New York, 1984.
2. B. Sklar, *Digital Communications Fundamentals and Applications*, Prentice-Hall, EnglewoodCliffs, N. J., 1988.
3. R. L. Pickholtz and D. L. Shilling, "*Theory of Spread Spectrum Communications*", IEEE Trans. Comm., Com-30, pp.855-884, May. 1982.
4. R. E. Ziemer and R.L. Peterson, *Digital Communications and Spread Spectrum systems*, Macmillan, New York, 1985.
5. R. C. Dixon, *Spread Spectrum Systems*, John Wiley & Sons, New York, 1984.
6. M. K. Simon and J. K. Omura, *Spread Spectrum Communications*, Vol. I, Computer Science Press, Maryland, 1985.
7. R. Gold, "*Optimal binary sequences for spread spectrum multiplexing*", IEEE Trans. Inform. Theory, IT-13, No.4, pp.619-621, Oct. 1976.
8. P. V. Kumar and R. A. Scholtz, "*Bound on the Linear Span of Bent Sequences*", IEEE Trans. Inform. Theory, IT-29, No. 6, pp.854-862, Nov. 1983.
9. I. Vajda and J. Landsman, "*Increasing the linear complexity of m-sequences using pseudorandom exponentiation*", Prob. Cont. Inform. Theory Hungary, Vol. 17, No. 5, pp. 311-317, 1988.
10. Kamaletdinov, B. ZH., "*New optimal ensembles of nonlinear binary sequences*", Probl. Pereda. Inf. USSR, Vol. 25, No. 3, pp.193-210, 1989.
11. J. DJ. Golic, "*On the linear complexity of functions of periodic GF(q) sequences*", IEEE Trans. Inform. Theory, Vol. 35, No. 1, JAN. 1989.
12. P. V. Kumar, "*Frequency hopping code sequence designs having large linear span*", GLOCOM 84, Vol.2, pp.989-993, 1984.
13. E. L. Key, "*An analysis of the structure and complexity of nonlinear binary sequence generators*", IEEE Trans. Inform. Theory, Vol. IT-22, No.6, pp.732-736, Nov.1976.
14. J. D. Olsen, R. A. Scholtz, and L. R. Welch, "*Bent-function sequences*," IEEE Trans. Inform. Theory, Vol.IT-28, No.6, pp.858-864, Nov.1982.
15. J. S. No and P.V.Kumar, "*A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span*" IEEE Trans. Inform. Theory, Vol.35, No.2, March 1989.
16. R. A. Scholtz and L. R. Welch, "*GMW sequences*", IEEE Trasn. Inform. Theory, Vol.IT-30, No.3, pp.548-553, May 1984.
17. B. ZH. Kamaletdinov, "*An optimal ensemble of binary sequences based on the union of the ensembles of Kasami and Bent function sequences*", PROBL. PERIDA. INF.(USSR), Vol.24, No. 2, pp.04-107, June 1988.


이 논문은 '91년 통신학술연구과제로서 체신부, 한국전기통신공사의 후원으로 이루어 졌습니다.


李 正 宰(Jeong Jae Lee) 正會員

1973年 2月 : 西江大學校 電子工學科 卒業(工學士)

1984年 2月 : 漢陽大學校 産業大學院(工學碩士)

1990年 8月 : 漢陽大學校 大學院(工學博士)

1979年~1984年 : 韓國機械硏究所 勤務

1986年~1987年 : 三星綜合技術院勤務

1987年~現在 : 東義大學校 電子通信工學科 助敎授

※主關心分野 : 帶域擴散通信시스템, 符號系列發生