JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 7 : 1577~1584 Jul. 2015

LFSR 기반의 패턴분류기의 생성 및 분석

권숙희[1] · 조성진[2*] · 최언숙[3] · 공길탁[1] · 김한두[4]

Generation and Analysis of Pattern Classifier based on LFSRs

Sook-Hee Kwon[1] · Sung-Jin Cho[2*] · Un-Sook Choi[3] · Gil-Tak Kong[1] · Doo-Han Kim[4]

[1]Department of Applied Mathmatics, Pukyong University, Pusan 608-737, Korea
[2*]Department of Applied Mathmatics, Pukyong University, Pusan 608-737, Korea
[3]Department of Information & Communications Engineering, Tongmyong University, Pusan 608-711, Korea
[4]Department of Applied Mathmatics, Inje University, Pusan 621-749, Korea

요 약

본 논문에서는 LFSR 기반의 패턴분류기를 생성법을 제안한다. 생성한 LFSR 기반의 패턴분류기는 도달불가능 상태를 쉽게 파악할 수 있고 0-기본경로를 이용하여 의존벡터를 구할 수 있다. 또한 주어진 의존벡터에 대응하는 LFSR 기반의 패턴분류기를 생성하는 방법을 제안한다.

ABSTRACT

In this paper, we propose a method for generating pattern classifier based on LFSR. The proposed pattern classifier bosed on LFSR is easy to see non-reachable state, and we can obtain dependency vector by using the 0-basic path. Also, we propose a method for generating pattern classifiers based on LFSR which correspond to given dependency vector.

키워드 : LFSR, 패턴분류기, 의존벡터, 끌개, 0-기본경로

Key word : LFSR, pattern classifier, dependency vector(DV), attractor, 0-basic path

Received 09 February 2015, **Revised** 05 March 2015, **Accepted** 19 March 2015

*** Corresponding Author** Sung-Jin Cho(E-mail:sjcho@pknu.ac.kr, Tel:+82-51-629-5527)
Department of Applied Mathmarics, Pukyong University, Busan 608-737, Korea

Open Access **http://dx.doi.org/10.6109/jkiice.2015.19.7.1577** print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

패턴인식의 처리 과정은 패턴의 특징을 파악하여 패턴이 속한 부류로 분류하는 과정으로 구성되며, 패턴인식의 대부분인 분류 작업은 패턴분류기에 의하여 이루어진다. 패턴분류기는 데이터로부터 패턴들의 중요한 특징이나 속성을 추출하여 패턴을 특정한 클래스에 할당한다[1-3]. 패턴분류기의 설계는 작은 저장 공간, 큰 데이터 처리량, 낮은 가격대로 구현하는 것을 고려하여야 한다.

메모리 량을 최소화 할 수 있는 방법으로 Maji 등은 클래스의 수가 2개인 패턴을 효과적으로 분류할 수 있는 MACA(Multiple Attractor Cellular Automata)를 합성하여 패턴분류기를 설계하였다[3]. Maji 등은 의존벡터(Dependency Vector, 이하 DV)를 이용하여 시간복잡도를 $O(n^3)$에서 $O(n)$으로 줄였다. 그러나 DV를 구하기 위하여 MACA에 대응하는 0-트리에 속하는 모든 원소를 구하여 그것을 계수로 하는 동차연립방정식의 해를 구하야 하므로 초기 설정시간이 오래 걸린다.

본 논문에서는 초기 설정시간을 효과적으로 줄이기 위해 LFSR(Linear feedback shift register) 기반의 패턴분류기를 생성한다. 생성한 LFSR 기반의 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬에 대한 특성을 분석하여 주어진 $\mathbb{C}_M^n$의 상태전이그래프에서 0-트리의 한 도달불가능한 상태를 구하는 방법을 제안한다. 따라서 $\mathbb{C}_M^n$에 대응하는 DV를 구하는 시간을 효과적으로 줄일 수 있다. 또한 주어진 n-셀 DV에 대응하는 LFSR 기반의 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 T_{M_n}에 대하여, DV_i에 대응하는 T_{M_i}를 합성하여 생성할 수 있다.

Ⅱ. 배경 지식

의사난수열 생성, 암호화 시스템 구현 등에 이용되는 LFSR은 시프트 레지스터의 일종으로, 레지스터에 입력되는 값이 이전 상태 값들의 선형 함수로 계산되고 유한체 위에서 정의된 선형점화식 수열을 효율적으로 발생시킬 수 있다. 이러한 수열의 특성은 점화식에 의해 유도되는 특성다항식에 의하여 결정된다[4, 5]. n개의 셀과 선형 피드백 함수(Linear feedback function) $f(s_0, s_1, \cdots, s_{n-1})$로 구성되는 n차 LFSR은 식(1)과 같다[6].

$$f(s_0, s_1, \cdots, s_{n-1}) = c_0 s_0 \oplus c_1 s_1 \oplus \cdots \oplus c_{n-1} s_{n-1} \quad (1)$$

여기서 $s_0, s_1, \cdots, s_{n-1}$는 레지스터에 입력되는 초깃값이고 $c_0, c_1, \cdots, c_{n-1} \in GF(2)$이다.

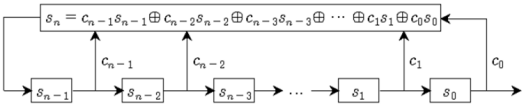

그림 1. LFSR의 구조
Fig. 1 Structure of LFSR

그림1은 n차 LFSR의 구조이다. 식(1)에 대한 다항식 $c_T(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$를 LFSR의 특성다항식(Characteristic polynomial)이라 한다[7].

다음은 본 논문에서 사용되는 용어에 대한 정의이다.

<정의2.1[8-10]>

(ⅰ) 끌개(attractor): 상태전이그래프에서 순환상태 중 사이클의 길이가 1인 상태
(ⅱ) α-트리: 순환상태 α를 루트로 하는 트리
(ⅲ) 깊이(depth): 상태전이그래프에서 임의의 도달불가능상태에서 가장 가까운 순환상태로 가는데 걸리는 최소단계 수
(ⅳ) α-기본경로: 깊이가 d인 α-트리의 도달불가능 상태 x는 d단계 후 그 상태가 α가 된다. 이때 상태전이 단계$(x \rightarrow Tx \rightarrow \cdots \rightarrow T^d x(=\alpha))$를 α-기본경로라 한다. 여기서 T는 상태전이행렬이다.
(ⅴ) 도달불가능상태(non-reachable state): 상태전이 그래프에서 직전자가 존재하지 않는 상태.
(ⅵ) 도달가능상태(reachable state): 상태전이그래프에서 직전자가 적어도 한 개 존재하는 상태

다항식 $f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1 x + c_0$ $(c_i \in GF(2),\ 0 \le i \le n-1)$에 대해 아래와 같은 $n \times n$ 행렬 T를 $f(x)$의 동반행렬(Companion matrix)이라고 하고[7], 다음 식(2)와 같이 4가지 형태로 나타낼 수 있다.

$$T^{(1)}=\begin{pmatrix}0&0&\cdots&0&|&c_0\\ -&-&-&-&-&-\\ 1&0&\cdots&0&|&c_1\\ 0&1&\cdots&0&|&\vdots\\ \vdots&\vdots&\ddots&\vdots&|&c_{n-2}\\ 0&0&\cdots&1&|&c_{n-1}\end{pmatrix},$$

$$T^{(2)}=\begin{pmatrix}c_{n-1}&|&1&\cdots&0&0\\ \vdots&|&\vdots&\ddots&\vdots&\vdots\\ c_2&|&0&\cdots&1&0\\ c_1&|&0&\cdots&0&1\\ --&-&-&-&-&-\\ c_0&|&c_1&\cdots&c_{n-2}&c_{n-1}\end{pmatrix},$$

$$T^{(3)}=\begin{pmatrix}c_{n-1}&c_{n-2}&\cdots&c_1&|&c_0\\ --&--&--&--&-&-\\ 1&0&\cdots&0&|&0\\ 0&1&\cdots&0&|&0\\ \vdots&\vdots&\ddots&\vdots&|&\vdots\\ 0&0&\cdots&1&|&0\end{pmatrix},$$

$$T^{(4)}=\begin{pmatrix}0&|&1&\cdots&0&0\\ \vdots&|&\vdots&\ddots&\vdots&\vdots\\ 0&|&0&\cdots&1&0\\ 0&|&0&\cdots&0&1\\ --&-&-&-&-&-\\ c_0&|&c_1&\cdots&c_{n-2}&c_{n-1}\end{pmatrix} \quad (2)$$

n차 LFSR은 $X_t = TX_{t-1}$로 표현할 수 있다. 여기서, X_i는 시간 i에서의 $n\times 1$ 상태벡터이고 T는 동반행렬로 표현할 수 있다. 동반행렬 T에 대하여 $c_T(x)=m_T(x)$이 성립한다[7]. 단 $m_T(x)$는 T의 최소다항식(Minimal polynomial)이다.

<정리 2.2[11]> 임의의 $m\times n$ 행렬 A에 대하여 다음이 성립한다.

$$rank(A)+\dim N(A)=n. \quad (3)$$

앞으로 $c_T(x)=m_T(x)=x^{n-1}(x+1)$인 2개의 끌개를 갖는 패턴분류기를 $\mathbb{C}_M^n$로 나타내기로 한다.

<정의 2.3[3]> 의존벡터(Dependency Vector, 이하 DV)는 n비트 패턴들로 구성된 벡터공간의 부분공간 $\mathbb{V}$의 모든 원소에 대하여 성립하는 변수들 간의 선형 종속 관계이다. DV와 0-트리의 성분의 내적은 0이다.

$DV=(101)$인 패턴분류기 $\mathbb{C}_M^3$의 상태전이행렬 T_{M_3}은 다음 식(4)과 같이 두 가지 경우가 있다.

$$T_{M_3}^{(5)}=\begin{pmatrix}1&1&0\\0&1&1\\0&1&1\end{pmatrix},\ T_{M_3}^{(6)}=\begin{pmatrix}1&1&0\\1&1&0\\0&1&1\end{pmatrix} \quad (4)$$

Ⅲ. LFSR 기반의 패턴분류기

이 절에서는 LFSR을 이용한 패턴분류기를 생성하고 0-기본경로를 이용하여 DV를 구할 수 있는 방법을 제안한다. n-셀 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 T_{M_n}에 대하여 $c_{T_{M_n}}(x)=m_{T_{M_n}}(x)=x^{n-1}(x+1)$이 성립한다. 이때 끌개의 개수는 2개이고, 0-트리의 상태의 개수는 2^{n-1}개다. 그리고 $rank\left(T_{M_n}\right)=n-1$이다. $c_{T_{M_n}}(x)=m_{T_{M_n}}(x)=x^{n-1}(x+1)$인 n-셀 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 T_{M_n}에 대하여 대각성분의 1의 개수는 홀수이다.

<정리 3.1[12]> 상태전이행렬이 T_{M_n}인 n-셀 패턴분류기 $\mathbb{C}_M^n$의 상태전이그래프에서, $\mathbf{x}$가 0-트리의 한 도달불가능상태일 때 DV는 0-기본경로 $(\mathbf{x}\rightarrow T_{M_n}\mathbf{x}\rightarrow\cdots\rightarrow T_{M_n}^{n-1}\mathbf{x}(=0))$의 성분을 각 행으로 하는 행렬 (B_0)의 영공간 $N(B_0)$의 기저벡터이고 유일하다.

위 정리로부터 0-트리의 도달불가능상태를 알면 0-기본경로를 알 수 있으므로 DV를 구하기가 쉽다는 것을 알 수 있다.

LFSR 기반의 n-셀 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 T_{M_n}은 다음 식(5)과 같이 4가지 형태로 나타낼 수 있다.

$$T_{M_n}^{(1)}=\begin{pmatrix}0&0&\cdots&0&0\\1&0&\cdots&0&0\\0&1&\cdots&0&0\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&1\end{pmatrix},\ T_{M_n}^{(2)}=\begin{pmatrix}1&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&1\\0&0&0&\cdots&0\end{pmatrix},$$

$$T_{M_n}^{(3)}=\begin{pmatrix}1&0&\cdots&0&0\\1&0&\cdots&0&0\\0&1&\cdots&0&0\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&0\end{pmatrix},\ T_{M_n}^{(4)}=\begin{pmatrix}0&1&\cdots&0&0\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&0\\0&0&\cdots&0&1\\0&0&\cdots&0&1\end{pmatrix} \quad (5)$$

<정리 3.2> 길이가 n인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 T_{M_n}에 대하여, $\mathbf{e}_i$를 크기가 n이고 i번째 성분이 1인 단위벡터 ($\mathbf{e}_i^t = (0 \cdots 010 \cdots 0)^t$)일 때, $\mathbb{C}_M^n$의 상태전이그래프에서 0-트리의 한 도달불가능한 상태 $\mathbf{x}$는 다음과 같다.

(ⅰ) $T_{M_n}^{(1)}$에 대하여 $\mathbf{y}=\mathbf{e}_1^t$일 때, $\mathbf{y}T_{M_n}^{(1)} = O$이고, $\mathbf{x}=(T_{M_n}^{(1)}+I)\mathbf{e}_1$이다.

(ⅱ) $T_{M_n}^{(2)}$에 대하여 $\mathbf{y}=\mathbf{e}_n^t$일 때, $\mathbf{y}T_{M_n}^{(2)} = O$이고, $\mathbf{x}=(T_{M_n}^{(2)}+I)\mathbf{e}_n$이다.

(ⅲ) $T_{M_n}^{(3)}$에 대하여 $\mathbf{y}=\mathbf{e}_1^t+\mathbf{e}_2^t$일 때, $\mathbf{y}T_{M_n}^{(3)} = O$이고, $\mathbf{x}=(T_{M_n}^{(3)}+I)\mathbf{e}_2$이다.

(ⅳ) $T_{M_n}^{(4)}$에 대하여 $\mathbf{y}=\mathbf{e}_{n-1}^t$일 때, $\mathbf{y}T_{M_n}^{(4)} = O$ 이고, $\mathbf{x}=(T_{M_n}^{(4)}+I)\mathbf{e}_n$이다.

증명> $\mathbb{C}_M^n$의 상태전이그래프에서 0-트리의 도달가능상태는 T의 모든 열들의 일차결합으로 표현된다.

먼저 (i)에 대하여 첫 번째 행이 영벡터이므로 $T_{M_n}\mathbf{e}_1 \neq \mathbf{e}_1$ 이다. 그런데 $(T_{M_n}^{(1)}+I)\mathbf{e}_1$은 $T_{M_n}^{(1)}$의 모든 열들의 일차결합으로 표현되지 않으므로 0-트리의 도달불가능상태가 된다. 따라서 $\mathbf{x}=(T_{M_n}^{(1)}+I)\mathbf{e}_i$는 $\mathbb{C}_M^n$의 0-트리의 도달불가능한 상태이다.

(ii)는 (i)과 같은 방법으로 증명할 수 있다.

(iii)에서 $T_{M_n}^{(3)}$은 1행과 2행이 같다. $\mathbf{y}$를 $\mathbf{y}=\mathbf{e}_1^t+\mathbf{e}_2^t$라 하면 $\mathbf{y}T_{M_n}^{(3)} = O$을 만족한다. 그런데 $(T_{M_n}^{(3)}+I)\mathbf{y}$은 $T_{M_n}^{(3)}$의 모든 열들의 일차결합으로 표현되지 않는다. 그리고

$$(T_{M_n}+I)\mathbf{y}=(T_{M_n}^{(3)}+I)(\mathbf{e}_1+\mathbf{e}_2)$$
$$=(T_{M_n}^{(3)}+I)\mathbf{e}_1+(T_{M_n}^{(3)}+I)\mathbf{e}_2$$

이므로 $(T_{M_n}^{(3)}+I)\mathbf{e}_1$와 $(T_{M_n}^{(3)}+I)\mathbf{e}_2$는 $T_{M_n}^{(3)}$의 모든 열들의 일차결합으로 표현되지 않으므로 0-트리의 도달불가능상태가 된다. 따라서 $\mathbf{x}=(T_{M_n}^{(3)}+I)\mathbf{e}_2$는 $\mathbb{C}_M^n$의 0-트리의 도달불가능한 상태이다.

(iv)는 (iii)과 같은 방법으로 증명할 수 있다. □

표 1. n-셀 LFSR 기반의 패턴분류기 $\mathbb{C}_M^n$
Table. 1 n-cell Pattern Classifier $\mathbb{C}_M^n$ based on LFSR

	T_{M_n}	non-reachable state	DV
i	$T_{M_n}^{(1)}$	$(110\cdots0)^t$	$(11\cdots1)$
ii	$T_{M_n}^{(2)}$	$(0\cdots011)^t$	$(11\cdots1)$
iii	$T_{M_n}^{(3)}$	$(010\cdots0)^t$, $(0110\cdots0)^t$	$(10\cdots0)$
iv	$T_{M_n}^{(4)}$	$(0\cdots010)^t$, $(0\cdots0110)^t$	$(0\cdots01)$

<정리 3.3> 길이가 n인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 $T_{M_n}^i (i=1,2,3,4)$에 대하여 DV는 다음과 같다.

$$T_{M_n}^{(1)} : DV=(11\cdots1),\ T_{M_n}^{(2)} : DV=(11\cdots1)$$
$$T_{M_n}^{(3)} : DV=(10\cdots0),\ T_{M_n}^{(4)} : DV=(0\cdots01)$$

증명> (i) $T_{M_n}^{(1)}$을 상태전이행렬로 갖는 $\mathbb{C}_M^n$의 상태전이그래프에서 0-트리의 한 도달불가능상태는 정리 3.2에 의하여 $\mathbf{x}=(110\cdots0)^t$이고 0-기본경로 $(\mathbf{x} \rightarrow T_{M_n}\mathbf{x} \rightarrow \cdots \rightarrow T_{M_n}^{n-1}\mathbf{x}(=0))$는 $(110\cdots0)^t \rightarrow (011\cdots0)^t \rightarrow \cdots \rightarrow (000\cdots0)^t$이다. 또한 0-기본경로의 성분을 각 행으로 하는 행렬 B_0는 식(6)과 같다.

$$B_0 = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \quad (6)$$

따라서 $N(B_0)=\{(00\cdots0)^t,(11\cdots1)^t\}$이므로 정리 3.2에 의하여 $DV=(1\cdots1)$이다.

(ii) , (iii), (iv)는 (i)과 같은 방법으로 증명할 수 있다.

표 1은 n-셀 LFSR 기반의 패턴분류기 $\mathbb{C}_M^n$에 대하여 상태전이행렬 $T_{M_n}^{(i)} (i=1,2,3,4)$에 대응하는 상태전이그래프에서 0-트리의 한 도달불가능한 상태와 $\mathbb{C}_M^n$의 DV를 나타낸다.

표 2. 4-셀 LFSR 기반의 패턴분류기 $\mathbb{C}_M^4$
Table. 2 4-cell Pattern Classifier $\mathbb{C}_M^4$ based on LFSR

T_{M_4}	non-reachable state	DV
$T_{M_4}^{(1)}=\begin{pmatrix}0000\\1000\\0100\\0011\end{pmatrix}$	$(1100)^t$	(1111)
$T_{M_4}^{(2)}=\begin{pmatrix}1100\\0010\\0001\\0000\end{pmatrix}$	$(0011)^t$	(1111)
$T_{M_4}^{(3)}=\begin{pmatrix}1000\\1000\\0100\\0010\end{pmatrix}$	$(0100)^t$	(1000)
$T_{M_4}^{(4)}=\begin{pmatrix}0100\\0010\\0001\\0001\end{pmatrix}$	$(0010)^t$	(0001)

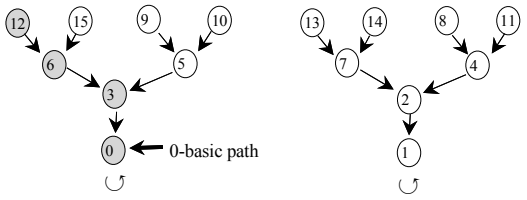

그림 2. $\mathbb{C}_M^4$의 상태전이그래프
Fig. 2 State-transition diagram of $\mathbb{C}_M^4$

<예제 3.1> 길이가 4인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^4$의 상태전이행렬이 $T_{M_4}^{(1)}$이라 하자. $T_{M_4}^{(1)}$은 식(7)과 같고, 0이 아닌 끌개는 1이고 도달불가능상태는 정리 3.2에 의해 $\mathbf{x}=(1100)^t$이다.

$$T_{M_4}^{(1)}=\begin{pmatrix}0000\\1000\\0100\\0011\end{pmatrix} \tag{7}$$

$T_{M_4}^{(1)}$의 상태전이그래프를 나타내면 그림 2와 같고 0-트리의 0-기본경로는 $((1100)^t\rightarrow(0110)^t\rightarrow(0011)^t\rightarrow(0000)^t=12\rightarrow6\rightarrow3\rightarrow0)$이다. 0-기본경로의 성분을 각 행으로 하는 행렬 B_0는 식(8)과 같다.

$$B_0=\begin{pmatrix}1100\\0110\\0011\\0000\end{pmatrix} \tag{8}$$

따라서 $N(B_0)=\{(0000)^t,(1111)^t\}$이므로 $DV=(1111)$이다.

길이가 4인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^4$의 상태전이행렬 $T_{M_4}^{(i)}(i=1,2,3,4)$에 대하여 DV는 표 2와 같다.

Ⅳ. LFSR 기반의 패턴분류기 합성

이 절에서는 주어진 DV에 대응하는 LFSR 기반의 패턴분류기를 합성하는 방법을 제안한다.

[1, 12]에서 언급한 $DV=(*\cdots*\underbrace{0\cdots0}_{(k\geq2)}*\cdots*)$인 경우와 $DV=(0*\cdots*0)$인 경우를 제외하고 n-셀 DV에 대응하는 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 T_{M_n}를 구성하는 방법이다. 다음 정리는 주어진 DV에 대응하는 LFSR 기반의 패턴분류기를 합성하는 방법이다.

<정리4.1> 길이가 n인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 T_{M_n}에 대하여 n-셀 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 T_{M_n}은 다음 표 3과 같다.

표 3. n-셀 LFSR 기반의 패턴분류기 $\mathbb{C}_M^n$
Table. 3 n-cell Pattern Classifier $\mathbb{C}_M^n$ based on LFSR

i	$DV=(v_1\cdots v_iv_{i+1}\cdots v_n)=(1\cdots10\cdots0)$
	$T_{M_n}=\begin{pmatrix}\begin{array}{c\|c}T_{M_i}^{(1)} & O\\\hline O & T_{M_{n-i+1}}^{(3)}\end{array}\end{pmatrix}=\begin{pmatrix}0&0&\cdots&0&0&&\\1&0&\cdots&0&0&&\\0&1&\cdots&0&0&&O\\\vdots&\vdots&\ddots&\vdots&\vdots&&\\0&0&\cdots&1&\boxed{1}&\cdots&0&0\\&&&&1&\cdots&0&0\\&&O&&\vdots&\ddots&\vdots&\vdots\\&&&&0&\cdots&1&0\end{pmatrix}$
ii	$DV=(v_1\cdots v_{i-1}v_i\cdots v_n)=(0\cdots01\cdots1)$
	$T_{M_n}=\begin{pmatrix}\begin{array}{c\|c}T_{M_i}^{(4)} & O\\\hline O & T_{M_{n-i+1}}^{(2)}\end{array}\end{pmatrix}=\begin{pmatrix}0&1&\cdots&0&&&&\\\vdots&\vdots&\ddots&\vdots&&&O&\\0&0&\cdots&1&&&&\\0&0&\cdots&\boxed{1}&1&0&0&0\\&&&&0&0&1&0\\&&&&\vdots&\vdots&\vdots&\ddots\\&O&&&0&0&0&\cdots&1\\&&&&0&0&0&\cdots&0\end{pmatrix}$
iii	$DV=(v_1\cdots v_i\cdots v_n)=(1\cdots101)$
	$T_{M_n}=\begin{pmatrix}\begin{array}{c\|c}T_{M_i}^{(1)} & O\\\hline O & T_{M_{n-i+1}}^{(5)}\end{array}\end{pmatrix}=\begin{pmatrix}0&0&\cdots&0&0&&\\1&0&\cdots&0&0&&\\\vdots&\vdots&\ddots&\vdots&\vdots&&O\\0&0&\cdots&0&0&&\\0&0&\cdots&1&\boxed{1}&1&0\\&&&&0&1&1\\&O&&&0&1&1\end{pmatrix}$

iv	$DV=(v_1\cdots v_i\cdots v_n)=(101\cdots1)$
	$T_{M_n}=\begin{pmatrix} & & & \\ & T^{(6)}_{M_i} & & O \\ & & & \\ & & & T^{(2)}_{M_{n-i+1}} \\ & O & & \end{pmatrix}=\begin{pmatrix} 1&1&0& & & O \\ 1&1&0& & & \\ 0&1&\boxed{1}&1&0&\cdots&0 \\ & & 0&0&1&\cdots&0 \\ O & & \vdots&\vdots&\vdots&\ddots&\vdots \\ & & 0&0&0&\cdots&1 \\ & & 0&0&0&\cdots&0 \end{pmatrix}$
v	$DV=(v_1\cdots v_i\cdots v_n)=(0\cdots0101)$
	$T_{M_n}=\begin{pmatrix} & & & \\ & T^{(4)}_{M_i} & & O \\ & & & \\ & & & T^{(5)}_{M_{n-i+1}} \\ & O & & \end{pmatrix}=\begin{pmatrix} 0&1&0&\cdots&0& \\ 0&0&1&\cdots&0& \\ \vdots&\vdots&\vdots&\ddots&\vdots& O \\ 0&0&0&\cdots&1& \\ 0&0&0&\cdots&\boxed{1}&1\ 0 \\ & & & & 0&1\ 1 \\ & & O & & 0&1\ 1 \end{pmatrix}$
vi	$DV=(v_1\cdots v_i\cdots v_n)=(1010\cdots0)$
	$T_{M_n}=\begin{pmatrix} & & & \\ & T^{(6)}_{M_i} & & O \\ & & & \\ & & & T^{(3)}_{M_{n-i+1}} \\ & O & & \end{pmatrix}=\begin{pmatrix} 1&1&0& & O \\ 1&1&0& & \\ 0&1&\boxed{1}&0&\cdots&0&0 \\ & & 1&0&\cdots&0&0 \\ & & 0&1&\cdots&0&0 \\ O & & \vdots&\vdots&\ddots&\vdots&\vdots \\ & & 0&0&\cdots&1&0 \end{pmatrix}$

여기서 $DV=(101)$인 패턴분류기 $\mathbb{C}_M^3$의 상태전이행렬 T_{M_3}은 다음 식(4)과 같다.

증명> 정리 3.2에 의하여 도달불가능상태 x는 $(110\cdots0)^t$이고 0-기본경로$((110\cdots0)^t\rightarrow(0110\cdots0)^t\rightarrow\cdots\rightarrow(0\cdots0110)^t\rightarrow(0\cdots010)^t\rightarrow(0\cdots001)^t$의 성분을 각 행으로 하는 행렬 B_0는 식(9)과 같다.

$$B_0=\begin{pmatrix} 1&1&0\cdots0&0&\cdots&0 \\ 0&1&1\cdots0&0&\cdots&0 \\ \vdots& &\ddots&\vdots&\ddots&\vdots \\ 0&0&0\cdots1&1&\cdots&0 \\ 0&0&0\cdots0&1&\cdots&0 \\ \vdots& &\ddots&\vdots&\ddots&\vdots \\ 0&0&0\cdots0&0&\cdots&1 \end{pmatrix} \tag{9}$$

$N(B_0)=\{(00\cdots00)^t,(1\cdots10)^t\}$ 이므로 $DV=(1\cdots10\cdots0)$이다.

(ii), (iii), (iv), (v), (vi)의 경우 (i)과 같은 방법으로 증명할 수 있다.

<예제 4.1> (i) $DV=(11110)$인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^5$의 상태전이행렬 T_{M_5}은 식(10)과 같다.

$$T_{M_5}=\begin{pmatrix} & & & \\ & T^{(1)}_{M_4} & & O \\ & & & \\ & & & T^{(3)}_{M_2} \\ & O & & \end{pmatrix}=\begin{pmatrix} 0&0&0&0&0 \\ 1&0&0&0&0 \\ 0&1&0&0&0 \\ 0&0&1&\boxed{1}&0 \\ 0&0&0&1&0 \end{pmatrix} \tag{10}$$

(ii) $DV=(11101)$인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^5$의 상태전이행렬 T_{M_5}은 다음 식(11)과 같다.

$$T_{M_5}=\begin{pmatrix} & & & \\ & T^{(1)}_{M_3} & & O \\ & & & \\ & & & T^{(5)}_{M_3} \\ & O & & \end{pmatrix}=\begin{pmatrix} 0&0&0&0&0 \\ 1&0&0&0&0 \\ 0&1&1&1&0 \\ 0&0&1&\boxed{1}&0 \\ 0&0&0&1&1 \end{pmatrix} \tag{11}$$

(iii) $DV=(00101)$인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^5$의 상태전이행렬 T_{M_5}은 다음 식(12)와 같다.

$$T_{M_5}=\begin{pmatrix} & & & \\ & T^{(4)}_{M_3} & & O \\ & & & \\ & & & T^{(5)}_{M_3} \\ & O & & \end{pmatrix}=\begin{pmatrix} 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&\boxed{1}&1&0 \\ 0&0&1&1&0 \\ 0&0&0&1&1 \end{pmatrix} \tag{12}$$

<예제 4.2> (i)$DV=(1101000)$인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^7$의 상태전이행렬 T_{M_7}은 식(13)과 같다.

$$T_{M_7}=\begin{pmatrix} & & & & & & \\ & T^{(1)}_{M_2} & & & & O & \\ & & & & & & \\ & & & T^{(5)}_{M_3} & & & \\ & & & & & & \\ & O & & & & T^{(3)}_{M_4} & \\ & & & & & & \end{pmatrix}=\begin{pmatrix} 0&0&0&0&0&0&0 \\ 1&\boxed{1}&1&0&0&0&0 \\ 0&1&1&0&0&0&0 \\ 0&0&1&\boxed{1}&0&0&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \end{pmatrix} \tag{13}$$

(ii)$DV=(1101010)$인 LFSR 기반의 패턴분류기 $\mathbb{C}_M^7$의 상태전이행렬 T_{M_7}은 식(14)와 같다.

$$T_{M_n}=\begin{pmatrix} & & & & & & \\ & T^{(1)}_{M_2} & & & & O & \\ & & & & & & \\ & & & T^{(5)}_{M_3} & & & \\ & & & & & & \\ & O & & & & T^{(5)}_{M_3} & \\ & & & & & & \\ & & & & & & T^{(3)}_{M_2} \\ & & & & & & \end{pmatrix}=\begin{pmatrix} 0&0&0&0&0&0&0 \\ 1&\boxed{1}&1&0&0&0&0 \\ 0&1&1&0&0&0&0 \\ 0&0&1&\boxed{1}&1&0&0 \\ 0&0&0&1&1&0&0 \\ 0&0&0&0&1&\boxed{1}&0 \\ 0&0&0&0&0&1&0 \end{pmatrix} \tag{14}$$

다음은 LFSR 기반의 패턴분류기 합성에 대한 알고리즘이다.

Algorithm 1
SynthesizeLFSRbased_PatternClassifier

Input: n-셀 $DV=(v_1 \cdots v_i \cdots v_j \cdots v_n)$,
i-셀 LFSR 기반의 패턴분류기 $\mathbb{C}_M^i$의 상태전이행렬 T_{M_i},
$DV=(101)$인 패턴분류기 $\mathbb{C}_M^3$의 상태전이행렬 T_{M_3}
Output: 패턴분류기의 $(n\times n)$ 상태전이행렬 T_{M_n}
Step1:
(i) $v_1 \cdots v_i = 101$이면 $T_{M_i}^{(6)}$을 생성한다.
(ii) $v_1 \cdots v_i = 1 \cdots 1$이면 $T_{M_i}^{(1)}$을 생성한다.
(iii) $v_1 \cdots v_i = 10 \cdots 0$이면 $T_{M_i}^{(3)}$을 생성한다.
(iv) $v_1 \cdots v_i = 0 \cdots 01$이면 $T_{M_i}^{(4)}$을 생성한다.
$i=n$이면 멈춘다. $i<n$이면 Step2를 시행한다.
Step2: $v_1 \cdots v_j = *\cdots * \underbrace{0\cdots 0}_{(k\geq 2)} *\cdots *$와
$v_1 \cdots v_j = 0*\cdots *0$인 경우는 제외하고 T_{M_i}를 생성한다.
(i) $v_i \cdots v_j = 101$이면 $T_{M_{j-i+1}}^{(5)}$을 생성하여 T_{M_i}의 (i,i)성분과 $T_{M_{j-i+1}}^{(5)}$의 $(1,1)$성분을 겹치게 하여 나머지 성분은 0을 채우고 T_{M_j}을 생성한다.
(ii) $v_i \cdots v_j = 1 \cdots 1$이면 $T_{M_{j-i+1}}^{(2)}$을 생성한다.
(iii) $v_i \cdots v_j = 10 \cdots 0$이면 $T_{M_{j-i+1}}^{(3)}$을 생성한다.
T_{M_i}의 (i,i)성분과 $T_{M_{j-i+1}}^{(3)}$의 $(1,1)$성분을 겹치게 하여 나머지 성분은 0을 채우고 T_{M_j}을 생성한다.
$j=n$이면 멈춘다.
$j<n$이면 Step2를 시행한다.
Step3: 패턴분류기의 $(n\times n)$ 상태전이행렬 T_{M_n}을 생성한다.

V. 결 론

본 논문에서는 LFSR 기반의 패턴분류기를 생성하였다. 생성한 LFSR 기반의 패턴분류기의 분석을 통해 상태전이그래프에서 0-트리의 한 도달불가능상태를 찾는 방법을 제안하였고 이를 통해 DV를 구하는 시간을 효과적으로 줄였다. 또한 주어진 길이가 n인 DV에 대응하는 LFSR 기반의 패턴분류기 $\mathbb{C}_M^n$의 상태전이행렬 T_{M_n}을 기본형이 되는 T_{M_i}를 합성하여 생성하는 방법을 제안하였다.

REFERENCES

[1] N. Ganguly, "Cellular Automata Evolution: Theory and Applications in Pattern Recognition and Classification," Ph. D. dissertation, CST Dept. BECDU India, 2003.

[2] C. Krishna, A. Jas and N.A. Touba, "Achieving high encoding efficiency with partial dynamic LFSR reseeding," *ACM Trans. Design Automation of Electronic Systems*, vol. 9, pp. 500-516, 2004.

[3] P. Maji, C. Shaw, N. Ganguly, B.K. Sikdar and P.P. Chaudhuri, "Theory and application of cellular automata for pattern classification," *Fundamenta Informaticae,* vol. 58, pp. 321-354, 2003.

[4] C. Krishna, A. Jas and N.A. Touba, "Achieving high encoding efficiency with partial dynamic LFSR reseeding," *ACM Trans. Design Automation of Electronic Systems*, vol. 9, pp. 500-516, 2004.

[5] C.C. Krishna and N.A. Touba, "Reducing test data volume using LFSR reseeding with seed compression," in *Proc. IEEE ITC*, pp. 321-330, 2002.

[6] S. Golomb, *Shift Register Sequences,* Aegean Park Press, California, 1967.

[7] R. Lidl and H. Niederreiter, *Finite Fields,* Cambridge University, 1997.

[8] A.K. Das and P.P. Chaudhuri, "Vector space theoretic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation," *IEEE Trans. Comput-Aided Des. Integr. Circuits Syst.,* vol. 42, pp. 340-352, 1993.

[9] P.P. Chaudhuri, D.R. Chowdhury, S. Nandy and C. Chattopadhyay, *Additive Cellular Automata; Theory and Applications*, vol. 1, IEEE Computer Society Press, California, 1997.

[10] S.J. Cho, U.S. Choi and H.D. Kim, "Behavior of complemented cellular automata derived from a linear cellular automata," *Mathematical and Computer Modelling,* vol. 36, pp. 979-986, 2002.

[11] G. Strang, *Introduction to Linear Algebra*, Wellesley-Cambridge Press, 2009.

[12] S.J. Cho, H.D. Kim, U.S. Choi, S.T. Kim, J.G. Kim, S.H. Kwon and G.T. Gong, "Generation of TPMACA for Pattern Classification," *LNCS,* vol. 8751, pp. 408-416, 2014.

권숙희(Sook-Hee Kwon)

2011년 부경대학교 응용수학과 졸업(이학석사)
2011년 ~ 현재 부경대학교 응용수학과 박사과정
※관심분야 : 정보보호, 부호이론

조성진(Sung-Jin Cho)

1988년 고려대학교 대학원 수학과 졸업(이학박사)
1988년 ~ 현재 부경대학교 응용수학과 교수
※관심분야 : 셀룰라 오토마타론, 정보보호

최언숙(Un-Sook Choi)

2004년 부경대학교 대학원 응용수학과 졸업(이학박사)
2009년 부경대학교 대학원 정보보호학과 졸업(공학박사)
2006년 ~ 현재 동명대학교 정보통신공학과 교수
※관심분야 : 셀룰라 오토마타론, 정보보호, 암호이론

공길탁(Gil-Tak Kong)

2011년 ~ 현재 부경대학교 응용수학과 석사과정
※관심분야 : 셀룰라 오토마타론, 암호이론

김한두(Han-Doo Kim)

1988년 고려대학교 대학원 수학과 졸업(이학박사)
1989년 ~ 현재 인재대학교 응용수학과 교수
※관심분야 : 전산수학, 셀룰라 오토마타론