creative commons
COMMONS DEED

저작자표시 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이차적 저작물을 작성할 수 있습니다.
- 이 저작물을 영리 목적으로 이용할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

이 학 석 사 학 위 논 문

LFSR 기반의 효과적인 패턴분류기 설계

2014년 8월

부경대학교 대학원

응 용 수 학 과

김 나 령

이 학 석 사 학 위 논 문

LFSR 기반의 효과적인 패턴분류기의 설계

지도교수 조 성 진

이 논문을 이학석사 학위논문으로 제출함.

2014년 8월

부경대학교 대학원

응 용 수 학 과

김 나 령

김나령의 이학석사 학위논문을 인준함.

2014년 8월 22일

주 심 이학박사 표 용 수 (인)

위 원 이학박사 박 진 한 (인)

위 원 이학박사 조 성 진 (인)

목 차

표 목차 ····· ii
그림 목차 ····· ii
Abstract(in English) ····· iii

Ⅰ. 서론 ····· 1

Ⅱ. 배경지식 ····· 3

2.1. 동반행렬 ····· 3
2.2. LFSR ····· 6

Ⅲ. LFSR 기반의 패턴분류기 설계 ····· 7

3.1. MACA 기반의 패턴분류기 ····· 7
3.2. LFSR 기반의 패턴분류기의 상태전이 그래프 ····· 11
3.3. 패턴의 Hamming weight ····· 15

Ⅳ. LFSR을 합성한 패턴분류기 설계 ····· 16

4.1. LFSR의 합성 ····· 16
4.2. 패턴의 도달가능 상태와 도달불가능 상태 ····· 19
4.3. LFSR 합성된 패턴분류기 분석 ····· 21
4.4. LFSR 기반의 두 단계 패턴분류기 ····· 24

Ⅴ. 결론 ····· 27

참고문헌 ····· 28

표 목차

[표 Ⅳ-1] A_1과 A_2의 직합 ····· 17

[표 Ⅳ-2] 패턴의 Hamming weight와 α-트리 ····· 21

그림 목차

[그림 Ⅱ-1] LFSR 구조 ····· 6

[그림 Ⅲ-1] T의 블록 대각 형태 ····· 9

[그림 Ⅲ-2] $c_T(x)=x^3(x+1)$의 상태전이 그래프 ····· 12

[그림 Ⅲ-3] $c_T(x)=x^2(x+1)$의 상태전이 그래프 ····· 12

[그림 Ⅳ-1] m개의 LFSR을 합성한 패턴분류기 T ····· 16

[그림 Ⅳ-2] T의 상태전이 그래프에서 0-트리 ····· 18

[그림 Ⅳ-3] T의 상태전이 그래프 ····· 22

[그림 Ⅳ-4] LFSR 기반의 두 단계 패턴분류기 ····· 24

Design of effcient Pattern Classifier based on LFSRs

Na-Roung Kim

Graduate School of Education

Pukyong National University

Abstract

The important prerequisites of designing a pattern classifier are huge processing of data, small space for storage, and low cost for production. Maji et al. proposed a pattern classifier by using Multiple Attractor Cellular Automata. The pattern classifier reduced the complexity of the classification algorithm from $O(n^3)$ to $O(n)$[12]. In order to pattern classification, they should know all the states of 0-tree. It needs lots of time for intial setting. To overcome this problem, it needs to be classified using Hamming weight of each pattern. Also, the proposed pattern classifier can not only make integrated pattern classifiers using several LFSRs, but also categorize groups of patterns in wide range of them.

Ⅰ. 서론

의사난수열 생성, 암호화 시스템 구현 등에 이용되는 LFSR(Linear feedback shift register)은 시프트 레지스터의 일종으로, 레지스터에 입력되는 값이 이전 상태 값들의 선형 함수로 계산되는 구조를 가지고 있다. 이러한 LFSR은 하드웨어로 구현할 수 있고, 시퀀스 확산스펙트럼(DSSS) 무선통신과 같은 매우 빠른 의사 난수 수열의 생성이 요구되는 응용에 많이 사용된다[9, 10, 14].

패턴분류기는 데이터로부터 패턴들의 중요한 특징이나 속성을 추출하여 패턴을 특정한 클래스에 할당한다. 패턴분류는 데이터베이스 시스템에서 레코드의 그룹화, VLSI 회로에서의 결함 찾는 것, 이미지 프로세싱 등에서 중요한 역할을 한다[1]. 데이터 처리량이 크고 저장 공간의 크기는 작으며 낮은 가격대로 패턴분류기를 구현할 수 있는지는 패턴분류기 설계에 있어 고려되어야 할 요소들이다

Maji 등[12]은 메모리 량을 최소화 할 수 있는 방법으로 Class의 수가 2개인 패턴을 효과적으로 분류할 수 있는 MACA(Multiple Attractor Cellular Automata)를 합성하여 패턴분류기를 설계하였다. 그들은 의존벡터(Dependency Vector, 이하 DV)를 이용하여 시간 복잡도를 $O(n^3)$에서 $O(n)$으로 줄였다. 그러나 DV를 구하기 위해서는 MACA에 대응하는 0-트리의 모든 원소를 구하여 그것을 계수로 하는 동차연립방정식의 해를 구해야하기 때문에 초기 설정시간이 오래 걸린다.

본 논문에서는 이를 보완하여 각 패턴의 Hamming weight를 이용하여 패턴을 효과적으로 분류할 수 있는 LFSR기반의 패턴분류기를 제안한다.

제안된 패턴분류기는 DV를 구할 필요 없이 각 패턴의 Hamming weight에 의해 패턴분류가 가능하므로 초기 설정시간이 요구되지 않는다. 이 때문에 공간 및 시간 복잡도가 향상된다. 이 패턴분류기(T)의 상태전이그래프에서 attractor는 0과 1이고, 0-트리의 기본경로는 0-트리의 기저가 된다[5]. 테스트 패턴의 Hamming weight가 짝수이면 0-트리로 홀수이면 1-트리로 각각 분류할 수 있다.

크기가 k, $n-k$인 두 개의 LFSR T_1과 T_2를 합성하여 만든 패턴분류기 T의 상태전이그래프에서 attractor가 $0, 1, 2^{n-k}$ 그리고 $2^{n-k}+1$이다. 입력되는 테스트 패턴은 각 패턴의 Hamming weight에 의하여 4개의 Class로 쉽게 분류할 수 있다. 이러한 특성을 갖는 패턴분류기는 여러 개를 합성하여 보다 큰 테스트 패턴집합을 분류할 수 있다. 그리고 LFSR 기반의 두 단계 패턴분류기는 m개의 LFSR을 합성하여 설계한 패턴분류기 T에 의해 생성된 n-비트 패턴 $\mathbf{x}$을 단일 비트(0 또는 1)에 맵핑하게 한다. 그러므로 본 논문에서 제안한 패턴분류기는 큰 테스트 패턴집합을 효율적으로 분류할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 사용되는 동반행렬, LFSR에 대해서 설명한다. 3장에서는 MACA 기반의 패턴분류기에 대해서 설명하고 LFSR 기반의 패턴분류기를 제안한다. 4장에서는 LFSR을 합성한 패턴분류기를 생성하고 LFSR 기반의 두 단계 패턴분류기에 대해서 분석하고 5장에서 결론을 맺는다.

Ⅱ. 배경지식

2.1 동반행렬

<정의 2.1.1> $f(x)=x^n+c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0$ ($c_i\in GF(2)$, $0\le i\le n-1$) 에 대해 아래와 같은 $n\times n$ 행렬 T를 $f(x)$의 동반행렬(companion matrix)이라고 한다.

여기서 I_{n-1}은 $(n-1)\times(n-1)$단위행렬이고, $C=(c_1,c_2,\cdots,c_{n-1})^t$이다.

(1) Type 1

$$T=\left(\begin{array}{ccc|c} 0 & 0 & \cdots & 0 & c_0 \\ \hline 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & \vdots \\ \vdots & \vdots & \ddots & \vdots & c_{n-2} \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{array}\right)=\left(\begin{array}{c|c} O_{1\times(n-1)} & C_0 \\ \hline I_{n-1} & C \end{array}\right)$$

(2) Type 2

$$T=\left(\begin{array}{c|ccc} c_{n-1} & 1 & 0 & \cdots & 0 \\ c_{n-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & 0 & 0 & \cdots & 1 \\ \hline c_0 & 0 & 0 & \cdots & 0 \end{array}\right)=\left(\begin{array}{c|c} C & I_{n-1} \\ \hline 1 & O_{1\times(n-1)} \end{array}\right)$$

<예제 2.1.2> Type 1

(1) $f(x)=x^4+x+1$라 하면 $f(x)$의 동반행렬은 다음과 같다.

PUKYONG NATIONAL UNIVERSITY 부경대학교

$$T=\begin{pmatrix}0001\\1001\\0100\\0010\end{pmatrix}$$

(2) $\mathbf{x}=(0,0,0,1)^t=1$라 하고

$$T\mathbf{x}, T^2\mathbf{x}, \cdots, T^{14}\mathbf{x}, T^{15}\mathbf{x}$$

를 구해보자. $T\mathbf{x}=(1,1,0,0)^t$ 가 된다. $(1,1,0,0)^t$를 십진법으로 표현하면 12가 된다. 마찬가지로 $T^2\mathbf{x}=(0,1,1,0)^t=6$이 되며

$$T^3\mathbf{x}=3,\ T^4\mathbf{x}=13,\ T^5\mathbf{x}=10,\ T^6\mathbf{x}=5,\ T^7\mathbf{x}=14,\ T^8\mathbf{x}=7,\ T^9\mathbf{x}=15,$$
$$T^{10}\mathbf{x}=11,\ T^{11}\mathbf{x}=9,\ T^{12}\mathbf{x}=8,\ T^{13}\mathbf{x}=4,\ T^{14}\mathbf{x}=2,\ T^{15}\mathbf{x}=1$$

이 된다.

(3) (2)에서 $T\mathbf{x}:=\alpha$라 하고 $T^0:=I_4$(4차 단위행렬)라 하면

$$\{T^{k-1}\alpha | k=1,2,\cdots,15\}=\{1,\alpha,\alpha^2,\cdots,\alpha^{14}\}$$

이 되며 $\alpha^{15}=1$이 된다.

<예제 2.1.3> Type 2

(1) $f(x)=x^4+x+1$라 하면 $f(x)$의 동반행렬은 다음과 같다.

$$T=\begin{pmatrix}0100\\0010\\1001\\1000\end{pmatrix}$$

(2) $x=(0,0,0,1)^t=1$라 하고

$$T\mathbf{x}, T^2\mathbf{x}, \cdots, T^{14}\mathbf{x}, T^{15}\mathbf{x}$$

를 구해보자. $T\mathbf{x}=(0,0,1,0)^t$ 가 된다. $(0,0,1,0)^t$를 십진법으로 표현하면 2가 된다. 마찬가지로 $T^2\mathbf{x}=(0,1,0,0)^t=4$가 되며

$T^3\mathbf{x}=8,\ T^4\mathbf{x}=3,\ T^5\mathbf{x}=6,\ T^6\mathbf{x}=12,\ T^7\mathbf{x}=11,\ T^8\mathbf{x}=5,\ T^9\mathbf{x}=10$,

$T^{10}\mathbf{x}=7,\ T^{11}\mathbf{x}=14,\ T^{12}\mathbf{x}=15,\ T^{13}\mathbf{x}=13,\ T^{14}\mathbf{x}=9,\ T^{15}\mathbf{x}=1$

이 된다.

(3) (2)에서 $T\mathbf{x}:=\alpha$라 하고 $T^0:=I_4$(4차 단위행렬)라 하면

$$\{T^{k-1}\alpha | k=1,2,\cdots,15\}=\{1,\alpha,\alpha^2,\cdots,\alpha^{14}\}$$

이 되며 $\alpha^{15}=1$이 된다.

2.2 LFSR

n차 LFSR은 그림 Ⅱ-1과 같이 n개 셀과 선형 피드백 함수(linear feedback function) $f(s_0, s_1, s_2, \cdots, s_{n-1})$로 구성된다.

$$f(s_1, \cdots, s_{n-1}) = c_0 s_0 \oplus c_1 s_1 \oplus \cdots \oplus c_{n-1} s_{n-1} \tag{2.1}$$

여기서 $c_0, c_1, c_2, \cdots, c_{n-1} \in GF(2)$이고, $s_0, s_1, s_2, \cdots, s_{n-1}$는 레지스터에 입력되는 초깃값이다.

그림 Ⅱ-1은 n차 LFSR의 구조이다. 식 (2.1)에 대한 다항식 $c_T(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_0$를 LFSR의 특성다항식(characteristic polynomial)이라 한다[7, 8]. 만약 LFSR의 초깃값이 모두 '0'이면 출력값은 모두 '0'이 된다. 초깃값 중 적어도 하나가 '0'이 아니라고 가정하자. 그러면 LFSR의 단이 가질 수 있는 상태는 $2^k - 1$보다 작거나 같다. 그러므로 LFSR의 출력 수열은 주기를 갖게 되며 주기의 최댓값은 $2^k - 1$이 된다[18, 19].

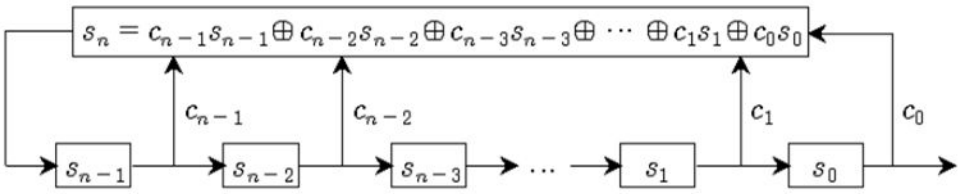


그림 Ⅱ-1. LFSR 구조

Ⅲ. LFSR 기반의 패턴분류기 설계

3.1 MACA 기반의 패턴분류기

다음은 본 논문에서 사용되는 용어에 대한 정의와 성질에 대해 기술한다 [2-4, 6, 13].

<정의 3.1.1> Attractor란 상태전이 그래프에서 순환상태들 중 사이클의 길이가 1인 상태로 어떤 상태 x가 attractor이면 $Tx=x$를 만족한다.

<정의 3.1.2> 도달가능상태(reachable state)란 상태전이 그래프에서 직전자가 적어도 한 개 존재하는 상태를 말한다.

<정의 3.1.3> 도달불가능상태(non-reachable state)란 상태전이 그래프에서 직전자가 존재하지 않는 상태를 말한다.

<정의 3.1.4> α-트리란 순환상태 α를 root로 하는 트리를 말한다.

<정의 3.1.5> Depth란 상태전이 그래프에서 임의의 도달 불가능한 상태에서 가장 가까운 순환상태로 가는데 걸리는 최소의 단계 수이다.

<정의 3.1.6> Depth가 d인 α-트리의 도달 불가능한 상태 x는 d단계 후 그 상태가 α가 된다. 이때의 상태전이 단계$\left(x \rightarrow Tx \rightarrow \cdots \rightarrow T^d x(=\alpha)\right)$ 를 α-기본경로라 한다. 여기서 T는 상태전이행렬이다.

<정의 3.1.7> 주어진 n-셀 CA의 상태전이행렬 T의 특성다항식 $c_T(x)$은 $GF(2)=\{0,1\}$상에서 $c_T(x)=|T\oplus xI|$이다. 여기서, I는 n차 단위행렬이다.

<정의 3.1.8> 특성다항식의 인수 중 T를 근으로 갖는 차수가 가장 낮은 다항식을 최소다항식(minimal polynomial)이라 하고 $m_T(x)$로 나타낸다.

<정리 3.1.9[11, 18]> 임의의 $m\times n$ 행렬 A에 대하여 다음이 성립한다.

$$rank(A)+\dim N(A)=n \tag{3.1}$$

상태전이행렬이 T인 n-셀 MACA에서 $T\oplus I$의 계수(rank)가 r이면 정리 3.1.9에 의하여 attractor의 개수는 2^{n-r}이다. 여기서 I는 n차 단위행렬이다.

<보조정리 3.1.10> 특성다항식과 최소다항식이 $x^{n-1}(x+1)$인 MACA에 대하여 다음이 성립한다.
(i) attractor의 개수는 2개다.
(ii) 0-트리의 상태의 개수는 2^{n-1}이다.

<증명> (i) 특성다항식이 $x^{n-1}(x+1)$이고, 상태전이행렬 T의 고유값(eigenvalue)은 특성방정식 $C_T(x)=0$의 근이므로 $x^{n-1}(x+1)=0$ 의 근은 (중복을 허락하여) $n-1$개의 0과 1개의 1이다. 그리고 특성다항식과 최소다항식이 $x^{n-1}(x+1)$이므로, $T\oplus xI$ 은 다음과 같은 대각행렬로 변형될 수 있다.

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & x^{n-1}(x+1) \end{pmatrix}, \text{ (여기서 대각선의 1의 개수는 } n-1\text{개)}$$

x가 attractor라면 $Tx = x$이므로 attractor는 $T \oplus I$ 의 영공간이다. $x = 1$일 때 $T \oplus I$ 은 다음 행렬로 생각하면 된다.

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{pmatrix}, \text{ (여기서 대각선의 1의 개수는 } n-1\text{개)}$$

그러므로 $T \oplus I$ 의 계수는 $n-1$이다. 따라서 정리 3.1.9에 의하여 $T \oplus I$ 의 영공간의 차원이 1이므로 attractor의 개수는 $2^1 = 2$개다.

(ii) attractor 트리에 있는 상태의 개수가 같으므로, 각 attractor 트리의 상태의 개수는 $2^n/2 = 2^{n-1}$이다.

m개의 MACA기반의 상태전이 행렬 $T_i (i = 1,2,\cdots,m)$를 블록 대각 형태(Block diagonal form)로 배열하여 구성한 다음과 같은 행렬 T의 특성다항식은 $c_T(x) = x^{n-m}(x+1)^m$이다.

$$T = \begin{bmatrix} [T_1] & & & \\ & \ddots & & \\ & & [T_i] & \\ & & & \ddots \\ & & & & [T_m] \end{bmatrix}$$

그림 Ⅲ-1. T의 블록 대각 형태

여기서 T_i의 특성다항식은 $c_{T_i}(x)=x^{n_i-1}(x+1)$이고 $n_1+n_2+\cdots+n_m=n$이다.

그림 Ⅲ-1의 상태전이행렬 T의 성질은 다음과 같다.

① 각 $i=1,2,\cdots,m$에 대하여 $c_{T_i}(x)=x^{k_i}(x+1)$이므로 T의 특성다항식은 $c_T(x)=x^{k_1+k_2+\cdots+k_m}(x+1)^m=x^{n-m}(x+1)^m$이다.

② 최소다항식은 $m_T(x)=x^{\max\{k_1,k_2,\cdots,k_m\}}(x+1)$이다.

③ T는 2^m개의 attractor를 갖는다.

④ 모든 도착가능상태의 직전자의 개수는 2^m개다.

⑤ 짝수 트리의 개수와 홀수 트리의 개수는 2^{m-1}개다.

Maji 등[12]에 의해 제안된 MACA 패턴분류기는 복잡도(complicity)를 $O(n^3)$에서 $O(n)$로 낮추었다. 그러나 패턴을 분류하기 위해서 0-트리의 모든 상태를 구해야 하므로 초기 설정시간이 걸린다. 다음 절에서는 이를 보완하여 각 패턴의 Hamming weight를 이용하여 패턴을 효과적으로 분류할 수 있는 LFSR기반의 패턴분류기를 제안한다.

PUKYONG NATIONAL UNIVERSITY 부경대학교

3.2. LFSR 기반의 패턴분류기의 상태전이 그래프

이 절에서는 시간과 공간의 복잡성을 개선하기 위해 LFSR을 이용한 패턴분류기를 제안한다. 그리고 생성된 패턴분류기의 attractor를 살펴본다.

LFSR 기반의 특성다항식 $c_T(x)$가 $x^{n-1}(x+1)$일 때 2개의 attractor를 갖는 n-셀 패턴분류기의 상태전이행렬 T은 식 (3.2)와 같다.

$$T=\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \end{pmatrix} \tag{3.2}$$

PUKYONG NATIONAL UNIVERSITY 부경대학교

<예제 3.2.1> $C_T(x)=x^3(x+1)$일 때 4×4 동반행렬은 다음과 같다.

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

I가 4차 단위행렬일 때, $N(T+I)=\{0,1\}$이고 attractor는 0과 1이다. T의 상태전이 그래프를 나타내면 그림 Ⅲ-2와 같고 depth는 3이다.

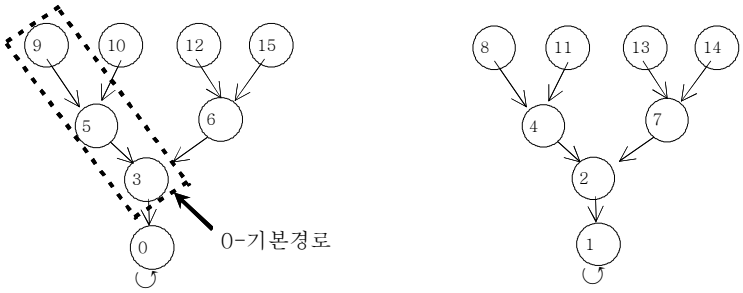


그림 Ⅲ-2. $c_T(x)=x^3(x+1)$의 상태전이 그래프

<예제 3.2.2> $C_T(x)=x^2(x+1)$일 때 3×3동반행렬은 다음과 같다.

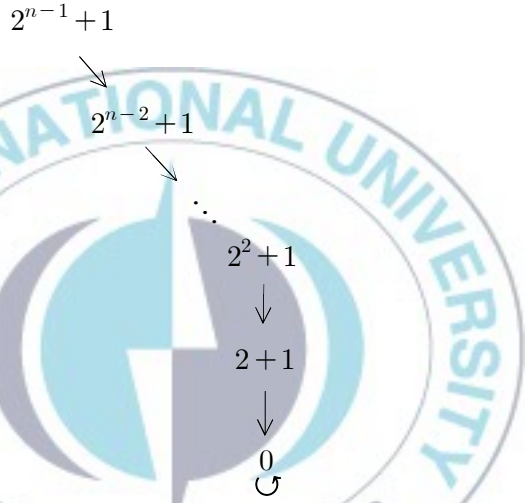
$$T=\begin{pmatrix}0&0&0\\1&0&0\\0&1&1\end{pmatrix}$$

I가 3차 단위행렬일 때, $N(T+I)=\{0,1\}$이고 attractor는 0과 1이다. T의 상태전이 그래프를 나타내면 그림 Ⅲ-3과 같고 depth는 2이다.

그림 Ⅲ-3. $c_T(x)=x^2(x+1)$의 상태전이 그래프

<예제 3.2.3> 그림 Ⅲ-2에서 0-기본경로는 9→5→3→0이고 0-트리의 모든 상태는 3, 5, 9의 일차결합으로 표현할 수 있으므로 0-트리는 $GF(2^4)$의 3차원 부분공간이고 기저는 $\{9(=1001), 5(=0101), 3(=0011)\}$이다. 또한 $1001 = 2^3+1=9$, $1010=2^2+1=5$, $0011=2+1=3$이다.

n차에 대하여 0-기본경로는



이고 $\{2^{n-1}+1, 2^{n-2}+1, \cdots, 2^2+1, 2+1\}$은 0-트리의 기저가 된다. 또한 0-트리는 $GF(2^n)$의 $n-1$차원 부분공간이다.

<정리 3.2.4> n-셀 LFSR 기반의 패턴분류기의 상태전이행렬 T에 대하여 T의 0이 아닌 attractor 는 $\alpha=1(=(00\cdots01)^t)$이다.

<증명> I 가 n차 단위행렬일 때, $T+I$는 식 (3.3)과 같다.

$$T+I=\begin{pmatrix}1&0&\cdots&0&0\\1&1&\cdots&0&0\\0&1&\cdots&0&0\\0&0&\ddots&\vdots&\vdots\\0&0&\cdots&1&0\end{pmatrix} \tag{3.3}$$

식 (3.3)에서 1행부터 $n-1$행까지가 일차독립이므로 $rank(T+I)=n-1$이다. 따라서 $\dim N(T+I)=1$이므로 attractor는 2개이다. 그런데 $(0\cdots 01)^t$에 대하여 $T(0\cdots 01)^t=(0\cdots 01)^t$이므로 attractor는 정확히 0과 1이다.

3.3. 패턴의 Hamming weight

<정리 3.3.1> 0-트리의 모든 원소 x의 Hamming weight $w_t(\mathrm{x})$는 식 (3.4)를 만족하므로 항상 짝수이다.

$$w_t(\mathrm{x}_{i_1}+\cdots+\mathrm{x}_{i_j}+\cdots+\mathrm{x}_{i_k}):=\begin{cases}k & ,k:\text{짝수}\\ k+1 & ,k:\text{홀수}\end{cases} \tag{3.4}$$

〈증명〉 $\{\mathrm{x_j} : j=1,\cdots,n-1\}$가 0-트리의 기저라면 0-트리의 원소 x는 $\mathrm{x_j}$들의 일차결합으로 표현된다. 여기서 $\mathrm{x}_j=(0\cdots\overset{j}{0}10\cdots01)^t$이고 두 기저벡터 $\mathrm{x_i}$와 x_j를 더하면 최하위비트는 0이 되고 그 비트의 1의 개수는 짝수 개이고 홀수 개 기저벡터들을 더하면 1의 개수도 짝수이다. 따라서 0-트리의 모든 성분의 Hamming weight는 짝수이다.

<예제 3.3.2> 예제 3.2.1에서 0-트리의 기저 {1001,0101,0011}의 $w_t(\mathrm{x})$는 짝수이고 1-트리 기저 {1000,0100,0010}의 $w_t(\mathrm{x})$는 홀수이다.

<예제 3.3.3> 예제 3.2.2에서 0-트리의 기저 {101,011}의 $w_t(\mathrm{x})$는 짝수이고 1-트리 기저 {100,010}의 $w_t(\mathrm{x})$는 홀수이다.

Ⅳ. LFSR을 합성한 패턴분류기 설계

4.1. LFSR의 합성

보다 큰 테스트 패턴 집합을 분류하기 위하여 m개의 LFSR을 합성하여 그림 Ⅳ-1과 같은 패턴분류기 T를 설계한다. 패턴분류기 T의 특성다항식은 $c_T(x)=x^{n-m}(x+1)^m$이고 I_i는 (n_i-1)차 단위행렬이다.

$$T=\begin{bmatrix} [T_1] & & & \\ & \ddots & & \\ & & [T_i] & \\ & & & \ddots \\ & & & [T_m] \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 0\cdots 0 \\ I_1 \quad \vdots \\ \quad 1 \end{bmatrix} & & & \\ & \ddots & & \\ & & \begin{bmatrix} 0\cdots 0 \\ I_i \quad \vdots \\ \quad 1 \end{bmatrix} & \\ & & & \ddots \\ & & & \begin{bmatrix} 0\cdots 0 \\ I_m \quad \vdots \\ \quad 1 \end{bmatrix} \end{bmatrix}$$

그림 Ⅳ-1. m개의 LFSR을 합성한 패턴분류기 T

여기서 T_i의 특성다항식은 $c_{T_i}(x)=x^{n_i-1}(x+1)$이고 $n_1+n_2+\cdots+n_m=n$이다.

그림 Ⅳ-1의 패턴분류기 T는 각 $i=1,2,\cdots,m$에 대하여 $c_{T_i}(x)=x^{k_i}(x+1)$이므로 T의 특성다항식은 $c_T(x)=x^{k_1+k_2+\cdots+k_m}(x+1)^m$ $=x^{n-m}(x+1)^m$이다. 그리고 최소다항식은 $m_T(x)=x^{\max\{k_1,k_2,\cdots,k_m\}}(x+1)$이며, T는 2^m개의 attractor를 갖는다. 또한, 모든 도착가능상태의 직전자의 개수는 2^m개이고, 짝수 트리의 개수와 홀수 트리의 개수는 2^{m-1}개다.

다음 예제는 두 개의 LFSR을 합성하여 패턴분류기를 설계하는 것을 보인다.

<예제 4.1.1> 7비트로 표현된 패턴집합을 분류하기 위하여 2개의 LFSR T_1, T_2를 합성하면 다음과 같은 패턴분류기 T를 생성할 수 있다.

$$T=\begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix}, \quad T_1=\begin{pmatrix} 0\,0\,0\,0 \\ 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,1 \end{pmatrix}, T_2=\begin{pmatrix} 0\,0\,0 \\ 1\,0\,0 \\ 0\,1\,1 \end{pmatrix}$$

이때 T_1에 의해 생성되는 0-트리는 $A_1=\{0,24,40,48,72,80,96,120\}$이고 T_2에 의해 생성된 0-트리는 $A_2=\{0,3,5,6\}$이다. $A_1 \cap A_2=\{0\}$이고 T의 0-트리의 모든 성분은 표 Ⅳ-1과 같이 A_1의 원소와 A_2 원소의 직합(Direct sum)으로 표현할 수 있다.

표 Ⅳ-1. A_1과 A_2의 직합

$\oplus$		A_1							
		0	24	40	48	72	80	96	120
A_2	0	0	24	40	48	72	80	96	120
	3	3	27	43	51	75	83	99	123
	5	5	29	45	53	77	85	101	125
	6	6	30	46	54	78	86	102	126

T의 상태전이 그래프에서 0-트리는 그림 Ⅳ-2와 같다.

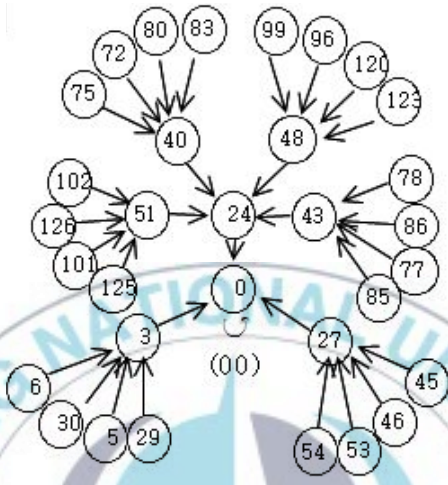


그림 Ⅳ-2. T의 상태전이 그래프에서 0-트리

n차 LFSR의 모든 상태의 수는 2^n이고, 0-트리와 1-트리는 동형(isomorphic)이므로 각각 트리를 이루는 성분의 수는 2^{n-1}이다[5]. 그런데 0-트리의 모든 성분의 Hamming weight가 짝수이므로 1-트리의 모든 성분의 Hamming weight는 홀수이다. 그러므로 각 패턴의 Hamming weight를 알면 그 패턴이 속하는 트리가 무엇인지 식별할 수 있다.

4.2. 패턴의 도달가능 상태와 도달불가능 상태

그림Ⅳ-2에서 0-트리의 도달가능 상태(reachable state)는 {0,3,24,27,40,43,48,51}이고 0-트리의 도달불가능 상태(non reachable state)는 {5,6,29,30,45,46,…,120,123,125,126}이다.

다음은 0-트리의 도달가능 상태와 도달불가능 상태에 개수에 관한 정리이다.

<정리 4.2.1> 크기가 각각 $k,(n-k)$인 LFSR T_1, T_2를 합성하여 설계된 패턴분류기 T에 대하여 0-트리의 도달가능 상태의 개수와 도달불가능 상태의 개수는 식 (4.1)과 같다.

$$\begin{cases} \text{도달가능 상태 개수} & : 2^{n-4} \\ \text{도달불가능 상태 개수} & : 3 \cdot 2^{n-4} \end{cases} \tag{4.1}$$

<증명> k차 상태전이 행렬 T_1의 0-트리의 모든 상태의 개수는 2^{k-1}이고 $\dim N(T_1)=1$이므로 T_1의 상태전이 그래프는 포화이진트리를 이룬다. 마찬가지로 $(n-k)$차인 상태전이 행렬 T_2의 0-트리의 도달가능 상태의 개수는 2^{n-k-2}이고 도달불가능 상태의 개수는 2^{n-k-2}이다. 따라서 합성된 T의 attractor가 4개이며 각 트리 원소의 개수가 2^{n-2}이고 0-트리에서 도달가능상태의 개수는 $2^{k-2} \cdot 2^{n-k-2} = 2^{n-4}$이고 도달불가능상태의 개수는 $2^{n-2} - 2^{n-4} = 3 \cdot 2^{n-4}$이다.

패턴분류기 T의 상태전이 그래프에서 모든 트리는 0-트리와 동형이므로 모든 트리의 도달가능 상태와 도달불가능 상태의 개수는 같다[4].

<예제 4.2.2> 예제 4.1.1의 T에 대한 0-트리의 도달가능상태의 개수는 $2^{n-4}=2^{7-4}=8$이고 도달불가능상태의 개수는 $3\cdot 2^{n-4}=3\cdot 2^{7-4}=24$이고 나머지 트리의 도달가능 상태의 개수와 도달불가능 상태의 개수는 동일하다.

4.3. LFSR 합성된 패턴분류기 분석

차수가 각각 $k, n-k$인 두 LFSR T_1과 T_2를 합성하여 설계된 패턴분류기 T에 대하여 길이가 n인 각 패턴을 k비트까지 B_1과 $k+1$비트에서 n비트까지를 B_2라 하면 패턴 x는 x= $B_1 \| B_2$이다. 각 B_i에 대하여 Hamming weight $w_t(B_i)$가 짝수이면 $w_i = 0$, 홀수이면 $w_i = 1$이라 하자. 패턴들을 표 Ⅳ-2와 같이 4개의 Class(00),(01),(10),(11)로 분류하면 각 패턴이 어느 트리에 속하는 지 알 수 있다.

표 Ⅳ-2. 패턴의 Hamming weight와 α-트리

Hamming weight of pattern		Class	α-tree
B_1	B_2		
even	even	(00)	0-tree
even	odd	(01)	1-tree
odd	even	(10)	2^{n-k}-tree
odd	odd	(11)	$(2^{n-k}+1)$-tree

<예제 4.3.1> 예제 4.1.1의 경우 패턴 54(=0110110)에 대하여 B_1(=0110)의 $w_t(B_1)$은 2이고 B_2(=110)의 $w_t(B_2)$도 2이다. 따라서 $(w_1 w_2)$=(00)이다. 그러므로 패턴 54는 0-트리에 속함을 알 수 있다. 패턴 108(=1101100)도 같은 방법으로 $(w_1 w_2)$를 구하면 (11)이므로 9-트리에 속함을 알 수 있다.

차수가 k_i인 LFSR $T_i (i = 1,2,\cdots,m)$를 그림 Ⅳ-3와 같이 m개 합성하여

패턴분류기 T를 설계할 수 있다. 특성다항식은 $x^{n-m}(1+x)^m$이다. 여기서 $\sum_{i=1}^{m} k_i = n$이다.

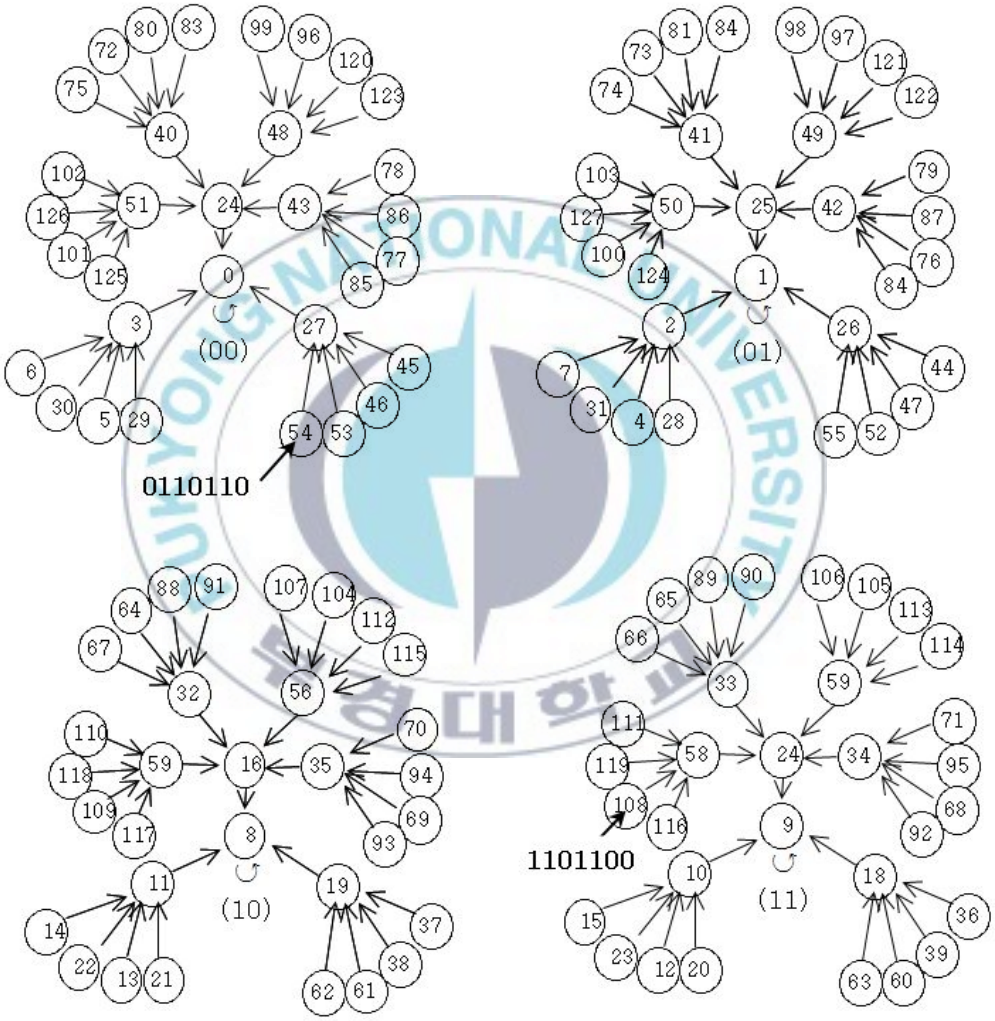


그림 Ⅳ-3. T의 상태 전이 그래프

주어진 n비트 패턴 $\mathbf{x}$를 $\mathbf{x}=B_1 \| B_2 \| \cdots \| B_m$이라 하자. 여기서 B_i의 길이는 k_i이다. $B_i(i=1,\cdots,m)$의 $w_t(B_i)$가 짝수이면 $w_i=0$, 홀수이면 $w_i=1$이라 하자. 그러면 $\mathbf{x}$가 2^m개의 Class$((00\cdots00),(00\cdots01),\cdots,(11\cdots11))$ 중 어느 Class에 속하는 지를 쉽게 분류할 수 있다. 따라서 본 논문에서 제안된 패턴분류기는 큰 테스트 패턴집합을 효율적으로 분류할 수 있다.

PUKYONG NATIONAL UNIVERSITY
부경대학교

4.4. LFSR 기반의 두 단계 패턴분류기

이 절에서는 LFSR 기반의 두 단계 패턴분류기에 대해 살펴본다.

LFSR 기반의 두 단계 패턴분류기는 그림 Ⅳ-4와 같고 1단계 분류기(Classifier 1, 이하 T_{C_1})에 의해 입력층(input layer)의 n-비트 패턴이 은닉층(hidden layer)의 m-비트 패턴에 맵핑되고 2단계 분류기(Classifier 2, 이하 T_{C_2})에 의해 m-비트 패턴이 출력층(output layer)의 단일 비트(0 또는 1)에 맵핑된다.

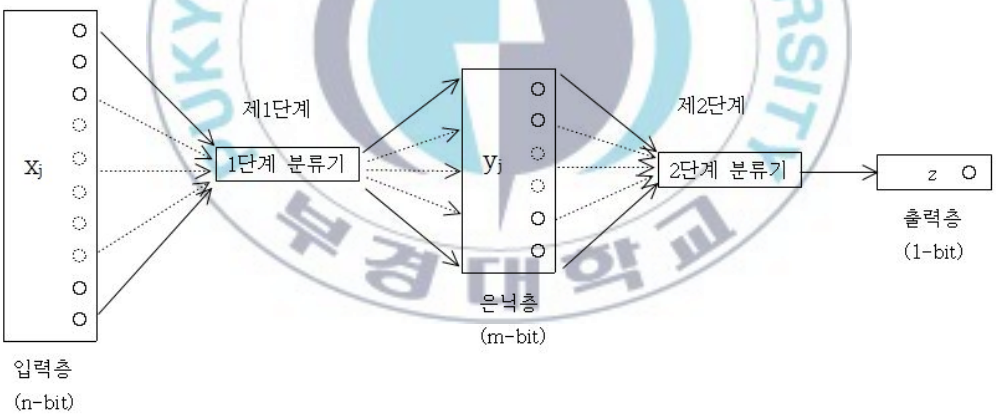


그림 Ⅳ-4. LFSR 기반의 두 단계 패턴분류기

다른 attractor에 속하는 두 개의 n-비트 패턴 집합 S_1와 S_2에 대하여 특성 다항식 $x^{n-m}(1+x)^m$에 해당하는 LFSR 기반의 패턴분류기 T_{C_1}는 다음 식 (4.2)와 같고 S_1과 S_2을 분류 할 수 있다.

$$T_{C_1} = \begin{bmatrix} \begin{bmatrix} 0 \cdots & 0 \\ I_1 & \vdots \\ & 1 \end{bmatrix} & & & \\ & \ddots & & \\ & & \begin{bmatrix} 0 \cdots & 0 \\ I_i & \vdots \\ & 1 \end{bmatrix} & \\ & & & \ddots \\ & & & \begin{bmatrix} 0 \cdots & 0 \\ I_m & \vdots \\ & 1 \end{bmatrix} \end{bmatrix} \tag{4.2}$$

그리고 임의의 두개의 n-비트 패턴 $x_1 \in S_1$과 $x_2 \in S_2$는 식 (4.3)를 만족한다.

$$T_{C_1} \cdot x_1 \neq T_{C_1} \cdot x_2 \tag{4.3}$$

x_1과 x_2가 각각 은닉층의 Class y_1과 y_2에 맵핑되면, attractor의 총 수는 2^m이고 y_j는 m-비트이다. 즉, 두 단계 분류기의 T_{C_1}는 n-비트 패턴 x_i에서 m-비트 Class y_j으로 맵핑된다.

T_{C_2}는 다음 식 (4.4)와 같고 y_j는 단일 비트 z=(0 또는 1)에 맵핑된다.

$$T_{C_2} = \begin{bmatrix} 0 \cdots & 0 \\ & \vdots \\ I_{m-1} & 0 \\ & 1 \end{bmatrix} \tag{4.4}$$

여기서, I_{m-1}는 $(m-1)$차 단위행렬이다.

<예제 4.4.1> $m=2$이고 $n=7$인 LFSR 기반의 두 단계 패턴분류기 T_{C_1}와 T_{C_2}는 각각 다음과 같다.

$$T_{C_1}=\begin{bmatrix}0\,0\,0\,0 & \\ 1\,0\,0\,0 & \\ 0\,1\,0\,0 & O \\ 0\,0\,1\,1 & \\ & 0\,0\,0 \\ O & 1\,0\,0 \\ & 0\,1\,1\end{bmatrix},\quad T_{C_2}=\begin{bmatrix}0\,0\\1\,1\end{bmatrix}$$

다른 attractor에 속하는 두 개의 n-비트 패턴 집합 S_1와 S_2에 대하여 $S_1=\{0000011, 0101000, 0110011, 1111011\}$, $S_2=\{0001000, 0001010, 0111000, 1100111\}$이라 하자. 임의의 두개의 n-비트 패턴 $x_1 \in S_1$과 $x_2 \in S_2$에 대하여 $x_1=(0110011)$와 $x_2=(0111000)$에 대하여, $T_{C_1} \cdot x_1 \neq T_{C_1} \cdot x_2$를 만족한다.

첫 번째 분류기 T_{C_1}에 의하여 x_1는 은닉층의 Class $y_1=(00)$, x_2는 $y_2=(10)$에 맵핑되고 두 번째 분류기 T_{C_2}에 의하여 y_1는 출력층의 단일 비트 $z=0$, y_2는 $z=1$에 맵핑된다.

즉, LFSR 기반의 두 단계 패턴분류기는 큰 테스트 패턴 집합을 분류하기 위하여 m개의 LFSR을 합성하여 설계한 패턴분류기 T에 의해 생성된 n-비트 패턴 **x**을 단일 비트(0 또는 1)에 맵핑하게 한다. 따라서 본 논문에서 제안된 패턴분류기는 큰 테스트 패턴집합을 효율적으로 분류할 수 있다.

Ⅴ. 결론

Maji 등[12]에 의해 제안된 MACA 기반의 패턴분류기는 시간을 $O(n^3)$에서 $O(n)$으로 줄였지만 0-트리를 구하는 초기설정 시간이 필요로 했다.

본 논문에서는 LFSR기반의 패턴분류기를 제안하였다. 제안된 LFSR 기반의 패턴분류기는 각 패턴의 Hamming weight를 알면 패턴분류가 가능하므로 초기 설정시간이 요구되지 않는다. 그리고 m개의 LFSR을 합성하여 패턴분류기 T를 설계하면 주어진 n비트 패턴 **x**가 2^m개의 Class 중 어느 Class에 속하는 지를 쉽게 분류할 수 있다. 그리고 LFSR 기반의 두 단계 패턴분류기는 m개의 LFSR을 합성하여 설계한 패턴분류기 T에 의해 생성된 n-비트 패턴 **x**을 단일 비트(0 또는 1)에 맵핑하게 한다. 따라서 본 논문에서 제안된 패턴분류기는 큰 테스트 패턴집합을 효율적으로 분류할 수 있다.

PUKYONG NATIONAL UNIVERSITY 부경대학교

참 고 문 헌

[1] S. Chattopadhyay, S. Adhikari, S. Sengupta, and M. Pal, "Highly Regular, Modular, and Cascadable Design of Cellular Automata-Based Pattern Classifier," *IEEE Trans. on VLSI Systems*, vol. 8, no. 6, pp. 724-735, 2000.

[2] 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.

[3] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim, and S. H. Heo, "New synthesis of one-dimensional 90/150 linear hybrid group cellular automata," *IEEE Trans. Comput-Aided Des. Integr. Circuits Syst.,* vol. 26, no. 9, pp. 1720-1724, 2007.

[4] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, and J.G. Kim, "Analysis of 90/150 Two Predecessor Nongroup Cellular Automata," *ACRI 2008*, LNCS 5191, pp. 128-135, 2008.

[5] S.J. Cho, U.S. Choi, and H.D. Kim, "Analysis of Complemented CA Derived from a linear TPMACA," *Computers and Mathematics with Applications 45*, pp. 689-698, 2003.

[6] 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.

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

[8] R.A. Horn and C.R. Johnson, *Matrix analysis*, Cambridge

University Press, 1985.

[9] 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 - 16, 2004.

[10] 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.

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

[12] 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.

[13] G.L. Mullen and D. Panario, *Handbook of finite fields,* Chapman and Hall/CRC, 2013.

[14] M. Yilmaz, K. Chakrabarty, and M. Tehranipoor, “Test-pattern grading and pattern selection for small-delay defects,” in *Proc. IEEE VTS*, pp. 233 - 239, 2008.

[15] N. Ganguly, P. Maji, B. K. Sikdar, and P. P. Chaudhuri, “Generalized multiple attractor cellular automata (GMACA) model for associative memory,” *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 16, no. 7, pp. 781-795, 2002.

[16] N. Ganguly, P. Maji, S. Dhar, B.K. Sikdar, and P. P. Chaudhuri, “Evolving Cellular Automata as Pattern Classifier,” *in Proceedings of Fifth International Conference on Cellular Automata for Research and Industry*, ACRI 2002, Switzerland, pp. 56-68, October 2002.

[17] 양명훈외 4인, “가변 길이의 다중 특성 다항식을 사용하는 LFSR을 이용한 새로운 Reseeding 방법”, 전자공학회논문지, 제42권, SD제3호, pp. 35-41, 2005.

[18] 조성진, “유한체 및 그 응용”, 교우사, pp. 97-148 , 2007.

[19] 조성진, 김한두, 최언숙, “첨단공학을 위한 정보수학”, 교우사, pp. 269-325, 2006.

[20] 황윤희 외 2인, “D1-MACA 기반의 최소 메모리량을 갖는 두 패턴 분류기의 구성”, 한국해양정보통신학회논문지 제13권 제5호, pp. 931-936, 2008.

[21] 권숙희 외 4인, “LFSR을 이용한 패턴분류기의 생성”, 한국전자통신학회논문지(투고중).

PUKYONG NATIONAL UNIVERSITY 부경대학교