

교육학석사 학위논문

가산 Nongroup 셀룰라 오토마타의 상태전이 행동 분석

2002 년 8 월

부경대학교 교육대학원

수 학 교 육 전 공

최 향 희

교육학석사 학위논문

가산 Nongroup 셀룰라 오토마타의 상태전이 행동 분석

지도교수 조 성 진

이 논문을 교육학석사 학위논문으로 제출함

2002 년 8 월

부경대학교 교육대학원

수 학 교 육 전 공

최 향 희

최향희의 교육학석사 학위논문을 인준함

2002년 6 월 21 일

주 심 이학박사 표 용 수 (인)

위 원 이학박사 박 용 범 (인)

위 원 이학박사 조 성 진 (인)

목 차

Abstract	ii
1. 서론	1
2. 셀룰라 오토마타	3
2.1 CA의 정의 및 분류	3
2.2 CA의 경계조건	7
2.3 CA의 전이행렬과 특성다항식	9
3. Nongroup셀룰라 오토마타	14
3.1 선형 Nongroup CA	14
3.2 여원 Nongroup CA	24
4. 선형 TPMACA로부터 유도된 여원 CA 상태 행동 분석	30
4.1 여원벡터가 선형 TPMACA의 0-트리의 비순환 상태인 여원 CA	30
4.2 여원벡터가 선형 TPMACA의 0-트리가 아닌 트리의 비순환 상태인 여원 CA	36
4.3 여원벡터가 선형 TPMACA의 0이 아닌 attractor인 여원 CA	47
5. 결론	51
참고 문헌	52

ANALYSIS OF THE STATE TRANSITION BEHAVIOR OF ADDITIVE NONGROUP CELLULAR AUTOMATA

Hyang-Hee Choi

Graduate School of Education
Pukyong National University

Abstract

A cellular automata(CA) is a discrete dynamic system, which consists of a uniform array of memories called cells. The states of cells in the array are updated according to a rule : the state of a cell at a given time depends only on its own state and the state of its neighbors at the previous step. Linear hybrid CA have been proposed as an alternative to linear feedback shift registers(LFSRs), in applications such as test pattern generation, pseudorandom number generation, cryptography and signature analysis. In this paper, we show some properties of linear TPMACA and investigate a detailed analysis of the behavior of complemented CA derived from a linear TPMACA.

1. 서론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 동역학계(dynamical system)를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루고, 이산적인 공간을 셀룰라 공간(cellular space)의 기본 단위인 각 셀이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템으로써 Von Neumann과 Ulam에 의해 스스로 조직화하고 재생산할 수 있는 모델로 소개되었다[15, 17]. CA는 그 후 Wolfram에 의하여 처음으로 암호학에 도입되었다[16]. 이후 Das 등에 의해서 선형대수학으로 분석이 이루어졌으며[11, 12], Chaudhuri, Nandi 등이 많은 분야에 CA를 폭넓게 활용하였다[7]. 그리고 Muzio, Kevin 등에 의해서 LFSR(Linear Feedback Shift Register)에 대응하는 CA에 대한 연구가 이루어 졌으며, 최소비용으로 최대길이를 갖는 CA를 찾는 연구가 수행되었다[4, 3, 5]. 최근에는 Imai 등에 의해서 고속 암호 알고리즘 구현에 CA가 이용되었다[13, 14].

CA는 난수성이 우수한 수열을 발생시키는 성질을 가지고 있어 혼돈과 확산의 효과가 뛰어나 암호 알고리즘 설계를 위해 최근 LFSR(Linear Feedback Shift Register)의 대안으로 제안되고 있다[10]. 또한 CA는 대수학적 성질에 따라 크게 group CA와 nongroup CA로 구분될 수 있는데, nongroup CA는 해쉬함수 생성이나 암호 알고리즘, 부울방정식의 해법, 이미지 압축 등에 응용되고 있다.

본 논문에서는 nongroup CA의 일반적 성질들을 살펴보고 특별히 임의의 상태에 대한 직전자 수가 두 개인 선형 TPMACA로부터 얻어지는 여원 CA의 상태들의 행동을 분석한다. 본 논문의 구성을 살펴보면 먼저 2장에서는 CA의 정의와 분류 등 CA의 전반적인 이론에 대해 살펴보고, 3

장은 nongroup CA를 선형 nongroup CA와 여원 nongroup CA로 나누어 그 성질들을 분석한다. 그리고 4장에서는 선형 TPMACA로부터 유도된 여원 CA의 상태들의 행동을 분석하고 5장에서 결론을 맺는다.

2. 셀룰라 오토마타

2.1 CA의 정의 및 분류

2.1.1. CA의 정의와 기호

CA란 동역학계를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루는 시스템이며 셀룰라 공간의 기본 단위는 하나의 셀이다. 각 셀이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다.

가장 간단한 구조를 가지는 1차원 CA(One-Dimensional CA, 이하 1-D CA)에서는 모든 셀들이 선형으로 배열되어 있고 1-D CA 중에서 국소적 상호작용이 세 개의 셀, 즉 자신과 인접한 두 셀에 의해 이루어지는 CA를 3-이웃 (3-neighbourhood) CA라 한다. 본 논문에서 다루는 CA는 3-이웃 CA에 국한시킨다. CA를 설명하기 위해서 다음의 기호들이 사용된다.

<Notation>

- i : 일차원으로 배열되어 있는 각 셀들의 위치
- t : 시간 단계
- $q_i(t)$: 시간 t 에서 i 번째 셀의 상태
- $q_i(t+1)$: 시간 $t+1$ 에서 i 번째 셀의 상태

2.1.2. CA의 rule

세 개의 이웃을 가지는 CA 에 대한 다음상태 전이함수(transition function)는 다음과 같이 나타낸다

$$q_i^{t+1} = f[q_{i-1}^t, q_i^t, q_{i+1}^t] \quad (2.1)$$

여기서 f 는 결합논리를 가지는 국소 전이함수이다. f 는 3개의 변수를 가지는 Boolean 함수이므로 2^{2^3} , 즉 256개의 다음 상태 전이함수들이 있으며 이것을 CA의 rule 이라고 한다.

CA의 셀들의 상태를 0 과 1 의 두 가지 값으로 다루고 주어진 CA의 다음상태 전이함수를 아래와 같이 표현한다.

이웃상태	111	110	101	100	011	010	001	000	rule
다음상태	0	0	1	1	1	1	0	0	rule 60
다음상태	1	0	0	1	0	1	1	0	rule 150

여기서 첫 행은 시간 t 에서 인접한 세 개의 셀들의 가능한 8가지 상태의 배열이고 다음 행들은 시간 $t+1$ 에서 i 번째 셀의 갱신된 상태이다.

이진법의 수 111100₍₂₎ 십진법의 수로 변환하면 $1 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 = 60$ 이므로 rule 60 이라 하고 같은 방법으로 이진법의 수 10010110₍₂₎ 십진법의 수로 변환하면 150 이므로 rule 150 이라 한다.

위의 rule에 대한 결합 논리는 다음 식으로 표현할 수 있고 $\oplus$ 는 XOR 논리를 나타낸다.

$$\text{rule 60 : } q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \quad (2.2)$$

$$\text{rule 150 : } q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t) \quad (2.3)$$

2.1.3. CA 의 분류

(1) 셀의 배열상태에 따라

- ① 1차원 CA : 셀이 선형으로 배열되어 있는 CA
- ② 2차원 CA : 셀이 평면으로 배열되어 있는 CA
- ③ 3차원 CA : 공간으로 배열되어 있는 CA

(2) 적용되는 rule 에 따라

① 가산 CA (Additive CA)

가. 선형 CA (Linear CA) : 모든 셀들의 rule이 XOR 논리로만 이루어진 CA

나. 여원 CA (Complemented CA) : 셀들의 rule 이 XNOR 과 XOR 논리로 이루어진 CA

② 비 가산 CA (Nonadditive CA) : 셀들의 rule이 AND-OR논리로 이루어진 CA

< 표2.1 >는 Additive CA에 이용되는 rule이다.

Linear rule	Complemented rule
rule $q_i(t+1) = q_{i-1}(t) \oplus q_i(t)$ 60	rule $q_i(t+1) = \overline{q_{i-1}(t) \oplus q_i(t)}$ 195
rule $q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$ 90	rule $q_i(t+1) = \overline{q_{i-1}(t) \oplus q_{i+1}(t)}$ 165
rule $q_i(t+1) = q_i(t) \oplus q_{i+1}(t)$ 102	rule $q_i(t+1) = \overline{q_i(t) \oplus q_{i+1}(t)}$ 153
rule $q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$ 150	rule $q_i(t+1) = \overline{q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)}$ 105
rule $q_i(t+1) = q_{i+1}(t)$ 170	rule $q_i(t+1) = \overline{q_{i+1}(t)}$ 85
rule $q_i(t+1) = q_i(t)$ 204	rule $q_i(t+1) = \overline{q_i(t)}$ 51
rule $q_i(t+1) = q_{i-1}(t)$ 240	rule $q_i(t+1) = \overline{q_{i-1}(t)}$ 15

< 표2.1 > Additive CA rule

(3) 모두 같은 rule이 적용되는 rule의 개수에 따라

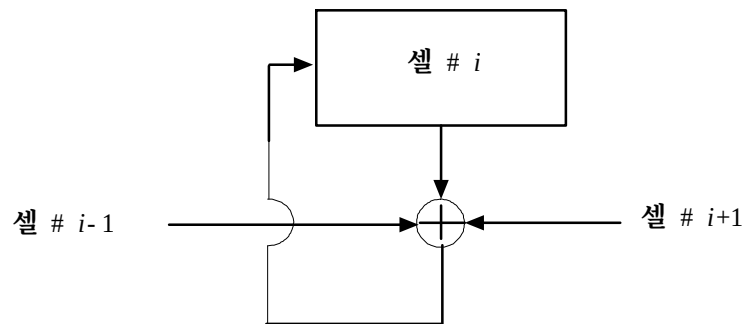
- ① Uniform CA : 모든 CA의 셀들이 같은 rule을 따르는 CA
- ② Hybrid CA : 2가지 이상의 서로 다른 rule이 적용된 CA

(4) 상태전이 그래프의 형태에 따라

- ① Group CA : 모든 셀들의 상태가 몇 개의 사이클을 이루며 반복되는 CA
- ② Nongroup CA : Group CA 가 아닌 CA

Group CA는 모든 셀들의 상태가 몇 개의 사이클을 이루며 반복되는 CA로 임의의 한 상태에 대한 이전상태가 유일하다. 이와 달리 Nongroup CA는 상태전이 그래프가 트리 구조를 이루고 있으며 상태전이 함수에 의해 얻어질 수 있는 상태인 도달 가능한 상태와 상태전이 함수에 의해 나타날 수 없는 도달 불가능한 상태로 나뉘어진다. Nongroup CA는 임의의 한 상태에 대한 이전상태가 존재하지 않거나 2개 이상이다.

< 그림 2.1 > 은 3- 이웃 선형 CA의 셀의 구조이다.

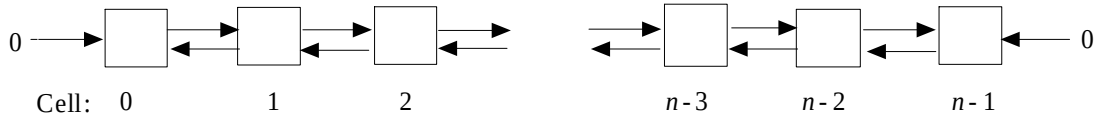


<그림 2.1> 3-이웃 선형 CA의 셀구조

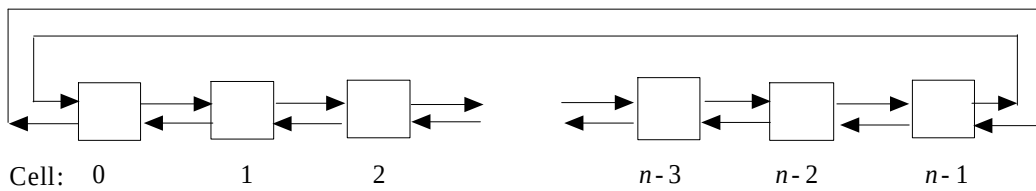
2.2. CA의 경계조건

CA에서 가장 왼쪽과 오른쪽의 셀은 2개의 이웃만을 가지므로 세 번째 이웃의 상태를 결정해 주어야 한다. 이것을 CA의 경계조건이라 하고 일반적으로 다음 세 가지의 경계조건이 있다. 제일 왼쪽과 오른쪽의 셀 들이 0 상태에 연결되어 있는 NBCA(Null Boundary CA), 양끝의 셀 들이 서로 연결되어 있는 PBCA(Periodic Boundary CA), 가장 왼쪽(오른쪽) 셀 의 다음 상태가 그 자신과

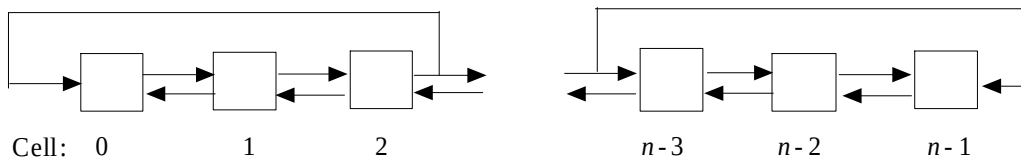
그것의 오른쪽(왼쪽) 이웃, 두 번째 오른쪽(왼쪽) 이웃 셀의 상태에 의존하는 IBCA(Intermediate Boundary CA) 이다. < 그림2.2 >은 각각의 경계조건을 나타낸 것이다. 본 논문에서는 NBCA 만 다룬다.



(1) Null Boundary CA



(2) Periodic Boundary CA



(3) Intermediate Boundary CA

<그림 2.2> 서로 다른 경계조건을 가지는 CA

2.3. CA의 전이행렬과 특성다항식

2.3.1. CA의 전이행렬

n 개의 셀을 가지는 선형 1-D CA에서는 현재 상태를 다음 상태로 전이시키는 전이함수를 $n \times n$ 행렬로 나타낼 수 있으며, 이것을 전이행렬(transition matrix)이라 한다. 전이행렬 T 에서 i 번째 행은 i 번째 셀에 적용되는 rule이며 그 셀의 다음 상태가 현재상태에 의존하면 1, 그렇지 않으면 0으로 쓴다. 3-이웃 CA의 전이행렬은 정방행렬의 주 대각선과 그 윗 대각선과 아래 대각선을 제외한 나머지가 0인 삼대각선 행렬(tridiagonal matrix)이다. 예를 들어 네 개의 셀을 가진 NBICA의 rule이 $\langle 60, 150, 102, 90 \rangle$ 이면 전이행렬은 다음과 같다.

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (2.4)$$

S_t 가 시간 t 에서 CA의 상태를 나타내면 시간 $t+1$ 에서 CA의 상태는 다음 식으로 표현된다.

$$S_{t+1} = T S_t \quad (2.5)$$

또한 시간 t 에서 CA의 상태는 다음과 같다.

$$S_{t+2} = T S_{t+1} = T(T S_t) = T^2 S_t \quad (2.6)$$

같은 방법으로 p 단계 후의 CA 의 상태는

$$S_{t+p} = T^p S_t \quad (2.7)$$

예를 들어 CA의 현재 상태가 $S_t = [1\ 0\ 1\ 0]^t$ 이면 다음 상태는 다음과 같이 구해진다.

$$S_{t+1} = T S_t = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

만약 CA의 전이행렬 T 가 정칙행렬 즉 $\det(T) = 1$ 이면 이 CA는 group CA이다.

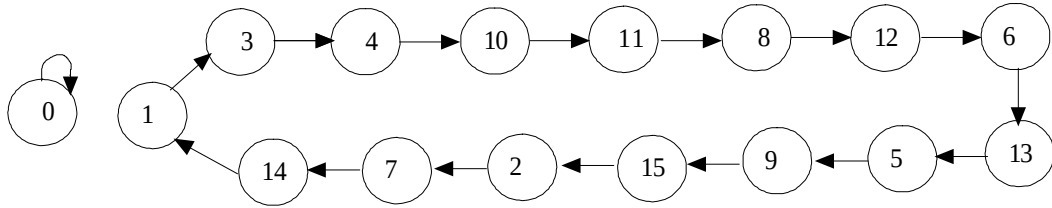
Group CA는 모든 상태들이 일정한 사이클을 이루며 T 에 의해 상태가 반복되는 것으로 임의의 상태에 대하여 유일한 이전상태를 가진다. 따라서 전이행렬의 역행렬을 구하여 현재 상태에 적용하면 이전상태를 명확하게 얻을 수 있다. 즉,

$$S_{t-1} = T^{-1} S_t \quad (2.8)$$

이다. Group CA는 최대 길이를 갖는 CA와 최대 길이를 갖지 않는 CA로 구별할 수 있다. n 개의 셀로 이루어진 CA에서 모든 셀의 상태가 0인 경우를 제외한

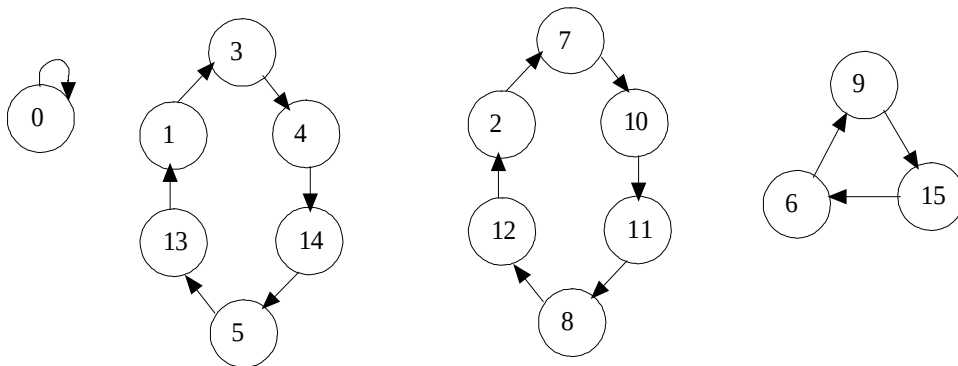
$2^n - 1$ 개의 상태가 하나의 주기 안에 있을 때 최대 길이를 가진다고 한다. 최대 길이를 갖는 CA의 특성 다항식은 primitive이다. n 차 primitive polynomial $C(x)$ 는 인수분해 되지 않고 $x^m + 1$ 을 나누는 m 의 최소값이 $2^n - 1$ 인 다항식이다.

< 그림 2.3 >은 rule이 < 150, 90, 150, 150 >인 4개의 셀로 구성된 최대길이를 가지는 선형 CA이다.



<그림 2.3> 최대 길이를 갖는 Group CA

< 그림 2.4 >은 최대길이를 가지지 않는 선형 CA로써 rule <150, 150, 150, 150 >을 갖는 uniform CA이다. 그림에서 알 수 있듯이 0을 제외한 다른 상태들이 몇 개의 서로 다른 사이클로 분리되어 있다. 각 사이클 길이의 최소공배수 6 이 CA의 주기가 된다.



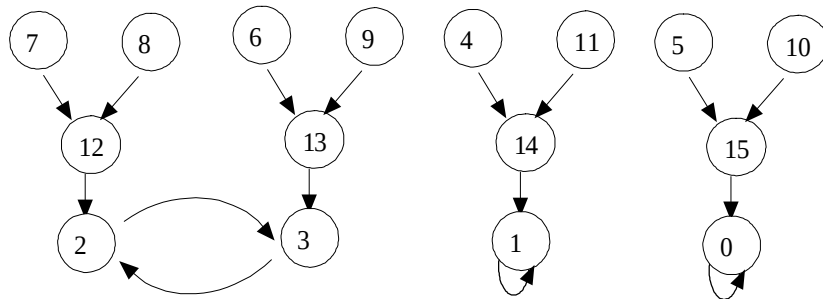
<그림 2.4> 최대 길이를 갖지 않는 Group CA

이와달리 group CA가 아닌 CA를 Nongroup CA라고 하는데 이 CA의 $\det(T) = 0$ 이다. 따라서 전이행렬 T에 대한 역행렬이 존재하지 않으므로 임의의 상태에 대하여 명확하게 알 수 없다.

< 그림2.5 > 는 rule < 102, 60, 60, 150 > Nongroup CA의 상태전이 그래프이다.

이 CA의 전이행렬은 $T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ 이고 상태전이 그래프는 트리 구조를

가진다.



<그림 2.5> Nongroup CA

2.3.2. CA의 특성 다항식

<정의 2.1> 특성다항식(characteristic polynomial) : 주어진 CA의 전이행렬 T 에 대하여 특성다항식은 $GF(2)$ 상에서 $(T + xI)$ 의 행렬식 값이다.

<정의 2.2> 최소다항식 (minimal polynomial) : 특성다항식의 인수 중 T 를 근으로 갖는 차수가 가장 낮은 다항식을 최소다항식 이라 한다.

CA의 전이행렬이 T 일 때, T 의 특성다항식 $C(x)$ 은 다음과 같다. 여기서 I 는 n 차 단위행렬이다.

$$C(x) = |T + xI| \quad (2.9)$$

예를 들어 행렬 (2.4)에 대한 특성다항식을 구해보면

$$\begin{aligned} |T + xI| &= \begin{vmatrix} 1+x & 0 & 0 & 0 \\ 1 & 1+x & 1 & 0 \\ 0 & 0 & 1+x & 1 \\ 0 & 0 & 1 & x \end{vmatrix} \\ &= (1+x) \begin{vmatrix} 1+x & 1 & 0 \\ 0 & 1+x & 1 \\ 0 & 1 & x \end{vmatrix} \\ &= x^4 + x^3 + x \\ &= x(x^3 + x^2 + 1) \end{aligned} \quad (2.10)$$

<그림 2.3>의 전이행렬은

$$T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad (2.11)$$

이고, 특성다항식은 $x^4 + x^3 + 1$ 로 primitive polynomial이다.

3. Nongroup 셀룰라 오토마타

Nongroup CA가 이미지 압축, 해쉬 함수, 부울 방정식의 해법, 암호 알고리즘 등에 응용[1, 2]이 되면서 최근 연구가 활발히 이루어지고 있다. 본 장에서는 nongroup CA의 정의와 자주 사용되는 용어들을 정의하고 nongroup CA의 성질에 대하여 살펴본다.

3.1 선형 Nongroup CA

선형 nongroup CA는 다음 상태를 결정짓는 상태전이 함수가 XOR 논리로만 이루어진 CA로 group CA가 아닌 CA이다. 즉, 사용되는 rule이 60, 90, 102, 150, 170, 204, 240 이고 상태전이 그래프가 트리 구조를 가지는 CA로 $\det(T)=0$ 으로 역 행렬이 존재하지 않는다. 그러므로 임의의 상태에 대한 이전상태 수는 0 이거나 2 이상이다. 어떤 상태의 이전상태 수가 0 이란 의미는 이전상태가 존재하지 않는다는 것으로 주어진 상태는 도달 불가능한 상태이다. 이와 달리 이전상태수가 2 이상이란 의미는 주어진 상태가 도달 가능한 상태이며, 2개 이상의 이전 상태가 존재한다는 것을 말한다. 이처럼 nongroup CA는 상태전이 함수가 일대일 대응 함수가 아니다. 그러므로 주어진 상태에 대하여 이전상태를 구하는 것이 불가능하다. 다음은 선형 nongroup CA와 이 논문의 전개에 필요한 몇 가지 용어들을 정의한다.

<정의 3.1> 선형 Nongroup CA : Nongroup CA 중 다음 상태를 결정짓는 상태전이 함수가 XOR 논리 이루어진 CA를 말한다.

<정의 3.2> 순환상태(cyclic state) : Nongroup CA의 상태 사이클(cyclic) 안에 존재하는 상태로 일정한 시간 단계 후 그 상태가 반복되는 상태로, 상태 y 가 순환상태이면 $T^k y = y$ 를 만족하는 k 가 존재한다. 여기서 k 의 최소값이 상태 y 가 놓이는 사이클의 길이 이다.

<정의 3.3> attractor : 순환상태들 중 사이클의 길이가 1인 상태로 어떤 상태 x 가 attractor이면 전이행렬 T 에 대하여 $Tx=x$ 를 만족한다

<정의 3.4> r -직전자(r -predecessor) : $T^r Y=X$ 을 만족하는 상태 Y 를 상태 X 의 r -직전자라 부른다($1 \leq r \leq 2^n - 1$). 특히 1-직전자를 간단히 직전자라 부른다.

<정의 3.5> MACA (Multiple- Attractor CA) : Nongroup CA의 모든 순환 상태들이 attractor인 CA를 MACA라 부른다. 특히 직전자 수가 2인 MACA를 TPMACA (Two Predecessor Multiple-Attractor CA)라 부른다. Attractor의 수가 1인 MACA를 SACA (Single-Attractor CA)라 부르며 특히 직전자의 수가 2인 SACA를 TPSACA라 부른다.

<정의 3.6> α -트리 : 순환상태 α 를 root로 하는 트리

<정의 3.7> depth : Nongroup CA의 상태전이 그래프에서 임의의 도달 불가능한 상태에서 가장 가까운 순환상태로 전이되는데 걸리는 최소 상태 전이 수

<정의 3.8> level : 어떤 상태 x 가 α -트리의 level l ($l \leq \text{depth}$)에 있다는 것은 상태 x 가 정확히 l 번 상태 전이후 상태 α 가 되는 위치에 있다는 것이다.

즉 $T^p x = \alpha$ 가 되는 p 값 중 최소값이 l 이다.

<정의 3.9> 주기 : 상태전이 그래프에서 나타나는 사이클의 길이의 최소공배수로 임의의 순환상태 y 에 대하여 $T^c y = y$ 인 최소의 c 가 주기가 된다.

<그림 2.5>에서 순환상태는 0, 1, 2, 3 이다. 특히 상태 0과 1은 사이클의 길이가 1 이므로 attractor 이다. 상태 2, 3 은 사이클의 길이가 2 인 사이클에 존재한다. 그러므로 이 CA의 주기는 1과 2의 최소공배수인 2 이다. 각 트리는 depth 는 2 이다. 2-트리는 상태 2를 root로 하는 트리 이므로 상태 7, 8, 12, 2가 2-트리에 속한다. 각 트리의 level 1의 상태는 12, 13, 14, 15 이고 level 2 에 있는 상태들은 4, 5, 6, 7, 8, 9, 10, 11 이다. 다음은 5-cell TPMACA의 예이다.

<예 3.1> 5개의 셀로 이루어진 CA가 rule <60, 240, 240, 240, 240>을 가질 때, 전이행렬은

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (3.1)$$

이고, 특성다항식은 $x^4 (x+1)$ 이며 최소다항식도 $x^4 (x+1)$ 이다. 주어진 T 의 계수 (rank)는 4 이다. <그림 3.1>은 <예 3.1>에서 주어진 CA에 대한 상태전이 그래프로 2개의 독립된 트리로 구성되는 TPMACA이다.

3.1.2. 선형 Nongroup CA의 성질

가. 0-트리

본 절에서는 선형 nongroup CA의 행동을 분석하는데 가장 기본적인 0-트리의 성질들을 살펴본다. 선형 nongroup CA에서 0-트리와 다른 순환상태를 root로 하는 트리는 매우 밀접한 관계를 가지고 있으므로 0-트리에 관한 연구는 필수적이며 매우 중요하다. 다음의 몇 가지 정리들은 선형 nongroup CA의 기본적인 것이며 다음에서 제시할 0-트리와 α -트리 사이의 관계를 밝히는데 있어 중요한 사실이다.

<정리 3.1> 선형 nongroup CA에서 상태 0은 attractor이다.

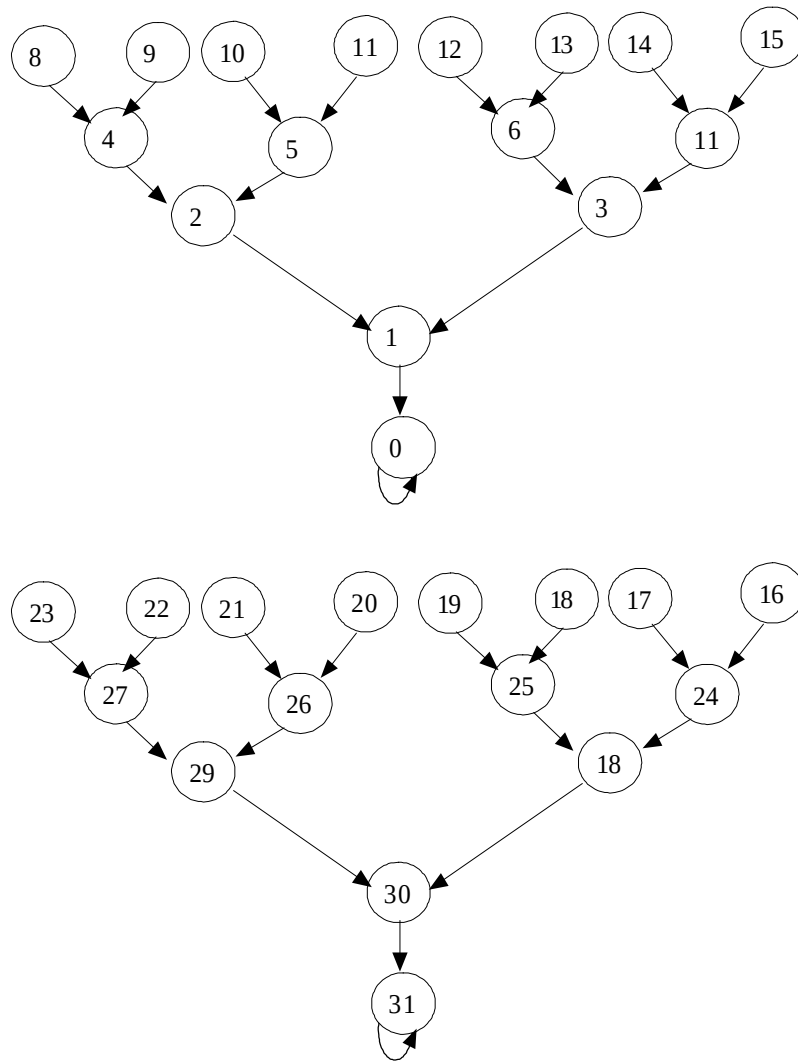
<증명> 임의의 전이행렬 T 에 대하여 $T0=0$ 이다. □

<보조정리 3.2> 선형 nongroup CA의 전이행렬 T 의 영공간 (null space)의 차원이 d 이면 상태 0의 직전자의 수는 2^d 이다.

<증명> 상태 0의 직전자 x 는 $Tx=0$ 을 만족한다. T 의 영공간의 차원이 d 이면 이 일차연립방정식은 자유변수가 d 개 존재한다. 자유변수가 가질 수 있는 값이 $GF(2)$ 에서 0 또는 1이므로 직전자의 수는 2^d 이다. □

<정리 3.3> 선형 nongroup CA에서 도달 가능한 상태의 직전자의 수는 상태 0의 직전자의 수와 같다.

<증명> 임의의 도달 가능한 상태를 α 라 하면 α 의 직전자 y 는 $Ty=\alpha$ 를 만족한다. α 가 도달 가능한 상태이므로 $\{y \mid Ty=\alpha\}$ 는 공집합이 아니다. 그러므로 $|\{y \mid Ty=\alpha\}| = |\{x \mid Tx=0\}|$ 이다. □



<그림 3.1> 5-cell TPMACA

나. 선형 nongroup CA에서 순환상태들의 트리와 0-트리와의 관계

선형 nongroup CA의 상태전이 그래프에서 α -트리의 구조는 0-트리와 동형이다. 그러므로 α -트리와 0-트리 사이의 관련성을 밝히는 것은 선형 nongroup CA의 행동을 분석하는데 있어 매우 중요한 문제이다. 이 절에서는 1차원 선형 nongroup CA의 0-트리와 $\alpha (\neq 0)$ -트리의 상태들간의 관계들을 밝힘으로 서로 대응되는 상태들을 찾을 수 있고, 선형 nongroup CA를 보다 효율적으로 분석할 수 있음을 보인다. 다음 정리에서 0-트리의 상태의 수를 알 수 있다.

<정리 3.4> 선형 nongroup CA의 상태전이 그래프에서 0-트리의 depth를 d 라고 하고 주어진 전이행렬 T 의 영공간의 차원이 r 이면 0-트리의 상태는 2^{rd} 이다.

<증명> 전이행렬 T 의 영공간의 차원이 r 이므로 <보조정리 3.2>와 <정리 3.3>에 의해 임의의 도달가능한 상태의 직전자의 수는 2^r 개다. α_i 를 0-트리의 level i 에 있는 상태들의 수라 하면 $\alpha_{i+1} = 2^r \alpha_i$ 이다. 따라서 0-트리의 level i 에 있는 상태들의 수는 $(2^r)^{i-1} (2^r - 1)$ 이다. 그러므로 0-트리에 속해있는 상태들의 수는 다음과 같다.

$$\begin{aligned} & 1 + (2^r - 1) + 2^r (2^r - 1) + \dots + (2^r)^{d-1} (2^r - 1) \\ &= 1 + \frac{(2^r - 1) \{ (2^r)^d - 1 \}}{2^r - 1} \\ &= 1 + (2^{rd} - 1) = 2^{rd} \end{aligned}$$

□

<보조정리 3.5> 도달 가능한 상태의 직전자의 수가 r 인 선형 Nongroup CA에서 상태 0의 i -직전자를 $P_1, P_2, P_3, \dots, P_{r^i}$ 라 하고, 도달 가능한 0이 아닌 임의의 상태 X 의 i -직전자중 하나를 X_1 이라 하면 X 의 i -직전자 집합은 다음과 같다.

$$\{X_1 \oplus P_j \mid j = 1, 2, 3, \dots, r^i\} \quad (\text{단, } \oplus \text{는 bitwise 덧셈연산})$$

<증명> 우선 B_i 를 상태 0의 i -직전자의 집합이라 하면 집합 B_i 는 다음과 같다. $B_i = \{Y \mid T^i Y = 0\} = \{P_1, P_2, \dots, P_{r^i}\}$ 여기서 $P_1 = 0$ 이다. 그리고 상태 X 의 i -직전자의 집합을 Q_i 라 하면 $Q_i = \{Y \mid T^i Y = X\}$ 이다. 상태 X_1 이 X 의 i -직전자 이므로 $X_1 \in Q_i$ 이다. $Q_i \neq \emptyset$ 이므로 $|Q_i| = |B_i| = r^i$ 이다. 한편

$$T^i(X_1 \oplus P_j) = T^i X_1 \oplus T^i P_j = T^i X_1 \oplus 0 = X \text{ 이므로}$$

$X_1 \oplus P_j, (j = 1, 2, \dots, r^i)$ 가 X 의 i -직전자 이다. 그러므로 X 의 i -직전자의 집합 Q_i 는 $\{X_1 \oplus P_j \mid j = 1, 2, 3, \dots, r^i\}$ 이다. □

<정리 3.6 [8]> 상태 0의 직전자 수가 r 일 때, P_{ij} 를 0-트리의 level i 의 j 번째 상태라 하고, R_i 를 상태 X 의 순환하는 i -직전자라 하자. 그리고 X_{ij} 를 X -트리의 level i 의 j 번째 상태라 하면 X_{ij} 는 다음을 만족한다.

$$X_{ij} = R_i \oplus P_{ij} \quad (3.2)$$

(단, $\oplus$ 는 bitwise 덧셈연산, $1 \leq i \leq \text{depth}, j = 1, \dots, (r-1)r^{i-1}$)

<증명> 위 식(3.2)을 수학적 귀납법으로 증명한다.

i) $i = 1$ 일 때 <보조정리 3.5> 에서 i 가 1인 경우이므로 성립.

ii) $i = k$ 일 때 $|\{X_{kj}\}| = |\{R_k \oplus P_{kj}\}|$ 이고 $X_{kj} = R_k \oplus P_{kj}$ 라면

(여기서 $j = 1, 2, \dots, (r-1)r^{i-1}$)

iii) $i = k+1$ 일 때

$$T(X_{k+1j} \oplus R_{k+1}) = X_{kj} \oplus R_k = P_{kj}$$

이는 $X_{k+1j} \oplus R_{k+1}$ 이 P_{kj} 의 직전 자중 하나인 P_{k+1j} 임을 의미하므로

따라서 $X_{k+1j} \oplus R_{k+1j} = P_{k+1j}$ 이고 $X_{k+1j} = R_{k+1j} \oplus P_{k+1j}$ 이다. 그러

므로 식 (3.2)은 $k = i+1$ 인 경우에도 성립한다. $\square$

위의 정리로부터 다음과 같은 따름 정리를 얻는다.

<따름정리 3.7> 상태 X 가 attractor이면 $X_{ij} = X \oplus P_{ij}$ 이다.

<증명> 상태 X 가 attractor이므로 X 의 순환하는 i - 직전자는 $R_i = X$ 이다. $\square$

<정리 3.8> X_l, X_m 이 X -트리의 level i 의 상태이고 j 번 단계 후 비로소 두 상태가 같은 상태가 될 때 즉, $T^k X_l = T^k X_m$ 인 최소의 k 값이 j ($\leq i$) 일 때 $X_l \oplus X_m$ 는 0-트리의 level j 상태중 하나이다.

<증명> $T^j X_l = T^j X_m$ 이므로 $T^j(X_l \oplus X_m) = 0$ 이다. 이는 $X_l \oplus X_m$ 가 상태 0의 j -직전자임을 의미한다. $X_l \oplus X_m$ 가 0-트리의 level p ($< j$)의 상태라

면 $T^p(X_l \oplus X_m) = 0$ 이고 $T^p X_l = T^p X_m$ 이 되어 가정에 모순이 된다. 그러므로 $X_l \oplus X_m$ 는 0-트리의 level j 상태중 하나이다. $\square$

위의 정리로부터 다음 따름정리를 얻는다.

<따름정리 3.9> 임의의 도달 가능한 상태의 서로 다른 직전자의 합은 상태 0의 0 이 아닌 직전자 이다.

선형 nongroup CA의 전이행렬의 최소다항식은 $m(x) = x^d \Phi(x)$ 로 표현된다. 여기서 d 는 CA의 depth가 되고 $\Phi(x)$ 가 $x^c + 1$ 를 나누는 c 중 최소의 c 가 주기가 된다. <그림 2.5> 선형 nongroup CA의 최소다항식은 $x^4 + x^3 + x^2 = x^2(x^2 + x + 1)$ 이다. 그러므로 depth는 2이고 $\Phi(x) = x^2 + x + 1$ 이다. $\Phi(x)$ 가 나누는 $x^c + 1$ 중 가장 낮은 차수의 다항식은 $x^3 + 1$ 이다. 그러므로 이 CA의 주기는 3 이다.

다. 선형 TPMACA 의 분석

선형 TPMACA 는 선형 nongroup CA 중 모든 순환상태들이 attractor 이고 임의의 도달가능한 상태에 대하여 직전자의 수가 2개인 CA를 말한다. 이 선형 TPMACA는 해쉬함수를 만드는데 효과적이다. 다음은 TPMACA의 성질들을 살펴본다.

<정리 3.10> n셀 선형 TPMACA의 전이행렬 T의 영공간의 차원은 1 이다.

<증명> TPMACA의 임의의 도달 가능한 상태에 대한 직전자 수는 2 개다.

α 를 임의의 도달 가능한 상태라고 하면 $|\{y \mid Ty = \alpha\}| = 2$ 이고 <정리 3.3>에

의하여 $|\{y \mid Ty = \alpha\}| = |\{x \mid Tx = 0\}|$ 이므로 $Tx=0$ 인 x 의 수가 2^1 이다. 그러므로 자유변수 개수가 1 이므로 T 의 영공간의 차원은 1 이다. $\square$

<예 3.1>에서 최소다항식은 $x^4(x+1)$ 이므로 depth는 4이고 $x+1$ 은 x^1+1 을 나누므로 주기가 1인 MACA이다. 그러므로 선형 TPMACA의 최소다항식은 $x^d(x+1)$ 이 된다.

<정리 3.11> n 셀 선형 TPMACA의 $(T \oplus I)$ 의 계수가 k 이면 attractor의 수는 2^{n-k} 이다.

<증명> 어떤 상태 x 가 attractor 이면 사이클의 길이가 1 이므로 $Tx = x$ 이다. 이는 $(T \oplus I)x = 0$ 이므로 attractor는 $(T \oplus I)x = 0$ 을 만족하는 해 x 이다. 그러므로 attractor의 수는 $(T \oplus I)$ 의 계수가 k 이므로 영공간의 차원은 $n-k$ 이므로 가능한 해의 수는 2^{n-k} 이다. $\square$

<정리 3.12[8]> C 를 TPMACA라 하자. α_{ij} 를 C 에서 α -트리의 level i 의 j 번째 상태라 하고 β_{ij} 를 C 에서 β -트리의 level i 의 j 번째 상태라 하면 다음을 만족한다.

$$\alpha_{ij} \oplus \beta_{ij} = \alpha \oplus \beta$$

<증명> P_{ij} 를 0-트리의 level i 의 j 번째 상태라 하면 <따름정리 3.7>에 의하여 $\alpha_{ij} = P_{ij} \oplus \alpha$ 이고, $\beta_{ij} = P_{ij} \oplus \beta$ 이다.

그러므로 $\alpha_{ij} \oplus \beta_{ij} = P_{ij} \oplus \alpha \oplus P_{ij} \oplus \beta = \alpha \oplus \beta$ $\square$

<정리 3.13> 선형 TPMACA에서 w 와 u 를 임의의 한 도달 가능한 상태의 서로 다른 직전자라 하고 P_1 을 상태 0의 0이 아닌 직전자라고 하면 $w \oplus u = P_1$ 이다.

<증명> 가정에 의하여 $Tw = Tu$ 이고 $T(w \oplus u) = 0$ 이다. 또한 w 와 u 는 서로 다른 상태이므로 $w \oplus u \neq 0$ 이다. 그러므로 $w \oplus u$ 는 상태 0의 0이 아닌 직전자 P_1 이다. $\square$

3.2. 여원 Nongroup CA

3.2.1. 여원 CA의 정의 및 일반적 성질

이 절에서는 여원 CA의 정의와 상태들의 전이 행동에 관한 분석을 그에 대응하는 선형 CA와 관련지어 살펴본다.

<정의 3.10> 각 셀에 적용되는 rule이 XOR 논리와 XNOR 논리의 조합으로 표현되는 CA를 여원 CA라 한다.

여원 CA는 XNOR논리가 상태 전이 함수로 사용된 것으로 rule 195, 165, 153, 105, 85, 51, 15가 여원 rule이다. rule 165는 <표2.1>에서와 같이 $q_i(t+1) = \overline{q_{i-1}(t) \oplus q_{i+1}(t)}$ 로 표현한다. 이것은 rule 60인 $q_i(t+1) = q_{i-1}(t) \oplus q_i(t)$ 의 결과값을 역으로 취하는 것으로 한 셀에 적용되는 여원 CA의 상태 전이 함수는 다음과 같다.

$$\overline{q_i^{t+1}} = f[q_{i-1}^t, q_i^t] \oplus 1 \quad (3.2)$$

여원 CA의 다음 상태를 구하는 연산자를 $\overline{T}$ 라 하면 이를 선형 CA와 관련지어 다음 상태를 구하는 식으로 유도할 수 있다. 여원 rule에 대응하는 선형 rule로 표현한 전이 행렬을 T 라 하고 식(3.2)와 같이 결과 값을 역으로 바꾸어야 하는 셀을 나타내는 위치가 1 이고 나머지는 0인 n 차원 벡터 F 를 여원 벡터라고 할 때 현재 CA의 상태를 S_t 라고 하면 CA의 다음 상태 S_{t+1} 은 다음과 같다.

$$S_{t+1} = \overline{T} S_t = T S_t \oplus F \quad (3.3)$$

<예 3.2> 앞의 <예 3.1>에서 선형 TPMACA에서 4번째 셀을 제외한 나머지 셀의 결과를 역으로 바꾼다면 이 CA에 사용되는 rule은 <153, 165, 195, 240, 153>이다. 여원벡터 F 는 4번째 위치만 0 이고 나머지는 모두 1 인 벡터로 $(1, 1, 1, 0, 1)^T$ 이다. CA의 현재 상태가 $(0, 1, 0, 1, 0)^T$ 라고 하면 다음 상태는 아래와 같이 구할 수 있다

$$\begin{aligned} S_{t+1} = \overline{T} S_t = T S_t \oplus F &= \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ &= 9 \end{aligned}$$

<정리 3.14> $\overline{T}^p$ 를 여원 CA의 연산자인 $\overline{T}$ 을 p 번 적용한 것이라 하면 현재 상태에서부터 p 시간 단계 후의 여원 CA의 상태 S_{t+p} 는 다음과 같다.

$$S_{t+p} = \overline{T}^p S_t = T^p S_t \oplus (I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1})F \quad (3.4)$$

<증명> 수학적 귀납법에 의해서

i) $n=1$ 일 때 식(3.3)에 의해서

$$S_{t+1} = \overline{T} S_t = T S_t \oplus F \text{ 이므로 자명하다.}$$

ii) $n=p-1$ 일 때

$S_{t+p-1} = T^{p-1} S_t \oplus (I \oplus T \oplus \cdots \oplus T^{p-2})F$ 가 성립한다고 가정하면

iii) $n=p$ 일 때

$$\begin{aligned} S_{t+p} &= \overline{T} S_{t+p-1} = T S_{t+p-1} \oplus F \\ &= T \{ T^{p-1} S_t \oplus (I \oplus T \oplus \cdots \oplus T^{p-2})F \} \oplus F \\ &= T^p S_t \oplus (T \oplus T^2 \oplus \cdots \oplus T^{p-1})F \oplus F \\ &= T^p S_t \oplus (I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1})F \quad \square \end{aligned}$$

여원 CA에서 여원 벡터 F 는 CA의 크기와 같은 n 차원 벡터이다. 그러므로 이 벡터의 종류는 모든 성분이 0인 0 벡터를 제외한 $2^n - 1$ 가지를 만들 수 있고 이것은 CA의 가능한 상태와 일대일 대응시킬 수 있다. 따라서 이 여원 벡터를 CA의 상태로 해석한다면 이 벡터가 동일한 전이행렬 T 를 따르는 선형 nongroup CA의 상태전이 그래프에 놓이는 위치에 따라 여러 가지 행동패턴을 보인다. 이렇게 같은 전이 행렬을 가지는 선형 CA를 여원 CA에 대응하는 CA라고 하고, 여원 CA는 선형 CA로부터 유도된 여원 CA라 한다. 본 논문은 선형 TPMACA와 같은 전이행렬을 가지는 여원 CA에 대하여 연구한다.

<정리 3.15> 여원 CA의 C' 의 한 상태 x' 가 도달 가능한 상태일 필요충분조건은 이 상태에 대응하는 선형 CA C 의 상태 $x = x' \oplus F$ 가 도달 가능한 상태이다.

<증명>

i) ($\Rightarrow$) x' 가 C' 에서 도달 가능한 상태이므로 x' 에 대한 직전자 y 가 존재한다. 즉,

$$x' = Ty \oplus F \quad (3.5)$$

따라서

$$\begin{aligned} x = x' \oplus F &= (Ty \oplus F) \oplus F \quad \text{「식(3.5)에 의하여」} \\ &= Ty \end{aligned}$$

그러므로 x 는 C 에서 도달 가능한 상태이다.

ii) ($\Leftarrow$) 같은 방법으로 x 가 C 에서 도달 가능한 상태 이므로

$x = Ty$ 인 x 에 대한 직전자가 존재하므로

$x' = x \oplus F = Ty \oplus F$ 이다. 그러므로

x' 은 C' 에서 도달 가능한 상태이다. □

위의 정리로부터 다음 따름 정리를 얻는다.

<따름정리 3.16> 여원 CA C' 의 한 상태 x' 가 도달 불가능한 상태일 필요충분 조건은 이 상태에 대응하는 선형 CA C 의 상태 $x = x' \oplus F$ 가 도달 불가능한 상태이다.

<정리 3.17> 선형 TPMACA C 로부터 유도되는 여원 CA의 도달 가능한 상태에 대한 직전자 수는 2 이다.

<증명> x' 을 C' 에서 $y_1', y_2' \cdots y_p'$ 를 직전자로 가지는 임의의 도달 가능한 상태라 하면

$$T y_1' \oplus F = T y_2' \oplus F = \cdots = T y_p' \oplus F = x' = (x' \oplus F) \oplus F$$

$$\therefore T y_1' = T y_2' = \cdots = T y_p' = x' \oplus F = x$$

그러므로 x 는 C 에서 도달 가능한 상태이고 x 는 가정에 의해 2개의 직전자를 가지므로 $p=2$ 이다.

<정리 3.19[6]> 여원 CA의 depth는 이에 대응하는 선형 CA의 depth와 같고 임의의 도달 가능한 상태의 이전상태의 수 또한 이에 대응하는 선형 CA의 그것과 같다.

<정리 3.20> TPMACA C 에 대응하는 여원을 갖는 CA C' 의 상태전이 그래프에서 임의의 도달 가능한 상태의 서로 다른 두 직전자의 합은 C 의 상태 0의 0이 아닌 직전자 이다.

<증명> x_i 와 y_i 를 C' 의 임의의 도달 가능한 상태의 서로 다른 두 직전자라 하자.

$$\overline{T} x_i = \overline{T} y_i$$

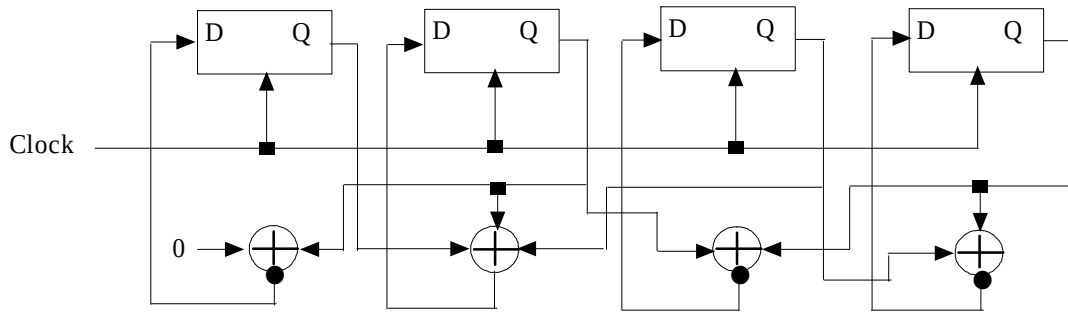
$$\Rightarrow T x_i \oplus F = T y_i \oplus F$$

$$\Rightarrow T x_i \oplus F \oplus T y_i \oplus F = 0$$

$$\Rightarrow T(x_i \oplus y_i) = 0 \text{ and } x_i \oplus y_i \neq 0 \text{ (} x_i \neq y_i \text{ 이므로)}$$

그러므로 $x_i \oplus y_i$ 는 C 의 상태 0의 0이 아닌 직전자다.

<그림 3.2>는 rule <165, 150, 165, 195>을 갖는 4개의 셀로 이루어진 여원 CA의 구조이다. 이 CA는 여원벡터가 $(1, 0, 1, 1)^T$ 이고 rule <90, 150, 90, 60>을 따르는 선형 CA로부터 유도된 여원 CA 이다.



<그림 3.2> rule 벡터가 <165, 150, 165, 195>인 여원 CA의 구조

4. 선형 TPMACA로부터 유도된 여원 CA 상태 행동 분석

이 절에서는 여원 CA 에 대응하는 선형 CA 가 TPMACA인 특별한 여원 CA 에 대하여 분석한다. 이러한 여원 CA는 여원 벡터가 그에 대응하는 선형 CA의 상태전이 그래프에서 놓이는 위치에 따라 3가지로 나눌 수 있다.

여원벡터 F 가 선형 TPMACA 의

- ① 0- 트리의 비 순환 상태
- ② 0- 트리가 아닌 다른 트리의 비 순환 상태
- ③ 0 이 아닌 attractor

인 경우이다. 이 세가지 경우에 대하여 여원 CA의 상태전이 그래프에서 나타나는 성질들을 다음 절에서 분석하고 이에 대한 예를 든다.

4.1 여원벡터가 선형 TPMACA의 0- 트리의 비순환 상태인 여원 CA

이 절에서는 선형 TPMACA로부터 유도된 여원을 갖는 CA의 행동을 분석하는데

특히 여원벡터 F 가 0- 트리에서 0이 아닌 상태인 선형 TPMACA의 여원 CA의 행동을 밝히도록 한다.

<보조정리 4.1> 선형 nongroup CA 의 전이행렬이 T 이고 그에 대응하는 여원을 갖는 CA에서 연산자 $\overline{T}$ 를 p 번 적용한 것을 $\overline{T}^p$ 라 하자. 그러면

$$\overline{T}^p F = [I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1} \oplus T^p] F$$

<증명> <정리 3.14>로부터 명백하다. □

<보조정리 4.2> C 는 depth가 d 인 TPMACA 이고, C 에서 0- 트리의 level i ($0 < i \leq d$)에 있는 상태 F 를 여원벡터라 하면 $\overline{T}^{i-1}F$ 는 C 에 대응하는 여원을 갖는 CA C' 에서 attractor 이다

<증명> F 가 0- 트리의 level i 의 상태 이므로 $T^i F = 0$ 이다.

$S = \overline{T}^{i-1}F$ 라 하자. <보조정리 4.1>에 의하여

$S = (T^{i-1} \oplus T^{i-1} \oplus T^{i-2} \oplus \cdots \oplus I)F$ 이다.

$$\begin{aligned}\overline{TS} &= TS \oplus F \\ &= T(T^{i-1} \oplus T^{i-2} \oplus \cdots \oplus I)F \oplus F \\ &= (T^i \oplus T^{i-1} \oplus \cdots \oplus I)F \\ &= T^i F \oplus (T^{i-1} \oplus \cdots \oplus I)F \\ &= 0 \oplus S \\ &= S\end{aligned}$$

따라서 S 는 C' 에서 attractor 이다. □

<정리 4.3> C 가 TPMACA 이고 C 에 대응하는 여원을 갖는 CA를 C' 이라 하고 여원벡터 F 를 C 의 트리의 level l 에 있는 비 순환 상태로 택하자. 그러면 다음이 성립한다.

- (1) C 에서 l 보다 더 큰 level에 있는 모든 상태는 C' 에서 변하지 않는다.
- (2) C 에서 l 보다 level에 있는 모든 상태는 C' 에서 l 보다 작은 level에 배열된다.
- (3) C 에서 l 보다 더 작은 level에 있는 모든 상태는 C' 에서 level l 에 배열된다.

(4) 상태 F 는 C' 에서 level $l-1$ 에 배열된다.

<증명> F 가 0- 트리의 level l 의 상태이므로 $T^l F = 0$ 이다.

(1) x 를 C 의 상태전이 그래프에서 level k ($> l$)에 있는 상태라 하자.

그러면

$$\begin{aligned}
 \overline{T}^k x &= T^k x \oplus (T^{k-1} \oplus \cdots \oplus T^l \oplus T^{l-1} \oplus \cdots \oplus T \oplus I)F \\
 &= T^k x \oplus (T^{l-1} \oplus \cdots \oplus T \oplus I)F \\
 &\quad (\text{모든 } i > l-1 \text{에 대해 } T^i F = 0 \text{이므로}) \\
 &= 0 \oplus (T^{l-1} \oplus \cdots \oplus T \oplus I)F \\
 &\quad (x \text{가 level } k (> l) \text{의 상태이므로}) \\
 &= T^{l-1} F (T^{l-2} \oplus \cdots \oplus T \oplus I)F \\
 &= \overline{T}^{l-1} F \text{ 이 성립한다.}
 \end{aligned}$$

또한 <보조정리 4.2>에 의하면 $\overline{T}^{l-1} F$ 이 C' 의 attractor 이므로 x 의 level 은 기껏해야 k 이다. 한편

$$\begin{aligned}
 \overline{T}^{k-1} x &= T^{k-1} x \oplus (T^{k-2} \oplus \cdots \oplus T^l \oplus T^{l-1} \oplus \cdots \oplus T \oplus I)F \\
 &= T^{k-1} x \oplus \overline{T}^{l-1} F
 \end{aligned}$$

여기서 $T^{k-1} x \neq 0$ 이므로 $T^{k-1} x \oplus \overline{T}^{l-1} F$ 은 C' 에서 attractor가 아니다. 따라서 x 의 level은 k 이다.

(2) z 를 C 에서 level l 에 있는 상태라 하자. 도달가능한 상태의 직전자의 수는 2 이므로 $T^{l-1} z = T^{l-1} F$ 와 $T^l z = T^l F = 0$ 이 성립한다. 한편

$$\overline{T}^{l-1} z = T^{l-1} z \oplus (T^{l-2} \oplus \cdots \oplus T \oplus I)F$$

$$\begin{aligned}
&= T^{l-1}F \oplus (T^{l-2} \oplus \cdots \oplus T \oplus I)F \\
&= \overline{T}^{l-1}F
\end{aligned}$$

이고 $\overline{T}^{l-1}F$ 이 C' 의 attractor 이므로 z 의 level 은 기껏해야 $l-1$ 이다.

(3) w 를 C 에서 l 보다 작은 level l 에 있는 상태라면 $T^l w = T^{l-1} w = 0$ 이다.

$$\begin{aligned}
\text{그리고 } \overline{T}^l w &= T^l w \oplus (T^{l-1} \oplus \cdots \oplus T \oplus I)F \\
&= T^l w \oplus \overline{T}^{l-1}F \\
&= \overline{T}^{l-1}F
\end{aligned}$$

와

$$\begin{aligned}
\overline{T}^{l-1} w &= T^{l-1} w \oplus (T^{l-2} \oplus \cdots \oplus T \oplus I)F \\
&= \overline{T}^{l-2}F \\
&\neq \overline{T}^{l-1}F
\end{aligned}$$

이 성립한다.

그러므로 $\overline{T}^{l-1}F$ 은 C' 의 attractor 이지만 $\overline{T}^{l-2}F$ 은 C' 의 attractor 가 아니므로 w 는 level l 에 배열된다.

(4) (3)에 의하여 상태 0은 C' 에서 level l 에 있다.

$$\overline{T}0 = T0 \oplus F = F \text{ 이므로 } F \text{는 level } l-1 \text{에 배열된다.} \quad \square$$

<정리 4.4> T 가 TPMACA C 의 전이행렬 이고 C 에 대응하는 여원을 갖는 CA를 C' 라 하자. F 를 C 의 0- 트리의 도달 불가능한 상태라 하자. 그러면 상태 0은 C' 의 상태전이 그래프에서 도달 불가능한 상태이다.

<증명> F 를 C 의 0- 트리에서 level l 의 상태라 하자. 그러면 <정리

4.3>(4)에 의하여 F 는 C' 의 level $l-1$ 에 배열되므로 $\overline{T}0 = T0 \oplus F = F$ 이다. 따라서 0은 level l 에 놓이므로 상태 0은 도달 불가능한 상태이다. $\square$

<정리 4.5[1]> n -셀 TPSACA의 depth는 n 이다.

<정리 4.6> C 를 n -셀 TPSACA라 하자. 그러면 C 의 최소다항식은 다음과 같다.

$$m(x) = x^n$$

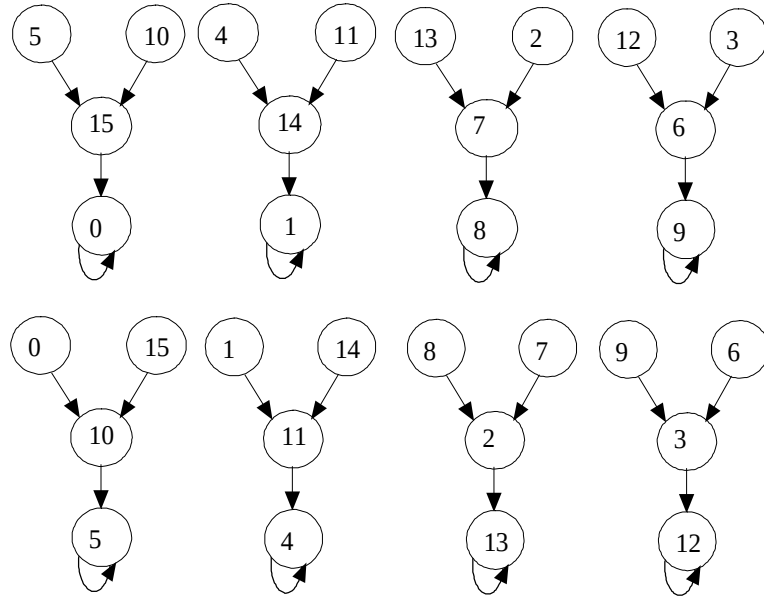
<증명> <정리 4.5>에 의하면 x^n 은 $m(x)$ 를 나누므로 $m(x) = x^n (x+1)^k$ (k 는 정수)이 성립한다. 전이행렬 T 의 특성다항식의 차수가 n 이므로 $k=0$ 이어야 한다. 따라서 $m(x) = x^n$ 이다. $\square$

<예 4.1> 4개의 셀로 이루어진 CA에 적용된 rule이 <102, 102, 60, 60>이고 전이행렬 T 는 다음과 같다.

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

이때 최소다항식은 $m(x) = x^2(x+1)$ 이다. <그림 4.1>은 이 TPMACA의 상태전이 그래프와 여원벡터를 level 2에 있는 비 순환상태 $F = (1 \ 0 \ 1 \ 0)^T$ 일 때 선형 TPMACA로부터 얻어지는 여원 CA의 상태전이 그래프이다. $\overline{T}F$ 는 C' 에서 attractor이다 <보조정리 4.2>. 또한 C 에서 level 2에 있는 모든 상태는 C' 에서 2보다 작은 level에 배열되었고<정리 4.3의 (2)>, C 에서 2보다

작은 level에 있는 모든 상태는 C' 에서 level 2에 배열되었으며 <정리 4.3의 (3)>, 상태 F 는 C' 에서 level 1에 배열되었다<정리 4.3의(4)>. 한편 C' 에서 상태2의 두 직전자 8 과 7의 합은 C 의 상태 0의 0이 아닌 직전자인 15 이다<정리 3.20> .



<그림 4.1 > 4-셀 TPMACA C 와 C' 의 상태전이 그래프

4.2 여원벡터가 선형 TPMACA의 0-트리가 아닌 다른 트리의 비순환 상태인 여원 CA

이 절에서는 선형 TPMACA로부터 유도되는 여원 CA 중 특별히 여원벡터 F가 0-트리를 제외한 임의의 트리의 비순환 상태인 경우에 대하여 살펴본다.

<보조정리 4.7> 여원벡터 F가 TPMACA C의 α -tree의 level i의 상태라 하고 β 를 C의 attractor라 하면 상태 $(\beta \oplus \overline{T}^{i-1}F)$ 는 C에 대응하는 여원 CA C'의 순환상태가 되고 그 사이클의 길이는 2이다.

<증명> $S = \beta \oplus \overline{T}^{i-1}F$ 라 하고, 위 보조정리를 증명하기 위하여 $\overline{T}S \neq S$ 이고 $\overline{T}^2S = S$ 임을 보이면 된다.

$$\begin{aligned}\overline{T}^{i-1}F &= \overline{T}^{i-1}F \oplus (T^{i-2} \oplus T^{i-3} \oplus \dots \oplus T \oplus I)F \\ &= (T^{i-1} \oplus T^{i-2} \oplus \dots \oplus T \oplus I)F\end{aligned}\quad (4.1)$$

가정에 의하여 $T\beta = \beta$, $\overline{T}^{i-1}F = 2$ 이다.

$$\begin{aligned}\text{i) } \overline{T}S &= TS \oplus F \\ &= T(\beta \oplus \overline{T}^{i-1}F) \oplus F \\ &= T\{\beta \oplus (T^{i-1} \oplus T^{i-2} \oplus \dots \oplus T \oplus I)F\} \oplus F \\ &\quad \text{「식(4.1)에 의하여」} \\ &= T\beta \oplus T^iF \oplus (T^{i-1} \oplus T^{i-2} \oplus \dots \oplus T \oplus I)F \\ &= \beta \oplus \alpha \oplus \overline{T}^{i-1}F \\ &\neq \beta \oplus \overline{T}^{i-1}F \quad \text{「} \because \alpha \neq 0 \text{」}\end{aligned}\quad (4.2)$$

$$\begin{aligned}
\text{ii)} \quad \overline{T}^2 S &= T(\overline{T} S) \oplus F \\
&= T (\beta \oplus \alpha \oplus \overline{T}^{i-1} F) \oplus F \\
&= T\beta \oplus T\alpha \oplus T(\overline{T}^{i-1} F) \oplus F \\
&= \beta \oplus \alpha \oplus \overline{T}^i F \oplus (T^{i-1} \oplus T^{i-2} \oplus \cdots \oplus T \oplus I) F \\
&= \beta \oplus \alpha \oplus \alpha \oplus \overline{T}^{i-1} F \\
&= \beta \oplus \overline{T}^{i-1} F \\
&= S
\end{aligned}$$

□

<정리 4.8> 여원벡터 F 가 C 의 $\alpha (\neq 0)$ -트리의 level i 의 상태이고 β 를 attractor라 하면 상태 $(\beta \oplus \alpha \oplus \overline{T}^{i-1} F)$ 와 $(\beta \oplus \overline{T}^{i-1} F)$ 는 C' 에서 같은 사이클에 놓이고 이 사이클의 길이는 2 이다.

(여기서 C 와 C' 은 < 보조정리 4.8>에서 정의된 것과 동일하다.)

<증명> 위 <보조정리 4.7>로 부터 $\beta \oplus \overline{T}^{i-1} F$ 는 C' 에서 길이가 2 인 사이클에 놓인다. 이 사이클을 j 라 하자.

$$\begin{aligned}
\text{먼저 } \overline{T} (\beta \oplus \alpha \oplus \overline{T}^{i-1} F) &= T (\beta \oplus \alpha \oplus \overline{T}^{i-1} F) \oplus F \\
&= T \{ \beta \oplus \alpha \oplus (T^{i-1} \oplus T^{i-2} \oplus \cdots \oplus T \oplus I) F \} \oplus F \\
&= T\beta \oplus T\alpha \oplus \overline{T}^i F \oplus (T^{i-1} \oplus T^{i-2} \oplus \cdots \oplus T \oplus I) F \\
&= \beta \oplus \alpha \oplus \alpha \oplus \overline{T}^{i-1} F \\
&= \beta \oplus \overline{T}^{i-1} F \\
&\neq \beta \oplus \alpha \oplus \overline{T}^{i-1} F
\end{aligned} \tag{4.3}$$

그리고

$$\overline{T}^2 (\beta \oplus \alpha \oplus \overline{T}^{i-1} F)$$

$$\begin{aligned}
&= T \{ \overline{T} (\beta \oplus \alpha \oplus \overline{T}^{i-1} F) \} \oplus F \\
&= T (\beta \oplus \overline{T}^{i-1} F) \oplus F \quad \text{「 식 (4.3) 에 의해 」} \\
&= \beta \oplus \alpha \oplus \overline{T}^{i-1} F \quad \text{「 식 (4.2) 에 의해 」}
\end{aligned}$$

그러므로 상태 $(\beta \oplus \alpha \oplus \overline{T}^{i-1} F)$ 는 사이클 j 에 놓인 나머지 한 상태가 된다. □

<따름정리 4.9> 여원벡터 F 가 TPMACA C 의 α -트리 의 level i 의 상태라 하고 β 를 C 의 attractor라 하면 C' 의 길이가 2인 사이클에 놓인 두 상태의 합은 항상 α 이다. (여기서 상태의 합은 bitwise 연산이다.)

<보조정리 4.10> 여원벡터 F 가 TPMACA C 의 α -트리의 level i 의 상태라 하고 β 를 C 의 attractor라 하면 상태 $\overline{T}^{i-1}F$ 는 C' 에서 길이가 2인 사이클에 놓인다.

<증명> $S = \overline{T}^{i-1}F$ 라 하고 이 보조정리를 증명하기 위해서 $\overline{T}S \neq S$ 이고 $\overline{T}^2S = S$ 임을 보이자. 우선 식(4.1)에 의해 $S = (T^{i-1} \oplus T^{i-2} \oplus \dots \oplus T \oplus I)F$ 이다. 또한 α 는 attractor이므로 $T\alpha = \alpha$ 이고 F 는 α -트리의 level i 의 상태이므로 $T^iF = \alpha$ 이다.

$$\begin{aligned}
\text{i) } \overline{T}S &= TS \oplus F \\
&= T (T^{i-1} \oplus T^{i-2} \oplus \dots \oplus T \oplus I)F \\
&= \overline{T}^iF \oplus (T^{i-1} \oplus T^{i-2} \oplus \dots \oplus T \oplus I)F \\
&= \alpha \oplus S \\
&\neq S
\end{aligned} \tag{4.4}$$

$$\begin{aligned}
\text{ii)} \quad \overline{T}^2 S &= T(\overline{TS}) \oplus F \\
&= T(\alpha \oplus S) \oplus F \\
&= T\alpha \oplus TS \oplus F \\
&= \alpha \oplus \alpha \oplus S \quad (T\alpha = \alpha \text{ and } \overline{TS} = \alpha \oplus S) \\
&= S
\end{aligned}$$

그러므로 $\overline{TS} \neq S$ 이고 $\overline{T}^2 S = S$ 이다.

<보조정리 4.11> 여원벡터 F 가 TPMACA C 의 α -트리의 level i 의 상태라 하고 β 를 C 의 attractor 라 하면 $\alpha \oplus \overline{T}^{i-1}F$ 는 C' 에서 $\overline{T}^{i-1}F$ 와 같은 사이클에 놓인다.

<증명> $S = \alpha \oplus \overline{T}^{i-1}F$ 라 하자.

$$\begin{aligned}
S &= \alpha \oplus \overline{T}^{i-1}F \\
&= T^i F \oplus (T^{i-1} \oplus T^{i-2} \oplus \cdots \oplus T \oplus I)F \\
&= \overline{T}^i F
\end{aligned} \tag{4.5}$$

$$\begin{aligned}
\text{i)} \quad \overline{TS} &= TS \oplus F \\
&= T(T^i \oplus T^{i-1} \oplus \cdots \oplus T \oplus I)F \\
&= T^{i+1}F \oplus T^i F \oplus (T^{i-1} \oplus \cdots \oplus T \oplus I)F \\
&= \overline{T}^{i-1}F \quad [\because T^{i+1}F = T^i F = \alpha] \\
&\neq S
\end{aligned}$$

$$\text{ii)} \quad \overline{T}^2 S = \overline{T}(\overline{TS}) = \overline{T}(\overline{T}^{i-1}F) = \overline{T}^i F = S$$

「 식 (4.5) 에 의해 」

□

다음 정리는 선형 TPMACA로 부터 유도되는 여원 CA 중 여원벡터 F가 0 이 아닌 α -트리의 level i 의 상태일 때 여원 CA의 상태 배열에 대한 정리이다.

<정리 4.12>

(1) 상태 x 가 C에서 α -트리의 level $i+j$ 에 놓여 있으면 C' 에서는

$\overline{T}^{i-1}F$ -트리의 level $i+j$ 상태가 된다. (단 j 는 홀수, $i+j \leq \text{depth}$)

(2) 상태 y 가 C에서 α -트리의 level $i+k$ 에 놓여 있으면 C' 에서는

$(\alpha \oplus \overline{T}^{i-1}F)$ -트리의 level $i+k$ 상태가 된다.

(단 k 는 홀수, $i+k \leq \text{depth}$)

<증명>

(1) F 가 C에서 α -트리의 level i 상태 이므로 $T^{i+j-1}F = \dots = T^iF = \alpha$ 이다. 그리고 $T^{i+j}x = 0$ 이다. 따라서

$$\begin{aligned}\overline{T}^{i+j}x &= T^{i+j}x \oplus (T^{i+j-1} \oplus \dots \oplus T^i \oplus T^{i-1} \oplus \dots \oplus T \oplus I)F \\ &= \alpha \oplus T^{i+j-1}F \oplus \dots \oplus T^iF \oplus (T^{i-1} \oplus \dots \oplus T \oplus I)F \\ &= \alpha \oplus \alpha \oplus \dots \oplus \alpha \oplus (T^{i-1} \oplus \dots \oplus T \oplus I)F\end{aligned}$$

여기서 α 의 수는 $j+1$ 개이고 j 가 홀수이므로 α 의 수는 짝수개로 그 합이 0 이다. 그러므로 $\overline{T}^{i+j}x = \overline{T}^{i-1}F$ (순환상태) 그러나

$$\begin{aligned}\overline{T}^{i+j-1}x &= T^{i+j-1}x \oplus (T^{i+j-2} \oplus \dots \oplus T \oplus I)F \\ &= T^{i+j-1}x \oplus T^{i+j-2}F \oplus \dots \oplus T^iF \oplus (T^{i-1} \oplus \dots \oplus I)F \\ &= T^{i+j-1}x \oplus \alpha \oplus \alpha \oplus \dots \oplus \alpha \oplus (T^{i-1} \oplus \dots \oplus I)F\end{aligned}$$

여기서 α 의 수는 $j-1$ 개로 짝수개이고 그 합이 0 이다.

그러므로 $\overline{T}^{i+j-1}x = T^{i+j-1}x \oplus \overline{T}^{i-1}F \neq \overline{T}^{i-1}F$ 또한 $T^{i+j-1}x$

$\neq \alpha$ 이므로 <보조정리 4.11>에 의하여 $T^{i+j-1}x \oplus \overline{T}^{i-1}F$ 는 순환상태가 아니다. 그러므로 x 는 C' 에서 $\overline{T}^{i-1}F$ -트리의 level $(i+j)$ 에 놓인다.

$$(2) \quad T^{i+j}F = \cdots = T^iF = \alpha \text{ 그리고 } T^{i+j}y = \alpha$$

$$\begin{aligned} \overline{T}^{i+j}y &= T^{i+j}y \oplus (T^{i+j-1} \oplus \cdots \oplus T \oplus I)F \\ &= \alpha \oplus T^{i+j-1}F \oplus \cdots \oplus T^iF \oplus (T^{i-1} \oplus \cdots \oplus I)F \\ &= \alpha \oplus \alpha \oplus \cdots \oplus \alpha \oplus \overline{T}^{i-1}F \end{aligned}$$

여기서 α 의 수는 $j+1$ 개로 j 가 짝수이므로 $j+1$ 은 홀수이다.

$$\overline{T}^{i+j}y = \alpha \oplus \overline{T}^{i-1}F \text{ (순환상태)}$$

$$\begin{aligned} \text{그러나 } \overline{T}^{i+j-1}y &= T^{i+j-1}y \oplus (T^{i+j-2} \oplus \cdots \oplus I)F \\ &= T^{i+j-1}y \oplus \alpha \oplus \cdots \oplus \alpha \oplus (T^{i-1} \oplus \cdots \oplus I)F \end{aligned}$$

α 의 수는 $j-1$ 개로 홀수이다.

$$\text{그러므로 } \overline{T}^{i+j-1}y = T^{i+j-1}y \oplus \alpha \oplus \overline{T}^{i-1}F$$

$T^{i+j-1}y \neq 0$ 이고 $T^{i+j-1}y \neq \alpha$ 이므로 y 는 C' 에서 $(\alpha + \overline{T}^{i-1}F)$ -트리의 level $(i+j)$ 상태에 놓인다. $\square$

이제 앞선 정리를 좀더 확장하여 F 가 선형 TPMACA의 α -트리의 level i 의 상태일 때 선형 TPMACA에 있는 상태들이 이에 대응하는 여원 CA에 어떻게 배열되는지 알 수 있다.

<정리 4.13> (1) x 가 C 에서 $\beta (\neq \alpha)$ -트리의 level $(i+j)$ 상태이면 C' 에서 $(\beta \oplus \alpha \oplus \overline{T}^{i-1}F)$ -트리의 $(i+j)$ 상태에 놓인다. (단 j 는 홀수, $i+j \leq \text{depth}$)

(2) y 가 C 에서 $\beta (\neq \alpha)$ -트리의 level $(i+j)$ 상태이면 C' 에서 $(\beta \oplus \overline{T}^{i-1}F)$ -트리의 $(i+j)$ 상태에 놓인다. (단 j 는 짝수, $i+j \leq \text{depth}$)

(3) w 가 C 에서 β -트리의 level i 보다 낮은 level에 있는 상태이면 C' 에서 $(\beta \oplus \overline{T}^{i-1}F)$ -트리의 level i 상태가 된다.

(4) C 에서 level i 에 있는 상태들은 C' 에서 level $(i-1)$ 이하의 상태가 된다.

<증명> F 가 선형 TPMACA C 의 α -트리의 level i 의 상태이므로

$$T^{i+j-1}F = \dots = T^iF = \alpha \text{ 이다.}$$

(1) 가정에 의하여 $T^{i+j}x = \beta$ 이다.

$$\begin{aligned} \overline{T}^{i+j}x &= T^{i+j}x \oplus (T^{i+j-1} \oplus \dots \oplus T^i \oplus \dots \oplus I)F \\ &= T^{i+j}x \oplus T^{i+j-1}F \oplus \dots \oplus T^iF \oplus (T^{i-1} \oplus \dots \oplus I)F \\ &= \beta \oplus \alpha \oplus \dots \oplus \alpha \oplus \overline{T}^{i-1}F \\ &\text{(여기에서 } \alpha \text{의 수는 } j \text{ 개로 홀수이다.)} \end{aligned}$$

$$\text{그러므로 } \overline{T}^{i+j}x = \beta \oplus \alpha \oplus \overline{T}^{i-1}F \text{ (순환상태)}$$

$$\begin{aligned} \text{그러나 } \overline{T}^{i+j-1}x &= T^{i+j-1}x \oplus (T^{i+j-2} \oplus \dots \oplus I)F \\ &= T^{i+j-1}x \oplus T^{i+j-2}F \oplus \dots \oplus T^iF \oplus (T^{i-1} \oplus \dots \oplus I)F \\ &= T^{i+j-1}x \oplus \alpha \oplus \alpha \oplus \dots \oplus \overline{T}^{i-1}F \\ &\text{(여기에서 } \alpha \text{의 수는 } j-1 \text{ 개로 짝수이다.)} \end{aligned}$$

$$\text{그러므로 } \overline{T}^{i+j-1}x = T^{i+j-1}x \oplus \overline{T}^{i-1}F$$

$T^{i+j-1}x$ 는 C 에서 β 의 β 가 아닌 직전자 이므로 $T^{i+j-1}x$ 는 0 도 α 도 아

니다. 그러므로 $\overline{T}^{i+j-1}x$ 는 순환상태가 아니다. 그러므로 x 는 C' 에서 $(\beta \oplus \alpha \oplus \overline{T}^{i-1}F)$ -트리의 level $(i+j)$ 의 상태가 된다.

$$\begin{aligned} (2) \quad \overline{T}^{i+j}y &= T^{i+j}y \oplus (T^{i+j-1} \oplus \cdots \oplus T^i \oplus \cdots \oplus I)F \\ &= \beta \oplus \alpha \oplus \cdots \oplus \alpha \oplus (T^{i-1} \oplus \cdots \oplus I)F \\ &\quad (\text{여기에서 } \alpha \text{의 수는 } j \text{ 개로 짝수개이다.}) \end{aligned}$$

그러므로 $\overline{T}^{i+j}y = \beta \oplus \overline{T}^{i-1}F$ (순환상태)

$$\begin{aligned} \text{그러나} \quad \overline{T}^{i+j-1}y &= T^{i+j-1}y \oplus (T^{i+j-2} \oplus \cdots \oplus I)F \\ &= T^{i+j-1}y \oplus \alpha \oplus \cdots \oplus \alpha \oplus (T^{i-1} \oplus \cdots \oplus I)F \\ &= T^{i+j-1}y \oplus \alpha \oplus \overline{T}^{i-1}F (\because \alpha \text{의 수가 } j-1 \text{ 개로 홀수}) \end{aligned}$$

그러므로 $\overline{T}^{i+j-1}y$ 는 $T^{i+j-1}y$ 가 α 도 β 도 아니므로 비순환 상태가 된다.

따라서 y 는 C' 에서 $(\beta \oplus \overline{T}^{i-1}F)$ -트리의 level $(i+j)$ 의 상태에 놓인다.

(3) w 가 C 에서 β -트리의 level $j (< i)$ 에 있는 상태라 하자.

그러면 $T^jw = T^{j+1}w = \cdots = T^iw = \beta$ 이다.

$$\begin{aligned} \overline{T}^iw &= T^iw \oplus (T^{i-1} \oplus \cdots \oplus I)F \\ &= \beta \oplus \overline{T}^{i-1}F \quad (\text{순환상태}) \end{aligned}$$

$$\begin{aligned} \text{그러나} \quad \overline{T}^{i-1}w &= T^{i-1}w \oplus (T^{i-2} \oplus \cdots \oplus I)F \\ &= \beta \oplus \overline{T}^{i-2}F \quad \text{이므로 } \overline{T}^{i-1}w \text{는 비순환 상태이다.} \end{aligned}$$

그러므로 w 는 C' 에서 $(\beta \oplus \overline{T}^{i-1}F)$ -트리의 level i 에 정확히 놓인다.

(4) z 를 선형 TPMACA C 에서 β -트리의 level i 의 상태라 하면 $T^{i-1}F$ 는 C 에서 α -트리의 level 1 상태이고 $T^{i-2}F$ 는 C 에서 β -트리의 level 1 상태이다. <보조정리 3.12>에 의하여 $T^{i-1}F \oplus T^{i-2}F = \alpha \oplus \beta$ 이고 $T^{i-1}z = \alpha \oplus \beta \oplus T^{i-2}F$ 이다.

$$\begin{aligned} \overline{T^{i-1}z} &= T^{i-1}z \oplus (T^{i-2} \oplus \cdots \oplus I)F \\ &= \alpha \oplus \beta \oplus T^{i-1}F \oplus (T^{i-2} \oplus \cdots \oplus I)F \\ &= \alpha \oplus \beta \oplus (T^{i-1} \oplus \cdots \oplus I)F \\ &= \alpha \oplus \beta \oplus \overline{T^{i-1}F} \text{ (순환상태)} \end{aligned}$$

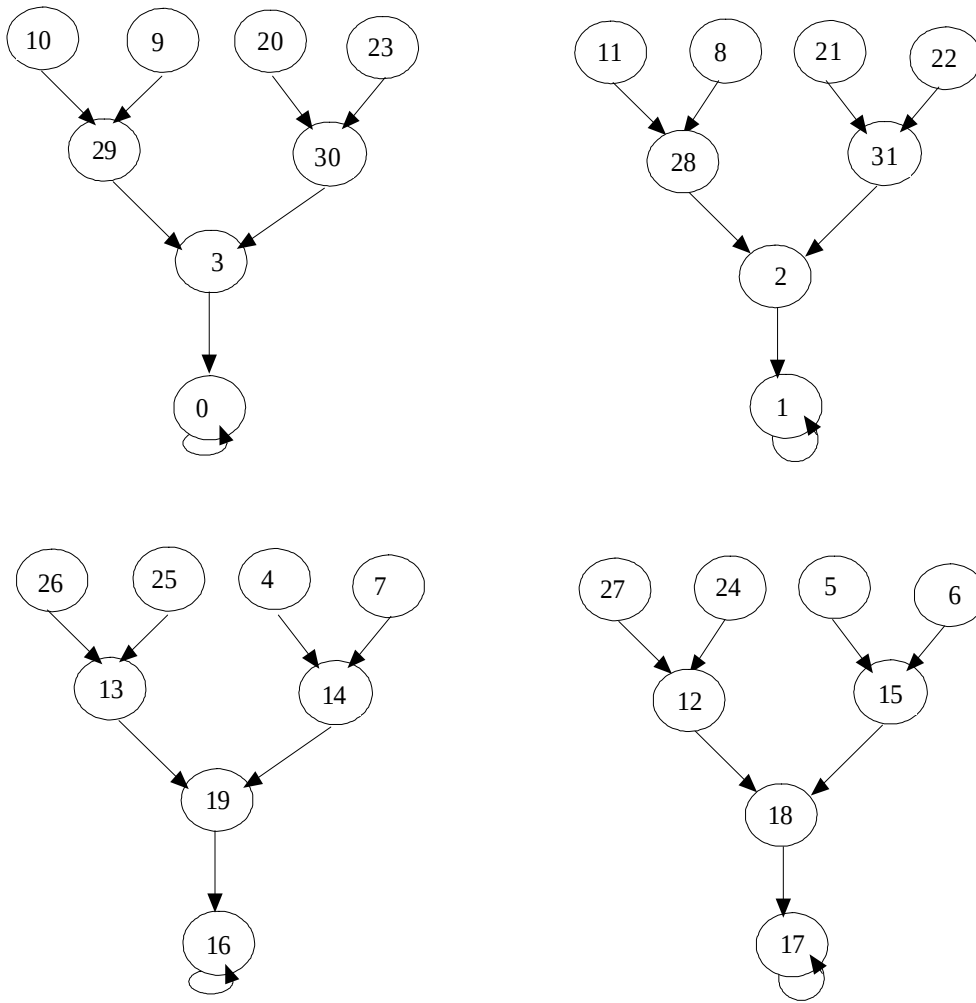
그러므로 z 는 C' 에서 level $i-1$ 이하에 놓인다. □

<예 4.2> 5개의 셀로 이루어진 CA에 적용된 rule 이 <102, 102, 60, 240, 60>이고 전이행렬 T 는 다음과 같다.

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

이때 최소다항식은 $m(x) = x^3(x+1)$ 이다.

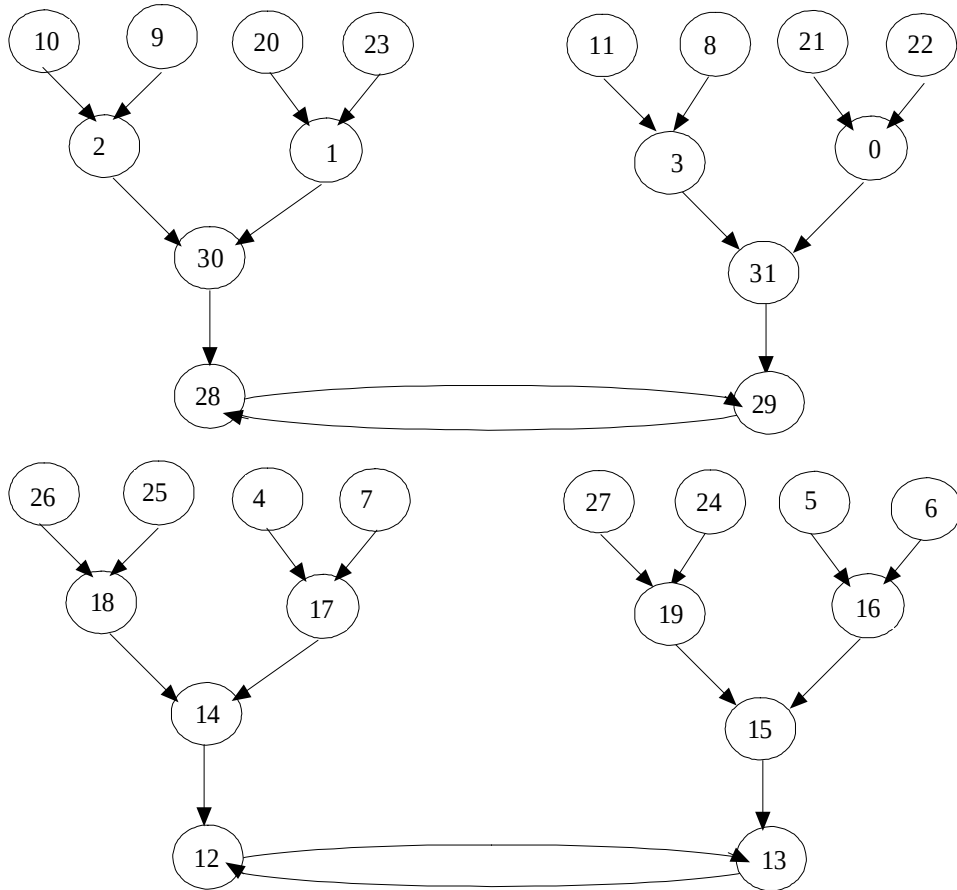
<그림 4.2>은 이 TPMACA의 상태전이 그래프이다.



<그림 4.2> 5-셀 TPMACA C 의 상태전이 그래프

<그림4.2>은 여원벡터 F 를 2-트리의 level 2에 있는 비 순환상태 $31 = (11111)^T$ 로 두었을 때 선형 TPMACA ζ 로부터 얻어지는 여원 CA C' 의 상태전이 그래프이다. C 에서 0-트리와 1-트리가 서로 결합하고 나머지 16-트리와 17-트리가 결합한다. C 에서 level 2보다 상위 level에 있는 상태(10, 9, 20, 23 등)들은 level이 그대로 유지되고, level 0과 level 1에 놓여 있는 상태들은 C' 에

서 level 2에 놓이고 C에서 level 2의 상태는 C'에서 level 2보다 낮은 level에 놓인다<정리 4.3>. C'에서 한 사이클에 놓여 있는 상태들의 합은 $(29 \oplus 28, 12 \oplus 13)$ 은 여원벡터가 있던 트리의 attractor 상태 1과 같다<정리 4.8>.



<그림 4.3> 선형 TPMACA로부터 얻어지는 여원 CA C' (여원벡터 : 31)

4.3 여원벡터가 선형 TPMACA의 0 이 아닌 attractor 인 여원 CA

이 절에서는 여원벡터의 위치에 따라 분류된 여원 CA 가운데 마지막인 여원 벡터가

선형 TPMACA의 0 이 아닌 attractor인 경우에 대하여 분석한다.

<보조정리 4.14> 여원벡터 F가 선형 TPMACA C의 0이 아닌 attractor라 하면 상태 0은 C에 대응하는 여원 CA C'에서 순환상태이다. 또한 그 사이클의 길이는 2가 된다.

<증명> F가 C에서 attractor이기 때문에 $TF=F$ 이다.

$$\begin{aligned}\overline{T} \cdot 0 &= T \cdot 0 \oplus F \\ &= 0 \oplus F \\ &\neq 0\end{aligned}$$

$$\begin{aligned}\text{그러나 } \overline{T}^2 \cdot 0 &= T^2 \cdot 0 \oplus (T \oplus I)F \\ &= 0 \oplus TF \oplus F \\ &= 0 \oplus F \oplus F \\ &= 0\end{aligned}$$

그러므로 상태 0은 여원 CA C'의 순환상태이고 그 사이클의 길이는 2이다.

□

<보조정리 4.15> 여원벡터 F가 선형 TPMACA C에서 0이 아닌 attractor α 라 하면 α 는 C에 대응하는 여원 CA C'에서 상태 0을 포함하는 길이가 2인 사이클에 놓이게 된다.

<증명> 가정에 의하여 $F = \alpha$ 이다.

$$\begin{aligned}
 \overline{T}\alpha &= T\alpha \oplus F \\
 &= T\alpha \oplus \alpha \quad \text{「 } F = \alpha \text{ 」} \\
 &= \alpha \oplus \alpha \quad \text{「 } T\alpha = \alpha \quad \because \alpha \text{ 는 } C \text{ 에서 attractor 」} \\
 &= 0 \\
 \overline{T}^2\alpha &= T^2\alpha \oplus (T \oplus I)F \\
 &= \alpha \oplus (T \oplus I)\alpha \\
 &= \alpha \oplus T\alpha \oplus \alpha \\
 &= \alpha
 \end{aligned}$$

따라서 α 는 C' 에서 상태 0을 포함하는 사이클의 순환상태이다. □

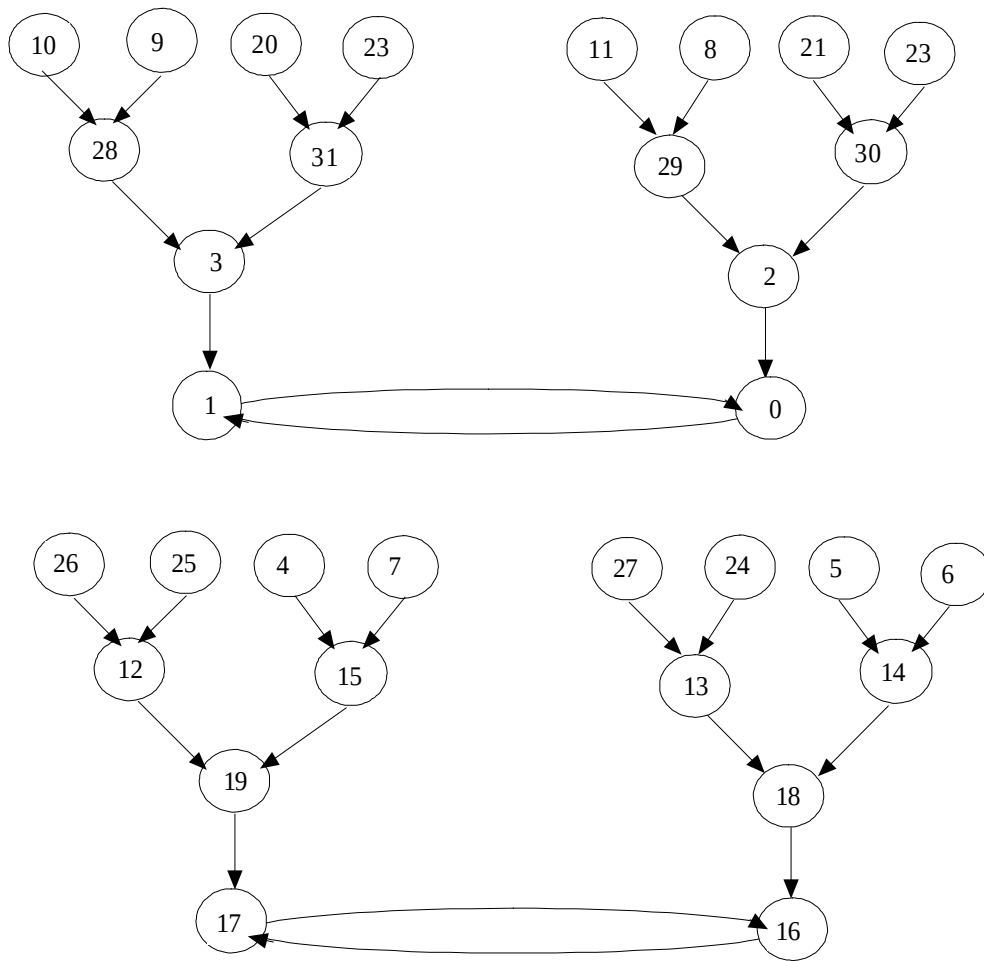
<정리 4.16 [9]> 여원벡터 F 가 선형 TPMACA C 에서 0이 아닌 attractor α 라 하고 β 를 또 다른 attractor 라 하면

- (1) $\beta \oplus \alpha$ 또한 C 의 attractor 이다.
- (2) β 와 $\beta \oplus \alpha$ 는 C 에 대응하는 여원 CA C' 에서 길이가 2 인 같은 사이클에 놓이게 된다.

<정리 4.17 [9]> 여원벡터 F 가 선형 TPMACA C 에서 0 이 아닌 attractor α 라 하고 x 가 β -트리의 level $2m$ 인 상태라면 x 는 C' 에서도 β -트리의 level $2m$ 에 놓인다.

<정리 4.18 [9]> 여원벡터 F 가 선형 TPMACA C 에서 0이 아닌 attractor α 라 하고 y 가 β -트리의 level $(2m-1)$ 인 상태라면 y 는 C 에 대응하는 C' 의 $(\beta \oplus \alpha)$ -트리에서 level 이 $(2m-1)$ 로 재배열되어진다. x 가 β -트리의 level $2m$ 인 상태라면 x 는 C' 에서도 β -트리의 level $2m$ 에 놓인다.

<예 4.3> <예 4.2>의 선형 TPMACA C 에서 0이 아닌 attractor들 중 1을 여원 벡터로 하여 얻어지는 여원 CA C' 의 상태전이 그래프는 <그림 4.4>와 같다. C' 에서 여원 벡터인 상태 1을 root로 하는 1-트리와 0-트리가 결합하고 나머지 트리들도 attractor의 합이 1이 되는 것끼리 결합한다<정리 4.16>. 또한 각 트리의 비순환 상태들의 level은 C 와 C' 을 비교할 때 같음을 볼 수 있다. 그러나 0-트리의 홀수 level인 level 1의 상태 3과 level 3의 상태인 10, 9, 20, 23은 C' 에서 결합된 상대트린인 1-트리의 level 1과 level 3에 배열된다<정리 4.18>.



<그림 4.4> 선형 TPMACA로부터 얻어지는 여원 CA C' (여원벡터 : 1)

5. 결론

CA는 LFSR과 비교하여 랜덤성이 우수하다는 것이 알려지면서 최근 LFSR의 대안으로 의사 랜덤 패턴 생성기, 해쉬 함수, 스트림 암호 알고리즘 등의 고속화 응용에 많이 활용되고 있다. 그러나 CA를 이용하여 암호 알고리즘이나 해쉬함수를 생성함에 앞서 CA에 대한 안전성 분석 및 CA의 행동분석이 먼저 이루어져야 할 것이다. 하지만 이에 대한 연구가 미비하여 CA를 암호학적 응용에 활용하기 위해서는 다소 어려움이 뒤따른다. 무엇보다 CA를 암호학 응용에 적용하기 위해서는 주어진 CA의 상태전이 행동분석이 이루어져야 할 것이며 이는 우선적으로 CA의 상태전이 그래프를 구성함으로써 수행될 수 있다. 본 논문은 선형 TPMACA로부터 얻어지는 여원 CA의 상태전이 그래프에서의 상태들의 배열을 정확히 얻을 수 있음을 보였다.

참 고 문 헌

- [1] S. Bhattacharjee, U. Raghavendra, D.R. Chowdhury, P.P. Chaudhuri, *"An efficient encoding algorithm for image compression hardware based on Cellular Automata"*, High Performance Computing 1996, Proc. IEEE 3rd International Conf., 1996, pp. 239-244.
- [2] S. Bhattacharjee, S. Sinha, S. Chattopadhyay, P.P. Chaudhuri, *"Cellular automata based scheme for solution of Boolean equations"*, IEEE, Proc.-Comput. Digit. Tech., Vol. 143, No. 3, 1996, pp. 174-180.
- [3] K. Cattell, J. Muzio, *"Analysis of one-dimensional linear hybrid cellular automata over $GF(q)$ "*, IEEE Transactions of Computers, Vol. 45, No. 7, 1996, pp. 782-792.
- [4] K. Cattell, J. Muzio, *"Synthesis of one-dimensional linear hybrid cellular automata"*, IEEE Transactions on Computer-Aided Design of Integrated Circuit and Systems, Vol. 15, No. 3, 1996, pp. 325-335.
- [5] K. Cattell, M. Serra, *"The analysis of one dimensional multiple-value linear cellular automata"*, IEEE Transaction on Computer-Aided Design of Intergrated Circuits and Systems, Vol. 9, Iss. 7, pp. 767-778.
- [6] S. Chattopadhyay, *"Some studies on theory and applications of additive cellular automata"*, Ph.D. Thesis, I.I.T., Kharagpur, India, 1996.
- [7] P. P. Chaudhuri, et. al., *"Additive cellular automata theory and applications"*, Vol. 1, IEEE Computer Society Press, California, USA,

1997.

- [8] S.J. Cho, U.S. Choi and H.D. Kim, "*Linear nongroup one-dimensional cellular automata characterization on $GF(2)$* ", J. Korea Multimedia Soc., Vol. 4, No. 1, 2001, pp. 91-95.
- [9] S.J. Cho, U.S. Choi and H.D. Kim, "*Analysis of complemented CA derived from a linear TPMA CA*", Comput. & Math. Appl.(Accepted).
- [10] S.J. Cho, H.D. Kim and U.S. Choi, "*Behavior of complemented cellular automata derived from a linear cellular automata*" (Submitted).
- [11] A.K. Das and P.P. Chaudhuri, "*Efficient characterization of cellular automata*" , Proc. IEE(part E), Vol. 137, No. 1, 1990, pp. 81-87.
- [12] 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., Vol. 42, 1993, pp. 340-352.
- [13] M. Mihaljevic, H. Imai, "*A family of fast keystream generations based on programmable linear cellular automata over $GF(q)$ and time-variant Table*", IEICE Transactions on Fundamentals, Vol. E82-A, No.1, 1999, pp. 32-39.
- [14] M. Mihaljevic, Y. Zheng, H. Imai, "*A fast and secure stream cipher based on cellular automata over $GF(q)$* ", IEEE Global Telecommunications Conference, GLOBECOM '98, Vol. 6, 1998, pp. 3250-3255.
- [15] J. Von Neumann, "*Theory of self-reproducing automata*", University of Illinois Press Urbana, 1966.

- [16] S. Wolfram, "*Cellular Automata and Complexity*", Addison-Wesley Publishing Company, 1994.
- [17] S. Wolfram, "*Statistical mechanics of cellular automata*", *Rev. Modern Physics*, Vol. 55, No. 3, 1983.

감사의 글

2년 6개월! 살같이 빠른 세월에 나의 부족함을 깊이 느끼는 시간이었습니다. 늘 노력하시는 모습으로 본을 보여 주시고 깊은 지식으로 한편의 논문이 완성되도록 지도해주신 조성진 지도교수님께 진심으로 감사를 드리며, 바쁘신 중에도 본 논문의 부족한 점에 대하여 검토, 보완해 주신 표용수 교수님, 박용범 교수님께 감사를 드립니다.

그동안 본 논문을 작성하는데 모든 일을 제쳐두고 내용을 다듬어 주신 최언숙 선생님과 토론과 검토를 같이한 연구실의 실원들께도 감사를 드립니다.

대학원 과정을 마칠 수 있도록 항상 격려해주신 교육과학연구원 허문수 원장님, 김옥중 연구사님, 신도중학교 김종태 교장선생님, 거제여중 김정순 교장선생님, 재송여중 김복수 교장선생님, 김영숙 교감선생님께 감사를 드립니다.

끝으로 이 논문이 완성되기까지 기도해주시고 격려해주신 어머니와 늘 용기를 가질수 있도록 외조를 아끼지 않았던 남편과 엄마의 부족한 손길에도 건강하게 잘 자라준 시은이와 규은이에게 작은 기쁨을 나누며 무엇보다 우리의 모든 것 되시는 하나님께 깊은 감사를 드립니다.

2002년 6월 27일

최 향희