Regular paper

Journal of the KIECS. pp. 133-140, vol. 13, no. 1, Feb. 28 2018, t. 87, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.1.133

생성원리를 통한 수열의 재배열

권민정* · 조성진** · 김진경*** · 최언숙****

Rearrangement of Sequences through the Generation Principle

Min-Jeong Kwon* · Sung-Jin Cho** · Jin-Gyoung Kim*** · Un-Sook Choi****

요 약

본 연구에서는 수열의 특성다항식이 원시다항식의 거듭제곱으로 표현될 때 수열의 생성원리를 밝힘으로써 수열의 재배열 방법을 제시한다. 이를 통하여 수열의 선형복잡도와 필요한 항을 효율적으로 구할 수 있다.

ABSTRACT

In this paper we discover the generation principle of a sequence when the characteristic polynomial of the sequence is a power of a primitive polynomial. With the generation principle, we can rearrange a sequence. Also we get the linear complexity and the required term of the sequence efficiently.

키워드

Generating Function, Characteristic Polynomial, Reciprocal Polynomial, Impulse Response Sequence, Linear Complexity
생성 함수, 특성 다항식, 상반 다항식, 충격 반응 수열, 선형 복잡도

Ⅰ. 서 론

생성함수로부터 얻어지는 수열에 대한 분석은 암호알고리즘을 설계하거나 암호알고리즘을 분석하는데 있어 매우 중요한 문제이다[1,2]. 선형점화식으로 표현된 수열에 대하여 시간 t일 때의 일반항을 알면 빠르게 t항을 얻을 수 있을 뿐만 아니라 t에 따른 각 항의 변화를 쉽게 관찰할 수 있으므로 수열의 분석이 용이해진다.

선형점화식으로 주어진 수열의 일반항을 구하는 문제는 Selmer, Ziele[3,4] 등에 의해 연구되었다. 그러나 특성다항식의 근의 중복도가 유한체의 표수보다 큰 경우 근 사이의 독립성을 보장하기 위한 방법은 McEliece가 특성다항식의 한 근에 대한 켤레근과 유한체 위에서의 이항계수를 이용함으로써 알려졌다[5]. 그 과정에서 McEliece는 독립변수의 개수를 줄였고 유한체의 표수와 관계없이 특성다항식의 근을 이용하여 선형점화식으로 표현된 수열의 일반항을 구하였다. 그러나 이 방법을 이용하여 수열의 일반항을 구하기 위해서는 부분분수로 분해하여 계수를 모두 구해야 하는 어려운 과정을 거쳐야 한다.

본 연구에서는 특성다항식이 원시다항식의 거듭제곱으로 표현되는 경우 특성다항식을 따르는 수열의 생성원리를 밝힌다. 이를 통해 수열의 일반항을 구하

* 부경대학교 응용수학과(mjblack02@pknu.ac.kr)
** 교신저자 : 부경대학교 응용수학과
*** 부경대학교 응용수학과(5892587@hanmail.net)
**** 동명대학교 정보통신공학과(choies@tu.ac.kr)
· 접 수 일 : 2017. 11. 30
· 수정완료일 : 2018. 01. 07
· 게재확정일 : 2018. 02. 15
· Received : Nov. 30, 2017, Revised : Jan. 07, 2018, Accepted : Feb. 15, 2018
· Corresponding Author : Sung-Jin Cho
Dept. of Applied Math., Pukyong National University,
Email : sjcho@pknu.ac.kr

기 위한 복잡한 계산이나 선형점화식을 이용하기 위해서 그 이전 항을 구하지 않고도 선형복잡도와 원하는 항을 효율적으로 구할 수 있다.

II. 사전지식

이진수열 $s_0, s_1, s_2, \cdots$ 로 수열 $s=(s_0, s_1, s_2, \cdots)$를 정의할 때, 임의의 t, $t=0,1,2,\cdots$ 에 관하여 $s_{t+e}=s_t$를 만족하는 최소의 자연수 e를 수열 s의 주기라고 한다. 수열 s를 간단히 $s=(s_t)$로 나타내고 수열 s의 한 주기까지의 항으로 이루어진 수열 $(s_0, s_1, s_2, \cdots, s_{e-1})$를 간단히 $\overline{s}$로 나타내자. 수열 $\overline{s}$에 대하여 항 s_i, $1 \le i \le e-1$부터 시작하고 길이 e인 수열 $(s_i, s_{i+1}, \cdots s_{e-1}, s_0, s_1, \cdots, s_{i-1})$는 $\overline{s_i}$, 모든 성분이 0이고 길이가 e인 수열은 $\overline{0}$로 나타낸다. 수열 $s=(s_t)$가 선형점화식

$$s_{t+n}=a_{n-1}s_{t+n-1}+\cdots+a_1s_{t+1}+a_0s_t \quad (1)$$

$a_i \in GF(2)$, $0 \le i \le n-1$을 만족할 때, n개의 항으로 이루어진 벡터 $\langle s_0, s_1, s_2, \cdots, s_{n-1}\rangle$를 수열 s의 초기상태벡터라 한다. 또한 수열 s의 모든 항은 식 (1)에 의하여 결정되므로 선형점화식 (1)을 간단히 LFSR(Linear Feedback Shift Register)라고 한다[6-8].

선형점화식 (1)에 의하여 생성되는 수열의 주기를 확인하기 위하여 그에 대응되는 $GF(2)$에서의 n차 다항식

$$f(x)=x^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0$$

를 수열 s의 특성다항식(characteristic polynomial)이라 한다.

정의 2.1. $GF(2)$ 위에서 정의된 n차 다항식 $f(x)=x^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0$에 대하여 $f^*(x)=x^nf\left(\frac{1}{x}\right)$로 정의된 다항식 $f^*(x)$를 $f(x)$의 상반다항식이라 한다.

정의 2.2. n차 선형점화식과 초기상태벡터 $\langle s_0, s_1, \cdots, s_{n-1}\rangle$, $s_0=s_1=\cdots=s_{n-2}=0$, $s_{n-1}=1$에 의하여 유일하게 얻어지는 수열 $s=(s_t)$를 충격반응수열(impulse response sequence)이라 한다.

선형점화식을 만족하는 수열 s는 초기상태벡터에 따라 서로 다른 주기의 수열이 생성될 수 있는데 그 중에서 충격반응수열의 주기가 가장 길다[9].

예제 2.3. 수열 $s=(s_t)$가 $s_{t+4}=s_{n+3}+s_{t+1}+s_t$를 만족한다고 하자. 초기상태벡터 (s_0, s_1, s_2, s_3)에 따라 다음과 같이 서로 다른 수열이 생성된다.

(1) 초기상태벡터 (0,0,0,1)일 때, 0,0,0,1,1,1,0,0,0,1,1,1,..., 주기 6인 수열 생성

(2) 초기상태벡터 (0,1,0,1)일 때, 0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,..., 주기 2인 수열 생성

(3) 초기상태벡터 (0,0,1,0)일 때, 0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,..., 주기 3인 수열 생성

정의 2.4. 수열 $s=(s_t)$에 대하여

$$g(x)=\sum_{i=0}^{\infty}s_ix^i \quad (2)$$

로 정의된 급수를 수열 s의 생성함수(generating function)라 한다.

특성다항식 $f(x)$에 의하여 생성된 수열 s의 주기를 e라 하면

$$g(x)=\sum_{i=0}^{\infty}x^{ei}\left(s_0+s_1x+\cdots+s_{e-1}x^{e-1}\right)$$

이므로 $s(x) \equiv g(x) \bmod x^e$라 두면

$$s(x)=s_0+s_1x+s_2x^2+\cdots+s_{e-1}x^{e-1} \quad (3)$$

이다. 주어진 주기의 수열을 생성하기 위해 필요한 항의 최소개수로 정의되는 선형복잡도는 $s(x)$에서 계수가 0이 아닌 항의 개수와 같다[10].

III. 생성함수와 특성다항식

보조정리 3.1. 수열 $s=(s_t)$의 특성다항식을 $f(x)$, $\deg f(x)=n$, 생성함수를 $g(x)$라 하면

$$g(x)=\frac{c(x)}{f^*(x)},\ 0 \le \deg c(x) \le n-1 \quad (4)$$

이다[11].

식 (4)의 $c(x)$는 초기상태벡터에 의하여 결정된다. 특성다항식 $f(x)$에 의하여 생성되는 충격반응수열을 $I=(I_t)$ 라 할 때, $c(x)=x^u$, $0 \le u \le n-1$ 인 경우, 수열 s에 대하여 $\overline{s}=\overline{I_{n-u-1}}$ 이다. 즉, 수열 s는 충격반응수열의 첫 번째 1이 $(u+1)$번째에 위치하는 수열이다.

예제 3.2. $f(x)=x^4+x+1$에 의해 생성되는 수열 $s=(0,0,0,1,0,0,1,1,0,1,0,1,1,1,1,\cdots)$ 에 대하여 $s_{t+4}=s_{t+1}+s_t,\ t=0,1,2,\cdots$ 이므로

$f^*(x)g(x)=s_0+s_1x+s_2x^2+(s_0+s_3)x^3$

이다. 수열 s는 초기상태벡터가 $(0,0,0,1)$인 충격반응수열이므로 $c(x)=x^3$이고 $g(x)=\dfrac{x^3}{f^*(x)}$ 이다.

특성다항식 $f(x)$에 의하여 생성된 수열 s의 주기를 e라 하면 식 (2)로부터

$$g(x)=\sum_{i=0}^{\infty}x^{ei}\left(s_0+s_1x+\cdots+s_{e-1}x^{e-1}\right)$$
$$=\frac{s_0+s_1x+\cdots+s_{e-1}x^{e-1}}{1+x^e}$$

이고 식 (4)로부터

$$g(x)=\frac{s_0+s_1x+\cdots+s_{e-1}x^{e-1}}{1+x^e}=\frac{c(x)}{f^*(x)}$$

이다. 특성다항식이 기약다항식인 경우, 생성되는 수열은 위상이동차만 다를 뿐 각 항이 배열되는 순서와 주기는 모두 같기 때문에 충격반응수열의 위상이동차를 확인함으로써 $c(x)$를 결정할 수 있다. 따라서 본 논문에서는 $c(x)=1$일 때 수열의 배열을 다루겠다.

보조정리 3.3. 수열 $s=(s_t)$의 특성다항식을 $f(x)$, or$df(x)=e$라 하자. $f(x)$에 의하여 생성되는 충격반응수열 $I=(I_t)$ 에 대하여 $\overline{s}=\overline{I_{n-1}}$ 이라 하면 다음이 성립한다.

$$s(x)=\frac{1+x^e}{f^*(x)}$$

다항식 $s(x)$의 계수는 수열 s의 $s_0,s_1,\cdots,s_{e-1}$ 이므로 0이 아닌 항의 개수는 수열 s에서 한 주기 내에 존재하는 1의 개수와 같다. 따라서 $s(x)$를 확인함으로써 수열 s의 배열과 선형복잡도를 알 수 있다.

이제 n차 기약다항식 $f(x)$, or$df(x)=e$에 대하여 $F(x)=\{f(x)\}^m$, $2^{r-1}<m\le 2^r$일 때, $F(x)$에 의하여 생성되는 수열에 대하여 살펴보자.

수열 $\sigma=(\sigma_t)$가 $F(x)$에 의해 생성되는 이진수열이라 하면 σ의 생성함수 $G(x)$는 보조정리 3.1로부터

$$G(x)=\frac{c(x)}{F^*(x)},\ 0\le \deg c(x)\le mn-1 \qquad (5)$$

이다. $F(x)$에 의하여 생성되는 충격반응수열을 $I=(I_t)$ 라 할 때, $c(x)=x^u$, $0\le u\le mn-1$ 이면 수열 σ에 대하여 $\overline{\sigma}=\overline{I_{mn-u-1}}$ 이다. 특성다항식이 기약다항식의 거듭제곱으로 표현되는 경우도, 생성되는 수열은 위상이동차만 다르고 그 배열이 같은 수열이므로 본 연구에서는 일반성을 잃지 않고 $c(x)=1$인 경우를 다루겠다. 따라서 $G(x)=\dfrac{1}{F^*(x)}$ 이다.

n차 기약다항식 $f(x)$에 의하여 생성되는 수열 s의 주기를 e라 하고 $F(x)$에 의하여 생성되는 수열 σ의 주기를 E라 하면 $E=2^r\cdot e$ 이다.

$\sigma(x)\equiv G(x) \bmod x^E$ 라 하면 다음이 성립한다.

$$\sigma(x)=\frac{1+x^E}{F^*(x)} \qquad (6)$$

예제 3.4. $f(x)=x^3+x+1$, $F(x)=\{f(x)\}^2$ 이라 하자. $F(x)$에 의하여 생성되는 충격반응수열 $I=(I_t)$에 대하여 $F(x)$에 의하여 생성되는 수열 σ를 $\overline{\sigma}=\overline{I_{mn-1}}$ 라 하면

$\sigma=(1,0,0,0,1,\ 0,1,0,1,0,0,0,0,0,1,0,0,0,\cdots)$

이고 주기는 14이고 생성함수는 다음과 같다.

$$G(x)=1+x^4+x^6+x^8+x^{14}(1+x^4+x^6+x^8)+\cdots$$
$$=\frac{1+x^4+x^6+x^8}{1+x^{14}}=\frac{1}{(1+x^2+x^3)^2}$$

Ⅳ. 수열의 재배열

이제 $F(x)$에 의해 생성되는 수열의 생성원리를 확

인하여 수열 σ를 재배열함으로써 원하는 항과 선형 복잡도를 효율적으로 구하고자 한다.

정리 4.1. 주기 e인 수열 $s=(s_t)$의 특성다항식을 $f(x)$라 하자. $F(x)=\{f(x)\}^m$, $2^{r-1}<m\le 2^r$ 일 때, $F(x)$에 의하여 생성되고 주기 E인 수열 $\sigma=(\sigma_t)$의 생성함수 $G(x)$를

$$G(x)=\frac{A(x)B(x)}{1+x^E},\ B(x)=[f^*(x)]^{2^r-m}$$

라 두면 $A(x)=[s(x)]^{2^r}$이다.

증명. $f(x)$에 의하여 생성되는 수열 s는 주기가 e이고 $2^{r-1}<m\le 2^r$이므로 $F(x)$에 의해 생성되는 수열 σ의 주기 E는 $E=2^r\cdot e$이다. 식 (5)에 의하여 $s(x)=\frac{1+x^e}{f^*(x)}$ 이고, 식 (6)으로부터 수열 σ의 생성함수 $G(x)$는

$$G(x)=\frac{\sigma(x)}{1+x^E}=\frac{1}{F^*(x)}$$
$$=\frac{1}{[f^*(x)]^m}=\frac{A(x)[f^*(x)]^{2^r-m}}{(1+x^e)^{2^r}}$$

이므로 $B(x)=[f^*(x)]^{2^r-m}$이라 두면

$$A(x)=\left[\frac{1+x^e}{f^*(x)}\right]^{2^r}=[s(x)]^{2^r}$$

이다.

$A(x)$에 의하여 생성되는 수열을 $\alpha=(\alpha_t)$라 하면 $A(x)=[s(x)]^{2^r}=s_0+s_1x^{2^r}+\cdots+s_{e-1}x^{(e-1)2^r}$이다. 수열 s의 주기가 e이므로 수열 α의 주기는 $2^r\cdot e$이고, $i=0,1,2,\cdots,e-1$에 대하여

$$\alpha_{i\cdot 2^r+j}=\begin{cases}s_i, & j=0\\ 0, & j\neq 0\end{cases} \quad (7)$$

이다. 이것은 $\overline{s}$의 각 항 사이에 2^r-1개의 0을 끼워 넣은 삽입수열이다.

예제 4.2. $f(x)=x^3+x+1$에 의하여 생성되는 충격반응수열을 $I=(I_t)$라 하자. $f(x)$를 따르는 수열 s에 대하여 $\overline{s}=\overline{I_2}$라 하면 $\overline{s}=(1,0,1,1,1,0,0)$이고 $s(x)=1+x^2+x^3+x^4$이다.

$A(x)=[s(x)]^2$라 두면 $A(x)=1+x^4+x^6+x^8$이므로 $A(x)$를 따르는 수열 α는 주기가 14이고, $i=0,1,2,\cdots,6$에 대하여

$$\alpha_{2i+j}=\begin{cases}s_i, & j=0\\ 0, & j\neq 0\end{cases}$$

이다. 이것은 $\overline{s}$의 각 항 사이에 0을 하나씩 끼워 넣은 수열이다.

표 1. $A(x)$를 따르는 수열 $\overline{\alpha}$
Table 1. The sequence $\overline{\alpha}$ by $A(x)$

α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}	α_{13}
1	0	**0**	0	**1**	0	**1**	0	**1**	0	**0**	0	**0**	0
s_0		s_1		s_2		s_3		s_4		s_5		s_6	

따라서 $\overline{\alpha}$의 각 성분 α_{2i+j}, $i=0,1,2,\cdots,6$는 2×7 행렬로 나타내면 1행은 $\overline{s}$와 같고 2행은 $\overline{0}$이다.

표 2. $A(x)$를 따르는 수열 $\overline{\alpha}$의 재배열
Table 2. Rearrangement of $\overline{\alpha}$ by $A(x)$

j \ i	0	1	2	3	4	5	6
0	**1**	**0**	**1**	**1**	**1**	**0**	**0**
1	0	0	0	0	0	0	0

이제 $F(x)$에 의하여 생성되는 수열 $\sigma=\sigma(t)$에 대해 알아보자. $A(x)$를 따르는 수열의 배열의 배열을 확인하였으므로 $A(x)$와 다항식이 곱해진 형태인 경우 생성되는 수열 α에 대하여 살펴보자. 우선 $x^tA(x)$, $0\le t\le e\cdot 2^r-1$를 따르는 수열 $\alpha=(\alpha_t)$의 배열부터 확인하고자 한다. 수열 α의 주기는 $e\cdot 2^r$이므로 $2^r\times e$ 행렬 M으로 나타낼 수 있다. 이때 행렬 M의 i열은 M_i, j행은 M^j로 간단히 나타내기로 한다[12].

표 3. $A(x)$를 따르는 수열 $\overline{\alpha}$
Table 3. The sequence $\overline{\alpha}$ by $A(x)$

$$M=\begin{pmatrix}
\alpha_0 & \alpha_{2^r} & \cdots & \alpha_{i\cdot 2^r} & \cdots & \alpha_{(e-1)2^r} & 0\\
\alpha_1 & \alpha_{2^r+1} & \cdots & \alpha_{i\cdot 2^r+1} & \cdots & \alpha_{(e-1)2^r+1} & 1\\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots\\
\alpha_j & \alpha_{2^r+j} & \cdots & \alpha_{i\cdot 2^r+j} & \cdots & \alpha_{(e-1)2^r+j} & j\\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots\\
\alpha_{2^r-1} & \alpha_{2\cdot 2^r-1} & \cdots & \alpha_{(i+1)2^r-1} & \cdots & \alpha_{e\cdot 2^r-1} & 2^r-1\\
0 & 1 & \cdots & i & \cdots & e-1 &
\end{pmatrix}$$

식 (7)에 의하여 $\overline{\alpha}$의 배열은 다음과 같다.

ⅰ) $x^tA(x),\ 0 \le t \le 2^r-1$

$$x^tA(x) = x^t[s(x)]^{2^r}$$
$$= s_0x^t + s_1x^{2^r+t} + \cdots + s_{e-1}x^{(e-1)2^r+t}$$

이므로 α의 각 항은

$$\alpha_{i\cdot 2^r+j} = \begin{cases} s_i & , j=t \\ 0 & , j \neq t \end{cases},\ i=0,1,2,\cdots,e-1$$

이다. 따라서 $\overline{\alpha}$를 행렬 M을 이용하여 배열하면

$$M^j = \begin{cases} \overline{s} & , j=t+1 \\ \overline{0} & , j \neq t+1 \end{cases}$$

이다.

표 4. $x^tA(x),\ 0 \le t \le 2^r-1$를 따르는 $\overline{\alpha}$
Table 4. $\overline{\alpha}$ by $x^tA(x),\ 0 \le t \le 2^r-1$

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ \boldsymbol{s_0} & \boldsymbol{s_1} & \boldsymbol{s_2} & \boldsymbol{s_3} & \cdots & \boldsymbol{s_{e-1}} \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

ⅱ) $x^tA(x),\ 2^r \le t \le e\cdot 2^r-1$

$t = k\cdot 2^r + l,\ k=1,2,\cdots,e-1$로 나타내면

$$x^tA(x) = x^l[x^ks(x)]^{2^r}$$
$$= x^l\left(s_0x^k + s_1x^{2^r+k} + \cdots + s_{e-1}x^{(e-1)2^r+k}\right)$$

이다. 따라서 수열 α는 $i=0,1,2,\cdots,e-1$ 에 대하여

$$\alpha_{i\cdot 2^r+j} = \begin{cases} s_{e-k+i} & , j=l,\ i=0,1,2,\cdots,k-1 \\ s_{i-k} & , j=l,\ i=k,k+1,\cdots,e-1 \\ 0 & , j \neq l \end{cases}$$

이고 행렬 M을 이용하여 수열 $\overline{\alpha}$를 배열하면

$$M^j = \begin{cases} \overline{s_{e-k}} & , j=l+1 \\ \overline{0} & , j \neq l+1 \end{cases}$$

이다.

표 5. $x^tA(x),\ 2^r \le t \le 2^re-1$를 따르는 $\overline{\alpha}$
Table 5. $\overline{\alpha}$ by $x^tA(x),\ 2^r \le t \le 2^re-1$

$$M = \begin{pmatrix} 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \boldsymbol{s_{e-k}} & \cdots & \boldsymbol{s_{e-1}} & \boldsymbol{s_0} & \boldsymbol{s_1} & \cdots & \boldsymbol{s_{e-k-1}} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

서로 다른 $t_1, t_2,\ 0 \le t_1, t_2 \le e\cdot 2^r-1$에 대하여 $x^{t_1}A(x)+x^{t_2}A(x)$를 따르는 수열 α는 다음과 같다.

ⅲ) $0 \le t_1, t_2 \le 2^r-1$ 인 경우

ⅰ)의 결과와 행렬 M을 이용하여 수열 $\overline{\alpha}$를 배열하면

$$M^j = \begin{cases} \overline{s} & , j=t_1+1, t_2+1 \\ \overline{0} & , otherwise \end{cases}$$

이다.

ⅳ) $0 \le t_1 \le 2^r-1,\ 2^r \le t_2 \le e\cdot 2^r-1$인 경우

$t_2 = k_2 2^r + l_2$라 두고 ⅰ), ⅱ)의 결과와 행렬 M을 이용하면 수열 $\overline{\alpha}$를 표현할 수 있다. $t_1 \neq l_2$이면

$$M^j = \begin{cases} \overline{s} & , j=t_1+1 \\ \overline{s_{e-k_2}} & , j=l_2+1 \\ \overline{0} & , otherwise \end{cases}$$

이고 $t_1 = l_2$이면

$$M^j = \begin{cases} \overline{s} \oplus \overline{s_{e-k_2}} & , j=t_1+1 \\ \overline{0} & , j \neq t_1+1 \end{cases}$$

이다.

ⅴ) $2^r \le t_1, t_2 \le e\cdot 2^r-1$

$t_1 = k_1 2^r + l_1,\ t_2 = k_2 2^r + l_2$라 두고 ⅰ)~ⅳ)의 결과와 행렬 M을 이용하여 수열 $\overline{\alpha}$를 표현할 수 있다. 우선 $l_1 \neq l_2$이면

$$M^j = \begin{cases} \overline{s_{e-k_1}} & , j=l_1+1 \\ \overline{s_{e-k_2}} & , j=l_2+1 \\ \overline{0} & , otherwise \end{cases}$$

이고 $l_1 = l_2$이면

$$M^j = \begin{cases} \overline{s_{e-k_1}} \oplus \overline{s_{e-k_2}} & , j=l_1+1 \\ \overline{0} & , j \neq l_1+1 \end{cases}$$

이다.

지금까지 $A(x)$에 의하여 생성되는 수열로부터 $A(x)$에 어떤 다항식이 곱해졌을 때 생성되는 수열의 배열을 살펴보았다. 이 결과로부터 $F(x)$를 따르는 수열 σ의 배열을 알기 위해서는 $A(x)$와 곱해진 다항식 $B(x)$의 형태를 확인할 필요가 있다.

$f(x)$가 n차 원시다항식이면 상반다항식 $f^*(x)$도 n차 원시다항식이다. 따라서 $B(x) = [f^*(x)]^{2^r-m}$라 정의하면, $\deg B(x) = n(2^r-m)$이고

$$B(x) = b_0 + b_1x + \cdots + b_{2^r}x^{2^r} + \cdots + b_{n(2^r-m)}x^{n(2^r-m)}$$

이다. 여기서 $N=\left[\frac{n(2^r-m)}{2^r}\right]$ 이라 두면

$$B(x)=\sum_{k=0}^{N}x^{k\cdot 2^r}\left(b_{k2^r}+b_{k2^r+1}x+\cdots+b_{(k+1)2^r-1}x^{2^r-1}\right)$$

이다.

보조정리 4.3. n차 원시다항식 $f(x)$에 대하여 $F(x)=\{f(x)\}^m$, $2^{r-1}<m\le 2^r$라 하자. $F(x)$에 의하여 생성되는 수열 σ의 생성함수 $G(x)$를

$$G(x)=\frac{A(x)B(x)}{1+x^E},\ B(x)=[f^*(x)]^{2^r-m}$$

로 나타내고 $N=\left[\frac{n(2^r-m)}{2^r}\right]$ 라 하면

$$B(x)=\sum_{k=0}^{N}x^{k\cdot 2^r}B_k(x),\ B_k(x)=\sum_{j=0}^{2^r-1}b_{k\cdot 2^r+j}x^j$$

이다.

정리 4.4. n차 원시다항식 $f(x)$에 대하여 $F(x)=\{f(x)\}^m$, $2^{r-1}<m\le 2^r$라 하자. $F(x)$에 의하여 생성되는 수열 σ의 생성함수 $G(x)$를

$$G(x)=\frac{A(x)B(x)}{1+x^E},\ B(x)=[f^*(x)]^{2^r-m}$$

로 나타내고 $N=\left[\frac{n(2^r-m)}{2^r}\right]$ 이라 하면

$$B(x)=\sum_{k=0}^{N}x^{k\cdot 2^r}B_k(x),\ B_k(x)=\sum_{j=0}^{2^r-1}b_{k\cdot 2^r+j}x^j$$

일 때, σ의 선형복잡도는 $2^{n-1}|P|$ 이다. 여기서 $P=\{j\,|P_j\neq\varnothing, j=0,1,2,\cdots,2^r-1\}$,
$P_j=\{k\,|b_{k\cdot 2^r+j}=1,\ k=0,1,2,\cdots,N\}$ 이다.

증명. 수열 σ의 선형복잡도를 구하기 위해 수열 $\overline{\sigma}$에 존재하는 1의 개수를 확인하고자 한다. 정리 4.1에 의하여 $A(x)$의 0이 아닌 항의 개수는 $s(x)$의 0이 아닌 항의 개수와 같다. 수열 s는 n차 원시다항식 $f(x)$에 의해 생성되는 수열이므로 $\overline{s}$에 존재하는 1의 개수는 2^{n-1}이고 이것은 $A(x)$의 0이 아닌 항의 개수와 같다. $B_k(x)=\sum_{j=0}^{2^r-1}b_{k\cdot 2^r+j}x^j$이므로 $A(x)B_k(x)$를 전개했을 때 소거되는 항은 없다. 따라서 w_k를 $B_k(x)$의 0이 아닌 항의 개수라 할 때, $A(x)B_k(x)$에서 0이 아닌 항의 개수는 $2^{n-1}w_k$이다.

$A(x)B(x)$를 따르는 $\overline{\sigma}$에 존재하는 1의 개수를 확인하기 위해 $2^r\times 2^n$ 행렬 M을 이용한다.

$P_j=\{k\,|b_{k\cdot 2^r+j}=1,\ k=0,1,2,\cdots,N\}$ 에 대하여, $P_j=\varnothing$이면, $M^{j+1}=\overline{0}$이다. $P_j\neq\varnothing$이면, iii)의 결과에 의하여 $M^{j+1}=\oplus_{k\in P_j}\overline{s_{2^n-1-k}}$이다. $\overline{s_{2^n-1-k}}$, $k\in P_j$는 모두 원시다항식 $f(x)$에 의하여 생성되는 수열이므로 $M^{j+1}=\overline{s_K}$, $0\le K\le 2^n-1$이고 M^{j+1}에 존재하는 1의 개수는 2^{n-1}개다. 즉, 수열 $\overline{\sigma}$에는 $P_j\neq 0$인 j의 개수만큼 2^{n-1}개의 1이 발생하므로 $\overline{\sigma}$에 존재하는 1의 개수는 $2^{n-1}|P|$ 이다.

정리 4.4의 결과로부터 $F(x)$에 의해 생성되는 수열 σ의 각 항이 배열되는 원리를 통해 수열 σ의 선형복잡도와 필요한 항을 효과적으로 구할 수 있다.

예제 4.5. $f(x)=x^3+x+1$, $F(x)=\{f(x)\}^5$이라 하자. $F(x)$에 의하여 생성되는 수열 σ의 생성다항식 $G(x)$를 $G(x)=\frac{A(x)B(x)}{(1+x^7)^8}$ 로 나타내면

$B(x)=\{f^*(x)\}^3$ 이다. $B(x)=(1+x^2+x^3)^3$
$=(1+x^2+x^3+x^4+x^7)+x^8(1+x)$이고 $f(x)$는 원시다항식이므로 주기는 2^3-1, 한 주기 내에 존재하는 1의 개수는 2^2개다.

표 6은 $F(x)$에 의하여 생성된 주기 56인 수열 σ에 대하여 항 σ_{2^3i+j}, $i=0,1,2,\cdots,7$ 를 8×7 행렬로 나타낸 것이다. 따라서 수열 σ에 대하여 $\overline{\sigma}$의 배열은 $(1,0,1,1,1,0,0,1,1,1,0,0,0,0,0,0,1,0,1,1,1,1,0,0,1,0,1,1,1,1,\cdots,0,0,0,0,0)$이다.

표 6. $F(x)$를 따르는 $\overline{\sigma}$
Table 6. $\overline{\sigma}$ by $F(x)$

$$M=\begin{pmatrix}1&1&1&0&0&1&0\\0&1&0&1&1&1&0\\1&0&1&1&1&0&0\\1&0&1&1&1&0&0\\1&0&1&1&1&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\\1&0&1&1&1&0&0\end{pmatrix}$$

Ⅴ. 결 론

본 연구에서는 수열의 특성다항식이 원시다항식의 거듭제곱으로 표현될 때 수열의 생성원리를 밝힘으로써 수열을 새로운 방식으로 배열하는 방법을 모색하였다. 이를 이용하여 수열의 선형복잡도와 필요한 항을 효과적으로 구할 수 있다. 본 연구의 결과는 앞으로 특성다항식이 기약다항식의 거듭제곱이 되는 90/50 셀룰라 오토마타의 연구에 도움에 되리라 사료된다.

감사의 글

본 논문은 Proceedings, ICEIC 2017 우수 논문[Representation of a Sequence in an Array Form]을 확장한 논문임.

References

[1] M. Song, Y. Kang and H. Kim, "Performance evaluation of big steam based high speed data storage," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 5, Oct. 2017, pp. 817-827.

[2] Y. Kim, "On efficient algorithms for generatinng fundamental units and their H/W implementations over number fields," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, Dec. 2017, pp. 1181-1187.

[3] E. Selmer, *Linear recurrence relations over finite fields*, Department of Mathematics, University of Bergen, Bergen, 1966.

[4] N. Zierler, "Linear recurring sequences," *J. of the Society for Industrial and Applied Mathematics*, vol. 7, no. 1, 1959, pp. 31-48.

[5] R. McEliece, *Linear recurring sequences over finite fields*, PhD Thesis, California Institute of Technology, 1967.

[6] S. Golomb, *Shift Register Sequences*, San Francisco: Holden Day, 1967.

[7] S. Kwon, S. Cho, U. Choi, H. Kim, and N. Na, "Generation of Pattern Classifier using LFSRs," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 5, 2014, pp. 673-679.

[8] U. Choi and S. Cho, "Number of Differenct Solutions to $x^5+bx^3+b^{2^m}x^2+1=0$ over $GF(2^n)$," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 8, no. 11, 2013, pp. 1749-1754.

[9] U. Choi, J. Kim, Y. Hwang, H. Kim, and S. Cho, "Computation Algorithm for the Phase Shifts of Maximum Length Cellular Automata by Using Impulse Response Sequence," *J. of The Korea Institute of Information Security and Cryptology*, vol. 16, no. 1, 2006, pp. 75-78.

[10] E. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Transactions on Information Theory*, vol. 22, no. 6, 1976, pp. 732-736.

[11] S. Cho, *Finite fields and its applications*, Kyowoosa, Seoul, 2012.

[12] M. Kwon, S. Cho, H. Kim, U. Choi, J. Kim, and S. Kang, "Representation of a Sequence in an Array Form," *Proceedings of the 21th International Confenrece on Electrinic and Information Communication*, vol. 11, no. 2, Jungwon University, Goesan, Korea, November, 2017, pp. 95-96.

저자 소개

권민정(Min-Jeong Kwon)

1997년 부산대학교 수학교육과 졸업(이학사)

2002년 부산대학교 교육대학원 수학과 졸업(교육학석사)

2013년 부경대학교 응용수학과 졸업(이학박사)

※ 관심분야 : 셀룰라 오토마타론, 정보보호

조성진(Sung-Jin Cho)

1979년 강원대학교 수학교육과 졸업(이학사)
1981년 고려대학교 대학원 수학과 졸업(이학석사)
1988년 고려대학교 대학원 수학과 졸업(이학박사)
1988년~현재 부경대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

김진경(Jin-Gyoung Kim)

2008년 부경대학교 응용수학과 졸업(이학석사)
2013년 부경대학교 응용수학과 졸업(이학박사)
※ 관심분야 : 셀룰라 오토마타론, 유한체

최언숙(Un-Sook Choi)

1992년 성균관대학교 산업공학과 졸업(공학사)
2000년 부경대학교 대학원 응용수학과 졸업(이학석사)
2004년 부경대학교 응용수학과 졸업(이학박사)
2009년 부경대학교 정보보호학과 졸업(공학박사)
2009~ 현재 동명대학교 정보통신공학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 암호이론