# 부울함수를 이용한 부호계열 발생알고리즘 분석 및 부호계열발생기 구성

# Analysis of Code Sequence Generating Algorism and Implementation of Code Sequence Generator using Boolean Functions

이 정 재*

Jeong-Jae Lee*

## 요 약

본 논문에서는 S.Bostas와 V.Kumar[7]에 의하여 제안되고 $GF(2^n)$에서 정의되는 부호계열 발생알고리즘을 분석하고, 길이 n인 이진벡터로 이루어지는 벡터공간 $F_2^n$으로부터, 두 원소로 정의되는 공간 $F_2$로 사상할 수 있는 부울함수를 이용하여 발생기 구성 함수를 도출하였다. 차수 n=5와 n=7인 두 종류의 최소다항식을 이용한 피드백 쉬프트레지스터를 기반으로 Trace 함수로부터 부호계열 발생기 구성 부울함수를 도출하고 발생기를 설계·구성하였으며 이를 이용하여 두 종류의 부호계열 군을 발생하였다. 발생된 부호계열의 주기는 각각 31과 127로서 주기 $L=2^n-1$을 만족하고 $\tau=0$을 제외한 자기상관함수 값과 상호상관함수 값이 각각 {-9, -1, 7}과 {-17, -1, 15}로서 상관함수 값 $R_{i,j}(\tau)=\{-2^{(n+1)/2}-1, -1, 2^{(n+1)/2}-1\}$의 특성을 만족하였다. 이 결과로부터 부울함수를 이용한 부호계열 발생기 설계와 구성이 타당함을 확인하였다.

## Abstract

In this paper we analyze the code sequence generating algorism defined on $GF(2^n)$ proposed by S.Bostas and V.Kumar[7] and derive the implementation functions of code sequence generator using Boolean functions which can map the vector space $F_2^n$ of all binary vectors of length n, to the finite field with two elements $F_2$. We find the code sequence generating boolean functions based on two kinds of the primitive polynomials of degree, n=5 and n=7 from trace function. We then design and implement the code sequence generators using these functions, and produce two code sequence groups. The two groups have the period 31 and 127 and the magnitudes of out of phase($\tau \neq 0$) autocorrelation and crosscorrelation functions {-9, -1, 7} and {-17, -1, 15}, satisfying the period $L=2^n-1$ and the correlation functions $R_{ij}(\tau)=\{-2^{(n+1)/2}-1, -1, 2^{(n+1)/2}-1\}$ respectively. Through these results, we confirm that the code sequence generators using boolean functions are designed and implemented correctly.

***Keywords:*** Code sequence, Trace function, Boolean function, Correlation function, LFSR, Linear span

## I. 서 론

부호계열은 암호, 개인보안, 다중접속, 디지털 동기시스템, 랜덤비트발생 그리고 거리측정 등에 사용되며 통신을 위한 부호계열은 발생군이 커야하고 이용자 간의 간섭을 피하기 위해서는 자기상관함수와 상호상관함수 특성이 좋아야 한다. 그리고 의도적인 방해자로부터 정보를 보호하기 위해서는 비선형성의 척도인 선형스팬이 커야한다. 1960년대부터 본격적으로 시작된 관련 분야에 대한 연구결과 S.W.Golomb[1]는 쉬프트레지스터를 이용한 부호계열 발생

* 동의대학교 정보통신공학과
투고 일자 : 2012. 9. 2 수정완료일자 : 2012. 10. 30
게재확정일자 : 2012. 11. 3
* 이 논문은 2011학년도 동의대학교 교내연구비에 의하여 연구되었음(2011AA169)

및 원리에 대하여 그리고 P.Fan과 M.Darnell[2]는 통신에 적용하기 위한 다양한 부호계열 설계에 관련한 저서를 저술하였다. 우수한 부호계열의 발생 알고리즘 및 발생기 구성은 최근까지 많은 연구가 진행되고 있으며 비선형성을 증가시킬 수 있는 함수로서 bent함수가 제안되었다[3]. 이 함수에 접근하기 위한 유사 bent함수 그리고 APN(almost perfect nonlinear)함수에 대한 연구도 활발히 진행되고 있다[4,5]. 이와 관련하여 최초에 연구되고 지금까지 많이 활용되고 있는 Gold 부호[6]는 선형성으로 인하여 특성이 비선형적으로 발생되는 발생알고리즘을 위한 연구가 지속적으로 진행되어 왔다. 특히 S.Bostas와 V.Kumar는 Gold부호와 유사한 상관함수 특성을 갖고 큰 선형스팬특성을 갖는 부호계열 발생알고리즘을 제시하였다[7].

본 논문에서는 S.Bostas와 V.Kumar에 의하여 제안된 유한장 $GF(2^n)$에서 $GF(2)$로 사상하는 Trace 함수를 이용한 부호계열 발생알고리즘을 분석하고 길이 n인 이진벡터로 이루어지는 벡터공간 $F_2^n$에서 이진 원소로 정의되는 $F_2$로 사상하는 부울함수를 이용하여 발생기를 구성할 수 있는 함수를 도출하였다. 그리고 발생된 부호계열의 특성분석을 통하여 부호계열 발생기 설계와 구성의 타당성을 확인하였다. 이를 위하여 제 II장에서는 Trace함수와 부울함수와의 관계를 검토하였다. 제 III장에서는 부호계열발생 알고리즘을 벡터공간에서 부울함수를 적용하여 표현하였다. 그리고 제 IV장에서는 최소다항식 차수가 n=5와 n=7인 두 경우에서 부호계열 발생기를 설계할 수 있는 함수를 유도하고 이를 이용하여 발생기를 구성하였다. 제 V장에서는 발생기로부터 부호계열을 발생시키고 상관함수 특성을 분석하였다. 마지막으로 제 VI장에서는 결론을 맺는다.

## II. Trace함수와 부울함수

유한장 GF($q^n$)과 GF(q)에서 만약 $\alpha$가 GF($q^n$)의 원소이면 Trace 함수는 다음 식 (1)과 같이 정의되며 GF($q^n$)으로부터 GF(q)에 사상한다[8].

$$Tr_q^n(\alpha)=\sum_{i=0}^{n-1}\alpha^{q^i}=\alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}} \quad (1)$$

q=2일 경우 $Tr_2^n(\alpha)$는 일반적으로 편리함을 위하여 $Tr(\alpha)$로 표현한다. Trace 함수는 모든 $\alpha,\beta\in$GF($2^n$)에 대하여 $Tr(\alpha)\in GF(2)$, $Tr(\alpha+\beta)=$Tr($\alpha$)+Tr($\beta$), $Tr(\lambda\alpha)=\lambda Tr(\alpha)$, Tr($\lambda$)=n$\lambda$, 여기서 $\lambda\in GF(2)$ 그리고 $Tr(\alpha^2)=Tr(\alpha)$인 관계를 갖는다. GF($2^n$)의 원소를 GF(2)상에서 표현하기 위한 대표적인 두 종류의 기저는 $\overline{\alpha_p}=\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$로 표현되는 다항식 기저(poly- nomial basis)와 $\overline{\alpha_N}=\{\alpha,\alpha^2,\alpha^{2^2}\cdots,\alpha^{2^{n-1}}\}$로 표현되는 정규기저(normal basis)가 있다. 그리고 두 기저 $\{\alpha_0,\alpha_1,\cdots\cdots,\alpha_{n-1}\}$와 $\{\beta_0,\beta_1,\cdots\cdots,\beta_{n-1}\}$가 다음과 같은 관계를 가지면 쌍대기저(dual basis 또는 complement- ary basis)라 한다.

$$Tr(\alpha_i\beta_j)=\begin{cases}1, & i=j\\ 0, & i\neq j\end{cases}$$

임의의 $x\in GF(2^n)$을 다항식 기저 $\overline{\alpha_p}$와 GF(2)상의 원소로 이루어지는 벡터 $X=(x_0,x_1,\cdots\cdots,x_{n-1})^T$, $x_i\in$GF(2), $i=0,1...,n-1$를 이용하여 유일하게 다음 식 (2)의 $x_p$와 같이 표현할 수 있다.

$$\begin{aligned}x_p&=x_0\alpha^0+x_1\alpha^1+\cdots+x_{n-1}\alpha^{n-1}\\&=\overline{\alpha_p}\cdot X=\sum_{i=0}^{n-1}x_i\alpha^i\end{aligned} \quad (2)$$

여기서 $\alpha^i\in GF(2^n)$, $i=0,1...,n-1$이며 $x_p$는 단순히 $GF(2^n)$에서 표현되는 x와 구분하기 위하여 달리 정의하였다. 따라서 모든 유한장 원소 $x\in GF(2^n)$을 $\overline{\alpha_p}\cdot X=\sum_{i=0}^{n-1}x_i\alpha^i$와 같이 GF(2)상의 원소로 이루어지는 n차원 벡터공간 $F_2^n$에서의 연산으로 정의할 수 있다. 식 (2)에 Trace 함수를 적용하면 다음 식 (3)과 같이 된다.

$$\begin{aligned}Tr(x_p)&=Tr(\sum_{i=0}^{n-1}x_i\alpha^i)\\&=x_0Tr(\alpha^0)\oplus x_1Tr(\alpha^1)\oplus\cdots\oplus x_{n-1}Tr(\alpha^{n-1})\end{aligned} \quad (3)$$

여기서 $Tr(\alpha^i)$, $i=0,1...,n-1$은 GF(2)의 원소 {0,1}을 갖기 때문에 모든 $x_p\in GF(2^n)$을 $F_2$=GF(2) 상의 벡터 X의 원소 $x_i$의 합 형태로 표현할 수 있다. 그리고 모든 부울 ⊕합은 MOD2 합으로 앞으로 +로 표현한다. 유한장 GF($2^n$)의 모든 원소는 $GF(2)$상에서 기저를 이용하여 n차원의 벡터로 표현될 수 있고 n차원 벡터공간 $F_2^n$으로부터 GF(2)로 사상하는 부울함수 f와 동일한 의미를 갖는다. 그러므로 $Tr(F(x))$는 하나의 부울 함수이며 F(x)는 $GF(2^n)$에서 $GF(2^n)$로 사상하는 임의의 함수다. 식 (2)의 양변을 m승하면 다음 식 (4)와 같이 표현된다.

$$x_p^m=\sum_{i=0}^{n-1}(x_i\alpha^i)^m=\sum_{i=0}^{n-1}x_i(\alpha^i)^m \quad (4)$$

여기서 $(x_i)^m=x_i$이다. 식 (4)의 양변에 Trace 함수를 적용하면 다음 식 (5)와 같다.

$$Tr(x_p^m)=\sum_{i=0}^{n-1}x_i\{Tr(\alpha^i)\}^m \tag{5}$$

그리고 Trace함수는 다음과 같은 특성을 가지며 유용하게 이용된다.

$$\{Tr(\alpha^m)\}^2=\{Tr((\alpha^m)^2)\}=Tr(\alpha^m) \tag{6}$$

여기서 $\alpha^m\in GF(2^n)$이다.

## Ⅲ. 부호계열 발생알고리즘

S.Bostas와 V.Kumar는 다음 식 (7)와 같은 발생알고리즘 $s_i(x)$를 제안하였다[7].

$$s_i(x)=\begin{cases}Tr(\lambda_i x)+\sum_{k=1}^{s}Tr(x^{1+2^k}), & 1\le i\le 2^n,\ \forall x\in GF(2^n)\\ Tr(x), & i=2^n+1,\ \forall x\in GF(2^n)\end{cases} \tag{7}$$

여기서 n=2s+1로서 홀수이며 $\lambda_i\in GF(2^n)$ 관계를 가진다. 따라서 서로 다른 $\lambda_i$로부터 발생군이 $2^n+1$개인 부호계열을 발생시킬 수 있다. 발생된 두 부호계열 $s_i(t)$와 $s_j(t)$간의 상관함수 $R_{i,j}(\tau)$는 다음 식 (8)과 같이 정의된다.

$$R_{i,j}(\tau)=\sum_{t=0}^{L-1}(-1)^{s_i(t+\tau)+s_j(t)} \tag{8}$$

여기서 연산은 $(t+\tau)$ MOD L이 적용되는 합이며 $i=j$이면 자기상관함수 그리고 $i\neq j$이면 상호상관함수가 된다. 주기는 $L=2^n-1$이며 이로부터 발생된 부호계열간의 상관함수 특성은 다음 식 (9)와 같이 계산되었다[7].

$$R_{i,j}(\tau)=\begin{cases}-1+2^n, & i=j,\ \tau=0,\\ -1, & \\ -1+2^{(n+1)/2}, & \\ -1-2^{(n+1)/2}, & \end{cases} \tag{9}$$

발생알고리즘 식 (7)의 $s_i(x)$에 식 (2)를 이용하여 선형결합으로 변화시키면 다음 식 (10)과 같이 정의된다.

$$\begin{aligned}S_i(x_p)&=S_i(\sum_{l=0}^{n-1}x_l\alpha^l)\\&=\begin{cases}Tr(\lambda_i\sum_{l=0}^{n-1}x_l\alpha^l)+\sum_{k=1}^{s}Tr((\sum_{l=0}^{n-1}x_l\alpha^l)^{1+2^k}),\\ Tr(\sum_{l=0}^{n-1}x_l\alpha^l)\end{cases}\end{aligned} \tag{10}$$

여기서 $1\le i\le 2^n$, $\forall x_p\in GF(2^n)$, 따라서 식 (10)을 해석하면 GF(2)에서 발생기를 구성할 수 있는 구성함수가 된다.

## Ⅳ. 부호계열발생기 구성

GF(2)에서 n차 최소다항식을 $f(x)=\sum_{i=0}^{n}a_ix^i$, $a_i\in GF(2)$ 그리고 원시원 $\alpha\in GF(2^n)$이라 하면 f(x)에 대응되는 Galois 형 피드백 쉬프트레지스터를 그림 1과 같이 구성 할 수 있다. 여기서 ⊕은 MOD 2 연산으로 1⊕1=0, 1⊕0=1 관계를 갖는다. 앞으로 MOD 2 합 연산 ⊕를 연산 수식의 간단함을 위하여 +로 표현한다. 부울함수를 이용하여 부호계열 발생기를 구성하기 위한 함수를 유도하기 위하여 n=5와 n=7인 두 경우를 고려한다. 이들에 대응되는 최소다항식 $f_5(x)$와 $f_7(x)$를 다음과 같이 설정하였다[2].

$$f_5(x)=x^5+x^2+1 \tag{11a}$$

$$f_7(x)=x^7+x+1 \tag{11b}$$

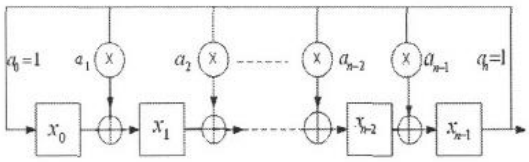


그림 1. f(x)에 대응한 Galois형 피드백 쉬프트레지스터.

Fig.1. Galois configuration of feedback shift register corresponding to f(x).

첫 번째로 n=5일때 최소다항식 $f_5(x)=x^5+x^2+1$로 이루어지는 $GF(2^5)$의 원시원 $\alpha$는 $\alpha^5=\alpha^2+1$을 만족한다. 여기서 n=2s+1에서 s=2가되며 식 (10)으로부터 $S_{i(5)}(x_p)$는 다음 식 (12)와 같이 표현된다.

$$\begin{aligned}&S_{i(5)}(x_p)\\&=\begin{cases}Tr(\lambda_i x_p)+Tr(x_p^3)+Tr(x_p^5), & 1\le i\le 2^n\\ Tr(x_p), & i=2^n+1\end{cases}\\&=\begin{cases}Tr(\lambda_i\sum_{l=0}^{4}x_l\alpha^l)+Tr((\sum_{l=0}^{4}x_l\alpha^l)^3)+Tr((\sum_{l=0}^{4}x_l\alpha^l)^5),\\ Tr(\sum_{l=0}^{4}x_l\alpha^l),\ i=2^n+1\end{cases}\end{aligned} \tag{12}$$

특별한 경우 $\lambda_i=1$로 하여도 일반성을 갖게 되므로 식 (3)의 $Tr(x_p)$는 다음 식 (13)과 같은 다항식으로 표현 할 수 있다.

$$\begin{aligned}Tr(x_p)&=Tr(\sum_{l=0}^{4}x_l\alpha^l)\\&=x_0Tr(\alpha^0)+x_1Tr(\alpha)+x_2Tr(\alpha^2)\\&\quad+x_3Tr(\alpha^3)+x_4Tr(\alpha^4)\end{aligned} \tag{13}$$

여기서 $\mathrm{Tr}(\alpha^0)=1$, $Tr(\alpha)=0$, $Tr(\alpha^2)=0$, $Tr(\alpha^3)=1$ 그리

고 $Tr(\alpha^4)=0$이 된다. 따라서 Tr($x_p$)는 다음 식 (14)로 표현된다.

$$Tr(x_p)=x_0+x_3 \tag{14}$$

Tr($x_p$)와 같은 방법으로 $Tr(x_p^3)$은 $x_p^3=x_p\cdot x_p^2$ 그리고 $Tr(x_p^5)$는 $x_p^5=x_p\cdot(x_p^2)^2$으로부터 각각 식 (15)와 식 (16)과 같이 구할 수 있다.

$$\begin{aligned}Tr(x_p^3)&=Tr(x_p\cdot x_p^2)\\&=x_0+x_1+x_2+x_3+x_4+x_1x_2+x_1x_3+x_2x_4\end{aligned} \tag{15}$$

$$\begin{aligned}Tr(x_p^5)&=Tr(x_p\cdot(x_p^2)^2)\\&=x_0+x_1+x_2+x_4+x_1x_3+x_1x_4+x_2x_3\end{aligned} \tag{16}$$

식 (14), 식 (15) 그리고 식 (16)을 식 (13)에 대입하면 부호계열 $S_{i(5)}(x_p)$는 다음 식 (17)과 같은 형태로 표현된다.

$$\begin{aligned}S_{i(5)}(x_p)&=(x_0+x_3)\\&\quad+(x_0+x_1+x_2+x_3+x_4+x_1x_2+x_1x_3+x_2x_4)\\&\quad+(x_0+x_1+x_2+x_4+x_1x_3+x_1x_4+x_2x_3)\\&=x_0+(x_1+x_3+x_4)x_2+x_1x_4\end{aligned} \tag{17}$$

식 (17)을 이용하여 최소다항식 $f_5(x)=x^5+x^2+1$를 기반으로 이루어지는 그림 1의 Galois형 피드백 쉬프트레지스터를 이용하여 그림 2와 같은 5단의 쉬프트레지스터를 갖는 부호계열 발생기를 구성할 수 있다.

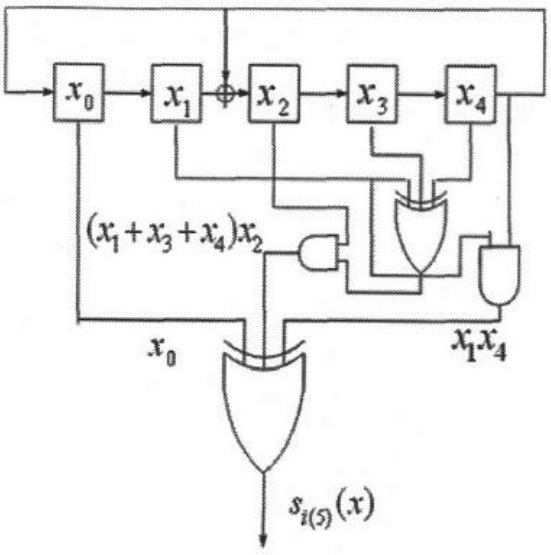


그림 2. 최소다항식 $x^5+x^2+1$을 기반으로 한 부호계열 발생기

Fig. 2. The code sequence generator based on the primitive polynomial equation $x^5+x^2+1$.

표 1은 최소다항식 $x^5+x^2+1$에 따른 순환 t와 쉬프트레지스터 내용 $X^T$, $Tr(\lambda_i x_p)$, Tr($x_p^3$), Tr($x_p^5$) 그리고 이들로부터 발생될 수 있는 부호계열 $s_{1(5)}(t)$를 보여준다.

표 1. 최소다항식 $x^5+x^2+1$에서 Trace 함수값과 발생 부호 $s_{1(5)}(t)$.

Table 1. Trace function values and generated code sequence $s_{1(5)}(t)$ for the primitive polynomial $x^5+x^2+1$.

| t | $X^T$ | Tr( ) | | | $s_{1(5)}(t)$ |
|---|---|---|---|---|---|
| | $x_0\cdots x_4$ | $(\lambda_i x_p)$ | $(x_p^3)$ | $(x_p^5)$ | |
| 0 | 10000 | 1 | 1 | 1 | 1 |
| 1 | 01000 | 0 | 1 | 1 | 0 |
| 2 | 00100 | 0 | 1 | 1 | 0 |
| 3 | 00010 | 1 | 1 | 0 | 0 |
| 4 | 00001 | 0 | 1 | 1 | 0 |
| 5 | 10100 | 1 | 0 | 0 | 1 |
| 6 | 01010 | 1 | 1 | 0 | 0 |
| 7 | 00101 | 0 | 1 | 0 | 1 |
| 8 | 10110 | 0 | 1 | 1 | 0 |
| 9 | 01011 | 1 | 0 | 0 | 1 |
| 10 | 10001 | 1 | 0 | 0 | 1 |
| 11 | 11100 | 1 | 0 | 1 | 0 |
| 12 | 01110 | 1 | 1 | 0 | 0 |
| 13 | 00111 | 1 | 0 | 1 | 0 |
| 14 | 10111 | 0 | 1 | 0 | 1 |
| --- | ----- | ----- | ----- | ------- | ------ |
| 20 | 00110 | 1 | 0 | 0 | 1 |
| 21 | 00011 | 1 | 0 | 1 | 0 |
| 22 | 10101 | 1 | 0 | 1 | 0 |
| 23 | 11110 | 0 | 0 | 1 | 1 |
| 24 | 01111 | 1 | 1 | 0 | 0 |
| 25 | 10011 | 0 | 1 | 0 | 1 |
| 26 | 11101 | 1 | 0 | 1 | 0 |
| 27 | 11010 | 0 | 0 | 1 | 1 |
| 28 | 01101 | 0 | 1 | 0 | 1 |
| 29 | 10010 | 0 | 0 | 1 | 1 |
| 30 | 01001 | 0 | 0 | 1 | 1 |

두 번째로 n=7인 경우 n=2s+1에서 s는 3이 되며 식 (7)과 식 (10)으로부터 다음 식 (18)과 같이 $S_{i(7)}(x_p)$를 구할 수 있다.

$$\begin{aligned}S_{i(7)}(x_p)&=\begin{cases}Tr(\lambda_i x_p)+Tr(x_p^3)+Tr(x_p^5)+Tr(x_p^9)\\Tr(x_p),\ i=2^n+1\end{cases}\\&=\begin{cases}Tr(\lambda_i\sum_{l=0}^{n-1}x_l\alpha^l)+Tr((\sum_{l=0}^{n-1}x_l\alpha^l)^3)+Tr((\sum_{l=0}^{n-1}x_l\alpha^l)^5)+Tr((\sum_{l=0}^{n-1}x_l\alpha^l)^9),\\Tr(\sum_{l=0}^{n-1}x_l\alpha^l),\ i=2^n+1\end{cases}\end{aligned} \tag{18}$$

그리고 최소다항식 식 $f_7(x)=x^7+x+1$로 이루어지는 $GF(2^7)$의 원시원 $\alpha$는 $\alpha^7=\alpha+1$을 만족한다. $\lambda_i=1$로 놓으면 $Tr(x_p)$는 다음 식 (19)와 같이 다항식 형태로 표현할 수 있다.

$$\begin{aligned}Tr(x_p)&=x_0Tr(1)+x_1Tr(\alpha)+x_2Tr(\alpha^2)+x_3Tr(\alpha^3)\\&\quad+x_4Tr(\alpha^4)+x_5Tr(\alpha^5)+x_6Tr(x^6)\end{aligned} \tag{19}$$

여기서 Tr(1)=1, $Tr(\alpha)=0$, $Tr(\alpha^2)=0$, $Tr(\alpha^3)=0$,

$Tr(\alpha^4)=0$, $Tr(\alpha^5)=0$ 그리고 $Tr(\alpha^6)=0$이 된다. 이를 이용하여 Tr($x_p$)를 구하면 식 (19)는 다음 식 (20)과 같이 된다.

$$Tr(x_p)=x_0 \tag{20}$$

$Tr(x_p^3)$은 $x_p^3=x_p\cdot x_p^2$, $Tr(x_p^5)$도 $x_p^5=x_p\cdot(x_p^2)^2$ 그리고 $Tr(x_p^9)$ 역시 $x_p^9=x_p\cdot((x_p^2)^2)^2$을 이용하여 다음 식 (21), (22) 그리고 (23)과 같이 구할 수 있다.

$$\begin{aligned}Tr(x_p^3)&=Tr(x_p\cdot x_p^2)\\&=x_0+(x_3+x_5+x_6)x_1+(x_3+x_6)x_2\\&\quad+x_5x_3+x_6x_4\end{aligned} \tag{21}$$

$$\begin{aligned}Tr(x_p^5)&=Tr(x_p\cdot(x_p^2)^2)\\&=x_0+x_5+(x_5+x_6)x_1+(x_3+x_5)x_2\\&\quad+(x_4+x_6)x_3+(x_5+x_6)x_4+x_5x_6\end{aligned} \tag{22}$$

$$\begin{aligned}Tr(x_p^9)&=Tr(x_p\cdot(((x_p^2)^2)^2)\\&=(x_0+x_3+x_5+x_6)+(x_3+x_6)x_1+(x_3+x_4)x_5\\&\quad+(x_3+x_5+x_2)x_6\end{aligned} \tag{23}$$

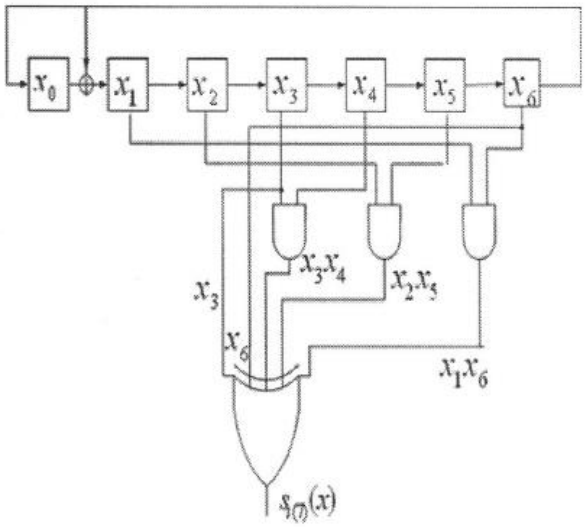


그림 3. 최소다항식 $x^7+x+1$을 기반으로 한 부호계열 발생기

Fig. 3. The code sequence generator based on the primitive polynomial equation $x^7+x+1$.

식 (20), (21), (22) 그리고 (23)을 식 (18)에 대입하면 $S_{i(7)}(x_p)$는 식 (24)와 같은 형태로 표현된다.

$$\begin{aligned}S_{i(7)}(x_p)&=x_0+\{x_0+(x_3+x_5+x_6)x_1+(x_3+x_6)x_2+x_5x_3+x_6x_4\}\\&\quad+\{x_0+x_5+(x_5+x_6)x_1+(x_3+x_5)x_2+(x_4+x_6)x_3\\&\quad+(x_5+x_6)x_4+x_5x_6\}+\{(x_0+x_3+x_5+x_6)+(x_3+x_6)x_1\\&\quad+(x_3+x_4)x_5+(x_3+x_5+x_2)x_6\}\\&=x_3+x_6+x_1x_6+x_5x_2+x_4x_3\end{aligned} \tag{24}$$

식 (24)를 이용하여 n=7일 경우 그림 3와 같이 부호계열 발생기를 구성할 수 있다. 표 2는 최소다항식 $x^7+x+1$에 따른 순환 t와 쉬프트레지스터 내용 $X^T$, $Tr(\lambda_i x_p)$, Tr($x_p^3$), Tr($x_p^5$), Tr($x_p^9$) 그리고 이들로부터 발생될 수 있는 부호계열 $s_{1(7)}(t)$을 보여준다.

표 2. 최소다항식 $x^7+x+1$에서 Trace 함수 값과 발생 부호 $s_{1(7)}(t)$.

Table 2. Trace function values and generated code sequence $s_{1(7)}(t)$ for the primitive polynomial $x^7+x+1$.

| t | $X^T$ | Tr( ) | | | | $s_{1(7)}(t)$ |
|---|---|---|---|---|---|---|
| | $x_0\cdots x_6$ | ($\lambda_i x_p$) | ($x_p^3$) | ($x_p^5$) | ($x_p^9$) | |
| 0 | 1000000 | 1 | 1 | 1 | 1 | 0 |
| 1 | 0100000 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0010000 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0001000 | 0 | 0 | 0 | 1 | 1 |
| 4 | 0000100 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0000010 | 0 | 0 | 1 | 1 | 0 |
| 6 | 0000001 | 0 | 0 | 0 | 1 | 1 |
| 7 | 1100000 | 1 | 1 | 1 | 1 | 0 |
| 8 | 0110000 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0011000 | 0 | 1 | 1 | 1 | 1 |
| --- | ------- | ---- | ------ | ---- | ----- | ----. |
| 61 | 1100011 | 1 | 1 | 1 | 1 | 1 |
| 62 | 1010001 | 1 | 0 | 1 | 1 | 1 |
| 63 | 1001000 | 1 | 1 | 1 | 0 | 1 |
| 64 | 0100100 | 0 | 0 | 0 | 0 | 0 |
| 65 | 0010010 | 0 | 0 | 0 | 1 | 1 |
| --- | ------- | ---- | ------ | ---- | ----- | ---- |
| 121 | 1111111 | 1 | 0 | 1 | 1 | 1 |
| 122 | 1011111 | 1 | 1 | 1 | 1 | 0 |
| 123 | 1001111 | 1 | 1 | 1 | 0 | 1 |
| 124 | 1000111 | 1 | 0 | 1 | 1 | 1 |
| 125 | 1000011 | 1 | 1 | 1 | 0 | 1 |
| 126 | 1000001 | 1 | 1 | 1 | 0 | 1 |

## V. 부호계열 발생과 상관함수특성

먼저 n=5일 때 그림 2와 같은 발생기로부터 표 1과 같은 동작을 통하여 두 종류의 부호계열 $s_{1(5)}(t)$와 $s_{2(5)}(t)$를 다음과 같이 발생시킬 수 있다. $s_{1(5)}(t)$는 피드백 쉬프트레지스터 초기값 $X=(10000)^T$, $\lambda_0=\alpha^0$에 의하여 발생된 부호계열이고 $s_{2(5)}(t)$는 초기값 $X=(00001)^T$, $\lambda_4=\alpha^4$에 의하여 발생된 부호계열로서 모두 주기 31이며 다음과 같다.

$s_{1(5)}(t)$=[10000 10101 10001 10011 10010 10111 1]

$s_{2(5)}(t)$=[10101 01111 10101 01000 10100 11000 1]

그리고 식 (8)을 이용한 부호계열 $s_{1(5)}(t)$의 자기상관함수 $R_{1,1(5)}(\tau)$와 부호계열 $s_{1(5)}(t)$와 $s_{2(5)}(t)$ 사이의 상호상관함수 $R_{1,2(5)}(\tau)$는 다음과 같으며 그림 4와 그림 5는 각각 이를 보여준다.

$R_{1,1(5)}(\tau)$=

[-1 -9 7 -9 7 7 7 -1 -9 -9 7 -1 -9 -1 -1 31
-1 -1 -9 -1 7 -9 -9 -1 7 7 7 -9 7 -9 -1 ]

$R_{1,2(5)}(\tau)$=

[-1 -1 -1 7 -1 7 -9 -1 -9 -1 -1 -1 -1 -1 7 -1
7 -9 7 -1 7 -1 -1 -1 -1 7 -1 -1 -9 -1 -1 ]

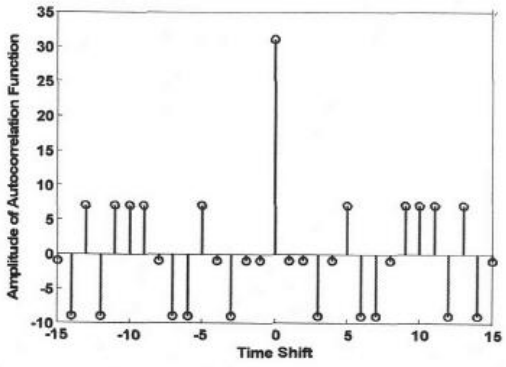


그림 4. $s_{1(5)}(t)$의 자기상관함수 $R_{1,1(5)}(\tau)$.

Fig. 4. Autocorrelation function of $s_{1(5)}(t)$, $R_{1.1(5)}(\tau)$.

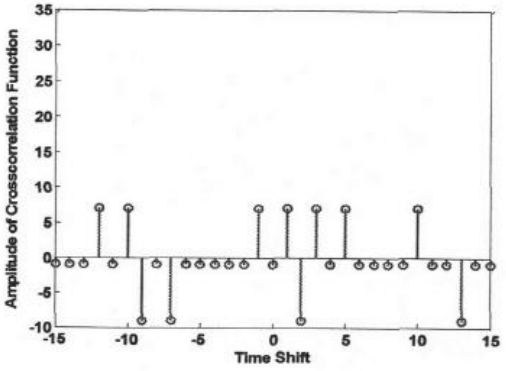


그림 5. 두 부호계열 $s_{1(5)}(t)$과 $s_{2(5)}(t)$간의 상호상관함수 $R_{1,2(5)}(\tau)$.

Fig.5. Crosscorrelation function of two code sequences, $s_{1(5)}(t)$ and $s_{2(5)}(t)$, $R_{1.2(5)}(\tau)$.

다음으로 n=7일 때 그림 3과 같은 발생기로부터 표 2와 같은 동작을 통하여 발생되는 두 종류의 부호계열 $s_{1(7)}(t)$와 $s_{2(7)}(t)$는 다음과 같다. 여기서 $s_{1(7)}(t)$는 $X=(1000000)^T$, $\lambda_0=\alpha^0$에 의하여 발생된 부호계열이고 $s_{2(7)}(t)$는 $X=(0000100)^T$, $\lambda_4=\alpha^4$에 의하여 발생된 부호계열 모두 주기 127이며 다음과 같다.

$s_{1(7)}(t)$= [00010 01001 00100 10110 01011 00000
11001 01100 01110 11010 00010 00100
10110 10010 01101 10001 00101 11000
10100 11001 01010 01000 01011 10001
11011 11]

$s_{2(7)}(t)$= [01001 00100 10110 01011 00000 11001
01100 01110 11010 00010 00100 10110
10010 01101 10001 00101 11000 10100
11001 01010 01000 01011 10001 11011
11000 10]

부호계열 $s_{1(7)}(t)$의 자기상관함수 $R_{1,1(7)}(\tau)$와 서로 다른 부호계열 $s_{1(7)}(t)$와 $s_{2(7)}(t)$ 사이의 상호상관함수 $R_{1,2(7)}(\tau)$는 각각 아래와 같으며 그림 6와 그림 7은 이를 보여준다.

$R_{1,1(7)}(\tau)$=

[-17 15-1-1-1 15-17-1-1 15-1-17 15 15 15 15-1-17-1 15-1
-1-1-1 15 15-1-1-17-1-1-17 15-1 15-1 15-17 15 15-17 15
-1-1 15-1-1-17-1-1-17 15 15-1-1-17-1 15-1-17 15-17-17
127-17-17 15-17-1 15-1-17-1-1 15 15-17-1-1-17-1-1 15-1
-1 15-17 15 15-17 15-1 15-1 15-17-1-1-17-1-1 15 15-1-1
-1-1 15-1-17-1 15 15 15 15-17-1 15-1-1-17 15-1-1-1 15-17]

$R_{1,2(7)}(\tau)$=

[-17-1-1 15-1-1 15-1-1 15 15-1-17 15-1-17 15-1-1-17 15-17
-1-17-1-1-17 15 15-1-1 15-1 15-1-1 15-17-1 15 15-17 15-17
-17-1-1-1-17-1-17 15-1-1 15-1-17 15 15-1 15 15-17-115-17
-1-1-17-1-1 15-17-17-17-1 15-17 15-1-17 15 15 15 -17 15-1
-1-1 15-1-1-1-1-17-1-1-1-1-17 15-1-1-1-1-1-1 15-1-1-1-1
15-1-1-1-1-17 15-1-1-17-1-17-1 15-1]

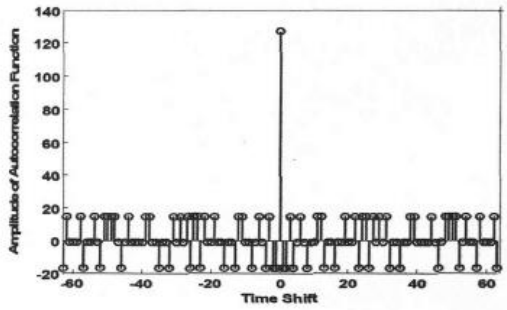


그림 6. $s_{1(7)}(t)$의 자기상관함수 $R_{1,1(7)}(\tau)$.

Fig. 6. Autocorrelation function of $s_{1(7)}(t)$, $R_{1,1(7)}(\tau)$

.

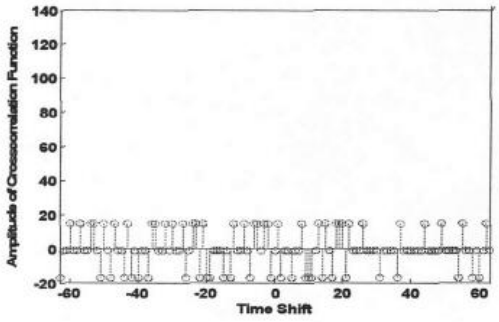


그림 7. 두 부호계열 $s_{1(7)}(t)$과 $s_{2(7)}(t)$간의 상호상관함수 $R_{1,2(7)}(\tau)$.

Fig.7. Crosscorrelation function of two code sequences, $s_{1(7)}(t)$ and $s_{2(7)}(t)$, $R_{1.2(7)}(\tau)$.

이러한 부호계열의 특성분석결과 n=5일 경우 주기 L=31, $\tau\neq 0$에서 자기상관 함수와 상호상관함수 값은 {-9,-1,7}이

며 n=7일 경우 주기 L=127, $\tau \neq 0$에서 자기상관함수와 상호상관함수 값이 {-17,-1, 15}로서 식 (9)로 제시된 상관함수 특성 $R_{i,j}(\tau)=\{-1+2^{(n+1)/2},\ -1,\ -1-2^{(n+1)/2}\}$를 만족함을 알 수 있다.

## VI. 결 론

본 논문에서는 S.Bostas와 V.Kumar에 의해 제시된 유한장에서 정의되는 Trace 함수로 이루어진 발생알고리즘을 분석하고 다항식 기저를 이용한 부울함수를 이용하여 부호계열 발생기 구성 함수를 도출하였다. 이 함수를 이용하여 부호계열 발생기를 설계·구성하고 부호계열을 발생하였다. 발생된 부호계열의 특성 분석을 통하여 부호계열 발생기 구성 함수의 유도와 발생기 구성이 정확하였음을 확인할 수 있었다. 본 연구 결과 부울함수를 이용한 발생기 구성함수는 수식적인 개념의 Trace 함수에 비하여 이진 디지털 하드웨어 구성에 보다 쉽게 접근할 수 있지만 구성함수의 도출에 따른 연산을 간단히 하기 위한 노력도 요구된다.

## 참 고 문 헌


[1] S.W.Golomb, Shift register sequences, Holden-Day, Inc. San Francisco, 1967.

[2] F.Fan and M.Darnell, Sequence design for communications applications, John Wiley & Sons Inc. New York, 1996.

[3] O.S. Rothaus, "On bent functions," J.Comb.Theory, series A20, pp.300-305, 1976.

[4] K.Khoo, G.Gong, and D.R.Stinson, "A new characterization of semi-bent and bent function on finite field," Designs, Codes, and Cryptography, VOL.38-2, pp.279-295, Feb.2006.

[5] C.Bracken, Z.Zha, "On the Fourier spectra of the infinite families of quadratic APN functions," Advaced in Math. of communications, VOL. 3, NO.3, pp.219-226, March 2009.

[6] R.Gold, "Optimal binary sequences for spread spectrum multiplexing," IEEE Trans. Inform. Theory, VOL. IT-13, pp.154-156, Oct. 1967.

[7] S.Bostas and V.Kumar, "Binary sequences with Gold-Like Correlation but larger linear span" IEEE Trans. on Inform. Theory, VOL.40 NO.2, pp.532-537, March 1994.

[8] R.J.McElicec, Finite fields for computer scientists and engineers, Kluwer, Boston, 1987.



**이 정 재** ( Jeong-Jae Lee)

**正會員**

1969.3-1973.2 서강대학교 전자공학과(공학사)

1981.3-1990.8 한양대학교 전자통신공학과 (공학석사, 공학박사)

1987.3-현재: 동의대학교 정보통신공학과 교수

관심분야: 디지털통신시스템, 이동통신, 부호이론