情報保護學會論文誌
第15券 第2號, 2005. 4

GF(2p) 위에서의 SACA의 상태전이 분석*

조 성 진,[1†] 최 언 숙,[2‡] 황 윤 희,[1] 김 한 두,[3] 표 용 수[1]
[1]부경대학교, [2]영산대학교, [3]인제대학교

The Analysis of State-Transition of SACA over GF(2p)

Sung-Jin Cho,[1†] Un-Sook Choi,[2‡] Yoon-Hee Hwang,[1] Yong-Soo Pyo,[1] Han-Doo Kim[3]
[1]Pukyong National University, [2]Youngsan University, [3]Inje University

요 약

GF(2) 셀룰라 오토마타가 비트단위로 데이터가 처리되는데 비하여 GF(2P) 셀룰라 오토마타는 비트단위 이상의 단위로 데이터를 처리할 수 있다. 본 논문에서는 GF(2p) 위에서의 유한체 성질을 이용하여 한 개의 트리로 구성되는 GF(2P)위에서의 nongroup 셀룰라 오토마타의 상태들의 움직임을 분석한다. 또한 기본경로를 이용하여 GF(2P)위에서 선형 SACA의 상태전이 그래프를 구성하는 방법과 선형 SACA의 상태전이 그래프를 이용하여 비선형인 여원 SACA의 상태전이 그래프를 구성하는 방법을 제시한다.

ABSTRACT

Though GF(2) CA can only handle data with bit units GF(2p) CA can handle data with units more than bit units. In this paper we analyze the state-transition of nongroup cellular automata(CA) with a single attractor over GF(2p). And we propose the constructing method the state-transition diagram of a linear SACA over GF(2p) by using the concept of basic path. Also we propose the state-transition diagram of the nonlinear complemented SACA by using the state-transition diagram of a linear SACA.

Keywords : *single attractor CA, cellular automata, GF(2p) CA, minimal polynomial, nongroup, state transition*

Ⅰ. 서 론

셀룰라 오토마타(CA)는 Von Neumann[1]에 의하여 스스로 조직화하고 재생산할 수 있는 모델로 처음 소개되었다. 이후 1980년대에 Wolfram[2]은 CA를 셀이라 불리는 메모리의 배열로 소개하고, 셀의 상태가 자기 자신 및 인접한 셀 상태의 국소적인 상호작용에 의해서 동시에 갱신되는 시스템으로 제안하였다. 또한 CA는 간단하고, 규칙적이며, 작은 단위로 확장 연결할 수 있는 구조이기 때문에 하드웨어 구현에 알맞다.

GF(2) 위에서의 CA에 대한 분석은 그 동안 많은 연구가 이루어졌으며, 이러한 CA는 폭 넓게 응용되었다. 특히 Cho 등은 GF(2) 위에서 TPMA-CA(Two Predecessor Multiple Attractor Cellular Automata)의 상태전이 그래프를 기본경로를 이용하여 상태전이 그래프를 구성하는 알고리즘을 제안하였다[3,4]. 또한 여원 CA가 비선형이기 때문에 선형 CA에 비하여 분석이 용이하지 못하다. 이러한 문제점을 해결하기위하여 여원 CA와 선형 CA사이의 관계를 밝힘으로써 선형 TPNCA(Two

접수일 : 2005년 3월 25일 ; 채택일 : 2005년 4월 12일
* 본 연구는 한국과학재단 목적기초연구지원사업(R01-2003-000-10663-0)에 의해 수행하였습니다.
† 주저자 : sjcho@pknu.ac.kr
‡ 교신저자 : choies@ysu.ac.kr

Predecessor Nongroup Cellular Automata)에 대응하는 여원 nongroup CA의 상태전이 행동을 분석하였다[5,6].

GF(2) 위에서의 CA는 셀이 한 개의 비트로 이루어져 있으므로 데이터 처리가 비트 단위로 이루어진다. 그러나 GF(2^p) 위에서의 CA는 여러 개의 비트가 한 개의 셀을 이룬다. 따라서 바이트 단위 이상의 단위로 데이터 처리가 가능하다. Sikdar 등은 테스트 패턴 생성을 위하여 계층적 구조를 갖는 GF(2^p) 위에서의 group CA를 사용하였으며[7], VLSI 회로의 결함을 진단하기 위하여 GF(2^p) MACA를 이용하였다[8].

본 논문에서는 GF(2^p) 위에서 선형 SACA(Single Attractor Cellular Automata)를 특성화하고 상태전이 그래프를 효과적으로 구성하는 알고리즘을 제안한다. 또한 선형 SACA에 대응하는 여원 SACA의 상태전이 그래프를 구성하는 알고리즘을 제안한다.

II. GF(2p) Cellular Automata

GF(2) CA는 한 셀의 상태가 {0,1}의 원소이다. 반면 GF(2^p) CA는 p개의 기억소자가 한 개의 셀을 이루기 때문에 셀의 상태는 {0, 1, 2, ···, 2^p-1}의 원소이다. 그림 1은 일반적인 GF(2^p) CA의 구조이다.

GF(2^p)는 GF(2)의 확대체로 2^p개의 원소로 이루어진다. GF(2^p)를 생성하는 다항식을 생성다항식이라 한다. CA의 다음상태를 결정하는 전이행렬은 다음과 같은 삼중대각행렬로 이루어진다. 이때 w_{ij}는 j번째 셀의 현재상태가 i번째 셀의 다음상태에 대한 의존도로써가중치라 하며 GF(2^p)의원소이다.

예를 들어 3 셀 GF(2^2) CA의 전이행렬이 다음

$$T=\begin{pmatrix} w_{11} & w_{12} & 0 & \cdots & 0 \\ w_{21} & w_{22} & w_{23} & \cdots & 0 \\ 0 & w_{32} & w_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & w_{nn} \end{pmatrix}$$

과 같다고 하자.

$$T=\begin{pmatrix} 0 & \alpha & 0 \\ \alpha & 0 & \alpha \\ 0 & \alpha^2 & 1 \end{pmatrix}$$

여기서 는 GF(2^2)를 생성하는 생성자이다. 따라서 GF(2^2)의 원소는 0, 1, α, α^2이다. 또한 α는 생성다항식 $g(x)=x^2+x+1$의 해가 된다. n셀 GF(2^p) CA의 현재 상태 x에 대하여 다음 상태 y는 $y=Tx$ 이다.

생성다항식을 특성다항으로 갖는 행렬 M을 생성행렬이라 한다. 위의 예에서 생성다항식 $g(x)=x^2+x+1$의 생성행렬은 $M=\begin{pmatrix}1&1\\1&0\end{pmatrix}$이다.

n셀 GF(2^p) CA의 상태 x는 n개의 GF(2^p)의 원소인 α^i로 이루어진 벡터로 표현된다. 유한체 위에서 곱셈과 덧셈을 위해 α^i와 M^i의 마지막 열벡터와 대응 시킨다. 예에서 $\alpha=\langle 10\rangle=2$, $\alpha^2=\langle 11\rangle=3$, $\alpha^3=1=\langle 01\rangle=1$, $0=\langle 00\rangle=0$이다. 따라서 GF(2^2)위에서 덧셈과 곱셈은 표 1과 같다.

표 1. GF(22)위에서의 곱셈과 덧셈

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

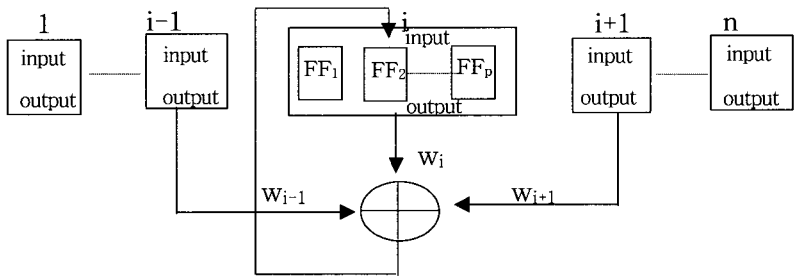


그림 1. GF(2p) CA의 일반적 구조

Ⅲ. GF(2p) Cellular Automata

3.1 선형 GF(2p) SACA

선형 n셀 GF(2^p) SACA C는 nongroup CA로 $|T|=0$이다. 상태 0만 유일한 어트랙터(attractor)로 C의 상태전이 그래프는 깊이가 n인 한 개의 트리로 구성된다. C의 모든 상태의 개수는 2^{np}이고, 임의의 도달가능한 상태의 직전자의 수는 2^p이다. 다음 정리는 C의 전이행렬 T의 성질을 나타낸다.

〈정리 1〉 선형 n셀 GF(2^p) SACA C의 전이행렬을 T라 하면 다음을 만족한다.

(1) $\mathrm{rank}(T) = n-1$.

(2) $\mathrm{rank}(T+I) = n$.

(3) T의 특성다항식과 최소다항식은 x^n이다.

(증명)(1)상태 0의 직전자의 집합은 $\mathrm{x}\,|\,\mathrm{Tx}=0$이다. C의 상태전이그래프에서 상태 0의 직전자의 수는 $|\mathrm{x}\,|\,\mathrm{Tx}=0\,|=2^p$이어야 하므로 행렬 방정식 $Tx=0$에서 자유변수는 1개이다. 따라서 $\dim N(T)=1$이므로 $\mathrm{rank}(T)=n-1$이다.

(2) C의 상태전이그래프에서 어트랙터는 상태 0뿐이므로 $\{\mathrm{x}\,|\mathrm{Tx}=\mathrm{x}\}=\{\mathrm{x}|(\mathrm{T}+\mathrm{I})\mathrm{x}=0\}$ $=\{0\}$이다. 따라서 $\dim N(T+I)=0$이므로 $\mathrm{rank}(T+I)=n$이다.

(3) C의 상태전이 그래프의 트리의 깊이는 n이므로 모든 상태 y에 대하여 $T^n y=0$이어야 한다. 따라서 $T^n=0$을 만족해야 하므로 T의 최소다항식은 $m(x)=x^n$이다. 그런데 T의 특성다항식은 n차 다항식이다. 그러므로 T의 최소다항식과 특성다항식은 모두 x^n이다.

〈정리 2〉 C에서 임의의 도달 가능한 상태의 서로 다른 두 직전자의 합은 상태 0의 0이 아닌 직전자 중의 하나이다.

(증명) 도달 가능한 상태 x의 서로 다른 직전자 y와 z에 대하여 $Ty=Tz=x$이다.

$T(y+z)=0$이므로 $y+z$는 0의 직전자이다. $y\neq z$이므로 $y+z\neq 0$이다. 따라서 $y+z$는 0이 아닌 0의 직전자 중 하나이다.

예를 들어 전이행렬이 $T=\begin{pmatrix}2&2\\2&2\end{pmatrix}$인 2셀 GF($2^2$) CA의 상태 전이그래프는 그림 2와 같다. 그림 2에서 상태 〈11〉의 직전자 중 〈30〉과 〈12〉의 합은 상태 0의 직전자 중 〈22〉와 같다.

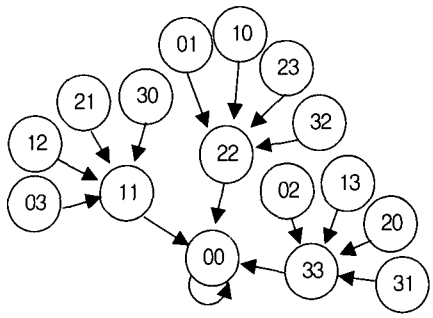


그림 2. 2셀 GF(22) SACA의 상태전이그래프

C의 한 임의의 도달 가능한 상태에서 가장 가까운 순환상태 k로 가는 상태변화를 **k-트리의 경로**라 한다. 그림 2에서 03→11→00은 0-트리의 경로중 하나이다.

〈정리 3〉 C에서 하나의 0-트리의 경로를 알 때 이를 기본경로로 하여 0-트리의 나머지 부분을 기본경로에 놓인 상태들의 합으로 구성할 수 있다.

(증명) 상태 x가 C의 상태전이 그래프에서 한 도달 불가능한 상태라 하고 x로부터 T를 연속하여 적용한 $x\rightarrow Tx\rightarrow\cdots\rightarrow T^{m-1}x(=0)$를 0-트리의 한 기본경로를 얻을 수 있다. $S_{l,0}=T^{m-l-1}x$라 하자. C의 상태전이그래프에서 레벨 l의 k번째 상태 $S_{l,k}(k=0,1,2,\cdots,n-1)$를 다음과 같이 두자.

$$S_{l,k}=(b_l+1)S_{l,0}+\sum_{i=1}^{l-1}b_i S_{i,0}$$

여기서 b_i는 k를 2^p진법으로 표현했을 때 각 자리의 수이다. 즉 $k=b_l b_{l-1}\cdots b_{1_{(2^p)}}$ $(0\leq k\leq(2^p)^l-1(2^p)-1)$이다. 그러면 레벨 1부터 레벨 n까지 상태 수는 다음과 같다.

$$\sum_{l=1}^{n}(2^p)^{l-1}(2^p-1)=(2^p)^n-1$$

어트랙터를 포함한 C의 상태전이 그래프의 모든 상태 수는 $(2^p)^n-1+1=2^{pn}$으로 n-셀 GF(2^p) CA의 모든 상태 수와 같다. 또한 다음이 성립한다.

$$TS_{l,k} = T((b_l+1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0})$$

$$= (b_l+1)TS_{l,0} + \sum_{i=1}^{l-1} b_i TS_{i,0}$$

$$= (b_l+1)S_{l-1,0} + b_{l-1}S_{l-2,0}$$

$$+\cdots + b_2 S_{1,0} + b_1 S_{0,0} \quad \cdots\cdots (1)$$

식 (1)에서 $S_{0,0}=0$ 이고, 상태전이 그래프에서 레벨이 하나 낮아질 때마다 상태의 수는 2^p 개씩 작아지므로 $k' = \left[\frac{k}{2^p}\right]$ 라 두면

$$k = b_l b_{l-1} \cdots b_{1_{(2^p)}} \quad k' = b_l b_{l-1} \cdots b_{2_{(2^p)}} = b'_{l-1} \cdots b'_{1_{(2^p)}}$$

이 된다. 따라서 식 (1)은 다음과 같다.

$$TS_{l,k} = (b'_{l-1}+1)S_{l-1,0} + \sum_{i=1}^{l-2} b'_i S_{i,0} = S_{l-1,k'}$$

그림 2에서 03→11→00를 0트리의 기본경로라 하면 레벨 2의 6번째 상태 $S_{2,6}$ = 〈23〉은 2 〈03〉 + 2 〈11〉 = 〈23〉 을 만족한다.

3.2 여원 GF(2p) SACA

각 셀에 적용되는 상태전이 규칙이 XOR논리와 XNOR 논리의 조합으로 이루어지는 여원 CA의 다음 상태를 나타내는 함수는 $y = \overline{T}x = Tx + F$이다. 여기서 F를 여원벡터라 한다. 예를 들어 전이행렬 T가 다음과 같은 4-셀 GF(2^2) CA를 생각해 보자.

$$T = \begin{pmatrix} 1&2&0&0 \\ 0&1&3&0 \\ 0&0&1&2 \\ 0&0&0&1 \end{pmatrix}$$

이때, 여원 벡터를 $F=[2\,0\,3\,1]^t$라 하면 주어진 4-셀 여원 GF(2^2) CA의 구조는 그림 3과 같다. 현재 상태가 $x=[3\,1\,2\,3]^t$ 일 때, 다음 상태 y는

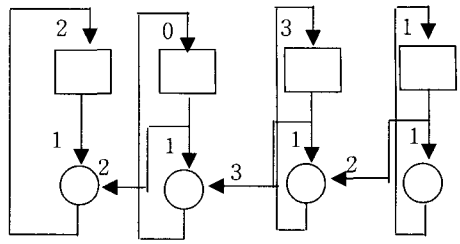


그림 3. 4-셀 GF(22) 여원 CA의 구조

$y = Tx + F$에 의해 구한다. 표 1을 이용하여 y를 구하면 다음과 같다.

$$y = \begin{pmatrix} 1&2&0&0 \\ 0&1&3&0 \\ 0&0&1&2 \\ 0&0&0&1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \\ 2 \\ 3 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 0 \\ 2 \end{pmatrix}$$

현재 상태 x에서 k단계 후의 상태는 다음 같다.

$$\overline{T}^k x = T^k x + (T^{k-1} + \cdots + T + I)F$$

GF(2^p)위에서 선형 n셀 SACA C에서 여원벡터 F가 C의 상태전이 그래프에서 레벨 l있는 상태라 하면 C에 대응하는 여원 CA 역시 SACA C′가 된다. 여원 벡터의 위치가 선형 SACA의 상태전이 그래프에서 레벨 l에 있을 때, 그래프에서 레벨 l에 있을 때, 여원 SACA C′의 상태전이 그래프는 표 2와 같은 규칙으로 재배열 된다.

예를 들어 그림 2의 C에서 여원벡터 F가 〈30〉t 일때, C에 대응하는 C′은 그림 4와 같다.

〈정리 4〉 C에서 하나의 0-트리의 경로를 알고, 주어진 여원 벡터에 의해 C로부터 유도되는 C′의

표 2. 선형 SACA와 여원 SACA의 상태배열 관계

GF(2p)위에서 선형 SACA	GF(2p)위에서 여원 SACA
레벨 l 보다 상위 레벨에 있는 상태	레벨이 변하지 않는다.
레벨 l보다 하위 레벨에 있는 상태	레벨 l에 재배열 된다.
상태 F(여원벡터)	레벨 $l-1$에 놓인다.
레벨 l에 있는 상태	레벨 l이하에 놓인다.

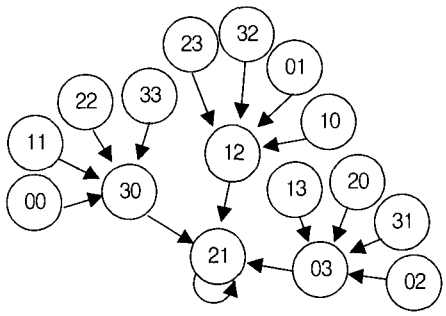


그림 4. GF(22) 여원 SACA의 상태전이그래프

기본 경로를 알면 이 두 경로에 의해 $\mathbb{C}'$의 상태전이 그래프를 구성할 수 있다.

(증명) $S_{n,0} \rightarrow S_{n-1,0} \rightarrow \cdots \rightarrow S_{0,0}(=0)$ 을 $\mathbb{C}$의 기본경로라 하고 $\overline{S_{n,0}} \rightarrow \overline{S_{n-1,0}} \rightarrow \cdots \overline{S}_{0,0}$ 를 $\mathbb{C}'$의 기본경로라 하자. $\mathbb{C}'$의 상태전이그래프에서 레벨 l의 k번째 상태 $\overline{S}_{l,k}(k=1, 2, \cdots n-1)$를 다음과 같이 정의하자.

$$\overline{S_{l,k}} = \overline{S_{l-1,0}} + (b_l + 1) S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}$$

여기서 b_i는 k를 2^p진법으로 표현했을 때 각 자리의 수이다. 즉 $k = b_l b_{l-1} \cdots b_{1_{(2^p)}}$ $(0 \leq k \leq (2^p)^{l-1}(2^p)-1)$ 이다. 그러면 레벨 1부터 레벨 n까지 상태 수는 다음과 같다.

$$\sum_{l=1}^{n} (2^p)^{l-1}(2^p-1) = (2^p)^n - 1$$

어트랙터를 포함한 $\mathbb{C}'$의 상태전이 그래프의 모든 상태 수는 $(2^p)^n - 1 + 1 = 2^{pn}$으로 n-셀 GF(2^p) CA의 모든 상태 수와 같다. 또한 다음이 성립한다.

$$\begin{aligned}
&\overline{T}\ \overline{S}_{l,k} \\
&= T(\overline{S}_{l,k}) + F \\
&= T(\overline{S}_{l-1,0} + (b_l+1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}) + F \\
&= T\,\overline{S}_{l-1,0} + F + (b_l+1)\,S_{l-1,0} + \sum_{i=1}^{l-2} b_{i+1} S_{i,0} \\
&= \overline{S}_{l-2,0} + (b'_{l-1}+1)\,S_{l-1,0} + \sum_{i=1}^{l-2} b'_i S_{i,0} \\
&= \overline{S}_{l-1,k}
\end{aligned}$$

여기서

$$k' = \left[\frac{k}{2^p}\right] = b_l b_{l-1} \cdots b_{2_{(2^p)}} = b'_{l-1} \cdots b'_{1_{(2^p)}}$$

이다.

Ⅳ. GF(2p) SACA 트리구성

정리 3과 정리 4에 의하여 다음과 같은 GF(2^p) 위에서 SACA상태전이 그래프 트리구성 알고리즘을 제안한다.

Step 1. 전이행렬 T에 대하여 $T^n x = 0$이고 $T^{n-1}x \neq 0$인 0-트리의 도달 불가능상태 x를 찾는다.

Step 2. x를 시작으로 하는 0-트리의 기본경로 $x(S_{n,0}) \rightarrow Tx(S_{n-1,0}) \rightarrow \cdots \rightarrow 0$를 찾는다.

Step 3. $S_{l,k} = (b_l+1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}$ 에 의하여 0-트리를 구성한다.

/* 여원 SACA 트리 구성*/

Step 4. 여원 SACA의 기본경로를 구한다. 여원 벡터 F가 도달 불가능한 상태면 $0(\overline{S}_{n,0}) \rightarrow \overline{T}0(\overline{S}_{n-1,0}) \rightarrow \cdots \rightarrow \overline{T}^n 0$ 가, 여원 벡터 F가 0이 아닌 도달가능한 상태이면 Step 1에서 구한 선형 SACA의 도달불가능한 상태 x에 대해

$$x(\overline{S}_{n,0}) \rightarrow \overline{T}x(\overline{S}_{n-1,0}) \rightarrow \cdots \rightarrow \overline{T}^n x$$

가 여원 SACA의 기본경로가 된다.

Step 5. $\overline{S}_{l,k} = \overline{S}_{l-1,0} + (b_l+1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}$에 의하여 $\mathbb{C}'$의 트리를 구성한다.

Ⅴ. 결 론

본 논문에서는 p개의 기억소자가 한 개의 셀을 이루는 GF(2^p) 위에서 n셀 선형 SACA의 특성을 분석하고 선형 SACA로부터 유도되는 여원 SACA의 상태전이 행동을 분석하였다. 또한 GF(2^p) 위에

서 선형 SACA의 기본경로와 여원 SACA의 기본경로를 통하여 SACA의 상태전이 그래프를 구성하는 알고리즘을 제안하였다.

참 고 문 헌

[1] J. Von Neumann, "Theory of self-reproducing automata", University of Illinois Press Urbana, 1966.

[2] S. Wolfram, "Statistical mechanics of cellular automata", Rev. Modern Physics, Vol. 55, No. 3, 1983.

[3] 조성진 ,최언숙, 김한두, "GF(2) 상에서 1차원 Linear Nongroup CA 특성에 관한 연구", 멀티미디어학회 논문지, 제 4권 1호, pp. 91-94, 2001.

[4] S.J. Cho, U.S. Choi and H.D. Kim, "Analysis of complemented CA derived from a linear TPMACA", Computers & Mathematics with Applications, Vol. 45, Issues 4-5, pp. 689-698, 2003.

[5] S.J. Cho, U.S. Choi and H.D. Kim," Behavior of complemented CA whose complement vector is acyclic in a linear TPMACA", Mathematical and Computer Modelling, Vol. 36, Issues 9- 10, pp. 979-986, 2002.

[6] 조성진, 최언숙, 황윤희, 김한두, 허성훈, "선형 TPNCA로부터 얻어지는 여원 TPNCA의 행동분석", 멀티미디어학회 논문지, 제 6권 3호, pp. 549-555, 2003.

[7] B.K. Sikdar, P. Majumder, M. Mukherjee, N. Ganguly, D.K. Das and P.P. Chaudhuri, "Hierarchical Cellular Automata As An On-Chip Test Pattern Generator", VLSI Design, Fourteenth International Conference on 2001, pp. 403-408, 2001.

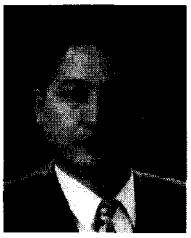
[8] B.K. Sikdar, N. Ganguly, P. Majumder, P.P. Chaudhuri, "Design of Multiple Attractor GF(2p) Cellular Automata for Diagnosis of VLSI Circuits", VLSI Design, Fourteenth International Conference on 2001, pp. 454-459, 2001.

〈著者紹介〉

조 성 진(Sung-Jin Cho) 정회원
1979년 2월: 강원대학교 수학교육과 학사
1981년 2월: 고려대학교 수학과 석사
1988년 2월: 고려대학교 수학과 박사
1988년~현재 : 부경대학교 수리과학부 정교수
〈관심분야〉 셀룰라 오토마타론, 정보보호, 부호이론

최 언 숙 (Un-Sook Choi)
1992년 2월: 성균관대학교 산업공학과 학사
2000년 2월: 부경대학교 응용수학과 석사
2004년 2월: 부경대학교 응용수학과 박사
2004년 3월~현재 : 영산대학교 자유전공학부 단임교수
〈관심분야〉 셀룰라 오토마타론, 정보보호, 부호이론

황 윤 희(Yoon-Hee Hwang)
2002년 2월 : 부경대학교 통계학과 학사
2004년 2월 : 부경대학교 응용수학과 석사
2004년 3월~현재 : 부경대학교 정보보호학과 박사과정
〈관심분야〉 셀룰라 오토마타론, 정보보호, 유한체론



김 한 두 (Han-Doo Kim)
1982년 2월 : 고려대학교 수학과 학사
1984년 2월 : 고려대학교 수학과 석사
1988년 2월 : 고려대학교 수학과 박사
1989년~현재 : 인제대학교 컴퓨터 응용과학부 정교수
〈관심분야〉 전산수학, 셀룰라 오토마타론

표 용 수 (Yong-Soo Pyo)
1980년 2월 : 계명대학교 수학과 학사
1982년 2월 : 계명대학교 수학과 석사
1987년 2월 : 계명대학교 수학과 박사
1983년~현재 : 부경대학교 수리과학부 정교수
〈관심분야〉 셀룰라 오토마타론, 유한체론