암호화를 위한 정규기저 기반 부호계열 발생 알고리즘 분석 및 발생기 구성

Analysis of Code Sequence Generating Algorithm and Its Implementation based on Normal Bases for Encryption

이정재*
Jeong-jae Lee*

요 약

원소 $\in F(p)$에 대하여 두 종류의 기저함수가 알려져 있다. 통상적인 다항식 기저(polynomial bases)는 $\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$로 이루어지고 이와 다르게 정규 기저(normal bases)는 $\{\alpha,\alpha^p,\alpha^{p^2},\cdots,\alpha^{p^{n-1}}\}$의 형태를 갖는다. 본 논문에서는 소수 p의 원소로 이루어지는 유한장 $GF(p)$상에서 n차원 벡터공간인 확대장 $GF(p^n)$을 이룰 수 있는 정규기저의 발생과 생성에 대하여 검토하고 정규기저를 기반으로 부호계열 발생알고리즘을 분석하여 발생기구성함수를 도출하였다. 차수 n=5와 n=7인 두 종류의 정규기저를 생성할 수 있는 정규다항식을 발견하고 부호계열 발생기를 설계·구성하였다. 마지막으로 Simulink를 이용하여 두 종류(n=5, n=7)의 부호계열 그룹을 발생시키고 발생된 부호계열간의 자기상관함수, $R_{i,i}(\tau)$와 상호상관함수, $R_{i,j}(\tau)$, $i \neq j$ 특성을 분석하였다. 이 결과로부터 정규기저를 이용한 부호계열 발생알고리즘의 분석, 그리고 부호계열 발생기 설계와 구성이 타당함을 확인하였다.

ABSTRACT

For the element $\alpha \in GF(p^n)$, two kinds of bases are known. One is a conventional polynomial basis of the form $\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$, and the other is a normal basis of the form $\{\alpha,\alpha^p,\alpha^{p^2},\cdots,\alpha^{p^{n-1}}\}$. In this paper we consider the method of generating normal bases which construct the finite field $GF(p^n)$, as an n-dimensional extension of the finite field $GF(p)$. And we analyze the code sequence generating algorithm and derive the implementation functions of code sequence generator based on the normal bases. We find the normal polynomials of degrees, n=5 and n=7, which can generate normal bases respectively, design, and construct the code sequence generators based on these normal bases. Finally, we produce two code sequence groups(n=5, n=7) by using Simulink, and analyze the characteristics of the autocorrelation function, $R_{i,i}(\tau)$, and crosscorrelation function, $R_{i,j}(\tau)$, $i \neq j$ between two different code sequences. Based on these results, we confirm that the analysis of generating algorithms and the design and implementation of the code sequence generators based on normal bases are correct.

Keywords : Normal bases, Finite field, Trace function, Code sequence, Correlation function, Normal polynomial

I. 서 론

유한장에서의 효율적인 연산과 구조는 부호이론, 컴퓨터 대수 시스템 그리고 암호 및 보안 등을 포함하는 많은 영역에 응용된다. 특히 유한장에서 연산을 통하여 발생되는 부호계열은 암호, 동기시스템, 랜덤비트발생, 그리고 거리측정 등에 사용된다. 따라서 유한장에서의 연산에 기본이 되는 기저함수의 발견은 유한장을 구성하는 원소를 생성하는 매우 중요한 기반요소다. 가장 관심 있는 기저에는 다항식기저(polynomial bases)와 정규기저(normal bases) 두 종류로 대별된다. 지금까지 정규기저에 대한 다양한 연구가 수행되었으며 S.Perlis[1]은 $n=q^k$(q는 소수, k는 임의의 정

* 동의대학교
투고 일자 : 2014. 3. 13 수정완료일자 : 2014. 4. 28
게재확정일자 : 2014. 5. 2
* 이 논문은 2013학년도 동의대학교 교내연구비에 의하여 연구되었음(2013AA141)

수)에 관련한 정규기저의 생성조건, Pei, Wang, 그리고 Omura[2]는 $=2^k$(r은 양의정수)인 생성조건에서 정규기저를 생성할 수 있는 정규다항식(normal polynomial)의 조건을 제시하였다. 그리고 Y.Chang 등 [3]은 유한장에서 정규기저를 생성할 수 있는 정규다항식 판단알고리즘을 제시하였다. 그리고 S.Gao[4]은 유한장에서 정규기저를 발견할 수 있는 다양한 방법을 검토하였다.

본 연구에서는 앞서 수행된 통상적인 다항식기저[5] 와 다른 정규기저를 기반으로 하여 S.Bostas와 V.Kumar[6]에 의하여 제안된 부호계열 발생알고리즘의 분석을 수행하고 발생기를 구성할 수 있는 발생함수를 도출하였다. 그리고 발생된 부호계열의 특성 분석을 통하여 정규기저기반 부호계열 발생기 설계와 구성이 타당함을 확인하였다. 이를 위하여 제 Ⅱ장에서는 정규기저와 정규다항식 함수의 생성과 특성에 대하여 검토하였다. 제 Ⅲ장에서는 정규기저를 이용하여 부호계열발생 알고리즘을 분석하고 n차원 벡터공간에서 표현하였다. 그리고 제 Ⅳ장에서는 정규기저를 생성할 수 있는 정규다항식 차수가 n=5와 n=7인 두 경우에서 부호계열 발생기를 설계할 수 있는 발생기 구성함수를 도출하고 이를 이용하여 발생기를 설계하였다. 제 Ⅴ장에서는 Simulink를 이용하여 부호계열 발생기를 동작시켜 발생된 부호계열의 상관함수 특성을 분석하였다. 이로부터 정규기저를 이용한 알고리즘 분석과 부호계열 발생기의 설계와 구성이 타당함을 확인하였다. 마지막으로 제 Ⅵ장에서는 결론을 맺는다.

Ⅱ. 정규 기저와 정규 다항식

유한장 p를 소수 그리고 n≥2인 정수라 하면 유한장 $F(p^n)$은 GF(p)상의 차수 n인 벡터공간에 기저를 이용하여 표현할 수 있다. 통상적인 다항식 기저(polynomial bases)는 $\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$로 표현되며 정규기저(normal bases)는 $\{\alpha,\alpha^p,\alpha^{p^2}\cdots,\alpha^{p^{n-1}}\}$로 이루어진다. 여기서 α를 GF(p)상에서 $GF(p^n)$의 정규원소(normal element)라 부른다. 만약 p=2면 $GF(2^n)$에서 $\{\alpha,\alpha^2,\alpha^{2^2}\cdots,\alpha^{2^{n-1}}\}$는 정규기저가 된다. GF(2)상에서의 모든 합은 MOD 2 합 연산으로 1⊕1=0, 1⊕0=1 관계를 가지며 앞으로 연산 ⊕를 간단함을 위하여 +로 표현한다. GF(2) 상에서 차수 n인 기약다항식을 다음 식 (1)과 같이 정의한다.

$$f(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots c_ix^i+\cdots+c_0 \tag{1}$$

여기서 $c_i\in GF(2)$, i=0,....n, 그리고 α를 $GF(2^n)$에서 f(x)의 근이라 하면 $\alpha,\alpha^2,\alpha^{2^2}\cdots,\alpha^{2^{n-1}}$는 f(x)의 모든 근을 형성한다[7]. 따라서 정규기저에서 원소들은 정확하게 정규다항식의 근과 같고 정규다항식은 정규기저를 표현할 수 있는 다른 방법이 된다. S.Perlis[1]는 기약다항식으로부터 정규기저를 근으로 하는 정규다항식을 얻기 위한 노력으로 $n=q^k$일 때 $GF(2^n)$에서 식 (1)의 필요충분조건은 $c_{n-1}\neq 0$임을 보였다. 식 (1)이 정규기저를 근으로 갖기 때문에 다음 식 (2)와 같은 표현이 가능하다.

$$\begin{aligned} f(x)&=(x-\alpha)(x-\alpha^2)(x-\alpha^{2^2})\cdots(x-\alpha^{2^{n-1}}) \\ &= +(\alpha+\alpha^2+\alpha^2+\cdots+\alpha^{2^{n-1}})x^{n-1}+\cdots+\alpha\alpha^2\alpha^{2^2}\cdot\alpha^{2^{n-1}} \end{aligned} \tag{2}$$

식 (1)과 식 (2)를 비교하면 정규기저의 총합으로 이루어지는 식 (3)을 구할 수 있으며

$$c_{n-1}=\alpha+\alpha^2+\alpha^{2^2}+\cdots+\alpha^{2^{n-1}} \tag{3}$$

이는 Trace함수 $Tr_2^n(\cdot)$를 이용하여 식 (4)와 같이 정의할 수 있다.

$$Tr_2^n(\alpha)=\sum_{i=0}^{n-1}\alpha^{2^i}=\alpha+\alpha^2+\alpha^{2^2}+\cdots+\alpha^{2^{n-1}} \tag{4}$$

GF(2)상에서 $c_{n-1}\neq 0$일 조건은 $c_{n-1}=1$을 의미하며 이는 식 (4)에서 $Tr_2^n(\alpha)=1$이 된다. 이 조건은 $n=q^k$인 기약다항식으로부터 정규기저를 근으로 하는 정규다항식을 얻기 위한 필요충분조건이 된다. $Tr_2^n(\alpha)$는 일반적으로 편리함을 위하여 $Tr(\alpha)$로 표현한다. 통상적인 다항식기저 $\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$와 GF(2)상의 원소로 이루어지는 n차원 벡터 $X_p=(x_0,x_1,\cdots\cdots,x_{n-1})$, $x_i\in$GF(2), $i=0,1\ldots,n-1$를 이용하여 $x_p\in GF(2^n)$을 다음 식 (5)와 같이 유일하게 표현할 수 있다.

$$\begin{aligned} x_p&=x_0+x_1\alpha+\cdots+x_{n-1}\alpha^{n-1} \\ &=\sum_{i=0}^{n-1}x_i\alpha^i \end{aligned} \tag{5}$$

한편 정규기저 $\{\alpha,\alpha^p,\alpha^{p^2}\cdots,\alpha^{p^{n-1}}\}$, p=2와 GF(2)상의 원소로 이루어지는 벡터 $X_{nor}=(x_0,x_1,\cdots\cdots,x_{n-1})$, $x_i\in$GF(2), $i=0,1\ldots,n-1$를 이용하여 다음 식 (6)과 같이 $x_{nor}\in GF(2^n)$을 유일하게 표현할 수 있다.

$$\begin{aligned} x_{nor}&=x_0\alpha+x_1\alpha^2+\cdots+x_{n-1}\alpha^{2^{n-1}} \\ &=\sum_{i=0}^{n-1}x_i\alpha^{2^i} \end{aligned} \tag{6}$$

여기서 $\alpha^{2^i}\in GF(2^n)$, $i=0,1\ldots,n-1$이다. 식 (5)와 (6)의 양변에 $Tr(\cdot)$를 취하면 다음 식 (7)과 식 (8)과 같이 표현된다.

$$\begin{aligned} Tr(x_p)&=\sum_{i=0}^{n-1}x_iTr(\alpha^i) \\ &=x_0Tr(\alpha^0)+x_1Tr(\alpha^1)+\cdots+x_{n-1}Tr(\alpha^{n-1}) \end{aligned} \tag{7}$$

$$\begin{aligned} Tr(x_{nor})&=\sum_{i=0}^{n-1}x_iTr(\alpha^{2^i}) \\ &=x_0Tr(\alpha^{2^0})+x_1Tr(\alpha^{2^1})+\cdots+x_{n-1}Tr(\alpha^{2^{n-1}}) \end{aligned} \tag{8}$$

식 (4)로부터 식 (7)은 , $i=0,1,2,\cdots,n-1$에 대한 모든 Trace 값을 알아야만 다항식 기저를 기반으로 한 x_p의 Trace 값을 파악할 수 있다. 그러나 정규기저를 기반으로 한 식 (8)에서는 $r(\alpha)=Tr(\alpha^2)=Tr(\alpha^{2^2})=\cdots=Tr(\alpha^{2^{n-1}})$의 관계를 가지므로 단지 $x_i\in$GF(2)에 의하여 식 (8)의 값이 결정되기 때문에 연산이 매우 간단하게 됨을 알 수 있다. 또한 이 결과는 앞에서 언급한 바와 같이 정규기저를 기반으로 한 $x_{nor}\in GF(2^n)$인 조건을 만족하기 위해서는 $Tr(\alpha)\neq 0$, 즉 $Tr(\alpha)=1$이 필수적임을 확인할 수 있다.

Ⅲ. 부호계열 발생 알고리즘

정규기저를 이용한 부호계열 발생알고리즘의 분석 예로서 S.Bostas와 V.Kumar[6]가 제안한 다음 식 (9)와 같은 알고리즘에 대하여 고려한다.

$$(x)=\begin{cases} r(\lambda_i x)+\sum_{k=1}^{s} Tr(x^{1+2}), & 1\le i\le 2^n,\ \forall x\in GF(2^n) \\ Tr(x), & i=2^n+1,\quad \forall x\in GF(2^n) \end{cases} \tag{9}$$

여기서 n=2s+1로서 홀수이며 $\lambda\in F(2^n)$ 관계를 가진다. 따라서 서로 다른 λ_i로부터 발생군이 2^n+1개인 부호계열을 발생시킬 수 있다. 그리고 발생된 두 부호계열 $s_i(t)$와 $s_j(t)$간의 상관함수 $R_{i,j}(\tau)$는 다음 식 (10)과 같이 정의된다. 여기서 x는 α^t와 대응되며 t는 시간영역에서의 쉬프트(shift)다.

$$R_{i,j}(\tau)=\sum_{t=0}^{-1}(-1)^{s\,(t+\tau)+s_j(t)} \tag{10}$$

여기서 $L=2^n-1$은 주기이며 연산은 $(t+\tau)$ MOD L로이루어진다. 상관함수 $R_{i,j}(\tau)$에서 $i=j$이면 자기상관함수(autocorrelation function) 그리고 $i\neq j$이면 상호상관함수(crosscorrelation function)이 된다. 이로부터 발생된 부호계열간의 상관함수 특성은 다음 식 (11)과 같이 분석되었다[6].

$$R_{i,j}(\tau)=\begin{cases} -1+2^{n}, & i=j,\ \tau=0, \\ -1, \\ -1+2^{(n+1)/2}, \\ -1-2^{(n+1)/2}, \end{cases} \tag{11}$$

발생알고리즘 식 (9)의 $s_i(x)$에 식 (6)을 이용하여 선형결합으로 변화시키면 다음 식 (12)와 같이 표현된다.

$$\begin{aligned} S_i(x_{nor}) &= S_i\Big(\sum_{l=0}^{n-1}x_l\alpha^{2^l}\Big) \\ &= \begin{cases} Tr\Big(\lambda_i\sum_{l=0}^{n-1}x_l\alpha^{2^l}\Big)+\sum_{k=1}^{s}Tr\Big(\Big(\sum_{l=0}^{n-1}x_l\alpha^{2^l}\Big)^{1+2^k}\Big), \\ Tr\Big(\sum_{l=0}^{n-1}x_l\alpha^{2^l}\Big),\ i=2^n+1 \end{cases} \end{aligned} \tag{12}$$

여기서 $1\le i\le 2^n+1$, $\forall x_{nor}\in GF(2^n)$이며 식 (12)를 분석하면 GF(2)에서 발생기를 구성할 수 있는 함수를 구할 수 있다.

Ⅳ. 부호계열 발생기 구성

GF(2)에서 n차 기약다항식 f(x)=$\sum_{i=0}^{n}c_ix^i$, $c_i\in GF(2)$ 그리고 원시원 $\alpha\in GF(2^n)$이라 하면 f(x)가 정규기저를 발생할 수 있는 정규다항식이 될 조건은 식 (1)로부터 $c_{n-1}\neq 0$이며 이는 $c_{n-1}=1$임을 의미한다. 또한 식 (4)로부터 $Tr(\alpha)=1$이 되어야 한다. 정규다항식을 구하고 부호계열 발생기 구성함수를 유도하기 위한 예로서 n=5와 n=7인 두 경우의 기약다항식을 고려한다. 먼저 n=5인 경우 이들에 대응되는 기약다항식은 다음 식 (13)과 같은 형태를 갖는다.

$$\text{f(x)}=\sum_{i=0}^{5}c_ix^i=c_5x^5+c_4x^4+\cdots+c_0x^0,\ c_i\in GF(2) \tag{13}$$

$GF(2^5)$를 구성할 수 있는 원시원 $\alpha\in GF(2^5)$이고 $c_5=c_4=1$, 즉 $Tr(\alpha)=1$을 만족하고 $n=q^k=5$에서 q=5, k=1이 된다. 이 조건과 n=5에서의 기약다항식[8, Table C]를 이용하면 다음 식 (14)와 같은 정규다항식을 얻을 수 있다.

$$f_5(x)=x^5+x^4+x^3+x^2+1 \tag{14}$$

같은 방법으로 n=7인 경우 식 (15)와 같은 형태를 갖는다.

$$\text{f(x)}=\sum_{i=0}^{7}c_ix^i=c_7x^7+c_6x^6+\cdots+c_0x^0,\ c_i\in GF(2) \tag{15}$$

여기서 $GF(2^7)$를 구성할 수 있는 원시원 $\alpha\in GF(2^7)$이라 하면 $c_7=c_6=1$, 즉 $Tr(\alpha)=1$을 만족하고 $n=q^k=7$에서 q=7, k=1이 된다. 이 조건과 n=7에서의 기약다항식[8, Table C]를 이용하면 다음 식 (16)과 같은 정규다항식을 얻을 수 있다.

$$f_7(x)=x^7+x^6+1 \tag{16}$$

식 (14)와 식 (16)을 이용하면 GF(2) 상에서 부호계열 발생기를 구성할 수 있는 부호계열 발생함수를 도출 할 수 있다.

먼저 n=5일 때 정규다항식 $f_5(x)=x^5+x^4+x^3+x^2+1$로 이루어지는 원시원 $\alpha\in GF(2^5)$는 $\alpha^5+\alpha^4+\alpha^3+\alpha^2+1=0$을 만족한다. 식 (9)의 조건에서 n=2s+1이므로 s=2가되며 식 (12), $_{(5)}\ x_{nor}$)을 다음 식 (17)과 같이 표현할 수 있다.

$$\begin{aligned} &S_{i(5)}(x_{nor}) \\ &= \begin{matrix} Tr(\lambda_i x_{nor})+Tr(x_{nor}^3)+Tr(x_{nor}^5),\ 1\le i\le 2^n \\ Tr(x_{nor}),\ i=2^n+1 \end{matrix} \end{aligned}$$

$$\begin{cases} r(\lambda \sum_{l=0}^{4} x_l\alpha^{2^l}) + Tr((\sum_{l=0}^{4} x_l\alpha^{2^l})^3) + Tr((\sum_{l=0}^{4} x_l\alpha^{2^l})^5), \\ Tr(\sum_{l=0}^{4} x_l\alpha^{2^l}),\ i = 2^n + 1 \end{cases} \quad (17)$$

식 (17)의 (x_{or})은 다음 식 (18)과 같은 다항식으로 표현할 수 있다.

$$\begin{aligned} Tr(x_{nor}) &= Tr(\sum_{l=0}^{4} x_l\alpha^{2^l}) \\ &= x_0 Tr(\alpha^{2^0}) + x_1 Tr(\alpha^{2^1}) + x_2 Tr(\alpha^{2^2}) \\ &\quad + x_3 Tr(\alpha^{2^3}) + x_4 Tr(\alpha^{2^4}) \end{aligned} \quad (18)$$

여기서 $Tr(\alpha^{2^0}) = Tr(\alpha^{2^1}) = Tr(\alpha^{2^2}) = Tr(\alpha^{2^3}) = Tr(\alpha^{2^4}) = 1$이므로 $Tr(x_{nor})$은 다음 식 (19)로 표현된다.

$$Tr(x_{nor}) = x_0 + x_1 + x_2 + x_3 + x_4 \quad (19)$$

$Tr(x_{nor})$와 같은 방법으로 $Tr(x_{nor}^3)$은 $x_{nor}^3 = x_{nor} \cdot x_{nor}^2$ 그리고 $Tr(x_{nor}^5)$는 $x_{nor}^5 = x_{nor} \cdot (x_{nor}^2)^2$으로부터 각각 식 (20), (21)과 같이 구할 수 있다.

$$\begin{aligned} Tr(x_{nor}^3) &= Tr(x_{nor} \cdot x_{nor}^2) \\ &= (x_0 + x_2 + x_3) + x_0(x_1x_2 + x_1x_3 + x_2x_4) \\ &\quad + x_1(x_2 + x_3 + x_4) + x_2(x_3 + x_4) + x_3x_4 \end{aligned} \quad (20)$$

$$\begin{aligned} Tr(x_{nor}^5) &= Tr(x_{nor} \cdot (x_{nor}^2)^2) \\ &= x_0(x_1 + x_4) + x_1x_2 + x_2x_3 + x_3x_4 \end{aligned} \quad (21)$$

식 (19), 식 (20) 그리고 식 (21)을 식 (17)에 대입하면 부호계열 $S_{i(5)}(x_{nor})$는 다음 식 (22)와 같은 형태로 표현된다.

$$\begin{aligned} S_{i(5)}(x_{nor}) &= (x_0 + x_1 + x_2 + x_3 + x_4) \\ &\quad + (x_0 + x_2 + x_3) + x_0(x_1x_2 + x_1x_3 + x_2x_4) \\ &\quad + x_1(x_2 + x_3 + x_4) + x_2(x_3 + x_4) + x_3x_4 \\ &\quad + x_0(x_1 + x_4) + x_1x_2 + x_2x_3 + x_3x_4 \\ &= x_4 + x_0(x_2 + x_3) + x_1(x_3 + x_4) + x_2x_4 \end{aligned} \quad (22)$$

식 (22)는 식 (14)의 정규다항식을 이용하여 정규기저를 기반으로 이루어지는 GF(2) 상에서의 부호계열 발생함수며 이를 이용하여 그림 1과 같은 부호계열 발생기를 구성할 수 있다.

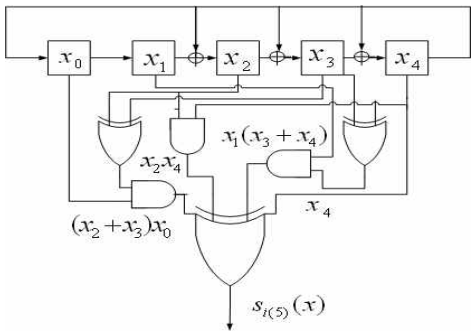

그림 1. n=5에서 정규기저를 기반으로 한 부호계열 발생기
Fig .1. The code sequence generator based on the normal bases for n=5.

두 번째로 n=7인 경우 n=2s+1에서 s는 3이 되며 식 (12)와 식 (16)으로부터 다음 식 (23)과 같이 $S_{i(7)}(x_{nor})$을 구할 수 있다.

$$\begin{aligned} S_{i(7)}(x_{nor}) &= \begin{matrix} Tr(\lambda_i x_{nor}) + Tr(x_{nor}^3) + Tr(x_{nor}^5) + Tr(x_{nor}^9) \\ Tr(x_{nor}),\ i = 2^n + 1 \end{matrix} \\ &= \begin{cases} r(\lambda_i \sum_{l=0}^{n-1} x_l\alpha^{2^l}) + Tr((\sum_{l=0}^{n-1} x_l\alpha^{2^l})^3) + Tr((\sum_{l=0}^{n-1} x_l\alpha^{2^l})^5) + Tr((\sum_{l=0}^{n-1} x_l\alpha^{2^l})^9), \\ Tr(\sum_{l=0}^{n-1} x_l\alpha^{2^l}),\ i = 2^n + 1 \end{cases} \end{aligned} \quad (23)$$

그리고 식 (16)의 정규다항식 $f_7(x) = x^7 + x^6 + 1$로 이루어지는 $GF(2^7)$의 원시원 α는 $\alpha^7 + \alpha^6 + 1 = 0$을 만족한다. 그리고 $Tr(x_{nor})$은 다음 식 (24)와 같이 다항식 형태로 표현할 수 있다.

$$\begin{aligned} Tr(x_{nor}) &= x_0 Tr(\alpha^{2^0}) + x_1 Tr(\alpha^{2^1}) + x_2 Tr(\alpha^{2^2}) + x_3 Tr(\alpha^{2^3}) \\ &\quad + x_4 Tr(\alpha^{2^4}) + x_5 Tr(\alpha^{2^5}) + x_6 Tr(\alpha^{2^6}) \end{aligned} \quad (24)$$

여기서 $Tr(\alpha^{2^0}) = Tr(\alpha^{2^1}) = Tr(\alpha^{2^2}) = Tr(\alpha^{2^3}) = Tr(\alpha^{2^4}) = Tr(\alpha^{2^5}) = Tr(\alpha^{2^6}) = 1$이 되므로 이를 이용하여 $Tr(x_{nor})$을 구하면 식 (24)는 다음 식 (25)와 같이 된다.

$$Tr(x_{nor}) = x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \quad (25)$$

$Tr(x_{nor}^3)$와 $Tr(x_{nor}^5)$은 각각 $x_{nor}^3 = x_{nor} \cdot x_{nor}^2$과 $x_{nor}^5 = x_{nor} \cdot (x_{nor}^2)^2$을 $Tr(x_{nor}^9)$는 $x_{nor}^9 = x_{nor} \cdot ((x_{nor}^2)^2)^2$을 이용하여 각각 다음 식 (26), (27) 그리고 (28)과 같이 구할 수 있다.

$$\begin{aligned} Tr(x_{nor}^3) &= Tr(x_{nor} \cdot x_{nor}^2) \\ &= x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \\ &\quad + x_0(x_2 + x_3 + x_4 + x_5) + x_1(x_3 + x_4 + x_5 + x_6) \\ &\quad + x_2(x_4 + x_5 + x_6) + x_3(x_5 + x_6) + x_4x_6 \end{aligned} \quad (26)$$

$$\begin{aligned} Tr(x_{nor}^5) &= Tr(x_{nor} \cdot (x_{nor}^2)^2) \\ &= x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_0(x_1 + x_2 + x_5 + x_6) \\ &\quad + x_1(x_2 + x_3 + x_6) + x_2(x_3 + x_4) + x_3(x_4 + x_5) \\ &\quad + x_4(x_5 + x_6) + x_5x_6 \end{aligned} \quad (27)$$

$$\begin{aligned} Tr(x_{nor}^9) &= Tr(x_{nor} \cdot (((x_{nor}^2)^2)^2) \\ &= x_0(x_1 + x_6) + x_1x_2 + x_3(x_2 + x_4) + x_5(x_4 + x_6) \end{aligned} \quad (28)$$

식 (25), (26), (27) 그리고 (28)을 식 (23)에 대입하면 $S_{i(7)}(x_{nor})$은 식 (29)와 같은 형태로 표현된다. n=7인 경우 식 (29)의 정규기저 기반 부호발생함수로부터 부호계열 발생기를 그림 2와 같이 구성할 수 있다.

$$\begin{aligned} S_{i(7)}(x_{nor}) &= Tr(x_{nor}) + Tr(x_{nor}^3) + Tr(x_{nor}^5) + Tr(x_{nor}^9) \\ &= x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \\ &\quad + x_0(x_3 + x_4) + x_1(x_4 + x_5) + x_2(x_5 + x_6) + x_3x_6 \end{aligned} \quad (29)$$

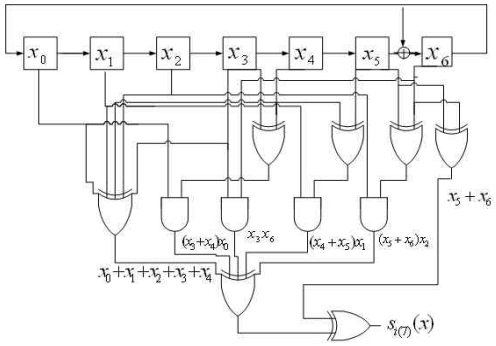

그림 2. n=7에서 정규기저를 기반으로 한 부호계열 발생기
Fig .2. The code sequence generator based on the normal bases for n=7.

V. Simullink를 이용한 부호계열 발생

그림 1의 부호계열발생기를 동작시키기 위하여 먼저 n=5일 때 Simulink를 이용하여 그림 3과 같은 발생기를 구성하였다. 발생기 동작을 보기 위한 스코프는 5단의 쉬프트레지스터 출력과 부호계열발생기 출력을 두 개의 입력으로 가진다.

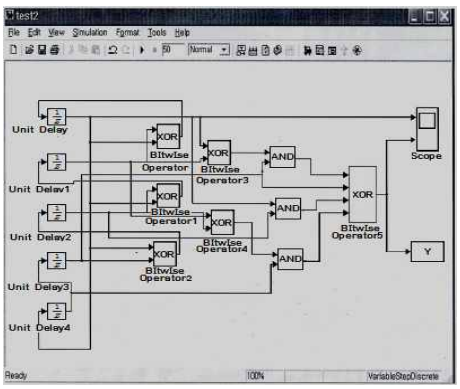

그림 3. n=5, 그림 1에 대한 Simulink를 이용한 부호계열발생기 구성
Fig .3. Implementation of code sequence generator using Simulink for n=5, Fig.1.

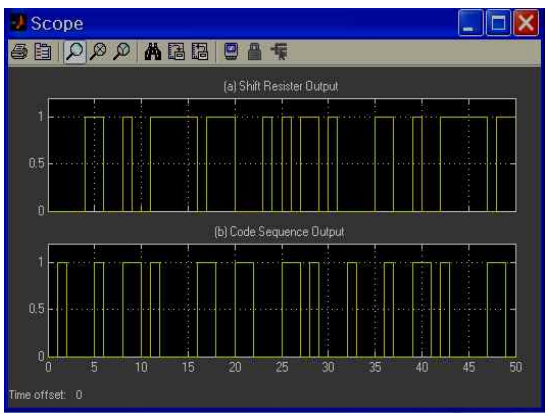

그림 4. (a). n=5에서 쉬프트레지스터 출력,[00001 10010 01111 10111 00010 10110 1]

(b). n=5에서 부호계열발생기 출력, $_{(5)}(t)$, [01000 10011 01000 01100 11000 11010 0]

Fig .4. (a). The shift register output for n=5, [01000 10011 01000 01100 11000 11010 0].

(b). The output of code sequence generator for n=5, $s_{1(5)}(t)$, [01000 10011 01000 01100 11000 11010 0].

그림 4는 스코프의 출력화면을 보여주며 그림 4(a)는 초기조건 $_{nor}$=(10000)에서 쉬프트레지스터로부터 발생되는 계열 [00001 10010 01111 10111 00010 10110 1]을 보여주고 그림 4(b)는 부호계열발생기로부터 발생된 부호계열 $s_{1(5)}(t)$=[01000 10011 01000 01100 11000 11010 0]을 보여준다. 여기서 $0 \le t \le 2^5-1$이며 t=31이 한 주기가 되며 화면상에서는 t=50까지를 보여준다. n=5에서 임의의 다른 부호계열도 쉬프트레지스터의 초기조건을 달리하여 발생시킬 수 있으며 초기조건 X_{nor}=(11011)에서 발생된 부호계열 $s_{2(5)}(t)$=[11110 00011 10001 01011 00011 01011 0]와 같으며 모두 주기 31을 갖는다. 그리고 식 (10)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 각각 그림 5와 그림 6과 같다.

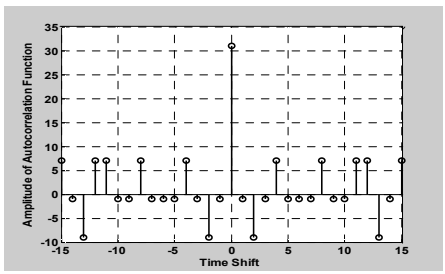

그림 5. $s_{1(5)}(t)$의 자기상관함수 $R_{1,1(5)}(\tau)$
Fig .5. Autocorrelation function of $s_{1(5)}(t)$, $R_{1,1(5)}(\tau)$.

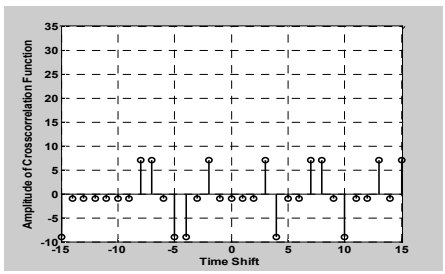

그림 6. 두 부호계열 $s_{1(5)}(t)$와 $s_{2(5)}(t)$간의 상호상관함수 $R_{1,2(5)}(\tau)$
Fig .6. Crosscorrelation function of two code sequences, $s_{1(5)}(t)$ and $s_{2(5)}(t)$, $R_{1,2(5)}(\tau)$.

그림 5에서 자기상관함수 $R_{1,1(5)}(\tau)$ 값은 $\tau=0$에서 부호계열의 길이와 같은 31이 되고 $\tau \neq 0$인 경우 {-9, -1, 7} 크기

를 보인다. 그리고 그림 6에서 상호상관함수 $_{,2(5)}\ \tau$) 값은 {-9, -1, 7}이다. 이는 S.Bostas와 V.Kumar[5]가 제안한 식 (11)에서의 상관함수 특성 $R_{i,j}(\tau)$={$-1-2^{(n+1)/2}$,-1, $-1+2^{(n+1)/2}$}를 n=5에서 만족함을 알 수 있다.

다음으로 n=7일 때 그림 2의 부호발생기를 동작시키기 위하여 Simulink를 이용하여 그림 7과 같은 발생기를 구성하였다. 그림 8은 부호계열발생기를 동작시켰을 때 발생기 출력에 대한 스코프상의 화면을 보여준다.

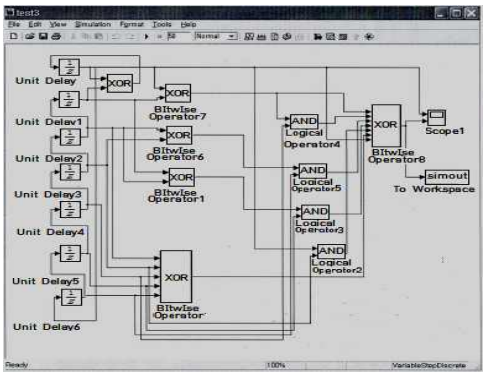

그림 7. n=7, 그림 2에 대한 Simulink를 이용한 부호계열발생기 구성

Fig .7. Implementation of code sequence generator using Simulink for n=7, Fig.2.

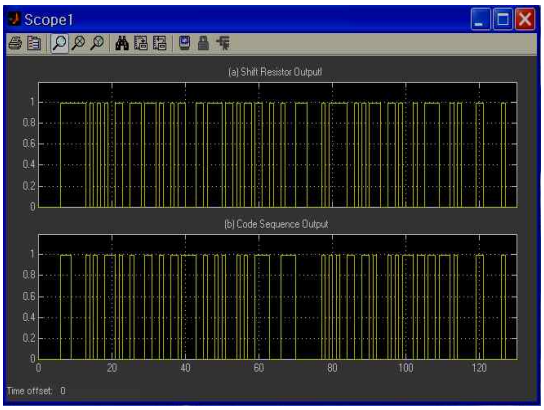

그림 8. (a). n=7에 대한 쉬프트레지스터 출력 [0000001111 1110101010 0110011101 1101001011…]

(b). n=7에 대한 부호계열발생기 출력,$s_{1(7)}(t)$, [0000001110 0001010011 1010010001 1001001101…]

Fig .8. (a). The shift register output for n=7, [0000001111 1110101010 0110011101 1101001011…].

(b) The output of code sequence generator for n=7, $s_{1(7)}(t)$,[0000001110 0001010011 1010010001 1001001101…].

그림 8(a)는 7단을 갖는 초기조건 X_{nor}=(10000)에서 쉬프트레지스터 출력계열 [0000001111 1110101010 01100 11101 1101001011 0001101111 0110101101…]을 보여준다. 그리고 그림 8(b)는 발생기로부터 발생된 출력 부호계열, $s_{1(7)}(t)$ =[0000001110 0001010011 1010010001 1001001101 11100100101 0001010011…]을 보여준다. 여기서 $0 \le t \le 2^7-1$이며 주기는 127이고 화면에서는 t=130까지를 보여준다. 초기조건을 달리하면 임의의 다른 부호계열을 발생시킬 수 있다. 초기조건 X_{nor}=(1010110)에서 $s_{2(7)}(t)$ =[0100110010 0100010000 10100 00001 1010110011 0100110100 1111110100…]이 발생된다.

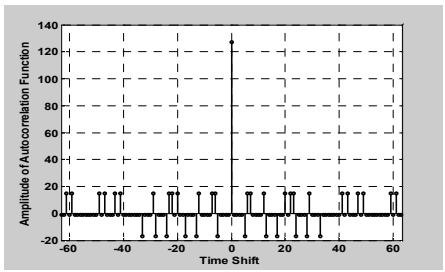

그림 9. $s_{1(7)}(t)$의 자기상관함수 $R_{1,1(7)}(\tau)$

Fig .9. Autocorrelation function of $s_{1(7)}(t)$, $R_{1,1(7)}(\tau)$.

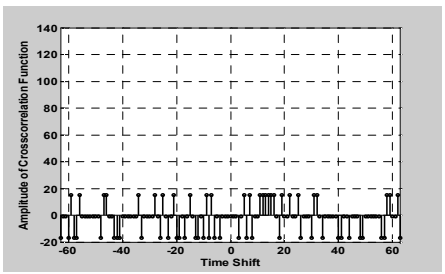

그림 10. 두 부호계열 $s_{1(7)}(t)$과 $s_{2(7)}(t)$간의 상호상관함수 $R_{1,2(7)}(\tau)$

Fig .10. Crosscorrelation function of two code sequences, $s_{1(7)}(t)$ and $s_{2(7)}(t)$, $R_{1,2(7)}(\tau)$.

식 (10)을 이용하여 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 $R_{1,2(7)}(\tau)$를 구한 결과는 각각 그림 9와 그림 10과 같다. 그림 9에서 자기상관함수 $R_{1,1(7)}(\tau)$ 값은 $\tau=0$에서 부호계열의 길이와 같은 127이 되고 $\tau \neq 0$인 경우 {-17, -1, 15} 크기를 보인다. 그리고 그림 10에서 상호상관함수 $R_{1,2(5)}(\tau)$ 값은 {-17,-1,15}이며 이는 n=7일 때 상관함수 특성 $R_{i,j}(\tau)$={$-1-2^{(n+1)/2}$, -1, $-1+2^{(n+1)/2}$}, $\tau \neq 0$을 만족한다. 따라서 n=5의 경우와 같이 n=7에서도 정규기저를 이용한 부호계열 발생알고리즘의 분석과 이 결과를 이용한 부호계열발생기의 설계와 구성이 타당하였음을 확인할 수 있다.

Ⅵ. 결 론

본 논문에서는 n차원 벡터공간에서 F_2)을 형성할 수 있는 통상적인 다항식기저와 다른 정규기저를 이용하여 부호계열발생알고리즘을 분석하였다. 이를 위하여 n=5와 n=7에서 정규기저를 근으로 갖는 정규다항식을 발견하고 부호계열발생기를 구성할 수 있는 정규기저 기반 발생함수를 도출하였다. 부호계열 발생함수를 이용하여 GF(2)에서 부호계열발생기를 설계·구성하였으며 Simulink를 이용하여 발생기의 동작을 확인하였다. 발생된 부호계열의 상관함수 특성 분석을 통하여 정규다항식의 발견, 정규기저의 생성, 그리고 정규기저를 기반으로 한 부호계열 발생기 구성 함수의 유도와 발생기 구성이 타당하였음을 확인하였다. 또한 정규기저를 이용한 발생알고리즘의 분석이 다항식 기저에 비하여 Trace 함수를 포함하는 부호계열발생알고리즘의 연산에 보다 간단함을 알 수 있었다.

참 고 문 헌

[1] S.Perlis, "Normal bases of cyclic fields of prime power degree," Duke Math. J., Vol.9, pp. 507-517, 1942.

[2] D.Y.Pei, C.C.Wang and J.K. Omura, "Normal bases of finite field $GF(2^m)$," IEEE Trans. Inform. Theory, Vol. IT-32, No. 2, pp. 285-287, 1986.

[3] Y.Chang, T.K.Truong, and I.S.Reed, "Normal bases over GF(q)," Journal of Algebra, Vol. 241, pp. 89-101, 2001.

[4] S.Gao, Normal bases over finite fields, Thesis, University of Waterloo, Ontario, Canada, 1993.

[5] 이정재, "부울함수를 이용한 부호계열 발생알고리즘 분석 및 부호계열발생기 구성," 신호처리·시스템학회 논문지, Vol. 13, No. 4, pp. 194-200, 2012. 10.

[6] 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.

[7] A.J.Menezes, et al., Application of finite fields, Boston, Kluwer Academic Pub., pp. 69-92, 1993.

[8] R.Lidl and H.Niederreiter, Finite Fields, London, Addison-Wesley Pub., pp. 553-555, 1983.

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

※주관심분야: 디지털통신시스템, 이동통신, 부호이론