90/150 SACA로부터 유도된 90/150 MACA의 분석

조성진[*]· 최언숙[**]· 김한두[***] · 황윤희[*]· 김진경[*]· 김봉수[*]
[*]부경대학교· [**] 동명대학교 · [***]인제대학교

Analysis of 90/150 MACA derived from 90/150 SACA

S.J. Cho[*]· U.S. Choi[**]· H.D. Kim[***] · Y.H. Hwang[*] · J.G. Kim[*] · B.S. Kim [***]
[*]Pukyong National University ·[**] Tongmyong University ·[***]Inje University
E-mail : sjcho@pknu.ac.kr

요 약

90/150 그룹 셀룰라 오토마타 (이하, CA)에 대한 합성 방법은 많은 연구자들에 의해 연구되어왔다. 그러나 90/150 비그룹 CA의 합성방법에 대한 연구는 매우 미비하다. 본 논문에서는 90/150 비그룹 CA중 순환상태의 사이클의 길이가 항상 1인 multiple-attractor CA의 특성을 분석한다. 90/150 multiple-attractor CA중 attractor의 수가 하나인 single-attractor CA를 구성하는 방법을 제안하고 이 결과를 이용하여 90/150 multiple-attractor CA를 합성하는 방법을 제안한다.

ABSTRACT

Many researchers have studied synthesis method of 90/150 group CA. However, there is a lack of researches for synthesis method of 90/150 nongroup CA. In this paper we report some interesting properties of 90/150 multiple-attractor CA in which all of the cycles are of unit length. 90/150 multiple-attractor CA is a class of nongroup CA. And we propose a construction of 90/150 single-attractor CA. Also we construct 90/150 multiple-attractor CA derived from 90/150 single-attractor CA.

키워드

90/150 MACA, 영공간, attractor, 전이규칙, CA 합성

Ⅰ. 서 론

셀룰라 오토마타(이하 CA)는 간단하고, 규칙적이며, 작은 단위로 확장 연결할 수 있는 구조이기 때문에 하드웨어 구현에 알맞다. CA는 이미지 압축, 해싱, 테스트 패턴 생성, 의사난수생성, 암호학, 오류정정부호 및 압축치 분석 등 여러 응용 분야에서 적용되고 있다. 이러한 응용분야에 적합한 CA를 합성하는 방법은 많은 연구자들의 주요한 관심분야중 하나이다[1,2]. 2007년 Cho 등은 90/150 선형 하이브리드 그룹 CA의 새로운 합성 알고리즘을 제안했다[3]. 그러나 90/150 비그룹 CA의 합성법에 대한 연구는 매우 미비하다.

본 연구는 한국과학재단 특정기초연구지원사업 (R01-2006-000-10260-0)에 의해 수행하였습니다.

Chattopadhyay[4]가 해쉬함수에 응용에 효과적인 multiple-attractor CA(이하 MACA)를 찾는 알고리즘을 처음으로 제안하였다. 그가 제안한 MACA는 선형 전이규칙인 규칙 60, 90, 102, 150, 170, 204, 240를 모두 사용하여 구성하는 방법이다. 그러나 90/150 CA는 그것의 전이행렬의 특성다항식과 최소다항식이 항상 같기 때문에 CA의 특성을 분석하기가 쉽고, 하드웨어 구현에도 효과적이다. 따라서 본 논문에서는 90/150 선형 하이브리드 비그룹 CA중 순환상태의 길이가 1인 90/150 MACA를 분석하고 이러한 CA의 합성방법을 제안한다. 먼저 90/150 SACA의 합성에 대한 방법을 제안하고 90/150 SACA로부터 유도된 90/150 MACA를 찾는 방법을 제안한다. 또한 이미지 압축과 해싱의 연구에 유용한 SACA와 MACA의 상태전이그래프에서 주어진 상태가 도달가능상태인지 도달불가능상태인지를 영공간 개념을 이용하여 결정하는 방법을 제시한다.

이 방법은 [5]에서 제안한 직전자를 두 개 가지는 MACA의 트리구성방법을 90/150 MACA에 대하여 효과적으로 개선할 수 있다.

II. CA의 배경지식

CA는 규칙적인 방법에 의해 공간적으로 배열된, 각 셀의 상태전이가 그 셀의 이웃에 의존하는 상호 연결된 셀들로 이루어진다. Wolfram에 의해 조사된 CA의 구조는 셀들의 이산격자로 간주될 수 있다. 단, 각 셀의 값은 0 또는 1로 가정하고, 한 셀의 다음상태는 자신과 그의 두 이웃에 의존한다고 하자. 본 논문에서 다루는 CA는 전이규칙으로 90과 150만을 사용한다. 전이규칙 90과 150의 결합논리는 다음 식으로 표현할 수 있고 $\oplus$는 XOR 논리를 나타낸다.

전이규칙 90: $q_i(t+1)=q_{i-1}(t)\oplus q_{i+1}(t)$

전이규칙150: $q_i(t+1)=q_{i-1}(t)\oplus q_i(t)\oplus q_{i+1}(t)$

다음은 본 논문의 전개에 필요한 몇 가지 기본적인 용어이다[4].

- **선형 비그룹 CA** : 비그룹 CA에서 다음 상태를 결정짓는 상태전이함수는 XOR 논리로만 이루어져 있어서 이 함수를 행렬로 표현할 수 있다. 이러한 CA를 선형 비그룹 CA라 한다.
- **도달가능상태** : 비그룹 CA의 상태전이그래프에서 진입차수가 1이상인 상태를 도달가능상태라 하고 진입차수가 0인 상태를 도달불가능상태라고 한다.
- **Attractor** : 비그룹 CA의 상태전이그래프에서 순환상태들 중 사이클(cycle)의 길이가 1인 상태를 attractor라 한다.
- **Depth** : 비그룹 CA의 상태전이그래프에서 임의의 한 도달불가능상태에서 가장 가까운 순환상태로 가는데 걸리는 최소 단계수를 depth라 한다.
- **Level** : 어떤 상태 x가 α-트리의 level $k(k\leq$ depth)에 있다는 것은 상태 x가 정확히 k단계후 상태 α가 되는 위치에 있다는 것이다. 즉, $T^p x=\alpha$가 되는 p값 중 최소값이 k이다.
- **Multiple-Attractor CA(MACA)** : 상태전이 그래프가 각 attractor를 root로 하는 서로 분리된 트리들로 구성되는 CA를 MACA라 한다.

n-셀 90/150 CA의 상태전이행렬 T_n은 다음과 같은 삼중대각행렬이 된다.

$$T_n=\begin{pmatrix} d_1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & d_2 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & d_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & d_n \end{pmatrix}$$

여기서 d_i는 i번 째 셀에 적용된 전이규칙이 90이면 '0'이고, 150이면 '1'이 된다. 본 논문에서는 간단히 $T_n=<d_1,d_2,\cdots,d_n>$으로 나타내기로 한다.

본 논문에서 다루는 90/150 CA는 특성다항식과 최소다항식이 항상 같기 때문에 최소다항식을 구할 필요 없이 특성다항식으로부터 CA의 구조를 분석할 수 있다[6].

Δ_n을 n-셀 90/150 CA의 상태전이행렬 $T_n=<d_1,d_2,\cdots,d_n>$의 특성다항식이라고 하자. 그러면 다음 식이 성립한다[1]:

$$\Delta_n=(x+d_n)\Delta_{n-1}+\Delta_{n-2}$$
$$\Delta_{-1}=0,\ \Delta_0=1 \qquad (1)$$

여기서 Δ_{n-1}은 행렬 T_n에서 1행부터 $n-1$행까지, 1열부터 $n-1$열까지의 부분행렬에 대한 행렬식이다.

III. 90/150 MACA의 합성 및 분석

이 절에서는 식 (1)의 점화관계로부터 n-셀 90/150 SACA를 합성하고 이로부터 90/150 MACA를 유도한다. 이러한 90/150 SACA와 90/150 MACA의 상태전이 행동을 분석한다. 이러한 n-셀 90/150 SACA의 특성다항식은 x^n이다. 따라서 이러한 CA의 상태전이그래프는 0을 root로 하는 depth가 n인 트리인 full 이진트리가 되어야 하므로 임의의 도달가능한 상태에 대한 직전자는 2개이다. 90/150 MACA의 도달가능한 상태의 직전자도 같은 이유로 2개이다.

<정리 1> $<d_1,d_2,\cdots,d_m>$을 m-셀 90/150 SACA라 하자. 각 $n=2m\,(m\in\mathbb{N})$에 대하여 다음은 $2m$-셀 90/150 SACA이다.

$<d_1,\cdots,d_{m-1},\overline{d_m},\overline{d_m},d_{m-1},\cdots,d_1>$

여기서 $\overline{d_m}$은 m번째 셀의 전이규칙이 90이면 150으로, 150이면 90으로 바꾸는 것을 의미한다. □

예를 들어 $n=1$이라 하면 $<0>$은 1-셀 90/150 SACA이다. 정리 1에 의하여 **<1,1>**은 2-셀 90/150 SACA이고, 2-셀 SACA로부터 4-셀 SACA를 합성하면 **<1,0,0,1>**이다.

다음 정리는 주어진 홀수개의 셀을 갖는 90/150 SACA의 합성방법이다.

<정리 2> $<d_1,d_2,\cdots,d_m>$을 m-셀 90/150 SACA라 하자. 각 $n=2m+1$에 대하여 다음은 $(2m+1)$-셀 90/150 SACA이다.

$<d_1,\cdots,d_{m-1},d_m,0,d_m,d_{m-1},\cdots,d_1>$ □

예를 들어, 3-셀 90/150 SACA $<0,0,0>$는 1-셀 SACA <0>으로부터 정리 2를 이용하여 합성하며 5-셀 90/150 SACA <1,1,0,1,1>는 2-셀 90/150 SACA <1,1> 로부터 합성한다.

정리 1과 정리 2를 통하여 모든 크기의 90/150 SACA를 합성할 수 있다.

90/150 SACA의 상태전이 행동을 분석하기 위해서 상태 0의 직전자에 대해 분석할 필요가 있다. 상태 0의 직전자는 주어진 상태전이행렬의 영공간으로부터 찾을 수 있으며 이런 영공간을 찾기 위해 $n \times n$ 선형연립방정식을 풀어야 한다. 그러나 정리 1과 정리 2에 의해 합성된 90/150 SACA는 전이규칙이 대칭적이므로 상태 0의 직전자인 상태전이행렬의 영공간도 다음과 같은 특성을 갖는다.

<정리 3> $N(T_m)=[(a_1,\cdots,a_m)^t]$을 m-셀 90/150 SACA의 상태전이행렬 T_m의 영공간이라 하면 다음이 성립한다.

(i) $n=2m(m\in\mathbb{N})$이고 $N(T_m)=[(a_1,\cdots,a_m)^t]$이면 $N(T_n)=[(a_1,a_2,\cdots,a_m,a_m,\cdots,a_2,a_1)^t]$이다.

(ii) $n=2m+1(m\in\mathbb{N})$이고 $N(T_m)=[(a_1,\cdots,a_m)^t]$이면 $N(T_n)=[(a_1,a_2,\cdots,a_m,0,a_m,\cdots,a_2,a_1)^t]$이다. □

예를 들어 $<1,1>$은 영공간이 $N(T_2)=[(1,1)^t]=\{0,3\}$인 2-셀 90/150 SACA이므로 $<1,0,0,1>$은 4-셀 90/150 SACA이고 T_4의 영공간은 $N(T_4)=[(1,1,1,1)^t]=\{0,15\}$이다. 그림 1은 4-셀 90/150 SACA <1,0,0,1> 의 상태전이그래프이다.

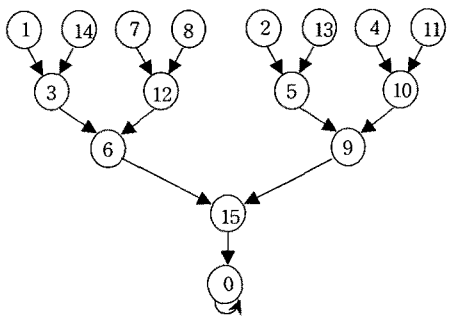

그림1. 4-셀 90/150 SACA <1,0,0,1>의 상태전이그래프

다음은 90/150 SACA로부터 90/150 MACA를 합성하는 방법을 제안한다. 주어진 n-셀 90/150 MACA의 최소다항식은 $x^{n-1}(x+1)$이다. 단 n은 홀수이다.

<정리 4> $<d_1,d_2,\cdots,d_n>(:=T_n)$이 n-셀 90/150 SACA의 상태전이행렬이면 $<d_1,\cdots,d_n,1,d_n,\cdots,d_1>(:=T_{2n+1})$은 최소다항식이 $x^{2n}(x+1)$인 $(2n+1)$-셀 90/150 MACA의 상태전이행렬이다. □

정리 4에서와 같이 SACA $\mathbb{C}$로부터 얻는 MACA를 $\mathbb{C}$로부터 유도된 MACA라 부른다. 표1에서 $N(T_S)$는 n-셀 90/150 SACA의 영공간, 표2에서 $N(T_M)$은 n-셀 90/150 MACA의 영공간, $N(T_M\oplus I)$는 n-셀 90/150 MACA의 모든 attractor들의 집합을 의미한다. 여기서 101은 $[(1,0,1)^t]$로 $(1,0,1)^t$의 생성공간을 의미한다.

다음 정리는 상태 0의 직전자를 찾는 정리로 주어진 상태전이행렬의 영공간으로 부터 상태0의 직전자를 찾는다. 90/150 SACA의 상태전이그래프인 트리를 구성하기 위하여 0-트리의 도달불가능한 상태를 찾는 것이 중요하다. 이를 위하여 $T^{n-1}x\neq 0$ 이고 $T^n x=0$ 인 상태 x를 찾기 위해 T^{n-1}를 분석한다.

<정리 5> $N(T_m)=[(a_1,\cdots,a_m)^t]$이 m-셀 90/150 SACA $\mathbb{C}_1$의 상태전이행렬 T_n의 영공간이라 하면 $\mathbb{C}_1$으로부터 유도된 $(2m+1)$-셀 90/150 MACA $\mathbb{C}_2$의 영공간은 다음과 같다.

$$N(T_{2m+1})=[(a_1,\cdots,a_{m-1},a_m,0,a_m,a_{m-1},\cdots,a_1)^t]$$

[표1] 90/150 SACA와 90/150 MACA

n	SACA	$N(T_S)$	MACA
1	0	1	1
2	11	11	
3	000	101	010
4	1001	1111	
5	11011	11011	11111
6	001100	101101	
7	0000000	1010101	0001000
8	10000001	11111111	
9	100101001	111101111	100111001
10	1101001011	1101111011	
11	11011011011	11011011011	11011111011
12	001101101100	101101101101	
13	0011000001100	1011010101101	0011001001100

[표2] 90/150 MACA의 attractor

n	MACA	$N(T_M)$	$N(T_M\oplus I)$
1	1	0	0
3	010	101	111
5	11111	11011	10101
7	0001000	1010101	1101011
9	100111001	111101111	101111101
11	11011111011	11011011011	10111111101
13	0011001001100	1011010101101	1101011101011

<정리 6> $\mathbb{C}$를 상태전이행렬이 T_n인 n-셀 90/150 SACA라 하고 $N(T_n)=[(a_1,\cdots,a_n)^t]$를 T_n의 영공간이라 하자. 그러면 T_n^{n-1}의 i열은 $a_i=0$이면 T_n^{n-1}의 i열은 $(0,\cdots,0)^t$이고 $a_i\neq 0$이면 T_n^{n-1}의 i열은 $(a_1,\cdots,a_n)^t$이다. □

$\mathbb{C}$를 상태전이행렬이 T_n인 n-셀 90/150 SACA라 하자. 정리 6에 의하여 $\mathbb{C}$의 상태전이그래프에서 도달불가능상태를 쉽게 구할 수 있다. $a_1x_1+a_2x_2+\cdots+a_nx_n\neq 0$이면 $x=(x_1,x_2,\cdots,x_n)^t$는 도달불가능상태이다. $\mathbb{C}$를 상태전이행렬이 T_n인 n-셀 90/150 SACA라 하자. $N(T_n)=[(b_1,b_2,\cdots,b_{n-1},1)^t]$이므로 $(0,\cdots,0,1)^t$는 도달불가능상태이다.

예제 1. $T=<1,1,0,1,1>$을 상태전이행렬이 T인 5-셀 90/150 SACA라 하자. 그러면 $N(T)=[(1,1,0,1,1)^t]$이다. 그러므로 $T^4=\begin{pmatrix}1&1&0&1&1\\1&1&0&1&1\\0&0&0&0&0\\1&1&0&1&1\\1&1&0&1&1\end{pmatrix}$이다. $T^4(0,0,0,0,1)^t\neq 0$이므로 $(0,0,0,0,1)^t$는 도달불가능상태이다.

$\mathbb{C}$를 상태전이행렬이 T인 n-셀 90/150 MACA라 하자. 그리고 $N(T\oplus I)$를 $T\oplus I$의 영공간이라 하자. 그러면 T^{n-1}의 영공간은 $N(T\oplus I)$이다.

<정리 7> $\mathbb{C}$를 상태전이행렬이 T인 n-셀 90/150 MACA라 하고 $N(T)=[(a_1,\cdots,a_n)^t]$를 T의 영공간이라 하자. 그러면 T^{n-1}의 i열은 $a_i=0$이면 T^{n-1}의 i열은 $(0,\cdots,0)^t$이고 $a_i\neq 0$이면 T^{n-1}의 i열은 $(a_1,\cdots,a_n)^t$이다. □

$\mathbb{C}$를 상태전이행렬이 T인 n-셀 90/150 MACA라 하고 α를 $\mathbb{C}$의 영이 아닌 attractor라 하자. 그러면 T^{n-1}의 마지막 열은 T^{n-2}의 마지막 열과 다르다. $\mathbb{C}$를 상태전이행렬이 T인 n-셀 90/150 MACA라 하고 α를 $\mathbb{C}$의 영이 아닌 attractor라 하자. 그러면 $(0,\cdots,0,1)^t$은 $\mathbb{C}$의 α-트리의 도달불가능상태이다. $\mathbb{C}$의 0-트리와 α-트리가 동형이므로[7] $\mathbb{C}$를 상태전이행렬이 T인 n-셀 90/150 MACA라 하고 α를 $\mathbb{C}$의 영이 아닌 attractor라 하자. 그러면 $(0,\cdots,0,1)^t+\alpha$는 $\mathbb{C}$의 0-트리의 도달불가능상태이다.

예제 2. $\mathbb{C}_M^7=<0,0,0,1,0,0,0>$를 상태전이행렬이 T인 7-셀 90/150 MACA라 하자. 그러면

$$T=\begin{pmatrix}0&1&0&0&0&0&0\\1&0&1&0&0&0&0\\0&1&0&1&0&0&0\\0&0&1&1&1&0&0\\0&0&0&1&0&1&0\\0&0&0&0&1&0&1\\0&0&0&0&0&1&0\end{pmatrix},\ T^6=\begin{pmatrix}0&1&1&1&1&1&0\\1&1&0&1&0&1&1\\1&0&1&0&1&0&1\\1&1&0&1&0&1&1\\1&0&1&0&1&0&1\\1&1&0&1&0&1&1\\0&1&1&1&1&1&0\end{pmatrix},\ T^6=\begin{pmatrix}1&1&0&1&0&1&1\\1&1&0&1&0&1&1\\0&0&0&0&0&0&0\\1&1&0&1&0&1&1\\0&0&0&0&0&0&0\\1&1&0&1&0&1&1\\1&1&0&1&0&1&1\end{pmatrix}$$

$N(T\oplus I)=\{0,107\}$이고 $(0,0,0,0,0,0,1)^t$이 107-트리의 도달불가능상태이므로 $(1,1,0,1,0,1,0)^t=(0,0,0,0,0,0,1)^t+(1,1,0,1,0,1,1)^t$도 0-트리의 도달불가능상태이다. □

Ⅳ. 결론

본 논문에서는 90/150 비그룹 CA인 90/150 SACA의 합성에 대한 방법을 제안하고 90/150 SACA로부터 유도된 90/150 MACA를 찾는 방법을 제안했다. 또한 이미지 압축과 해싱의 연구에 유용한 SACA와 MACA의 상태전이그래프에서 주어진 상태가 도달가능상태인지 도달불가능상태인지를 영공간 개념을 이용하여 결정하는 방법을 제시하였다. 이 방법은 [1]에서 제안한 90/150 MACA의 트리구성방법을 개선한 것이다.

참고문헌

[1] K. Cattell and Jon C. Muzio, Synthesis of one-dimensional linear hybrid cellular automata, IEEE Trans. Comput-Aided Des. Integr. Circuits Syst., Vol. 15(3). pp. 325-335, 1996.

[2] S. Chakraborty, D.R. Chowdhury, P.P.Chaudhuri, Theory and application of nongroup cellular automata for synthesis of easily testable finite state machines, IEEE Trans. Computers, Vol. 45(7), pp. 769-781, 1996.

[3] S.J. Cho, U.S. Choi, H.D. Kim and Y. H. Hwang, New synthesis of one-dimensional 90/150 linear hybrid group cellular automata, IEEE Trans. Comput-Aided Des. Integr. Circuits Syst., Vol. 26(9), pp. 1720-1724, 2007

[4] S. Chattopadhyay, Some studies on theory and application of additive cellular automata, PhD thesis, I.I.T., Kharagpur, India, 1995.

[5] S.J. Cho, U.S. Choi and H.D. Kim, Analysis of complemented CA derived from a linear TPMACA, Computers Math. Appli., 45, pp. 689-698, 2003.

[6] R.A.Horn and C.R.Johnson, Matrix Analysis, Cambridge University Press, 1985.

[7] S.J. Cho, U.S. Choi and H.D. Kim, Behavior of complemented CA whose complement vector is acyclic in a linear TPMACA, Math. Comput. Modelling, Vol. 36, pp. 979-986, 2002.