

이학박사 학위논문

가산 셀룰라 오토마타의
상태전이 행동분석 및 응용

지도교수 조 성 진

이 논문을 위한 박사 학위논문으로 제출함



2004년 2월






부경대학교 대학원

응용수학과

최 언 숙

최언숙의 이학박사 학위논문을 인준함

2003년 12월 26일

주 심	이학박사	이 경 현	
부 심	이학박사	김 한 두	
위 원	공학박사	박 지 환	
위 원	이학박사	표 용 수	
위 원	이학박사	조 성 진	

목 차

그림 목차	vi
표 목차	vii
Abstract	viii
1. 서론	1
2. 셀룰라 오토마타	4
2.1 CA의 정의 및 분류	4
2.2 CA의 전이행렬과 특성다항식	10
3. Group 셀룰라 오토마타	16
3.1 선형 group CA의 성질	16
3.2 CA의 최소다항식과 CA의 사이클 구조	17
4. Nongroup 셀룰라 오토마타	26
4.1 선형 Nongroup CA의 성질	26
4.2 LNCA의 성질	29
4.3 LNCA로부터 유도된 여원 CA의 상태전이행동 분석	39
5. Nongroup 셀룰라 오토마타의 응용	66
5.1 선형 TPNCA의 트리구성 알고리즘	66
5.2 여원 TPNCA의 트리구성 알고리즘	77
5.3 TPSACA를 기반으로 하는 완전해싱 기술	98

6. 결론 109

참고 문헌 110

그림 목 차

<그림 2.1> 3-이웃 선형 CA의 셀 구조	4
<그림 2.2> 서로 다른 경계조건을 가지는 CA	9
<그림 2.3> 최대길이를 갖는 CA	11
<그림 2.4> 최대길이를 갖지 않는 group CA	12
<그림 2.5> Nongroup CA	13
<그림 3.1> 규칙 <90, 90, 150, 90>인 group CA	21
<그림 3.2> 규칙 <90, 90, 90, 150>인 group CA	23
<그림 3.3> 규칙 <150, 150, 150, 150>인 group CA	25
<그림 4.1> 4-셀 TPSACA	29
<그림 4.2> 5-셀 선형 TPMACA C의 상태전이 그래프	38
<그림 4.3> 4-셀 선형 TPMACA C와 C'의 상태전이 그래프	46
<그림 4.4> 선형 TPMACA로부터 얻어지는 여원 CA C' (여원벡터 : 31)	57
<그림 4.5> 선형 TPMACA로부터 얻어지는 여원 CA C' (여원벡터 : 1)	62
<그림 5.1> 5-셀 TPMACA의 상태전이 그래프	74
<그림 5.2> 5-셀 선형 TPNCA	76
<그림 5.3> 5-셀 여원 TPNCA	97
<그림 5.4> 4-셀 TPSACA의 구조 및 상태전이 그래프	101
<그림 5.5> 여원벡터가 2인 4-셀 여원 TPSACA의 상태전이 그래프	106

표 목 차

<표 2.1> 선형규칙	7
<표 2.2> 여원규칙	8
<표 3.1> GF(2) 상에서 기약다항식과 원시다항식	19
<표 5.1> 주어진 키의 해시과정	104
<표 5.2> 주어진 키 집합 X_2 를 해시하는 과정	106

Analysis of The State Transition Behavior of Additive Cellular Automata and Its Application

Un Sook Choi

*Department of Applied Mathematics, Graduate School,
Pukyong National University*

Abstract

Cellular Automata(CA) is a discrete dynamical 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. Since a CA has a simple, regular, modular and cascable structure, it is useful for hardware implementation for VLSI. 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. As every linear CA can be represented by a transition matrix, it can be analyzed with its characteristic polynomial. But a complemented CA is nonlinear. So it is more difficult to analyze properties of complemented CA than a linear CA. In this thesis, we investigate some properties of additive CA. Especially we analyze characteristic of linear TPNCA and investigate a detailed analysis of the state transition behavior of complemented CA C' derived from a linear TPNCA C . We present an algorithm for the construction of trees in C and C' . Also we give a perfect hashing algorithm based on TPSACA using the tree construction algorithm.

1. 서론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 Von Neumann[24]에 의하여 스스로 조직화하고 재생산할 수 있는 모델로 처음 소개되었다. 이후 1980년대에 Wolfram[27]은 CA를 셀이라 불리는 메모리의 배열로 소개하고, 셀의 상태가 자기 자신 및 인접한 셀 상태의 국소적인 상호작용에 의해서 동시에 갱신되는 시스템으로 제안하였다. 특히 CA 가운데 다음 상태를 결정하는 함수가 선형적인 CA는 LFSR(Linear Feedback Shift Register)의 대안으로 제안되고, 이로 인해 test pattern generation[20, 16], 의사 난수열 생성기[21, 25], 암호[28], 부울 방정식의 해법[2], 오류정정부호[13, 14, 15], 신호 분석[8, 19], 이미지 압축[1] 등 많은 분야에서 응용되었다. 1990년에 이르러 Das 등은 행렬대수학을 이용하여 선형 CA의 상태전이 행동 분석을 하였다[17, 18]. CA는 Wolfram에 의하여 처음으로 암호학에 도입되었고[26], Chaudhuri, Nandi 등이 많은 분야에 CA를 폭넓게 활용하였다[6, 7, 9, 26]. 그리고 Muzio, Cattel 등에 의해서 LFSR에 대응하는 CA에 대한 연구가 이루어졌으며, 최소비용으로 최대길이를 갖는 CA를 찾는 연구가 수행되었다[3, 4, 5]. 최근에는 Imai 등에 의해서 고속 암호 알고리즘 구현에 CA가 이용되었고[22, 23], Cho 등은 nongroup CA의 특성에 관한 연구를 하였다[10, 11, 12].

CA는 VLSI 하드웨어 구현의 용이성과 랜덤성의 우수함으로 인해 다양한 응용의 증대와 장점에도 불구하고 일반화와 분석이 거의 이루어지지 않고 있다. 본 논문은 가산 CA중 선형 CA와 여원 CA에 관하여 분석하였다. CA는 대수학적 성질에 따라 group CA와 nongroup CA로 구분된다. Group CA는 주어진 전이행렬의 최소다항식을 구함으로써, 최소다항식의 유형별로 나누어 다양한 주기를 갖는 group CA의 사이클 구조를

특성화한다. 본 논문에서는 선형 nongroup CA의 상태전이 그래프를 0-트리의 최상위 레벨에 있는 한 상태의 전이행동으로부터 나머지 모든 상태의 전이행동을 명확히 밝힘으로써 상태전이 그래프를 구성하는 알고리즘을 제안한다. 이 알고리즘은 선형 CA에 비해 분석이 더욱 어려운 비선형 CA중 XNOR 규칙이 적용되는 여원 CA의 분석을 가능케 한다. 알고리즘을 이용하여 여원벡터의 위치를 정확히 파악하고, 여원 nongroup CA에 대응하는 선형 nongroup CA의 전이행렬을 이용하여 여원 nongroup CA를 선형 nongroup CA와 관련지어 분석한다. 특히 선형 TPMACA로부터 얻을 수 있는 모든 여원 TPNCA의 상태전이 행동을 분석하고 상태전이 그래프를 얻을 수 있는 알고리즘을 제안한다. 이 알고리즘은 행렬의 곱셈을 이용하여 상태전이 그래프를 얻어내는 기존의 분석방법을 덧셈연산으로 대체함으로써 계산속도를 현저하게 향상시킬 수 있다. 이러한 nongroup CA에 관한 분석에 대한 응용으로 임의의 도달 가능한 상태에 대한 직전사 수가 두 개인 선형 TPSACA(Two Predecessor Single Attractor CA)를 이용하여 완전 해싱 알고리즘을 제안한다.

본 논문의 구성은 먼저 2장에서는 CA의 정의와 여러 기준에 따른 분류를 소개한다. 또한 CA의 상태를 변화시키는 상태전이 함수인 전이규칙에 대해 서술한다. 특별히 선형 CA의 전이함수는 선형변환이므로, 이 선형변환을 표준행렬로 표현한 전이행렬과 전이행렬에 대한 특성다항식에 대하여 소개하고, 선형 CA와 관련지어 분석이 가능한 여원 CA에 대한 정의와 일반적인 성질을 서술한다.

3장은 group CA의 전반적인 성질을 바탕으로 상태전이 행동을 CA의 전이행렬의 최소다항의 형태별로 분류하여, 상태전이 그래프에서 나타나는 사이클들의 길이와 개수를 유도한다. 이를 통해 group CA의 사이클 구조에 대한 정확히 분석한다.

4장은 선형 nongroup CA의 성질을 0-트리와 관련지어 분석한다. 특별

히 선형 TPNCA(Two Predecessor Nongroup Attractor CA) 상태전이 행동에 대한 분석과 선형 nongroup CA로부터 유도된 여원 nongroup CA를 분석한다. 5장은 CA의 응용으로 선형 TPMACA(Two Predecessor Multiple Attractor CA)의 트리 구성 알고리즘 및 선형 TPMACA로부터 유도된 여원 CA의 트리 구성 알고리즘을 제안한다. 또한 TPMACA의 특별한 경우인 TPSACA를 기반으로 하여 완전 해싱 알고리즘을 새로운 개념인 MRT(Minimal Running Time)을 이용하여 제안하고 6장에서 결론을 맺는다.

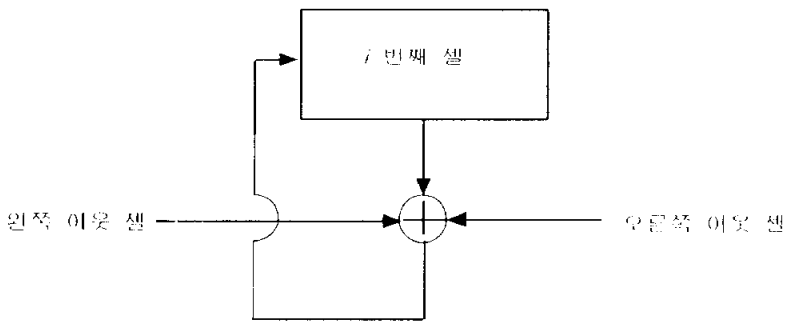
2. 셀룰라 오토마타

2.1 CA의 정의 및 분류

2.1.1 CA의 정의와 규칙

CA란 이산 시간의 동적 시스템으로 셀이라는 기본 단위 메모리의 배열로 이루어진다. 이 시스템에서 셀의 다음 상태는 어떤 규칙에 따라 정해진다. 즉, 각 셀들은 자기 자신과 이웃 셀의 함수값에 의해 다음 상태가 결정되어 동시에 갱신된다. CA는 간단하고, 규칙적이며, 작은 단위로 확장 연결할 수 있는 구조이기 때문에 VLSI 하드웨어 구현에 알맞다.

가장 간단한 구조를 가지는 1차원 CA에서는 모든 셀이 선형으로 배열되어 있고, 이 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 NBCA(Null Boundary CA)에 국한시킨다. 또한 셀의 크기는 1 비트로 제한한다. 그림 2.1은 3-이웃 선형 CA의 셀의 구조이다.



<그림 2.1> 3-이웃 선형 CA의 셀 구조

세 개의 이웃을 가지는 CA 에 대한 다음 상태전이 함수(state transition function)는 다음과 같이 나타낸다

$$s_i^{t+1} = f(s_{i-1}^t, s_i^t, s_{i+1}^t) \tag{2.1}$$

여기서 s_i^t 는 시간 t 에서 i 번째 셀의 상태를 나타내고, f 는 결합논리를 가지는 국소전이 함수이다. f 는 3개의 변수를 가지는 Boolean 함수로 $f: \{000, 001, 010, \dots, 110, 111\} \rightarrow \{0, 1\}$ 이다. 그러므로 다음 상태 전이함수 f 는 2^3 , 즉 256개가 있으며 이것을 CA의 규칙이라고 한다. 예를 들어 아래와 같이 f 가 정의된다고 하자.

이웃상태	111	110	101	100	011	010	001	000	규칙
다음상태	0	0	1	1	1	1	0	0	60
다음상태	1	0	0	1	0	1	1	0	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. 두 번째 행의 다음 상태 결과를 이진법의 주로 간주하고 이진법의 수 $111100_{(2)}$ 를 십진법의 수로 변환하면 $1 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 = 60$ 이므로 이 함수를 규칙 60이라 한다. 같은 방법으로 세 번째 행 또한 이진법의 수 $10010110_{(2)}$ 를 십진법의 수로 변환하면 150이므로 이 함수를 규칙 150이라 한다. 위의 규칙에 대한 결합논리는 다음 식으로 표현할 수 있고 \oplus 는 XOR 논리를 나타낸다.

$$\text{규칙 60} : s_j(t+1) = s_{j-1}(t) \oplus s_j(t) \quad (2.2)$$

$$\text{규칙 150} : s_j(t+1) = s_{j-1}(t) \oplus s_j(t) \oplus s_{j+1}(t) \quad (2.3)$$

2.1.2 CA의 분류

CA는 배열된 구조에 따라, 적용되는 규칙의 논리에 따라, 적용된 규칙의 개수에 따라 그리고 상태전이 그래프의 모양에 따라 아래와 같이 분류된다.

(1) 셀의 배열상태에 따른 분류

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

(2) 적용되는 규칙의 논리에 따른 분류

① 가산 CA (Additive CA)

가. 선형 CA (Linear CA) : 모든 셀의 규칙이 XOR 논리로만 이루어진 CA

나. 여원 CA (Complemented CA) : 셀의 규칙이 XNOR 과 XOR 논리의 조합으로 이루어진 CA

② 비가산 CA(Nonadditive CA) : 셀들의 규칙이 AND-OR논리로 이루어진 CA

표 2.1은 선형 CA에 적용되는 선형 규칙이고 표 2.2는 여원 CA에 적용되는 여원규칙이다.

(3) 적용되는 규칙의 개수에 따른 분류

① Uniform CA : 모든 CA의 셀이 같은 규칙을 따르는 CA

② Hybrid CA : 2가지 이상의 서로 다른 규칙이 적용된 CA

(4) 상태전이 그래프의 형태에 따른 분류

① Group CA : 모든 셀의 상태가 몇 개의 사이클을 이루며 반복되는 CA

② Nongroup CA : Group CA 가 아닌 CA

Group CA는 모든 셀의 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 나누어진다. Nongroup CA는 임의의 한 상태에 대한 이전상태가 존재하지 않거나 2개 이상이다.

선형규칙	의존도			전이 함수
	L	S	R	
규칙 150	1	1	1	$s_i(t+1) = s_{i-1}(t) \oplus s_i(t) \oplus s_{i+1}(t)$
규칙 60	1	1	0	$s_i(t+1) = s_{i-1}(t) \oplus s_i(t)$
규칙 90	1	0	1	$s_i(t+1) = s_{i-1}(t) \oplus s_{i+1}(t)$
규칙 102	0	1	1	$s_i(t+1) = s_i(t) \oplus s_{i+1}(t)$
규칙 240	1	0	0	$s_i(t+1) = s_{i-1}(t)$
규칙 204	0	1	0	$s_i(t+1) = s_i(t)$
규칙 170	0	0	1	$s_i(t+1) = s_{i+1}(t)$

<표 2.1> 선형 규칙

여원규칙	의존도			전이 함수
	L	S	R	
규칙 105	1	1	1	$s_i(t+1) = \overline{s_{i-1}(t) \oplus s_i(t) \oplus s_{i+1}(t)}$
규칙 195	1	1	0	$s_i(t+1) = \overline{s_{i-1}(t) \oplus s_i(t)}$
규칙 165	1	0	1	$s_i(t+1) = \overline{s_{i-1}(t) \oplus s_{i+1}(t)}$
규칙 153	0	1	1	$s_i(t+1) = \overline{s_i(t) \oplus s_{i+1}(t)}$
규칙 15	1	0	0	$s_i(t+1) = \overline{s_{i-1}(t)}$
규칙 51	0	1	0	$s_i(t+1) = \overline{s_i(t)}$
규칙 85	0	0	1	$s_i(t+1) = \overline{s_{i+1}(t)}$

<표 2.2> 여원 규칙

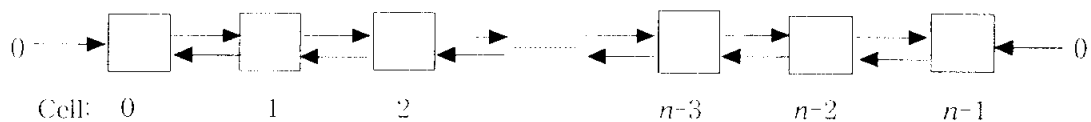
(5) 경계조건에 따른 분류

1차원으로 배열된 CA의 대부분의 셀은 자기 자신을 기준으로 하여 왼쪽과 오른쪽의 인접한 셀을 이웃으로 갖는다. 그러나 양쪽 마지막 두 셀 즉, 가장 왼쪽과 오른쪽의 셀은 자신을 포함하여 2개의 이웃만을 가지므로 세 번째 이웃 셀을 결정해 주어야 한다. 양쪽 끝셀의 세 번째 이웃 셀을 정하는 기준에 따라 다음과 같이 분류된다.

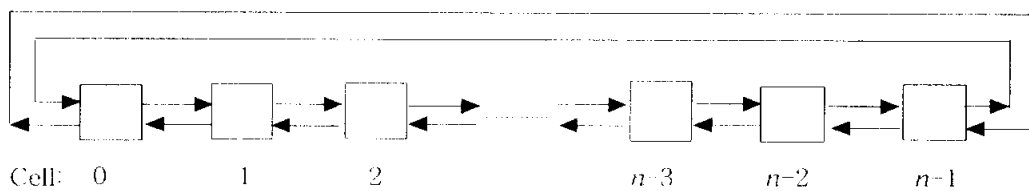
- ① NBCA(Null Boundary CA) : 세 번째 이웃 셀의 상태를 0으로 정의한 CA
- ② PBCA(Periodic Boundary CA) : 양끝의 셀 들이 서로 연결되어 있는 CA
- ③ IBCA(Intermediate Boundary CA) : 첫 번째 셀의 왼쪽 이웃을 세 번째 셀로 정의하고 마지막 셀의 오른쪽 이웃을 마지막 셀로부터 두 번째 왼쪽 셀로 정의한 CA

그림 2.2은 경계조건에 따라 분류된 CA의 연결상태를 나타낸 것이다. 본 논문에

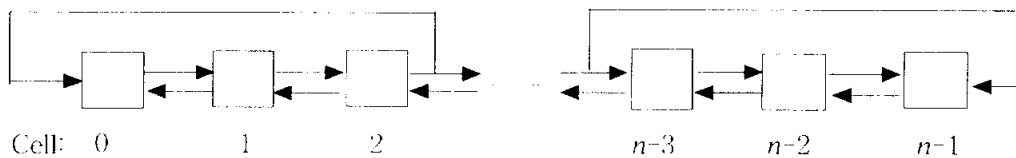
서는 일반적으로 응용이 가장 많이 되는 NBCA만 다룬다.



(1) NBCA



(2) PBCA



(3) IBCA

<그림 2.2> 서로 다른 경계조건을 가지는 CA

2.2. CA의 전이행렬과 특성다항식

2.2.1 CA의 전이행렬

n 개의 셀로 이루어진 n -셀 선형 CA의 상태전이 함수는 선형변환이므로, 이 선형변환을 $n \times n$ 표준행렬로 나타낼 수 있으며, 이를 전이행렬(transition matrix) 또는 특성행렬(characteristic matrix)이라 한다. 전이행렬 $T = (t_{ij})$ 에서 i 번째 행은 i 번째 셀의 규칙을 나타낸다. CA가 다음 상태로 전이될 때 i 번째 셀이 j 번째 셀에 영향을 받으면 $t_{ij} = 1$ 이고 그렇지 않으면 $t_{ij} = 0$ 이다. 3-이웃 NBCA의 전이행렬은 정방행렬의 주 대각선과 그 위 대각선과 아래 대각선을 제외한 나머지가 0인 삼중 대각행렬(tridiagonal matrix)이다. 예를 들어 4-셀 NBCA의 규칙이 $\langle 102, 90, 150, 204 \rangle$ 이면 전이행렬은 다음과 같다.

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

S_t 가 시간 t 에서 CA의 상태를 나타내면 시간 $t+1$ 에서 CA의 상태는 다음과 같다.

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

또한 시간 $t+2$ 에서 CA의 상태는 다음과 같다.

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

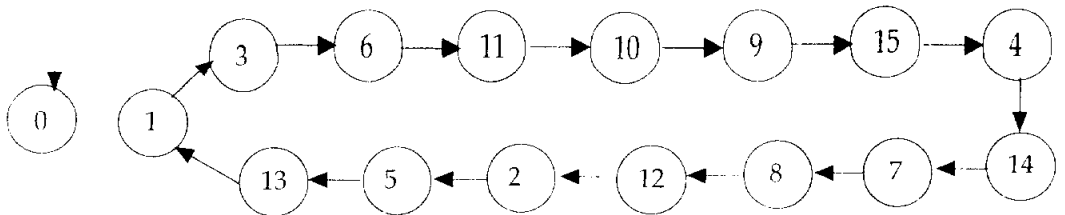
같은 방법으로 p 단계 후의 CA의 상태는

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

이다. CA의 전이행렬 T 가 정칙이면 $GF(2)$ 위에서 $\det(T) = 1$ 이고, 이 CA는 group CA이다. Group CA는 모든 상태들이 일정한 사이클을 이루며 임의의 상태에 대하여 유일한 이전상태를 가진다. 따라서 전이행렬의 역행렬을 구하여 현재 상태에 적용하면 이전상태를 명확하게 얻을 수 있다. 즉,

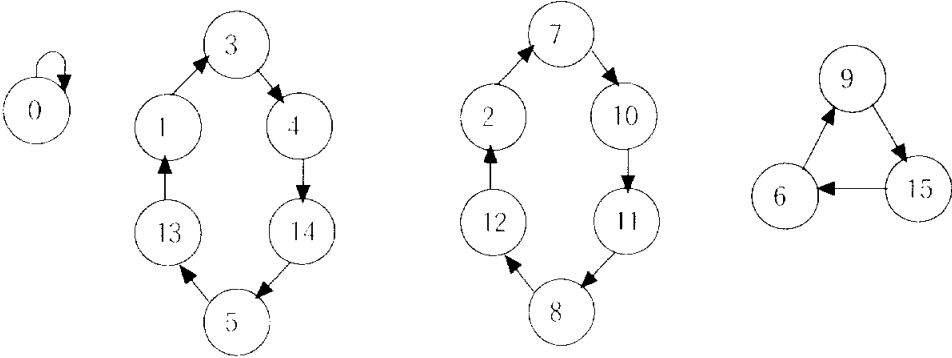
$$S_{t-1} = T^{-1}S_t \quad (2.8)$$

이다. Group CA는 최대길이를 갖는 CA와 최대길이를 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 있는 CA를 최대길이 CA(Maximal length CA, 이하 MLCA)라 한다. 그림 2.3은 전이규칙이 $\langle 150, 150, 90, 150 \rangle$ 인 4-셀 MLCA의 상태전이 그래프이다.



<그림 2.3> 최대길이를 갖는 CA

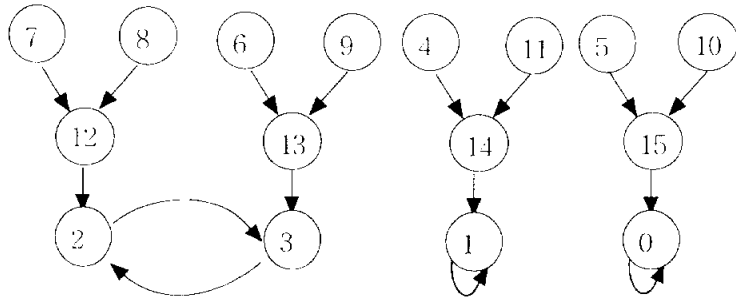
그림 2.4는 최대길이를 가지지 않는 선형 CA로 전이규칙이 <150, 150, 150, 150>인 uniform CA이다. 그림에서 알 수 있듯이 0을 제외한 다른 상태들이 몇 개의 서로 다른 사이클로 분리되어 있다. 각 사이클 길이의 최소공배수 6이 CA의 주기가 된다.



<그림 2.4> 최대길이를 갖지 않는 group CA

Group CA가 아닌 Nongroup CA는 전이행렬 T 가 비정칙이다. 따라서 T 의 역행렬이 존재하지 않으므로 임의의 상태에 대하여 이전상태를 명확하게 알 수 없다. 그림 2.5는 전이규칙이 <150, 60, 60, 150>인 nongroup CA의 상태전이 그래프이다. 이 CA의 전이행렬은 다음과 같고, 상태전이 그래프는 트리 구조를 가진다.

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



<그림 2.5> Nongroup CA

2.2.2 CA의 특성다항식

<정의 2.1> 특성다항식(characteristic polynomial) : 주어진 CA의 전이행렬 T 에 대하여 특성다항식 $C(x)$ 은 GF(2) 위에서 다음과 같다.

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

여기서 I 는 n 차 단위행렬이다.

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

예를 들어 식 2.4의 행렬에 대한 특성다항식을 구하면 다음과 같다.

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

그림 2.3의 전이행렬은

$$T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \tag{2.11}$$

이고, 특성다항식은 $x^4 + x^3 + 1$ 로 GF(2) 위에서 원시다항식이다. n 차 원시다항식 $C(x)$ 는 인수분해되지 않고 $C(x)$ 가 $x^m - 1$ 을 나눌 때, m 의 최소값이 $2^n - 1$ 이다. n -셀 MLCA의 특성다항식은 원시다항식이다.

2.2.3 여원 CA의 정의 및 일반적 성질

이 절에서는 각 셀에 적용되는 규칙이 XOR 논리와 XNOR 논리의 조합으로 표현되는 여원 CA의 정의와 상태들의 전이행동에 관한 분석을 그에 대응하는 선형 CA와 관련지어 살펴본다. 여원 CA의 i 번째 셀에 적용되는 규칙이 여원규칙이면 i 번째 셀의 상태전이 함수는 다음과 같다.

$$\overline{s}_i^{t+1} = f[s_i^{t-1}, s_i^t, s_i^{t+1}] \oplus 1 \quad (2.12)$$

여기서 f 는 여원규칙에 대응되는 선형규칙이다. 여원 CA의 다음 상태를 구하는 연산자를 \overline{T} 라 하면 이를 선형 CA와 관련지어 다음 상태를 구하는 식으로 유도할 수 있다. 여원 규칙에 대응하는 선형 규칙으로 표현한 전이 행렬을 T 라 하고 식 2.12와 같이 결과 값을 역으로 바꾸어야 하는 셀을 나타내는 위치의 성분 값이 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.

$$S_{t+1} = \overline{T}S_t = TS_t \oplus F \quad (2.13)$$

일반적으로 \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.

$$S_{t+p} = \overline{T}^p S_t = T^p S_t \oplus (I \oplus T \oplus T^2 \oplus \dots \oplus T^{p-1}) F \quad (2.14)$$

3. Group 셀룰라 오토마타

Group CA는 LFSR의 대안으로 제안되면서 test pattern generation, 의사 난수열 생성, 오류정정부호의 설계 등에 응용[16, 20, 21, 25, 13, 14, 15]되면서 활발하게 연구되어져왔다. 본 장에서는 group CA의 기본적인 성질을 먼저 알아보고, 상태전이 함수인 전이행렬의 특성다항식으로부터 최소다항식을 구하여 group CA의 상태전이 그래프의 구조인 사이클의 길이와 사이클의 개수를 정확히 유도한다.

3.1 선형 group CA의 성질

전이행렬 T 를 가지는 CA가 cyclic group을 이룬다면

$$f_{t+m}(x) = T^m \cdot f_t(x) = f_t(x) \quad (3.1)$$

인 자연수 m 이 존재한다[9]. 즉, $T^m = I$ 인 T 를 전이행렬로 갖는 CA가 group CA이다.

<정리 3.1> T 가 CA의 전이행렬일 때, 이 CA가 group CA이기 위한 필요충분 조건은 $|T| = 1$ 이다.

<증명>

(\Rightarrow) n 셀 CA가 group CA이면 CA의 상태전이 그래프는 사이클을 이루어야 하므로 CA의 임의의 한 상태 y 에 대하여 $Tx = y$ 인 x 가 유일해야 한다. 그

러므로 T 는 정칙이다. 즉 $|T| = 1$ 이다.

(\Leftarrow) n 셀 CA가 nongroup CA이면 상태 0에 대한 직전자가 2개 이상 존재한다. 즉, $Tx = 0$ 을 만족하는 x 가 2개 이상 존재하므로 $\dim N(T) \geq 1$ 이다. 그러므로 $\text{rank}(T) < n$ 이고 따라서 T 는 정칙이 아니다. 즉, $|T| = 0$ 이다. \square

<정리 3.2[17]> Group CA가 0이 아닌 상태로 시작하면서 길이가 p 또는 p 의 인수인 cycle을 가지는 필요충분조건은 $|T^p \oplus I| = 0$ 이다.

<정리 3.3[17]> T 에 의해 특성화된 group CA의 주기가 소수가 아니면 사이클의 길이는 그것의 인수뿐이다.

3.2 CA의 최소다항식과 CA의 사이클 구조

Group CA는 MLCA 그림 2.3과 그렇지 않는 CA 그림 2.4로 분류될 수 있다. n -셀 MLCA는 0이 아닌 모든 상태가 한 개의 사이클을 이루며 상태가 전이되고 이 사이클의 길이는 $2^n - 1$ 이다. Group CA의 상태전이 그래프에서 사이클의 구조는 CA의 최소다항식에 의해 특성화된다. Group CA의 전이행렬에 대한 최소다항식은 i) 원시다항식인 경우, ii) 원시다항식이 아닌 기약다항식인 경우, iii) 거듭제곱으로 표현되지 않는 다항식들의 곱으로 인수분해되는 경우, iv) 한 기약다항식의 거듭제곱으로 인수분해되는 경우, v) 다항식들의 거듭제곱으로 인수분해되는 경우로 분류된다. 본 절에서는 최소다항식의 유형에 따라 group CA의 상태전이 그래프의 구조, 즉 사이클의 구조를 특성화한다. 그러나 최소다항식의 다섯 번째 유형인 다항식들의 거듭제곱으로 인수분해되는 group CA는

같은 최소다항식에 대하여 주어진 CA의 전이행렬이 다른 경우 서로 다른 사이의 구조를 가지므로 특성화할 수 없다. 다음은 다섯 번째 유형을 제외한 네 가지 유형에 대하여 group CA를 특성화한다.

(1) 최소다항식이 원시다항식인 group CA

<정의 3.1> 다항식의 차수가 n 이고 인수분해되지 않는 다항식을 n 차 기약다항식(irreducible polynomial)이라 한다.

n 차 기약다항식 $f(x)$ 는 $x^{2^n-1} + 1$ 을 나눈다. 그러나 $f(x)$ 가 기약다항식이 아닌 경우는 일반적으로 $x^{2^n-1} + 1$ 를 나누지 않는다. 예를 들어 $f(x) = x^3 + 1 = (x+1)(x^2+x+1)$ 라 하면 $f(x) \nmid x^7 + 1$ 이다.

CA가 최대길이를 갖는지 갖지 않는지는 그 CA의 최소다항식이 원시다항식인지 아닌지와 관계가 있다. 다음은 원시다항식의 정의이다.

<정의 3.2> n 차 다항식 $p(x)$ 가 기약다항식이고 $p(x)$ 가 $x^m + 1$ 을 나누는 최소의 m 의 값이 $2^n - 1$ 일 때 $p(x)$ 를 원시다항식(primitive polynomial)이라 한다.

표 3.1은 GF(2) 상에서 6차까지의 기약다항식과 원시다항식을 나타낸 표이다. 표 3.1에 의하면 $x^4 + x^3 + x^2 + x + 1$ 은 기약다항식이지만 원시다항식은 아니다.

<정리 3.4> n -셀 MLCA의 최소다항식은 n 차 원시다항식이다.

<증명> n 셀 MLCA의 상태전이 그래프는 0과 사이클의 길이가 $2^n - 1$ 인 하나의 사이클을 이룬다. 그러므로 0이 아닌 임의의 상태 x 에 대하여 $T^p x = x$ 인 p 의 최소값이 $2^n - 1$ 이다. 이는 n 셀 MLCA의 최소다항식을 $f(x)$ 라 하면 $\min \{ m: f(x) | x^m - 1 \} = 2^n - 1$ 이어야 하므로 정의 3.2에 의해 $f(x)$ 는 원시다항식이다. \square

차수	기약다항식	원시다항식
1	$x, x + 1$	$x + 1$
2	$x^2 + x + 1$	$x^2 + x + 1$
3	$x^3 + x + 1, x^3 + x^2 + 1$	$x^3 + x + 1, x^3 + x^2 + 1$
4	$x^4 + x + 1, x^4 + x^3 + 1$ $x^4 + x^3 + x^2 + x + 1$	$x^4 + x + 1, x^4 + x^3 + 1$
5	$x^5 + x^2 + 1, x^5 + x^3 + 1$ $x^5 + x^4 + x^2 + x + 1$ $x^5 + x^3 + x^2 + x + 1$ $x^5 + x^4 + x^3 + x + 1$ $x^5 + x^4 + x^3 + x^2 + 1$	$x^5 + x^2 + 1, x^5 + x^3 + 1$ $x^5 + x^4 + x^2 + x + 1$ $x^5 + x^3 + x^2 + x + 1$ $x^5 + x^4 + x^3 + x + 1$ $x^5 + x^4 + x^3 + x^2 + 1$
6	$x^6 + x + 1, x^6 + x^3 + 1$ $x^6 + x^5 + 1$ $x^6 + x^4 + x^2 + x + 1$ $x^6 + x^5 + x^4 + x^2 + 1$ $x^6 + x^5 + x^4 + x + 1$ $x^6 + x^5 + x^2 + x + 1$ $x^6 + x^5 + x^3 + x^2 + 1$ $x^6 + x^4 + x^3 + x + 1$	$x^6 + x + 1$ $x^6 + x^5 + 1$ $x^6 + x^5 + x^4 + x + 1$ $x^6 + x^5 + x^2 + x + 1$ $x^6 + x^5 + x^3 + x^2 + 1$ $x^6 + x^4 + x^3 + x + 1$

<표 3.1> GF(2) 상에서 기약다항식과 원시다항식

최소다항식의 원시다항식인 group CA의 사이클의 구조는 상태 0과 길이가 $2^n - 1$ 인 사이클 하나로 이루어진다. 이를 $[1, 1(2^n - 1)]$ 로 표현한다.

(2) 최소다항식이 원시다항식이 아닌 기약다항식인 group CA

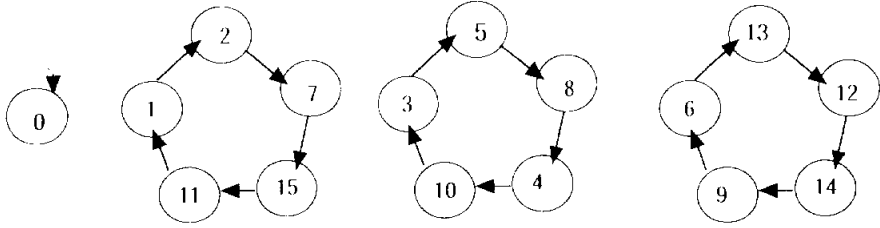
<정리 3.5> $2^n - 1$ 이 소수인 n 차 기약다항식은 원시다항식이다.

<증명> 다항식 $f(x)$ 가 n 차 기약다항식이라 하자. 그러면 $f(x) \mid x^{2^n-1} + 1$ 이다. $2^n - 1$ 이 소수이므로 $x^{2^n-1} + 1$ 은 인수분해되지 않는다. 그러므로 $\min \{ m: f(x) \mid x^m - 1 \} = 2^n - 1$ 이다. 따라서 $f(x)$ 는 원시다항식이다. \square

정리 3.5에 의해 최소다항식이 원시다항식이 아닌 기약다항식을 갖는 CA는 셀의 수 n 에 대해 $2^n - 1$ 이 소수가 아닌 경우에 존재한다. k 가 $2^n - 1$ 의 약수이고 $f(x)$ 가 CA의 최소다항식이라 할 때, $f(x) \mid x^k + 1$ 이면 CA의 0을 제외한 임의의 상태의 사이클의 길이는 k 이고 CA의 상태전이 그래프는 길이가 k 인 사이클을 $\frac{2^n-1}{k} (= N)$ 개 갖는다. 즉, $[1, N(k)]$ 이다.

<예 3.1> 4-셀 CA의 전이규칙이 $\langle 90, 90, 150, 90 \rangle$ 일 때 전이행렬 T 의 최소다항식은 $f(x) = x^4 + x^3 + x^2 + x + 1$ 이고 이는 원시다항식이 아닌 기약다항식이다. 또한 $f(x) \mid x^5 + 1$ 이다. 그러므로 이 group CA의 사이클 길이는 모두 5이고(0 제외) 사이클의 개수는 $15 \div 5 = 3$ 이다. 즉 $[1, 3(5)]$ 이다. 그림 3.1은 주어진

예의 상태전이 그래프이다.



<그림 3.1> 규칙 <90, 90, 150, 90>인 group CA

(3) 최소다항식이 서로 다른 두 개 이상의 기약다항식의 곱인 group CA

Group CA의 최소다항식이 $f(x) = m_1(x) m_2(x) \cdots m_k(x)$ 라 하자 여기서 $m_i(x)$ 는 기약다항식이다. $f(x)$ 에 의해 특성화되는 CA의 모든 상태집합을 전 공간 S 라 하면 각각의 $m_i(x)$ 에 의해 특성화되는 CA의 부분공간 S_i 의 사이클 구조는 $[1, \mu_i(k_i)]$ 이다. 이때 k_i 는 S_i 의 사이클의 길이로 다음과 같다.

$$\min \{ p: m_i(x) \mid x^p + 1 \} = k_i \tag{3.2}$$

$m_i(x)$ 의 차수가 d_i 라 하면 $m_i(x)$ 에 의해 특성화되는 S_i 의 상태의 수는 2^{d_i} (0 포함)이다. 그러므로 S_i 의 사이클 개수 μ_i 는 다음과 같다.

$$\mu_i = \frac{2^{d_i} - 1}{k_i} \tag{3.3}$$

또한 CA의 전공간 S 는 $S_1 \oplus \cdots \oplus S_k$ 에 의해 생성된다. 간단한 설명을 위해 $f(x) = m_1(x) m_2(x)$ 라 하자. 식 3.2와 식 3.3에 의해 $m_1(x)$ 에 의해 특성화되는 부분공간 S_1 의 사이클 구조는 $[1, \mu_1(k_1)]$ 이고, $m_2(x)$ 에 의해 특성화되는 부분공간 S_2 의 사이클 구조는 $[1, \mu_2(k_2)]$ 라 하자. 그러면 CA의 모든 상태로 이루어진 전공간 S 는 $S_1 \oplus S_2$ 에 의해 생성된다. 그러므로 이 CA의 사이클 구조는 다음과 같다.

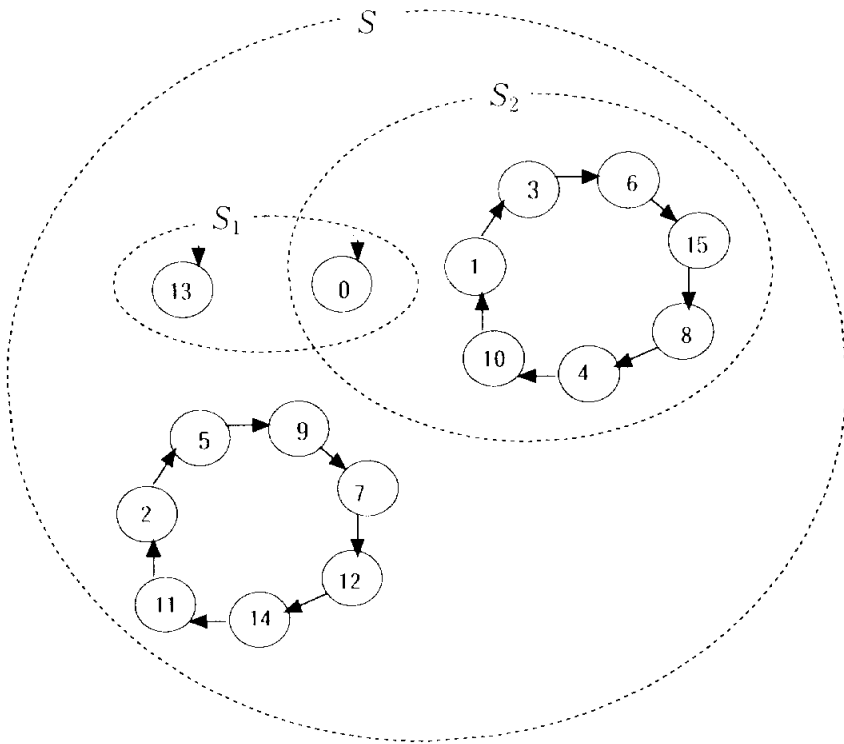
$$\begin{aligned} S_1 \oplus S_2 &= [1 + \mu_1(k_1)][1 + \mu_2(k_2)] = [1 + \mu_1(k_1) + \mu_2(k_2) + \mu_{12}(k_{12})] \\ &= [1, \mu_1(k_1), \mu_2(k_2), \mu_{12}(k_{12})] \end{aligned}$$

여기서 $k_{12} = \text{lcm}(k_1, k_2)$ 이고, $\mu_{12} = \mu_1 \mu_2 \text{gcd}(k_1, k_2)$ 이다.

<예 3.2> 4-셀 CA의 전이규칙이 $\langle 90, 90, 90, 150 \rangle$ 일 때 전이행렬 T 의 최소다항식은 $f(x) = (x+1)(x^3+x+1)$ 이다. 여기서 $m_1(x) = x+1$ 라 하면 $k_1 = 1$ 이고 $\mu_1 = (2^1 - 1) \div 1 = 1$ 이므로 S_1 의 구조는 $[1, 1(1)]$ 이다. 또한 $m_2(x) = x^3+x+1$ 는 원시다항식이므로 $k_2 = 7$ 이고 $\mu_2 = 1$ 이다. 그러므로 CA의 전공간 S 는 다음과 같다.

$$\begin{aligned} S &= [1+1(1)][1+1(7)] = [1+1(7)+1(1)+(1 \times 1 \times \text{gcd}(1,7))(\text{lcm}(1,7))] \\ &= [1+1(1)+1(7)+1(7)] = [1, 1(1), 2(7)] \end{aligned}$$

그림 3.2는 주어진 CA의 상태전이 그래프이다.



<그림 3.2> 규칙 <90, 90, 90, 150>인 group CA

(4) 최소다항식이 한 원시다항식의 거듭제곱인 group CA

Group CA의 최소다항식이 $f(x) = [m(x)]^p$ 라 하자 여기서 $m(x)$ 는 원시다항식이다. $f(x)$ 에 의해 특성화되는 CA의 모든 상태집합을 전공간 S 라 하면 S 는 다음과 같은 영공간이다.

$$S = \{ X | f(T)X = 0 \}$$

$m(x)^i (i \leq p)$ 에 의해 생성되는 S 의 부분공간을 S_i 라 하면 S_i 의 임의의 원소 X 에 대하여 $m(T)^{i+1}X = m(T)\{m(T)^i X\} = m(T) \cdot 0 = 0$ 이므로 $S_i \subset S_{i+1}$ 이다. $m(x)$ 의 차수가 d 일 때 $m(x)$ 에 의해 특성화되는 부분공간 S_1 의 차원은 d 이고 상태 0을 제외한 나머지 상태들은 모두 주기가 $2^d - 1$ 인 한 사이클에 놓인다. 그러므로 S_1 의 사이클 구조는 $[1, 1(2^d - 1)]$ 이다. 일반적으로 S_i 의 차원은 $i \cdot d$ 이다. 또한 S_i 에 속하며 S_{i-1} 에 속하지 않는 원소의 개수는 $2^{id} - 2^{(i-1)d} = 2^{(i-1)d} \cdot (2^d - 1)$ 이다. $m(x)$ 의 주기가 k 이고, $r_i = \min\{a \mid 2^a \geq i\}$ 라 하면 $S_i \setminus S_{i-1}$ 에 속한 상태들의 사이클의 주기 k_i 와 사이클의 개수 μ_i 는 다음과 같다.

$$k_i = k2^{r_i} \tag{3.4}$$

$$\mu_i = \frac{2^{i \cdot d} - 2^{(i-1)d}}{k2^{r_i}} \tag{3.5}$$

이다.

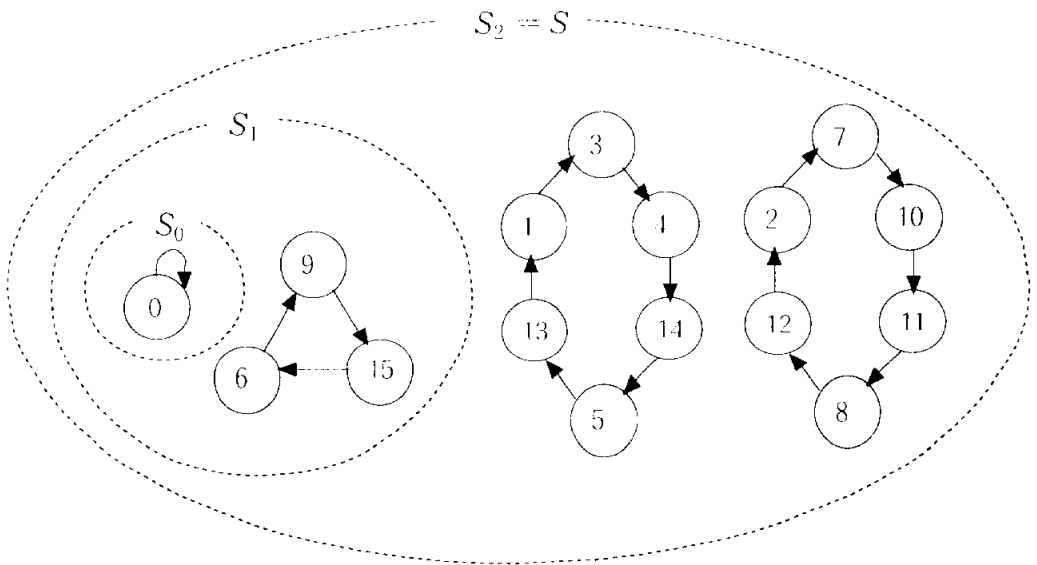
<예 3.3> 전이규칙이 $\langle 150, 150, 150, 150 \rangle$ 인 4-셀 uniform CA를 생각해 보자. 주어진 전이규칙을 따르는 CA의 전이행렬을 T 라 할 때 T 의 최소다항식은 $f(x) = (x^2 + x + 1)^2$ 이다. $f(x)$ 에 의해 특성화되는 전공간 S 는 다음과 같은 부분공간 $S_0, S_1, S_2 (= S)$ 를 포함한다.

$$S_0 = \{X \mid m(x)^0 X = 0\} = \{X \mid I(x) X = 0\} = \{0\}$$

$$S_1 = \{X \mid m(x) X = 0\} = \{0, 6, 9, 15\}$$

$$S_2 = \{X \mid m(x)^2 X = 0\} = \{0, 1, 2, \dots, 15\} = S$$

여기서 $m(x) = x^2 + x + 1$ 이다. $x^2 + x + 1 \mid x^3 + 1$ 이므로 $S_1 \setminus S_0$ 는 사이클의 길이가 3인 1개의 사이클로 표현된다. $S_2 \setminus S_1$ 에 속한 상태의 수는 $2^{2 \cdot 2} - 2^2 = 16 - 4 = 12$ 이다. 식 3.4와 3.5에 의해 사이클의 길이는 $k_2 = 3 \times 2^1 = 6$ 이고 사이클의 개수는 $\mu_2 = 12 \div 6 = 2$ 이다. 그러므로 CA의 전공간 S 의 구조는 $[1, 1(3), 2(6)]$ 이다. 그림 3.3은 주어진 CA의 상태전이 그래프이다.



<그림 3.3> 규칙 <150, 150, 150, 150>인 group CA

4. Nongroup 셀룰라 오토마타

Nongroup CA는 이미지 압축, 해쉬 함수, 부울 방정식의 해법, 암호 알고리즘 등에 응용[1, 2, 6]이 되면서 최근 이에 대한 연구가 활발히 이루어지고 있다. 본 장에서는 nongroup CA의 정의와 자주 사용되는 용어들을 정의하고 nongroup CA의 성질에 대하여 살펴본다.

4.1 선형 Nongroup CA

선형 nongroup CA는 다음 상태를 결정짓는 상태전이 함수가 XOR 논리로만 이루어진 CA로 group CA가 아닌 CA이다. 즉, 사용되는 규칙이 60, 90, 102, 150, 170, 204, 240 이고 상태전이 그래프가 트리 구조를 가지는 CA로 $\det(T) = 0$ 으로 역행렬이 존재하지 않는다. 그러므로 임의의 상태에 대한 이전상태 수는 0 이거나 2 이상이다. 어떤 상태의 이전상태 수가 0이면 도달 불가능한 상태이다. 이전상태수가 2이상이란 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[9].

<정의 4.1> 선형 Nongroup CA(이하 LNCA) : Nongroup CA 중 다음 상태를 결정짓는 상태전이 함수가 XOR 논리만으로 이루어진 CA를 말한다.

<정의 4.2> 순환상태(cyclic state) : Nongroup CA의 상태 중 사이클 안에 존재

하는 상태로 일정한 시간 단계 후 그 상태가 반복되는 상태이다. 상태 y 가 순환 상태이면 $T^k y = y$ 를 만족하는 k 가 존재한다. 여기서 k 의 최소값이 상태 y 가 놓이는 사이클의 길이이다.

<정의 4.3> Attractor : 순환상태들 중 사이클의 길이가 1인 상태로 어떤 상태 x 가 attractor이면 전이행렬 T 에 대하여 $Tx=x$ 를 만족한다

<정의 4.4> 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 4.5> MACA(Multiple-Attractor CA) : Nongroup CA의 모든 순환상태들이 attractor인 CA를 MACA라 한다. 특히 직전자의 수가 2인 MACA를 TPMACA(Two Predecessor Multiple-Attractor CA)라 한다. Attractor의 수가 1인 MACA를 SACA(Single-Attractor CA)라 하며, 직전자의 수가 2인 SACA를 TPSACA라 한다.

<정의 4.6> α -트리 : 순환상태 α 를 root로 하는 트리를 말한다.

<정의 4.7> Depth : Nongroup CA의 상태전이 그래프에서 임의의 도달 불가능한 상태에서 가장 가까운 순환상태로 전이되는데 걸리는 최소 상태전이 수

<정의 4.8> Level : 어떤 상태 x 가 α -트리의 level l ($l \leq \text{depth}$) 상태라고 하면, 상태 x 가 정확히 l 번 상태전이 후 상태 α 가 된다. 즉 $T^l x = \alpha$ 가 되는 l 값 중 최소값이 l 이다.

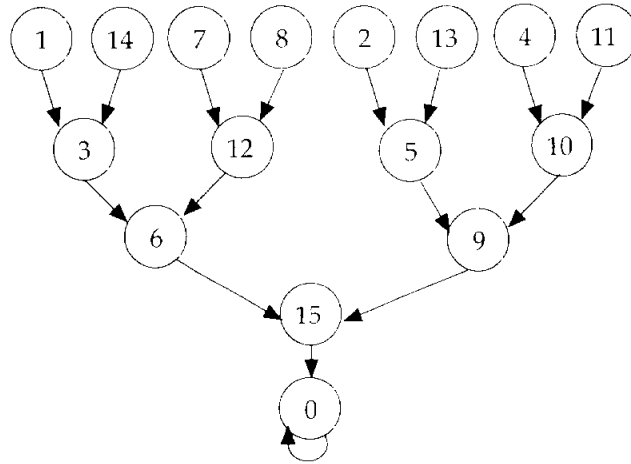
<정의 4.9> 주기 : 상태전이 그래프에서 나타나는 사이클의 길이의 최소공배수로 임의의 순환상태 y 에 대하여 $T^c y = y$ 인 최소의 c 가 주기가 된다.

그림 2.5에서 순환상태는 0, 1, 2, 3 이다. 특히 상태 0과 1은 사이클의 길이가 1이므로 attractor 이다. 상태 2, 3 은 사이클의 길이가 2 인 사이클에 존재한다. 그러므로 이 CA의 주기는 1과 2의 최소공배수인 2이다. 각 트리는 depth가 2 이다. 2-트리는 상태 2를 root로 하는 트리이므로 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 4-cell TPMACA의 예이다.

<예 4.1> 4-셀 CA의 전이규칙이 $\langle 150, 90, 90, 150 \rangle$ 일 때, 전이행렬은

$$T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad (4.1)$$

이고, 특성다항식은 x^4 이며 최소다항식도 x^4 이다. 주어진 T 의 계수(rank)는 3 이다.



<그림 4.1> 4-셀 TPSACA

그림 4.1은 예 4.1에서 주어진 CA에 대한 상태전이 그래프로 TPSACA이다.

4.2 LNCA의 성질

4.2.1 0-트리

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

<정리 4.1> 선형 CA 에서 상태 0 은 attractor 이다.

<증명> 선형 CA에 대응하는 임의의 전이행렬 T 에 대하여 $T0 = 0$ 이다. \square

<보조정리 4.2> LNCA의 전이행렬 T 의 영공간 (null space)의 차원이 r 이면 상태 0의 직전자의 수는 2^r 이다.

<증명> 상태 x 가 상태 0의 직전자라 하면 $Tx=0$ 을 만족한다. T 의 영공간의 차원이 r 이면 이 일차연립방정식은 자유변수가 d 개 존재한다. 각 자유변수가 가질 수 있는 값이 GF(2)에서 0 또는 1이므로 직전자의 수는 2^r 이다. \square

<정리 4.3> LNCA에서 도달 가능한 상태의 직전자의 수는 상태 0의 직전자의 수와 같다.

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

<정리 4.4> LNCA의 상태전이 그래프에서 0-트리의 depth를 d 라 하고 주어진 전이행렬 T 의 영공간의 차원이 r 이면 0-트리는 2^{rd} 개의 상태를 포함한다.

<증명> 전이행렬 T 의 영공간의 차원이 r 이므로 보조정리 4.2와 정리4.3에 의해 임의의 도달가능한 상태의 직전자는 2^r 개다. a_i 를 0-트리의 level i 에 있는 상태 수라 하면 $a_{i+1} = 2^r a_i$ 이다. 0-트리의 level 1에 속한 상태의 수는 상태 0의 0이 아닌 직전자의 수이므로 $a_1 = 2^r - 1$ 이다. 그러므로 depth가 d 인

0-트리의 모든 상태들의 수는 다음과 같다.

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

□

4.2.2 LNCA에서 순환상태들의 트리와 0-트리와의 관계

LNCA의 상태전이 그래프에서 α -트리의 구조는 0-트리와 동형이다[9]. 그러므로 α -트리와 0-트리 사이의 관련성을 밝히는 것은 LNCA의 행동을 분석하는데 있어 매우 중요한 문제이다. 이 절에서는 1차원 LNCA의 0-트리와 $\alpha (\neq 0)$ -트리의 상태들 사이의 관계들을 조사하여 서로 대응되는 상태들을 찾을 수 있고, LNCA를 보다 효율적으로 분석할 수 있음을 보인다. 다음 정리에서 0-트리의 상태의 수를 알 수 있다.

<보조정리 4.5> 도달 가능한 상태의 직전자의 수가 r 인 LNCA에서 상태 0의 i -직전자를 $P_1, P_2, P_3, \dots, P_r$ 라 하고, 도달 가능한 0이 아닌 임의의 상태 X 의 i -직전자중 하나를 X_i 이라 하면 X 의 i -직전자 집합은 다음과 같다.

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

<증명> 우선 B_i 를 상태 0의 i -직전자의 집합이라 하면 집합 B_i 는 다음과 같다.

$B_i = \{Y | T^i Y = 0\} = \{P_1, P_2, \dots, P_r\}$, 여기서 $P_1 = 0$ 이다. 그리고 상태 X 의 i -직전자의 집합을 Q_i 라 하면 $Q_i = \{Y | T^i Y = X\}$ 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 $T^i(X_1 \oplus P_j) = T^i X_1 \oplus T^i P_j = T^i X_1 \oplus 0 = X$ 이므로 $X_1 \oplus P_j$ ($j = 1, 2, \dots, r^i$)가 X 의 i -직전자이다. 그러므로 X 의 i -직전자의 집합 $Q_i = \{X_1 \oplus P_j | j = 1, 2, 3, \dots, r^i\}$ 이다. \square

<정리 4.6> 상태 0의 직전자의 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.

$$X_{ij} = R_i \oplus P_{ij} \tag{4.2}$$

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

<증명> 위 식 4.2를 수학적 귀납법으로 증명한다.

i) $i = 1$ 일 때: 보조정리 4.5에서 i 가 1인 경우이므로 성립.

ii) $i = k$ 일 때: $|\{X_{kj}\}| = |\{R_k \oplus P_{kj}\}|$ 이고 $X_{kj} = R_k \oplus P_{kj}$ 라 하자.

(여기서 $j = 1, 2, \dots, (r-1)r^{i-1}$)

iii) $i = k+1$:

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

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 4.2는 $i=k+1$ 인 경우에도 성립한다. □

위의 정리로부터 다음과 같은 따름 정리를 얻는다.

<따름정리 4.7> 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. □

<정리 4.8> 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 상태라면 $T^p(X_l \oplus X_m) = 0$ 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. □

위의 정리로부터 다음 따름정리를 얻는다.

<따름정리 4.9> 임의의 도달 가능한 상태의 서로 다른 직전자의 합은 상태 0의 0이 아닌 직전자이다.

LNCA의 전이행렬의 최소다항식은 $m(x) = x^d \Phi(x)$ 로 표현된다. 여기서 d 는 CA의 depth가 되고 LNCA의 순환상태의 주기는 $\min\{k | \Phi(x) | x^k + 1\}$ 이다. 그림 2.5의 LNCA의 최소다항식은 $x^1 + x^2 = x^2(x^2 + 1)$ 이다. 그러므로 depth는 2이고 $\Phi(x) = x^2 + 1$ 이다. $\Phi(x)$ 가 나누는 $x^c + 1$ 중 가장 낮은 차수의 다항식은 $x^2 + 1$ 이다. 그러므로 이 CA의 주기는 2이다. 다음 정리는 두 개의 직전자를 갖는 선형 nongroup CA(이하 TPLNCA)의 사이클의 구조를 분석한 것이다.

<정리 4.10> 선형 TPNCA에서 $R_1 \rightarrow R_2 \rightarrow \dots \rightarrow R_n \rightarrow R_1$ 이 길이가 n 인 사이클이고 β 가 attractor이면 $R_1 \oplus \beta \rightarrow R_2 \oplus \beta \rightarrow \dots \rightarrow R_n \oplus \beta \rightarrow R_1 \oplus \beta$ 도 길이가 n 인 사이클이다.

<증명> $TR_i = R_{i+1}$, ($i = 1, 2, \dots, n-1$), $TR_n = R_1$ 이고 β 가 attractor 이므로

$$T(R_i \oplus \beta) = TR_i \oplus T\beta = R_{i+1} \oplus \beta, \quad i = 1, 2, \dots, n-1$$

이고

$$T(R_n \oplus \beta) = TR_n \oplus T\beta = R_1 \oplus \beta$$

이다.

따라서 $R_1 \oplus \beta \rightarrow R_2 \oplus \beta \rightarrow \dots \rightarrow R_n \oplus \beta \rightarrow R_1 \oplus \beta$ 도 길이가 n 인 사이클이다.

□

4.2.3 선형 TPMACA

선형 TPMACA 는 LNCA 중 모든 순환상태들이 attractor이고 임의의 도달 가능한 상태에 대하여 적전자의 수가 2개인 CA를 말한다. 특별히 TPSACA는 완전 해쉬함수를 만드는데 효과적이다. 다음은 TPMACA의 성질들을 살펴본다.

<정리 4.11> n 셀 선형 TPMACA의 전이행렬 T 의 영공간의 차원은 1 이다.

<증명> TPMACA의 임의의 도달 가능한 상태에 대한 직전자의 수는 2이다.

α 를 임의의 도달 가능한 상태라고 하면 $|\{y \mid Ty = \alpha\}| = 2$ 이고 정리 4.3에 의하여 $|\{y \mid Ty = \alpha\}| = |\{x \mid Tx = 0\}|$ 이다. $Tx = 0$ 을 만족하는 해의 수가 2^1 이므로 자유변수 개수가 1이다. 따라서 T 의 영공간의 차원은 1 이다. \square

예 4.1에서 T 의 계수가 3이므로 영공간의 차원은 1이다. 그러므로 임의의 도달 가능한 상태의 직전자의 수는 2이다. 또한 MACA는 주기가 1이므로 최소다항식 $x^d \Phi(x)$ 에서 $\Phi(x) = x+1$ 이다. 그러므로 트리의 depth가 d 인 선형 TPMACA의 최소다항식은 $x^d(x+1)$ 이다.

<정리 4.12> n 셀 선형 TPMACA의 $(T \oplus I)$ 의 계수가 k 이면 attractor의 수는 2^{n-k} 이다.

<증명> 어떤 상태 x 가 attractor 이면 이 순환상태 x 의 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 라면 영공

간의 차원은 $n-k$ 이므로 가능한 해의 수는 2^{n-k} 이다. □

<정리 4.13> 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 4.7에 의하여

$$\alpha_{ij} = P_{ij} \oplus \alpha \text{ 이고, } \beta_{ij} = P_{ij} \oplus \beta \text{ 이다. 그러므로 } \alpha_{ij} \oplus \beta_{ij} = P_{ij} \oplus \alpha \oplus P_{ij} \oplus \beta = \alpha \oplus \beta \quad \square$$

<예 4.2> 5개의 셀로 이루어진 CA에 적용된 전이규칙이 $\langle 102, 102, 60, 240, 60 \rangle$ 이면 전이행렬 T 는 다음과 같다.

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

일차독립인 행의 수가 4이므로 $\text{rank}(T) = 4$ 이다. 그러므로 T 의 영공간의 차원은 1이다. 그러므로 주어진 선형 CA는 2개의 직전자를 가지는 nongroup CA이다. $(T \oplus I)$ 를 구하면 다음과 같다.

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

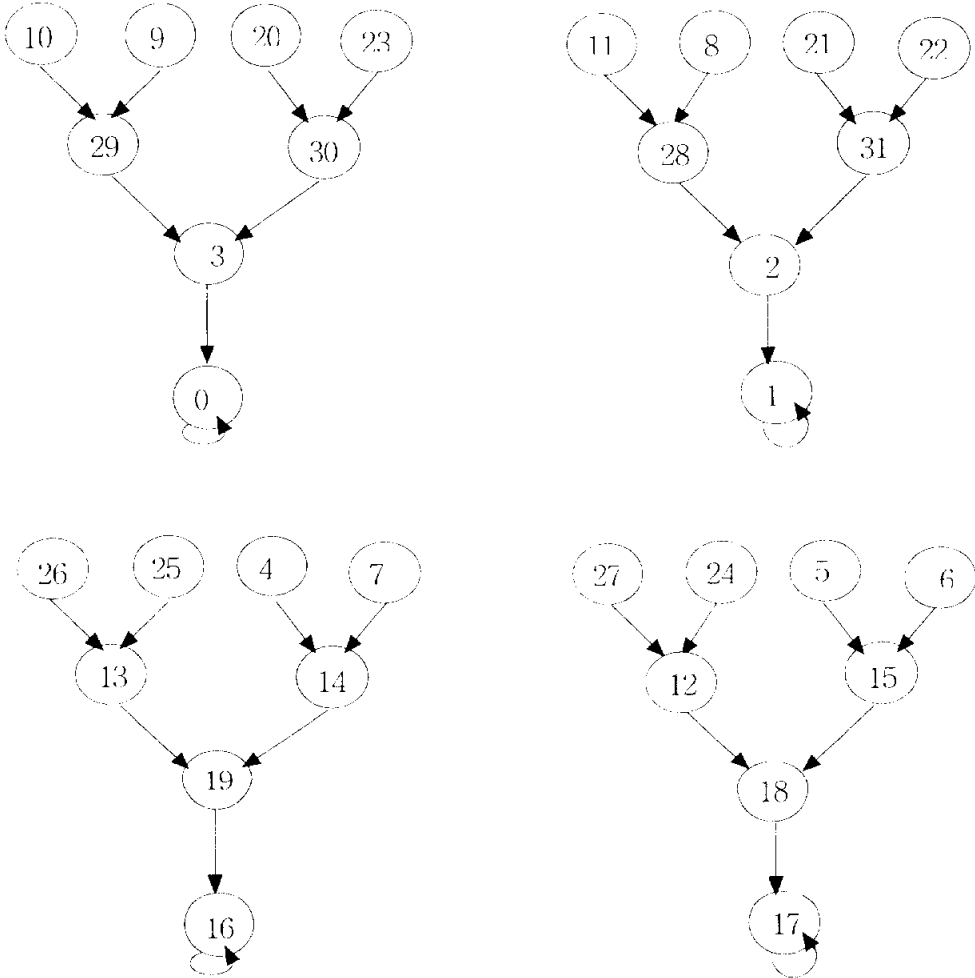
$(T \oplus I)$ 의 계수는 3이다. 그러므로 attractor의 수는 $2^{5-3} = 2^2 = 4$ 이다. 또한 T 의 최소다항식은 $m(x) = x^3(x+1)$ 이다. 그러므로 이 선형 CA는 depth가 3이고 attractor가 4개인 선형 TPMACA이다. 그림 4.2는 이 TPMACA의 상태전이 그래프이다. 1-트리의 level 2의 첫 번째 상태인 28=(11100)과 17-트리의 level 2의 첫 번째 상태 12=(01100)의 합은 $11100 \oplus 01100 = 10000 = 16$ 이다. 이는 상태 1과 상태 17의 합인 $00001 \oplus 10001 = 10000 = 16$ 과 같다. 상태 19의 서로 다른 두 직전자 13(01101)과 14(01110)의 합은 $01101 \oplus 01110 = 00011 = 3$ 으로 상태 0의 0이 아닌 직전자 3과 같다.

선형 TPSACA는 예 4.1과 그림 4.1에서와 같이 임의의 한 도달 가능한 상태에 대하여 서로 다른 두 개의 직전자를 가지며 상태 0만 순환상태인 선형 TPMACA를 말한다. n -셀 선형 TPSACA의 전이행렬 T 의 계수는 $(n-1)$ 이고, 최소다항식은 x^n 이다. TPSACA의 상태전이 그래프는 depth가 n 인 한 개의 이진트리로 나타난다.

<정리 4.14> 선형 TPMACA에서 w 와 u 를 임의의 한 도달 가능한 상태의 서로 다른 직전자라 하고 P_1 을 상태 0의 0이 아닌 직전자라고 하면 다음이 성립한다.

$$w \oplus u = P_1$$

<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. □



<그림 4.2> 5-셀 선형 TPMACA C의 상태전이 그래프

4.3 LNCA로부터 유도된 여원 CA의 상태 행동 분석

여원 CA에서 여원 벡터 F 는 CA의 크기와 같은 n 차원 벡터이다. 그러므로 이 벡터의 종류는 모든 성분이 0 인 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 LNCA의 상태전이 그래프에 놓이는 위치에 따라 여러 가지 행동패턴을 보인다. 이렇게 같은 전이행렬을 가지는 선형 CA를 여원 CA에 대응하는 CA라고 하고, 여원 CA는 선형 CA로부터 유도된 여원 CA라 한다. 이 절에서는 선형 TPMCA와 같은 전이행렬을 가지는 여원 CA에 대하여 연구한다.

4.3.1 선형 TPMACA로부터 유도된 여원 CA

<정리 4.15> 여원 CA 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>

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

$$x' = Ty \oplus F \quad (4.3)$$

따라서

$$x = x' \oplus F = (Ty \oplus F) \oplus F = Ty \quad \text{「 식 4.3에 의하여 」}$$

그러므로 x 는 C 에서 도달 가능한 상태이다.

(\Leftarrow) 같은 방법으로 x 가 C 에서 도달 가능한 상태이므로 $x = Ty$ 인 y 가 존

재한다. 따라서 $x' = x \oplus F = Ty \oplus F$ 이다. 그러므로 x' 은 C' 에서 도달 가능한 상태이다. \square

위의 정리로부터 다음 따름정리를 얻는다.

<따름정리 4.16> 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 4.17> 선형 TPMACA C 로부터 유도되는 여원 CA의 도달 가능한 상태에 대한 직전자의 수는 2이다.

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

$$Ty_1' \oplus F = Ty_2' \oplus F = \dots = Ty_p' \oplus F = x' = (x' \oplus F) \oplus F$$

이고, $Ty_1' = Ty_2' = \dots = Ty_p' = x' \oplus F = x$ 이다. 그러므로 x 는 C 에서 도달 가능한 상태이고 x 는 가정에 의해 2개의 직전자를 가지므로 $p = 2$ 이다. \square

여원 CA의 depth는 이에 대응하는 선형 CA의 depth와 같고, 정리 4.17에 의해 임의의 도달 가능한 상태의 직전자의 수가 여원 CA에 대응하는 선형 CA의 직전자의 수와 같으므로 여원 CA의 순환상태를 root로 하는 트리는 선형 CA의 트리와 그 구조가 같음을 알 수 있다. 그러므로 선형 TPMACA로부터 유도되는 여원 CA는 여원 TPNCA이다.

다음 정리는 여원 CA의 임의의 도달 가능한 상태의 직전자들의 관계를 밝힌다.

<정리 4.18> TPMACA C 에 대응하는 여원 CA C' 의 임의의 도달 가능한 상태의 서로 다른 두 직전자의 합은 C 의 상태 0의 0이 아닌 직전자이다.

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

$$\begin{aligned} \overline{Tx_i} &= \overline{Ty_i} \\ \Rightarrow Tx_i \oplus F &= Ty_i \oplus F \\ \Rightarrow Tx_i \oplus F \oplus Ty_i \oplus F &= 0 \\ \Rightarrow T(x_i \oplus y_i) &= 0 \end{aligned}$$

그런데 $x_i \neq y_i$ 이므로 $x_i \oplus y_i \neq 0$ 이다. 그러므로 $x_i \oplus y_i$ 는 C 의 상태 0의 0이 아닌 직전자이다. □

선형 TPMACA로부터 유도되는 여원 TPNCA는 여원벡터 F 가 선형 TPMACA의 상태전이 그래프에서 어떤 위치에 있느냐에 따라 여원 TPNCA는 이 상태전이 행동이 다르다. n 셀 선형 TPMACA의 각 셀의 상태를 역으로 바꾸는 여원벡터를 F 라 할 때, 이 F 는 n 차원 벡터이며 선형 CA의 셀 값을 역으로 취하고자 하는 셀의 위치성분이 1이다. 이 여원벡터를 선형 TPMACA의 한 상태로 보았을 때 F 가 상태전이 그래프에서 위치한 곳에 따라 세가지 유형으로 나눌 수 있다. 다음은 이 세가지 경우에 대하여 여원 TPNCA의 상태전이 그래프

에서 나타나는 성질들을 분석하고 예를 든다.

4.3.1.1 여원벡터가 선형 TPMACA의 0-트리의 비순환상태인 여원 TPNCA

이 절에서는 선형 TPMACA로부터 유도된 여원을 갖는 CA의 행동을 분석하는데 특히 여원벡터 F 가 0-트리에서 0이 아닌 상태인 여원 CA의 행동을 밝히도록 한다.

<보조정리 4.19> LNCA의 전이행렬이 T 이고 그에 대응하는 여원을 갖는 CA에서 연산자 \overline{T} 를 p 번 적용한 것을 \overline{T}^p 라 하자. 그러면

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

<증명> 식 2.14에 의해 명백하다. □

<보조정리 4.20> C 는 depth가 d 인 TPMACA이고, 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 attractor이다.

<증명> x 가 C' 에서 attractor이면 $\overline{T}'x = x$ 임을 보이면 된다. 보조정리 4.19에 의하여 $\overline{T}(\overline{T}^{i-1}F)$ 는 다음과 같다.

$$\begin{aligned}
\overline{T}(\overline{T^{i-1}F}) &= T(\overline{T^{i-1}F}) \oplus F \\
&= T([I \oplus T \oplus T^2 \oplus \dots \oplus T^{i-2} \oplus T^{i-1}]F) \oplus F \\
&= [T \oplus T^2 \oplus \dots \oplus T^{i-1} \oplus T^i]F \oplus F \\
&= [I \oplus T \oplus T^2 \oplus \dots \oplus T^{i-1}]F \oplus T^i F \\
&= \overline{T^{i-1}F} \oplus 0 = \overline{T^{i-1}F}
\end{aligned}$$

따라서 $\overline{T^{i-1}F}$ 는 C' 에서 attractor 이다. □

<정리 4.21> C 가 TPMACA 이고 C 에 대응하는 여원을 갖는 CA를 C' 이라 하고 어원벡터 F 를 C 의 0 트리의 level l 에 있는 비순환상태로 택하면 다음이 성립한다.

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

$$\begin{aligned}
\overline{T^k x} &= T^k x \oplus (T^{k-1} \oplus \dots \oplus T^l \oplus T^{l-1} \oplus \dots \oplus T \oplus I)F \\
&= T^k x \oplus (T^{l-1} \oplus \dots \oplus T \oplus I)F \\
&\quad (\text{모든 } i > l-1 \text{ 에 대해 } T^i F = 0 \text{ 이므로})
\end{aligned}$$

$$\begin{aligned}
&= 0 \oplus (T^{l-1} \oplus \dots \oplus T \oplus I)F \\
&\quad (x \text{가 level } k (> l) \text{의 상태이므로}) \\
&= (T^{l-1} \oplus \dots \oplus T \oplus I)F \\
&= \overline{T}^{l-1}F
\end{aligned}$$

그런데 보조정리 4.20에 의해 $\overline{T}^{l-1}F$ 이 \mathbb{C}' 의 attractor이므로 x 의 level은 k 보다 작거나 같다. 한편

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

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

(2) z 를 \mathbb{C} 에서 0 트리의 level l 에 있는 상태라 하자. 선형 TPMACA는 도달 가능한 상태의 직전자의 수가 2이므로 $T^{l-1}z = T^{l-1}F$ 와 $T^l z = T^l F = 0$ 이 성립한다.

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

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

러므로 z 는 C' 에서 level l 보다 낮은 level에 배열된다.

(3) w 를 C 에서 l 보다 작은 level에 있는 상태라 하면 $T^l w = T^{l-1} w = 0$ 이다. 그리고

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

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

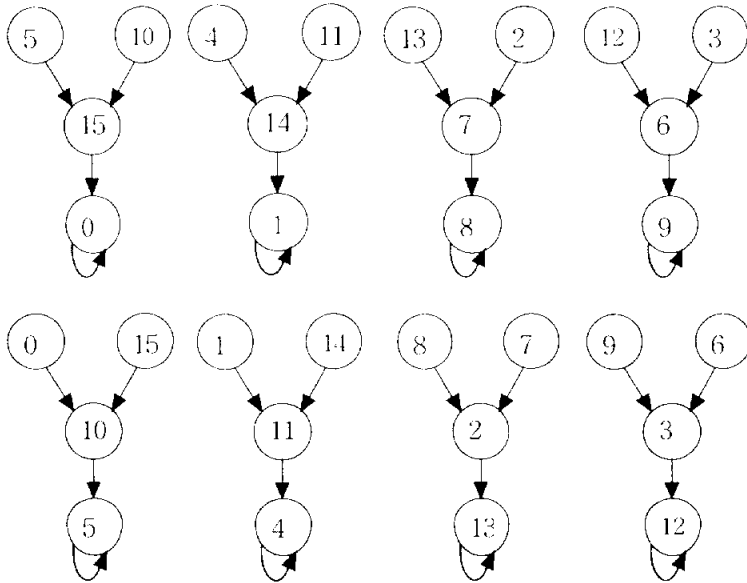
이 성립한다. 그러므로 $\overline{T}^{l-1} F$ 은 C' 의 attractor이지만 $\overline{T}^{l-2} F$ 은 C' 의 attractor가 아니므로 w 는 level l 에 배열된다.

(4) (3)에 의하여 상태 0은 C 에서 level l 에 있다. $\overline{T}0 = T0 \oplus F = F$ 이므로 F 는 C' 에서 상태 0보다 한 단계 낮은 level $l-1$ 에 배열된다. \square

<예 4.3> 4개의 셀로 이루어진 CA에 적용된 전이규칙이 $\langle 102, 102, 60, 60 \rangle$ 일 때, 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 4.3은 주어진 TPMACA의 상태전이 그래프와 0 트리의 level 2에 있는 비순환상태 10(1010)이 여원벡터 $F = (1\ 0\ 1\ 0)^T$ 일 때 선형 TPMACA로부터 얻어지는 여원 TPNCA의 상태전이 그래프이다.



<그림 4.3> 4-셀 TPMACA C와 C'의 상태전이 그래프

$\overline{T}^{2^{-1}}F = TF \oplus F = (1111)^T \oplus (1010)^T = (0101)^T = 5$ 는 C'에서 attractor이다(보조정리 4.20). 또한 C에서 level 2에 있는 모든 상태 (5, 10, 4, 11, 13,

2, 12, 3)는 C' 에서 level이 2보다 작은 위치에 배열되었고, C 에서 level 이 2보다 작은 모든 상태 (15, 14, 7, 6, 0, 1, 8, 9)는 C' 에서 level 2에 배열되었으며, 상태 F 는 C' 에서 level 1에 배열되었다(정리 4.21). 한편 C' 에서 상태 2의 두 직전자 $8(1000)^T$ 과 $7(0111)^T$ 의 합 $(11111)^T$ 은 C 의 상태 0의 0이 아닌 직전자인 15이다(정리 4.18).

4.3.1.2 여원벡터가 선형 TPMACA의 0 아닌 트리의 비순환상태인 여원 TPNCA

이 절에서는 선형 TPMACA C 로부터 유도되는 여원 TPNCA C' 중 특별히 여원벡터 F 가 0-트리를 제외한 임의의 트리의 비순환상태인 경우에 대하여 살펴본다. 여원벡터가 선형 TPMACA의 α -트리의 비순환상태라 하면 선형 TPMACA의 0-트리와 α -트리가 여원 TPNCA의 상태전이 그래프에서 서로 결합하고 선형 TPMACA의 나머지 트리들도 attractor의 합이 α 가 되는 것끼리 여원 TPNCA에서 결합이 되고 여원벡터가 0-트리의 비순환상태인 경우와 달리 각 트리의 비순환상태들도 여원 TPNCA에서 트리 사이의 이동이 일어난다.

<보조정리 4.22> 여원벡터 F 가 TPMACA C 의 α -트리의 level i 의 상태라 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

$\overline{T}^2 S = S$ 임을 보이자. 보조정리 4.19에 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 $T^i F = \alpha$ 이다.

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

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

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

<보조정리 4.23> 여원벡터 F 가 TPMACA \mathbb{C} 의 α -트리 of level i 의 상태라 하면 $\alpha \oplus \overline{T}^{i-1} F$ 는 \mathbb{C}' 에서 $\overline{T}^{i-1} F$ 와 같은 사이클에 놓인다.

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

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

$$\begin{aligned}
\text{i) } \overline{TS} &= TS \oplus F \\
&= T(T^i \oplus T^{i-1} \oplus \dots \oplus T \oplus I)F
\end{aligned}$$

$$\begin{aligned}
&= T^{i+1}F \oplus T^iF \oplus (T^{i-1} \oplus \dots \oplus T \oplus I)F \\
&= \overline{T}^{i-1}F \quad [\because T^{i+1}F = T^iF = \alpha_1] \\
&= S
\end{aligned}$$

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

「식 4.5에 의해」

□

<보조정리 4.24> 여원벡터 F 가 TPMACA C 의 α -tree 의 level i 의 상태라 하고 β 를 C 의 attractor 라 하면 상태 $(\beta \oplus \overline{T}^{i-1}F)$ 는 C 에 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 $\overline{TS} \neq S$ 이고 $\overline{\overline{T}^2S} = S$ 임을 보이면 된다.

$$\begin{aligned}
\overline{T}^{i-1}F &= \overline{T}^{i-1}F \oplus (T^{i-2} \oplus T^{i-3} \oplus \dots \oplus T \oplus I)F \\
&= (T^{i-1} \oplus T^{i-2} \oplus \dots \oplus T \oplus I)F
\end{aligned} \tag{4.6}$$

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

$$i) \quad \overline{TS} = TS \oplus F$$

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

$$= T\{\beta \oplus (T^{i-1} \oplus T^{i-2} \oplus \dots \oplus T \oplus I)F\} \oplus F$$

「식 4.6에 의하여」

$$= T\beta \oplus T^iF \oplus (T^{i-1} \oplus T^{i-2} \oplus \dots \oplus T \oplus I)F$$

$$= \beta \oplus \alpha \oplus \overline{T}^{i-1}F \quad (4.7)$$

$$\neq \beta \oplus \overline{T}^{i-1}F \quad \because \alpha \neq 0$$

$$\text{ii) } \overline{T}^2S = T(\overline{TS}) \oplus F$$

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

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

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

$$= \beta \oplus \alpha \oplus \alpha \oplus \overline{T}^{i-1}F$$

$$= \beta \oplus \overline{T}^{i-1}F$$

$$= S$$

□

<정리 4.25> 여원벡터 F 가 \mathbb{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 \mathbb{C}' 에서 같은 사이클에 놓이고 이 사이클의 길이는 2이다.

<증명> 보조정리 4.24로부터 $\beta \oplus \overline{T}^{i-1}F$ 는 \mathbb{C}' 에서 길이가 2인 사이클에 놓인다. 이 사이클을 j 라 하자. 먼저

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

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

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

$$= \beta \oplus \alpha \oplus \alpha \oplus \overline{T}^{i-1}F$$

$$= \beta \oplus \overline{T}^{i-1}F$$

$$= \beta \oplus \alpha \oplus \overline{T}^{i-1}F \quad (4.8)$$

그리고

$$\begin{aligned} & \overline{T}^2 (\beta \oplus \alpha \oplus \overline{T}^{i-1}F) \\ &= T \{ \overline{T} (\beta \oplus \alpha \oplus \overline{T}^{i-1}F) \} \oplus F \\ &= T(\beta \oplus \overline{T}^{i-1}F) \oplus F \quad \text{「 식 4.8에 의해 」} \\ &= \beta \oplus \alpha \oplus \overline{T}^{i-1}F \quad \text{「 식 4.7에 의해 」} \end{aligned}$$

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

<따름정리 4.26> 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.)

다음 정리는 선형 TPMACA로부터 유도되는 여원 CA 중 여원벡터 F 가 0이 아닌 α 트리의 level i 의 상태일 때 여원 CA의 상태 배열에 대한 정리이다.

<정리 4.27>

(1) 상태 x 가 C 에서 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 C 에서 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 \mathbb{C} 에서 α -트리의 level i 상태이므로 $T^{i+j-1}F = \dots = T^iF = \alpha$ 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 0이다. 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 0이다.

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 4.11에 의하여 $T^{i+j-1}x \oplus \overline{T}^{i-1}F$ 는 순환상태가 아니다. 그러므로 x 는 \mathbb{C} 에서 $\overline{T}^{i-1}F$ -트리의 level $(i+j)$ 에 놓인다.

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

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

$$= \alpha \oplus \alpha \oplus \cdots \alpha \oplus \overline{T}^{i-1}F$$

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 $(\alpha \oplus \overline{T}^{i-1}F)$ -트리의 level $(i+j)$ 상태에 놓인다. □

이제 위 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 4.28>

- (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 level $(i+j)$ 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 level $(i+j)$ 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> F가 선형 TPMACA C의 α -트리의 level i 의 상태이므로 $T^{i+j-1}F \dots \dots = T^i F = \alpha$ 이다.

(1) 가정에 의하여 $T^{i+j}x = \beta$ 이다.

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

(여기에서 α 의 수는 j 개로 홀수이다.)

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

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

(여기에서 α 의 수는 $j-1$ 개로 짝수이다.)

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

$T^{i+j-1}x$ 는 C에서 β 의 β 가 아닌 직전자이므로 $T^{i+j-1}x$ 는 0도 α 도 아니다. 따라서 $\overline{T}^{i+j-1}x$ 는 순환상태가 아니다.

그러므로 x 는 C에서 $(\beta \oplus \alpha \oplus \overline{T}^{i-1}F)$ -트리의 level $(i+j)$ 상태가 된다.

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

(여기에서 α 의 수는 j 개로 짝수개이다.)

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

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

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

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

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

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

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

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

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. 정리 4.13에 의하여

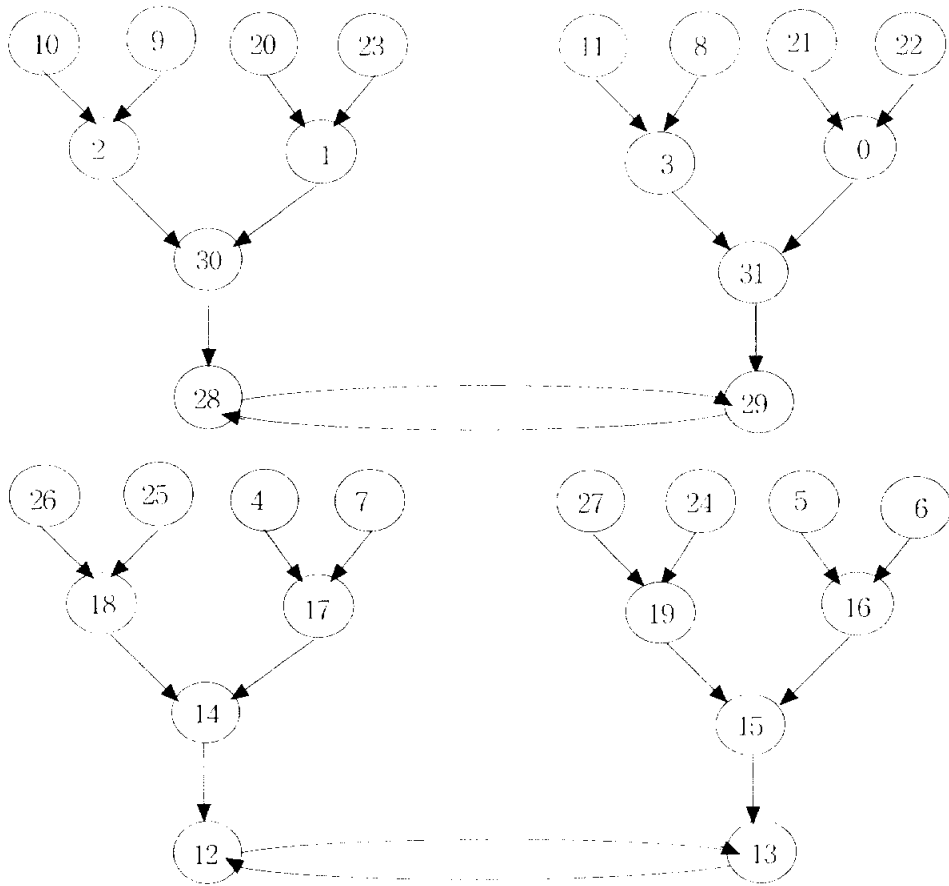
$$T^{i-1}F \oplus T^{i-1}z = \alpha \oplus \beta \text{이고 } T^{i-1}z = \alpha \oplus \beta \oplus T^{i-1}F$$

이다.

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

그러므로 z 는 C' 에서 level $i-1$ 이하에 놓인다. □

<예 4.4> 그림 4.4는 그림 4.2의 5-셀 선형 TPMACA로부터 유도된 여원 TPNCA이다. 여원벡터 F 를 선형 TPMACA의 1-트리의 level 2에 있는 비순환상태 $31 = (11111)^T$ 로 두었을 때 선형 TPMACA ζ 로부터 얻어지는 여원 CA C' 의 상태전이 그래프이다. C 에서 0-트리와 1-트리가 서로 결합하고(보조정리 4.23), 나머지 16-트리와 17-트리가 결합한다(정리 4.25). 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' 에서 level 2에 놓이고 C 에서 level 2의 상태는 C' 에서 level 2보다 낮은 level에 놓인다(정리 4.28). C' 에서 한 사이클에 놓여 있는 상태들의 합($29 \oplus 28, 12 \oplus 13$)은 여원벡터가 있던 트리의 attractor인 상태 1과 같다(따름정리 4.26).



<그림 4.4> 선형 TPMACA로부터 얻어지는 여원 CA C' (여원벡터 : 31)

4.3.1.3 여원벡터가 선형 TPMACA의 0이 아닌 attractor인 여원 CA

이 절에서는 여원벡터의 위치에 따라 분류된 여원 CA 가운데 마지막인 여원벡터가 선형 TPMACA의 0이 아닌 attractor인 경우에 대하여 분석한다.

<보조정리 4.29> 여원벡터 F 가 선형 TPMACA C 의 0이 아닌 attractor라 하면

상태 0은 C 에 대응하는 여원 $CA \subset C'$ 에서 순환상태이다. 또한 그 사이클의 길이는 2이다.

<증명> F 가 C 에서 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 $CA \subset C'$ 의 순환상태이고 그 사이클의 길이는 2이다.

[]

<보조정리 4.30> 여원벡터 F 가 선형 TPMACA C 에서 0이 아닌 attractor α 라 하면 α 는 C 에 대응하는 여원 $CA \subset C'$ 에서 상태 0을 포함하는 길이가 2인 사이클에 놓이게 된다.

<증명> 가정에 의하여 $F = \alpha$ 이다.

$$\begin{aligned} \overline{T}\alpha &= T\alpha \oplus F \\ &= T\alpha \oplus \alpha \quad [F = \alpha] \\ &= \alpha \oplus \alpha \quad [T\alpha = \alpha, \because \alpha \text{는 } C \text{에서 attractor}] \\ &= 0 \end{aligned}$$

$$\overline{T}^2\alpha = T^2\alpha \oplus (T \oplus I)F$$

$$- a \oplus (T \oplus I) a$$

$$- a \oplus T a \oplus a$$

$$- a$$

따라서 a 는 C' 에서 상태 0을 포함하는 사이클의 순환상태이다. \square

<정리 4.31> 여원벡터 F 가 선형 TPMACA C 에서 0이 아닌 attractor a 라 하고 β 를 또 다른 attractor 라 하면

(1) $\beta \oplus a$ 또한 C 의 attractor 이다.

(2) β 와 $\beta \oplus a$ 는 C 에 대응하는 여원 CA C' 에서 길이가 2인 같은 사이클에 놓이게 된다.

<증명>

(1) a 와 β 가 attractor이므로 $T a = a$ 이고 $T \beta = \beta$ 이다.

$T(a \oplus \beta) = T a \oplus T \beta = a \oplus \beta$ 이므로 $a \oplus \beta$ 는 attractor이다.

(2) $\overline{T} \beta = T \beta \oplus F = T \beta \oplus a = \beta \oplus a \neq \beta$ 이고

$$\begin{aligned} \overline{T}^2 \beta &= T^2 \beta \oplus (T \oplus I) F = \beta \oplus (T \oplus I) a \\ &= \beta \oplus T a \oplus a = \beta \oplus a \oplus a \\ &= \beta \end{aligned}$$

그러므로 β 와 $\beta \oplus a$ 는 길이가 2인 같은 사이클에 놓이게 된다. \square

<정리 4.32> 여원벡터 F 가 선형 TPMACA C 에서 0이 아닌 attractor a 라 하고 x 가 β -트리의 level $2m$ 인 상태라면 x 는 C' 에서도 β -트리의 level $2m$

에 놓인다.

<증명> \mathbb{C} 에서 β -트리 of level 1에 있는 상태를 $B_{1,0}$ 라 하자. 먼저

$$\begin{aligned} \overline{T}^{2m} x &= T^{2m} x \oplus (T^{2m-1} \oplus T^{2m-2} \oplus \dots \oplus I) F \\ &= \beta \oplus T^{2m-1} F \oplus \dots \oplus T F \oplus F \\ &= \beta \end{aligned}$$

이므로,

$$\begin{aligned} \overline{T}^{2m-1} x &= T^{2m-1} x \oplus (T^{2m-2} \oplus T^{2m-3} \oplus \dots \oplus I) F \\ &= B_{1,0} \oplus T^{2m-2} F \oplus \dots \oplus T F \oplus F \\ &= B_{1,0} \oplus F \end{aligned}$$

이다. 그런데 $B_{1,0} \neq 0$, $B_{1,0} \neq F$. 그리고 $B_{1,0} \neq \beta$ 이다.

그러므로 $B_{1,0} \oplus F$ 는 \mathbb{C}' 에서 비순환상태이다. 따라서 x 는 \mathbb{C}' 의 β -트리의 level $2m$ 에 놓인다. □

<정리 4.33> 여원벡터 F 가 선형 TPMACA \mathbb{C} 에서 0이 아닌 attractor α 라 하고 y 가 β -트리의 level $(2m-1)$ 인 상태라면 y 는 \mathbb{C} 에 대응하는 \mathbb{C}' 의 $(\beta \oplus \alpha)$ -트리에서 level 이 $(2m-1)$ 로 재배열된다.

<증명> \mathbb{C} 에서 β -트리의 level 1에 있는 상태를 $B_{1,0}$ 라 하자. 먼저

$$\begin{aligned}
\overline{T}^{2m-1} y &= T^{2m-1} y \oplus (T^{2m-2} \oplus \dots \oplus I) F \\
&= \beta \oplus F \oplus \dots \oplus F \\
&= \beta \oplus F \\
&= \beta \oplus \alpha
\end{aligned}$$

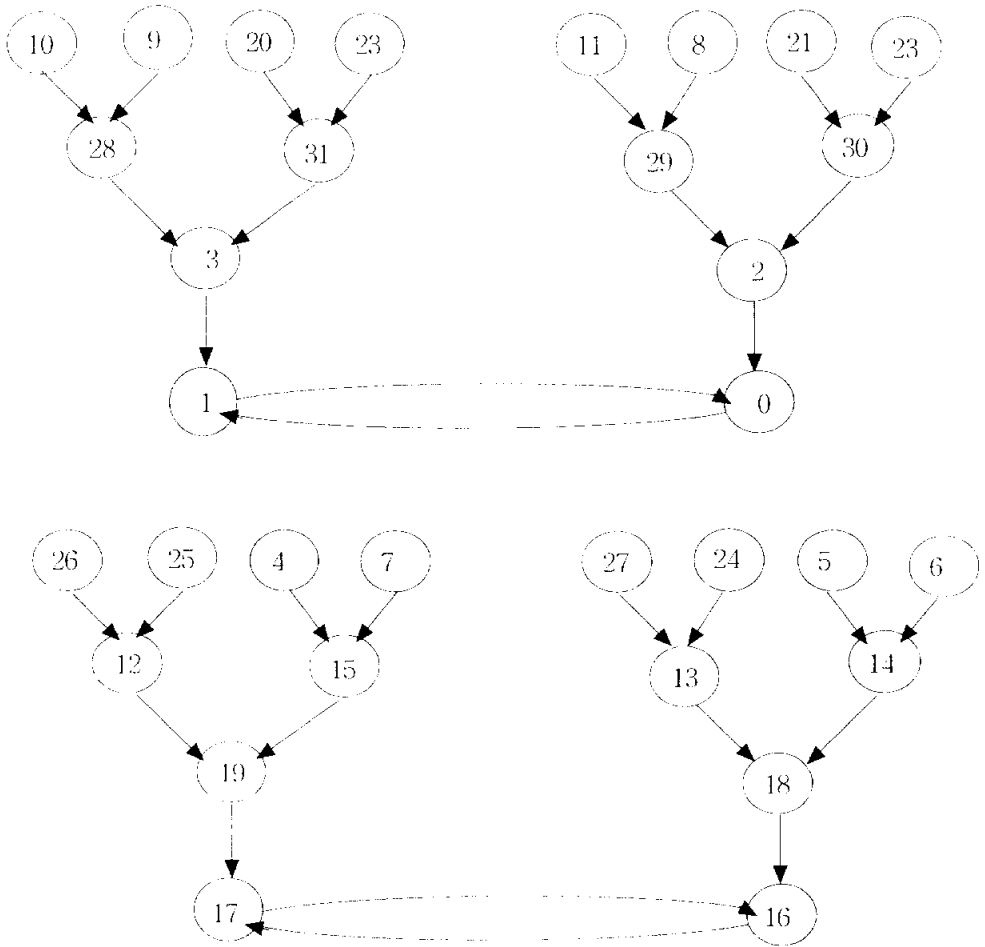
이므로 y 는 $\beta \oplus \alpha$ -트리의 level $(2m-1)$ 이하에 있다. 그리고

$$\begin{aligned}
\overline{T}^{2m-2} y &= T^{2m-2} y \oplus (T^{2m-3} \oplus \dots \oplus I) F \\
&= B_{1,0} \oplus F \oplus \dots \oplus F \\
&= B_{1,0}
\end{aligned}$$

이다. $\overline{TB}_{1,0} = TB_{1,0} \oplus F = \beta \oplus \alpha$ 이고, 가정에 의해 $B_{1,0} \neq \beta$ 이고 $B_{1,0} \neq \beta \oplus \alpha$ 이므로 $B_{1,0}$ 는 C' 의 $\beta \oplus \alpha$ -트리의 level 1에 있는 비순환상태이다. 따라서 y 는 C' 의 $\beta \oplus \alpha$ -트리의 level $(2m-1)$ 에 놓인다. \square

<예 4.5> 그림 4.2의 선형 TPMACA C 에서 0이 아닌 attractor중 1을 여원벡터로 하여 얻어지는 여원 CA C' 의 상태전이 그래프는 그림 4.5와 같다.

C' 에서 여원벡터인 상태 1을 root로 하는 1-트리와 0-트리가 결합하고 나머지 트리들도 attractor의 합이 1이 되는 것까지 결합한다(정리 4.30). 또한 각 트리의 비순환상태들의 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 상대트리인 1-트리의 level 1과 level 3에 배열된다(정리 4.32).



<그림 4.5> 선형 TPMACA로부터 얻어지는 여원 CA C' (여원벡터 : 1)

4.3.2. 선형 TPNCA로부터 유도된 여원 TPNCA

<정리 4.34> C는 depth가 d 인 선형 TPNCA이고, C에서 0-트리의 level i ($0 < i \leq d$)에 있는 한 상태를 여원벡터 F 로 택할 때, β 가 선형 TPNCA의

attractor라면 $\overline{T}^{i-1}F \oplus \beta$ 는 \mathbb{C} 에 대응하는 여원 TPNCA \mathbb{C}' 에서 attractor이다.

<증명>

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

이므로 $\overline{T}^{i-1}F \oplus \beta$ 는 \mathbb{C} 에 대응하는 여원 TPNCA \mathbb{C}' 에서 attractor이다. \square

<정리 4.35> 선형 TPNCA \mathbb{C} 에서 $R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_n \rightarrow R_1$ 가 길이가 n 인 사이클을 이루고 여원벡터 F 가 \mathbb{C} 의 0-트리의 level i 에 있는 비순환상태라 하면 \mathbb{C}' 에서 $\overline{T}^{i-1}F \oplus R_1 \rightarrow \overline{T}^{i-1}F \oplus R_2 \rightarrow \cdots \rightarrow \overline{T}^{i-1}F \oplus R_n \rightarrow \overline{T}^{i-1}F \oplus R_1$ 은 길이가 n 인 사이클을 이룬다.

<증명> $R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_n \rightarrow R_1$ 가 길이가 n 인 사이클을 이루고 여원벡터 F 가 \mathbb{C} 의 0-트리의 level i 에 있는 비순환상태이므로 $T^i F = 0$ 이고 $T^{i-1}F \neq 0$ 이다.

$$\begin{aligned}
\overline{T}(\overline{T}^{i-1}F \oplus R_j) &= T(\overline{T}^{i-1}F \oplus R_j) \oplus F \\
&= T(T^{i-1} \oplus \cdots \oplus I)F \oplus TR_j \oplus F \\
&= T^iF \oplus (T^{i-1} \oplus \cdots \oplus I)F \oplus TR_j \\
&= \overline{T}^{i-1}F \oplus R_{j+1} \quad (j=1,2,\dots,n-1)
\end{aligned}$$

이고

$$\begin{aligned}
\overline{T}(\overline{T}^{i-1}F \oplus R_n) &= T^iF \oplus \overline{T}^{i-1}F \oplus R_n \oplus F \\
&= T^iF \oplus \overline{T}^{i-1}F \oplus TR_n \\
&= \overline{T}^{i-1}F \oplus R_1
\end{aligned}$$

이므로

$\overline{T}^{i-1}F \oplus R_1 \rightarrow \overline{T}^{i-1}F \oplus R_2 \rightarrow \cdots \rightarrow \overline{T}^{i-1}F \oplus R_n \rightarrow \overline{T}^{i-1}F \oplus R_1$ 은 길이가 n 인 사이클을 이룬다. □

<정리 4.36> 여원 TPNCA에서 $R_1' \rightarrow R_2' \rightarrow \cdots \rightarrow R_n' \rightarrow R_1'$ 가 길이가 n 인 사이클을 이루고 β 가 attractor이며 여원벡터 F 가 \mathbb{C} 의 0-트리의 level i 에 있는 비순환상태라 하면 \mathbb{C}' 에서 $R_1' \oplus \beta \rightarrow R_2' \oplus \beta \rightarrow \cdots \rightarrow R_n' \oplus \beta \rightarrow R_1' \oplus \beta$ 은 길이가 n 인 사이클이다.

<증명> 임의의 $j(1 \leq j \leq n-1)$ 에 대하여

$$\begin{aligned}
\overline{T}(R_j' \oplus \beta) &= T(R_j' \oplus \beta) \oplus F \\
&= TR_j' \oplus T\beta \oplus F \\
&= \overline{T}(R_j') \oplus \beta \\
&= R_{j+1}' \oplus \beta
\end{aligned}$$

이고 마찬가지로 $\overline{T}(R_n' \oplus \beta) = R_1' \oplus \beta$ 이므로 $R_1' \oplus \beta \rightarrow R_2' \oplus \beta \rightarrow \cdots \rightarrow R_n' \oplus \beta \rightarrow R_1' \oplus \beta$ 은 길이가 n 인 한 사이클이다. \square

5. Nongroup 셀룰라 오토마타의 응용

5.1 선형 TPNCA의 트리 구성 알고리즘

5.1.1 선형 TPMACA의 트리 구성

CA의 셀의 수가 많아질수록 CA의 상태 수는 지수적으로 증가하기 때문에 다음상태를 구함에 있어 소프트웨어로 CA를 구현한 경우는 행렬 연산의 횟수가 지수적으로 증가하게 된다. CA는 효율적으로 혼돈과 확산이 이루어지는 장점을 가지고 있으나 CA의 행동을 분석하여 평가하는 것이 어렵다는 단점을 가지고 있다. 이러한 CA의 상태전이 행동분석을 위해 상태전이 그래프를 구성하는 것은 필수적이다. 다음에서는 선형 TPMACA에서 0-트리의 임의의 도달 불가능한 상태에 대하여 전이행렬 T 를 연속적으로 적용하여 상태 0이 나올 때까지의 경로를 기본경로로 하여 $(T \oplus I)x=0$ 에서 얻은 attractor를 이용하여 선형 TPMACA의 상태전이 그래프의 트리를 구성하는 알고리즘을 제안한다.

<정의 5.1> Depth가 d 인 선형 TPNCA에서 α -트리의 도달 불가능한 상태 x 는 d 단계 후 그 상태가 α 가 된다. 이때의 상태전이 단계 즉,

$$x \rightarrow Tx \rightarrow \dots \rightarrow T^d x (= \alpha) \quad (5.1)$$

를 α -트리의 α -기본경로(α -basic path)라 한다. □

선형 TPMACA의 상태전이 그래프에서 0-트리의 각 level l 에서 첫 번째 상태

들을 $S_{l,0}$ 라 하면

$$S_{d,0} \rightarrow S_{d-1,0} \rightarrow \cdots \rightarrow S_{1,0} \rightarrow 0 \quad (5.2)$$

는 선형 TPMACA의 0-트리의 0-기본경로이다. 이 0-기본경로를 이용하여 나머지 0-트리를 구성할 수 있다.

<정리 5.1> 선형 TPMACA C의 상태전이 그래프에서 $S_{l,k}$ 를 0-트리의 level l 의 $(k+1)$ 번째 상태라 하면 다음 두 식이 성립한다.

$$\sum_{k=0}^{2^{l-1}-1} S_{l,k} = 2^{l-1} S_{l,0} \oplus 2^{l-2} (S_{1,0} \oplus S_{2,0} \oplus \cdots \oplus S_{l-1,0}) \quad (5.3)$$

(단, $l \leq \text{depth}$ 이고 kS 는 S 를 k 번 XOR한 값이다.)

$$S_{l,k} = S_{l,0} \oplus \sum_{i=1}^{l-1} b_i S_{i,0} \quad (5.4)$$

여기서 b_i 는 k 를 이진수로 표현했을 때 각 bit의 값이고 $k \leq 2^{l-1} - 1$ 이다.

<증명> (1) 먼저 식 5.3이 성립함을 보이기 위하여 수학적 귀납법을 이용한다.

$l = 1$ 일 때, 0-트리의 level 1에 있는 상태는 $S_{1,0}$ 이다.

i) $l = 2$ 일 때, 정리 4.8에 의해 $S_{2,1} \oplus S_{2,1} = S_{1,0}$ 이므로

$$\sum_{k=0}^1 S_{2,k} = 2S_{2,0} \oplus S_{1,0}$$

이다. 그러므로 $l = 2$ 일 때 식 5.3은 성립한다.

ii) $l = m$ 일 때, 다음이 성립한다고 가정하자.

$$\sum_{k=0}^{2^{m-1}-1} S_{m,k} = 2^{m-1} S_{m,0} \oplus 2^{m-2} (S_{1,0} \oplus S_{2,0} \oplus \cdots \oplus S_{m-1,0})$$

iii) $l = m + 1$ 일 때 성립함을 보인다.

\mathbb{C} 의 0-트리 of level m 에 있는 상태의 개수는 정리 4.4에 의해 2^{m-1} 이다.

$2^r \leq k \leq 2^{r+1} - 1$ 인 정수 k 에 대하여 다음이 성립한다.

$$\min \{ k \mid T^k S_{m+1,k} = T^k S_{m+1,0} \} = r$$

따라서 정리 4.8에 의해 $S_{m+1,0} \oplus S_{m+1,k}$ ($2^r \leq k < 2^{r+1} - 1$) 은 \mathbb{C} 의 0-트리의 level r 상태 중 하나이다. 또한 다음이 성립한다.

$$\begin{aligned} & (S_{m+1,0} \oplus S_{m+1,2^r}) \oplus (S_{m+1,0} \oplus S_{m+1,2^r+1}) \oplus \cdots \oplus (S_{m+1,0} \oplus S_{m+1,2^{r+1}-1}) \\ &= (S_{m+1,0} \oplus \cdots \oplus S_{m+1,0}) \oplus (S_{m+1,2^r} \oplus S_{m+1,2^r+1} \oplus \cdots \oplus S_{m+1,2^{r+1}-1}) \\ & \quad (\text{단, } S_{m+1,0} \text{ 의 개수는 } 2^r \text{ 이다.}) \\ &= S_{m+1,2^r} \oplus S_{m+1,2^r+1} \oplus \cdots \oplus S_{m+1,2^{r+1}-1} \end{aligned}$$

$$\begin{aligned}
& \sum_{k=0}^{2^m-1} S_{m+1,k} \\
&= (S_{m+1,0} \oplus S_{m+1,1}) \oplus (S_{m+1,2} \oplus S_{m+1,2^2-1}) \oplus (S_{m+1,2^2} \oplus S_{m+1,2^3-1}) \oplus \cdots \\
&\quad \oplus (S_{m+1,2^{m-1}} \oplus S_{m+1,2^m-1}) \\
&= S_{1,0} \oplus (S_{2,0} \oplus S_{2,1}) \oplus (S_{3,0} \oplus S_{3,1} \oplus S_{3,2^2-1}) \oplus \cdots \\
&\quad \oplus (S_{m,0} \oplus S_{m,1} \oplus \cdots \oplus S_{m,2^{m-1}-1}) \\
&= S_{1,0} \oplus \{2^{2-1}S_{2,0} \oplus 2^{2-2}S_{1,0}\} \oplus \{2^{3-1}S_{3,0} \oplus 2^{3-2}(S_{2,0} \oplus S_{1,0})\} \\
&\quad \oplus \{2^{4-1}S_{4,0} \oplus 2^{4-2}(S_{3,0} \oplus S_{2,0} \oplus S_{1,0})\} \\
&\quad \oplus \cdots \oplus \{2^{m-2}S_{m-1,0} \oplus 2^{m-3}(S_{m-2,0} \oplus \cdots \oplus S_{1,0})\} \\
&\quad \oplus \{2^{m-1}S_{m,0} \oplus 2^{m-2}(S_{m-1,0} \oplus \cdots \oplus S_{1,0})\} \\
&= (1+2^{2-2}+2^{3-2}+2^{4-2}+\cdots+2^{m-3}+2^{m-2})S_{1,0} \\
&\quad \oplus (2^{2-1}+2^{3-2}+2^{4-2}+\cdots+2^{m-3}+2^{m-2})S_{2,0} \\
&\quad \oplus (2^{3-1}+2^{4-2}+\cdots+2^{m-3}+2^{m-2})S_{3,0} \oplus \cdots \\
&\quad \oplus (2^{(m-1)-1}+2^{m-2})S_{m-1,0} \oplus 2^{m-1}S_{m,0} \\
&= \left(1 + \frac{2^{m-1}-1}{2-1}\right)S_{1,0} \oplus \left(2^1 + \frac{2^1(2^{m-2}-1)}{2-1}\right)S_{2,0} \\
&\quad \oplus \left(2^{3-1} + \frac{2^2(2^{m-3}-1)}{2-1}\right)S_{3,0} \oplus \cdots \oplus (2^{m-2}+2^{m-2})S_{m-1,0} \oplus 2^{m-1}S_{m,0} \\
&= 2^{m-1}S_{1,0} \oplus 2^{m-1}S_{2,0} \oplus \cdots \oplus 2^{m-1}S_{m,0} \\
&= 2^{m-1}(S_{1,0} \oplus S_{2,0} \oplus \cdots \oplus S_{m,0}) \\
&= 2^m S_{m+1,0} \oplus (S_{1,0} \oplus \cdots \oplus S_{m,0}) \quad (\because 2^m: \text{ 짝수})
\end{aligned}$$

그러므로 $l = m+1$ 일 때도 성립한다.

(2) 임의의 level $l (\leq \text{depth})$ 에 대하여 식 5.4이 성립함을 보이기 위해 수학적 귀납법을 이용한다.

i) $k = 1$ 일 때,

정리 4.8에 의하여 $S_{l,1} \oplus S_{l,0} = S_{1,0}$ 이므로 $S_{l,1} = S_{l,0} \oplus S_{1,0}$ 이다.

ii) $k = n$ 일 때, 다음이 성립한다고 가정하자.

$$S_{l,n} = S_{l,0} \oplus \sum_{i=1}^{l-1} b_i S_{i,0}$$

iii) $k = n + 1$ 일 때 성립함을 보이기 위해 $n + 1$ 이 홀수일 때와 짝수일 때로 나누어 보인다.

① $n + 1$ 이 홀수일 때:

b_i^n 을 n 을 이진수로 표현했을 때 i 번째 비트 값이라 하자. n 이 짝수이므로 $b_1^n = 0$ 이고, $b_1^{n+1} = 1$ 이다. 즉, $b_1^{n+1} \oplus b_1^n = 1$ 이다. 또한 $2 \leq j \leq l-1$ 인 j 에 대하여 $b_j^{n+1} = b_j^n$ 이다. $TS_{l,n} = TS_{l,n+1}$ 이므로 $T(S_{l,n} \oplus S_{l,n+1}) = 0$ 이다. 그러므로 $S_{l,n} \oplus S_{l,n+1} = S_{1,0}$ 이다. 그러므로 다음이 성립한다.

$$\begin{aligned} S_{l,n+1} &= S_{l,n} \oplus S_{1,0} \\ &= \left(S_{l,0} \oplus \sum_{i=1}^{l-1} b_i^n S_{i,0} \right) \oplus S_{1,0} \\ &= S_{l,0} \oplus b_{l-1}^n S_{l-1,0} \oplus \cdots \oplus b_2^n S_{2,0} \oplus S_{1,0} \quad (\because b_1^n = 0) \\ &= S_{l,0} \oplus b_{l-1}^{n+1} S_{l-1,0} \oplus \cdots \oplus b_2^{n+1} S_{2,0} \oplus b_1^{n+1} S_{1,0} \\ &\quad (\because b_1^{n+1} = 1, b_j^{n+1} = b_j^n) \\ &= S_{l,0} \oplus \sum_{i=1}^{l-1} b_i^{n+1} S_{i,0} \end{aligned}$$

(b) $n + 1$ 이 짝수일 때:

$\min \{ k \mid T^k S_{l,n+1} = T^k S_{l,n} \} = r$ ($2 \leq r \leq l-1$)이면 정리 4.8에 의해 $S_{l,n+1} \oplus S_{l,n}$ 은 \mathbb{C} 의 0-트리의 level r 중 한 상태이다. 그리고

$$b_i^{n+1} \oplus b_i^n = \begin{cases} 1 & , 1 \leq i \leq r \\ 0 & , r+1 \leq i \leq l-1 \end{cases} \quad (*)$$

이므로 $S_{l,n+1} \oplus S_{l,n} = S_{r,2^{r-1}-1}$ 이다. 그러므로 다음이 성립한다.

$$\begin{aligned} S_{l,n+1} &= S_{l,n} \oplus S_{r,2^{r-1}-1} \\ &= \left(S_{l,0} \oplus \sum_{i=1}^{l-1} b_i^n S_{i,0} \right) \oplus \left(S_{r,0} \oplus \sum_{i=1}^{r-1} b_i^{2^{r-1}-1} S_{i,0} \right) \\ &= \left(S_{l,0} \oplus \sum_{i=1}^{l-1} b_i^n S_{i,0} \right) \oplus \left(S_{r,0} \oplus S_{r-1,0} \oplus \cdots \oplus S_{1,0} \right) \\ &= S_{l,0} \oplus \sum_{i=1}^r (b_i^n + 1) S_{i,0} \oplus \sum_{i=r+1}^{l-1} b_i^n S_{i,0} \\ &= S_{l,0} \oplus \sum_{i=1}^r b_i^{n+1} S_{i,0} \oplus \sum_{i=r+1}^{l-1} b_i^n S_{i,0} \quad ((*) \text{에 의해}) \\ &= S_{l,0} \oplus \sum_{i=1}^{l-1} b_i^{n+1} S_{i,0} \end{aligned}$$

(a), (b)에 의해 $k = n+1$ 일 때도 성립한다. □

0-기본경로와 식 5.4을 이용하여 0-트리의 나머지 부분을 구성할 수 있다. 선형 TPMACA의 0이 아닌 α -트리를 구성하기 위하여 0-트리의 각 level의 첫 번째 상태인 $S_{l,0}$ 로부터 α -트리의 각 level의 첫 번째 상태인 $S_{l,0}^\alpha$ 를 다음의 정리에

의해 구할 수 있다.

<정리 5.2> 선형 TPMACA \mathbb{C} 에서 식 5.4를 \mathbb{C} 의 0-기본경로에 대응하는 α -기본경로라 하자.

$$S_{d,0}^\alpha \rightarrow S_{d-1,0}^\alpha \rightarrow \cdots \rightarrow S_{1,0}^\alpha \rightarrow \alpha \quad (5.5)$$

그러면 $S_{l,0}^\alpha$ 는 다음을 만족한다.

$$S_{l,0}^\alpha = S_{l,0} \oplus \alpha \quad (5.6)$$

<증명> 정리 4.13에 의해 $S_{l,0}^\alpha \oplus S_{l,0} = \alpha \oplus 0$ 이고 $S_{l,0}^\alpha = S_{l,0} \oplus \alpha$ 이다. \square

<정리 5.3> 선형 TPMACA \mathbb{C} 의 상태전이 그래프에서 $S_{l,k}^\alpha$ 를 α -트리의 level l 의 $(k+1)$ 번째 상태라 하면 다음을 만족한다.

$$S_{l,k}^\alpha = S_{l,0}^\alpha \oplus \sum_{i=1}^{k-1} b_i S_{i,0} \quad (5.7)$$

<증명> 정리 4.13에 의해 $S_{l,k}^\alpha = S_{l,k} \oplus \alpha$ 이다. 그러므로 정리 5.1의 식 5.4에 의해 다음이 성립한다.

$$\begin{aligned}
S_{l,k}^a &= S_{l,k} \oplus \alpha \\
&= \left(S_{l,0} \oplus \sum_{i=1}^{k-1} b_i S_{i,0} \right) \oplus \alpha \\
&= (S_{l,0} \oplus \alpha) \oplus \sum_{i=1}^{k-1} b_i S_{i,0} \\
&= S_{l,0}^a \oplus \sum_{i=1}^{k-1} b_i S_{i,0}
\end{aligned}$$

□

<예 5.1> 5개의 셀로 이루어진 CA가 전이규칙 $\langle 204, 240, 240, 240, 240 \rangle$ 을 가질 때, 전이행렬 T 는 다음과 같다.

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

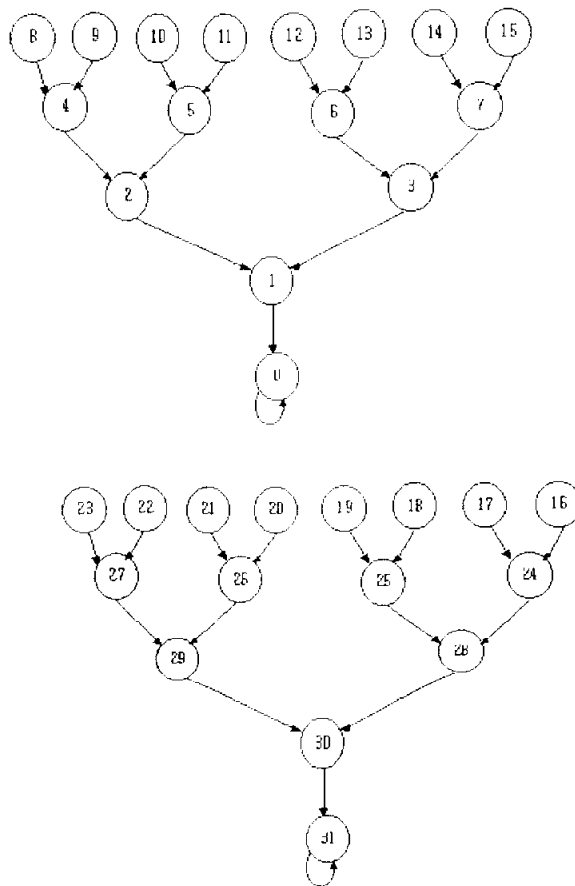
이때 최소다항식은 $m(x) = x^4(x+1)$ 이고 $(T \oplus I)x = 0$ 를 만족하는 attractor x 는 0과 31이다. 여기서 $8 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow 0$ 을 0-기본경로라 하면, 0-트리의 level 4의 6번째 상태인 $S_{4,5}$ 는 식 5.4로부터 다음과 같이 구한다.

$$\begin{aligned}
S_{4,5} &= S_{4,0} + b_1 S_{1,0} + b_2 S_{2,0} + b_3 S_{3,0} \\
&= (01000)^T + 1 \cdot (00001)^T + 0 \cdot (00010)^T + 1 \cdot (00100)^T \\
&= (01101)^T = 13
\end{aligned}$$

이 기본경로에 대응하는 31-기본경로는 식 5.6에 의하여 0-트리의 각 기본경로에 31을 더한 값으로 $23 \rightarrow 27 \rightarrow 29 \rightarrow 30 \rightarrow 31$ 이다. 31-트리의 나머지 부분도 식 5.7에 의하여 구한다. 31-트리의 level 4의 7번째 상태인 $S_{4,6}^{31}$ 를 구하면

$$\begin{aligned}
S_{4,6}^{31} &= S_{4,0}^{31} + b_1 S_{1,0} + b_2 S_{2,0} + b_3 S_{3,0} \\
&= (10111)^T + 0 \cdot (00001)^T + 1 \cdot (00010)^T + 1 \cdot (00100)^T \\
&= (10001)^T = 17
\end{aligned}$$

이다. 그림 5.1은 예 5.1의 TPMACA의 상태전이 그래프이다.



<그림 5.1> 5-셀 TPMACA의 상태전이 그래프

5.1.2 선형 TPNCA의 트리 구성

<정리 5.4> 선형 TPNCA의 상태전이 그래프에서 $S_{i,0}$ 를 0-기본경로의 level i 의 상태, $X_{i,0}$ 을 X -기본경로의 level i 의 상태, X -트리의 level i 의 $(j+1)$ 상태를 $X_{i,j}$ 라 하면 다음이 성립한다.

$$X_{i,j} = S_{i,0} \oplus R_i \oplus \sum_{k=1}^{j-1} b_k S_{k,0} \quad (5.8)$$

여기서 $b_{j-1}b_{j-2}\cdots b_1$ 는 j 의 이진법 표현의 수이며 최대값은 $2^{j-1} - 1$ 이고 R_i 는 상태 X 의 순환하는 i -직전자이다.

<증명> 정리 4.6에 의하여 $X_{i,j} = R_i \oplus S_{i,j}$ 이고 정리 5.1에 의하여

$$S_{i,j} = S_{i,0} \oplus \sum_{k=1}^{j-1} b_k S_{k,0} \text{ 이다. 따라서 식 5.8을 얻는다. } \quad \square$$

<예 5.2> 전이규칙이 <150, 60, 90, 60, 60>인 5-셀 선형 CA의 전이행렬 T 는 아래와 같다.

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

또한 특성다항식 $c(x)$ 과 최소다항식 $m(x)$ 은 $c(x) = m(x) = x^2(x^3 + 1)$ 이다. 그림 5.2는 이 선형 TPNCA의 상태전이 그래프이다. 여기서 $13 \rightarrow 31 \rightarrow 0$ 을 0-트리

5.2 여원 TPNCA의 트리 구성 알고리즘

5.2.1 여원 TPNCA의 기본경로

선형 TPMACA C 로부터 유도되는 여원 TPNCA C' 의 트리 구성은 선형 TPMACA와 마찬가지로 먼저 0-기본경로에 대응되는 $\overline{T}^{i-1}F$ -기본경로와 C' 의 각 트리의 기본경로를 구해야한다. 여원 TPNCA는 여원벡터의 위치에 따라 각 트리의 기본경로를 다음과 같이 구한다.

(1) 여원벡터가 비순환상태인 경우

여원벡터가 비순환 상태인 여원 CA의 상태전이 그래프의 트리를 구성하기 위하여 기본경로를 여원벡터가 도달 불가능한 상태인 경우와 도달 가능한 상태인 경우로 나누어 구한다.

먼저 여원벡터 F 가 depth가 d 인 선형 TPMACA의 level d 인 상태인 경우는 상태 0이 여원 CA의 상태전이 그래프에서 도달 불가능한 상태가 된다. 그러므로 상태 0으로부터 여원 CA의 연산자인 \overline{T} 를 연속적으로 d 번 적용하여 얻은 경로

$$0 \rightarrow \overline{T}0 (= F) \rightarrow \dots \rightarrow \overline{T}^d 0 (= \overline{T}^{i-1} F) \quad (5.9)$$

가 $\overline{T}^{i-1}F$ -기본경로이다. 식 5.10는 여원 TPNCA에서 상태 0이 속한 $\overline{T}^{i-1}F$ -트리의 기본경로를 구하는 식으로 $\overline{S}_{l,0}$ 는 각 level l 의 기본경로가 되는 상태로 상태전이 그래프에서 각 트리의 첫 번째 상태이다.

$$\overline{S_{l,0}} = \overline{T}^{d-i} \cdot 0 \quad (5.10)$$

다음은 여원벡터 F 가 선형 TPMACA의 0이 아닌 도달 가능한 상태인 경우이다. 이 경우 여원 CA의 상태전이 그래프에서 F 가 위치했던 level보다 상위 level의 상태는 level의 변화가 없다. 그러므로 선형 TPMACA의 0-트리의 임의의 도달 불가능한 상태 y 로부터 여원 CA의 연산자인 \overline{T} 를 연속적으로 d 번 적용하여 얻은 경로 $y \rightarrow \overline{T}y \rightarrow \dots \rightarrow \overline{T}^d y (= \overline{T}^{i-1} F)$ 가 $\overline{T}^{i-1} F$ -기본경로가 된다. 식 5.11는 이를 식으로 표현한 것이다.

$$\overline{S_{l,0}} = \overline{T}^{d-l} \cdot y \quad (5.11)$$

여기서 y 는 여원 CA에 대응하는 선형 TPMACA의 상태전이 그래프에서 0-트리의 임의의 도달 불가능한 상태이다.

<정리 5.5> Depth가 d 인 선형 TPMACA C 에서 여원벡터 F 를 0-트리의 level i 에 있는 비순환상태라 하자. 또한 α 를 C 의 0이 아닌 attractor라 하자. 그러면 C 로부터 유도된 여원 TPNCA C' 의 상태전이 그래프에서 α 가 속한 트리는 $\overline{T}^{i-1} F \oplus \alpha$ -트리이고 상태 $\overline{T}^{i-1} F \oplus \alpha$ 는 attractor이다.

<증명> 먼저 $\overline{T}^{i-1} F \oplus \alpha$ 가 attractor임을 보이자. 보조정리 4.20에 의하여 $\overline{T}^{i-1} F$ 는 C' 에서 attractor이므로 $\overline{T}(\overline{T}^{i-1} F) = \overline{T}^{i-1} F$ 이다. 또한 가정에서 α 가 C 에서 attractor이므로 $T\alpha = \alpha$ 이다. 그러므로

$$\begin{aligned}
\overline{T}(\overline{T}^{i-1}F \oplus \alpha) &= T(\overline{T}^{i-1}F \oplus \alpha) \oplus F \\
&= T(\overline{T}^{i-1}F) \oplus F \oplus T\alpha \\
&= \overline{T}(\overline{T}^{i-1}F) \oplus \alpha \\
&= \overline{T}^{i-1}F \oplus \alpha
\end{aligned}$$

이다. 따라서 $\overline{T}^{i-1}F \oplus \alpha$ 는 C' 에서 attractor이다. 다음은 상태 α 가 $\overline{T}^{i-1}F \oplus \alpha$ -트리에 있음을 보이자. 정리 4.21에 의하여 α 는 C' 에서 level i 에 있다. 그러므로 C' 에서 상태 α 의 i 시간 후의 상태는

$$\begin{aligned}
\overline{T}^i\alpha &= T^i\alpha \oplus (I \oplus T \oplus \dots \oplus T^{i-1})F \\
&= \alpha \oplus \overline{T}^{i-1}F \quad (\because \text{보조정리 4.19에 의해})
\end{aligned}$$

이다. 그러므로 상태 α 는 C' 에서 $\overline{T}^{i-1}F \oplus \alpha$ -트리의 level i 에 있는 상태이다. □

보조정리 4.23와 정리 5.5에 의해 선형 TPMACA C 에서 attractor α 는 C' 에서 $\overline{T}^{i-1}F \oplus \alpha$ -트리 임을 알 수 있다. 다음은 선형 TPMACA의 attractor α 가 속하는 $\overline{T}^{i-1}F \oplus \alpha$ -트리의 기본경로 $\overline{S}_{i,0}^\alpha$ 를 구하는 정리이다.

<정리 5.6> 여원벡터 F 가 depth가 d 인 선형 TPMACA C 의 0-트리의 비순환 상태라 하고, α 를 C 의 0이 아닌 attractor라 하자. C 로부터 유도된 여원 TPNCA C' 의 상태전이 그래프에서 α 가 속한 트리의 기본경로의 level l 의 상

태를 $\overline{S}_{l,0}^{\alpha}$ 라 하면 다음을 만족한다.

$$\overline{S}_{l,0}^{\alpha} = \overline{S}_{l,0} \oplus \alpha \quad (5.12)$$

여기서 $\overline{S}_{l,0}$ 는 C' 의 상태 0이 속한 트리의 각 level $l(0 < l \leq d)$ 의 기본경로가 되는 상태로 $\overline{T}^{i-1}F$ -트리의 첫 번째 상태이다.

<증명> $\overline{S}_{l,0}$ 이 $\overline{T}^{i-1}F$ -트리의 level l 상태이므로 $\overline{T}^l \overline{S}_{l,0} = \overline{T}^{i-1}F$ 이다.

$$\begin{aligned} \overline{T}^l (\overline{S}_{l,0} \oplus \alpha) &= T^l (\overline{S}_{l,0} \oplus \alpha) \oplus (T^{l-1} \oplus \dots \oplus I) F \\ &= T^l \overline{S}_{l,0} \oplus (T^{l-1} \oplus \dots \oplus I) F \oplus T^l \alpha \\ &= \overline{T}^l (\overline{S}_{l,0}) \oplus \alpha \\ &= \overline{T}^{i-1} F \oplus \alpha \end{aligned}$$

그리고

$$\begin{aligned} \overline{T}^{l-1} (\overline{S}_{l,0} \oplus \alpha) &= T^{l-1} (\overline{S}_{l,0} \oplus \alpha) \oplus (T^{l-2} \oplus \dots \oplus I) F \\ &= \overline{T}^{l-1} (\overline{S}_{l,0}) \oplus T^{l-1} \alpha \\ &= \overline{T}^{l-1} (\overline{S}_{l,0}) \oplus \alpha \\ &\neq \overline{T}^{i-1} F \oplus \alpha \end{aligned}$$

이므로 $\overline{S}_{l,0} \oplus \alpha$ 는 $\overline{T}^{l-1} F \oplus \alpha$ -트리의 level l 상태이다. 다음은 $\overline{T}(\overline{S}_{l,0}^{\alpha}) = \overline{S}_{l-1,0}^{\alpha}$ 임을 보이자.

$$\begin{aligned} \overline{T}(\overline{S}_{l,0} \oplus \alpha) &= T(\overline{S}_{l,0} \oplus \alpha) \oplus F \\ &= T(\overline{S}_{l,0}) \oplus F \oplus T\alpha \\ &= \overline{T} \overline{S}_{l,0} \oplus \alpha \\ &= \overline{S}_{l-1,0} \oplus \alpha \end{aligned}$$

그러므로 C' 의 상태전이 그래프에서 α 가 속한 트리의 기본경로의 level l 의 상태 $\overline{S}_{l,0}^{\alpha}$ 는 식 5.12를 만족한다. \square

(2) 여원벡터가 0이 아닌 attractor인 경우

선형 TPMACA C 의 상태가 0이 아닌 attractor를 여원벡터 F 로 하여 유도되는 여원 TPNCA C' 은, F 가 비순환상태인 경우와 달리 각 트리의 순환상태는 변하지 않음을 보조정리 4.29와 보조 정리 4.30에 의해 알 수 있다. 0이 아닌 attractor β 가 여원벡터 F 일 때 C' 의 상태전이 그래프는 0-트리와 β -트리가 결합하고 나머지 트리도 두 attractor의 합(bitwise 덧셈)이 β 가 되는 트리끼리 결합이 된다(정리 4.31). 다음 정리들에 의해 C' 의 기본경로를 구한다.

<정리 5.7> Depth가 d 인 선형 TPMACA C 에서 0-기본경로가 $S_{d,0} \rightarrow S_{d-1,0} \rightarrow \dots \rightarrow S_{1,0} \rightarrow 0$ 이고, 여원벡터가 0이 아닌 attractor β 라 하면 C 에 대응하는 C' 의 0-기본경로를 $\overline{S}_{d,0} \rightarrow \overline{S}_{d-1,0} \rightarrow \dots \rightarrow \overline{S}_{1,0} \rightarrow 0$ 라 할때 level l 의 기본경로에 놓이는 상태 $\overline{S}_{l,0}$ 는 다음을 만족한다.

$$\bar{S}_{l,0} = \begin{cases} S_{l,0} & l: \text{짝수} \\ S_{l,0} \oplus \beta & l: \text{홀수} \end{cases} \quad (5.13)$$

<증명> 가정에 의해 $T^d S_{d,0} = 0$ 이고, $T^d F = T^{d-1} F = \dots = TF = F$ 이다.

i) d 가 홀수인 경우

$$\begin{aligned} \bar{T}^d \bar{S}_{d,0} &= \bar{T}^d (S_{d,0} \oplus F) \\ &= T^d (S_{d,0} \oplus F) \oplus (T^{d-1} \oplus \dots \oplus T \oplus I) F \\ &= T^d S_{d,0} \oplus T^d F \oplus T^{d-1} F \oplus \dots \oplus TF \oplus F \\ &= 0 \oplus F \oplus F \oplus \dots \oplus F \oplus \quad (F\text{의 수} : d+1) \\ &= 0 \end{aligned}$$

그러나

$$\begin{aligned} \bar{T}^{d-1} \bar{S}_{d,0} &= \bar{T}^{d-1} (S_{d,0} \oplus F) \\ &= T^{d-1} (S_{d,0} \oplus F) \oplus (T^{d-2} \oplus \dots \oplus T \oplus I) F \\ &= T^{d-1} S_{d,0} \oplus T^{d-1} F \oplus T^{d-2} F \oplus \dots \oplus TF \oplus F \\ &= S_{1,0} \oplus F \oplus F \oplus \dots \oplus F \oplus \quad (F\text{의 수} : d) \\ &= S_{1,0} \oplus F \end{aligned}$$

이다.

ii) d 가 짝수인 경우

$$\begin{aligned}
\overline{T}^d \overline{S}_{d,0} &= \overline{T}^d S_{d,0} \\
&= T^d S_{d,0} \oplus (T^{d-1} \oplus \cdots \oplus T \oplus I) F \\
&= T^d S_{d,0} \oplus T^{d-1} F \oplus \cdots \oplus T F \oplus F \\
&= 0 \oplus F \oplus F \oplus \cdots \oplus F \oplus \quad (F\text{의 수} : d) \\
&= 0
\end{aligned}$$

그러나

$$\begin{aligned}
\overline{T}^{d-1} \overline{S}_{d,0} &= \overline{T}^{d-1} S_{d,0} \\
&= T^{d-1} S_{d,0} \oplus (T^{d-2} \oplus \cdots \oplus T \oplus I) F \\
&= T^{d-1} S_{d,0} \oplus T^{d-2} F \oplus \cdots \oplus T F \oplus F \\
&= S_{1,0} \oplus F \oplus F \oplus \cdots \oplus F \oplus \quad (F\text{의 수} : d-1) \\
&= S_{1,0} \oplus F
\end{aligned}$$

이다. i), ii)에서 $S_{1,0} \neq 0$ 이고 $S_{1,0} \neq F$ 이므로 정리 4.31에 의해 $S_{1,0} \oplus F$ 는 순환상태가 아니다. 따라서 $S_{d,0} \oplus F$ 는 C' 에서 0-트리의 level d 에 있는 도달 불가능한 상태이다.

iii) 마지막으로 $\overline{T} \overline{S}_{i,0} = \overline{S}_{i-1,0}$ 임을 보이면 된다.

(a) i 가 홀수인 경우

$$\begin{aligned}
\overline{T} \overline{S}_{i,0} &= \overline{T}(S_{i,0} \oplus F) \\
&= T(\overline{S}_{i,0} \oplus F) \oplus F \\
&= S_{i-1,0} \\
&= \overline{S}_{i-1,0} \quad (\because i-1 : \text{짝수})
\end{aligned}$$

⑥ i 가 짝수인 경우

$$\begin{aligned}
 \overline{T} \overline{S}_{i,0} &= \overline{T}(S_{i,0}) \\
 &= T(S_{i,0}) \oplus F \\
 &= S_{i-1,0} \oplus F \\
 &= \overline{S}_{i-1,0} \quad [\because i-1 : \text{홀수}]
 \end{aligned}$$

그러므로 모든 i 에 대하여 $\overline{T} \overline{S}_{i,0} = \overline{S}_{i-1,0}$ 가 성립한다. □

<보조정리 5.8> β 가 선형 TPMCA C 에서 attractor라 하자. C 에 대응하는 여원 TPNCA C' 의 상태전이 그래프에서 상태 0을 포함하고 있는 $\overline{T}^{i-1} F$ -트리의 level i 의 $(k+1)$ 번째 상태 $\overline{S}_{i,k}$ 와 β 를 포함하고 있는 $\overline{T}^{i-1} F \oplus \beta$ -트리의 level i 의 $(k+1)$ 번째 상태 $\overline{S}_{i,k}^\beta$ 는 여원벡터의 위치와 관계없이 다음과 같은 관계를 만족한다.

$$\overline{S}_{i,0}^\beta = \overline{S}_{i,k} \oplus \beta \quad (k = 0, 1, \dots, 2^{i-1} - 1) \quad (5.14)$$

<증명> 수학적 귀납법을 이용해서 증명한다. 가정에 의해 $T\beta = \beta$ 이다.

i) $i = 1$ 일 때

C' 에서 β -트리의 level 1의 상태는 $\overline{S}_{1,0}^\beta$ 뿐이다. $\overline{T} \overline{S}_{1,0} = 0$ 이므로

$$\begin{aligned}
 \overline{T}(\overline{S}_{1,0} \oplus \beta) &= T(\overline{S}_{1,0} \oplus \beta) \oplus F \\
 &= \overline{T} \overline{S}_{1,0} \oplus T\beta \\
 &= \beta
 \end{aligned}$$

이다. $\overline{S}_{1,0} \oplus \beta \neq \beta$ 이기 때문에, $\overline{S}_{1,0} \oplus \beta$ 는 β -트리의 level 1의 상태이므로

$i = 1$ 일 때 성립한다.

ii) $i = k$ 일 때 $\overline{S}_{i,0}^\beta = \overline{S}_{i,k} \oplus \beta$ 라 가정하자. $i = k+1$ 에 대하여 다음이 성립한다.

$$\begin{aligned}
 \overline{T}(\overline{S}_{k+1,j} \oplus \beta) &= T(\overline{S}_{k+1,j} \oplus \beta) \oplus F \\
 &= (T\overline{S}_{k+1,j} \oplus F) \oplus T\beta \\
 &= \overline{T}\overline{S}_{k+1,j} \oplus T\beta \\
 &= \overline{T}\overline{S}_{k,j} \oplus \beta \\
 &= \overline{S}_{k,j}^\beta
 \end{aligned}$$

□

<정리 5.9> Depth가 d 인 TPMACA C 에서 attractor β 를 여원벡터로 갖는 C 에 대응하는 여원 TPNCA C' 의 β -트리의 β -기본정로는 다음과 같다.

$$\overline{S}_{d,0}^\beta \rightarrow \overline{S}_{d-1,0}^\beta \rightarrow \cdots \rightarrow \overline{S}_{1,0}^\beta \rightarrow \beta$$

여기서 $\overline{S}_{i,0}^\beta$ 와 $\overline{S}_{i,0}$ 는 각각 보조정리 5.8과 정리 5.7에 있는 상태이다.

<증명> 보조정리 5.8에 의해 다음이 성립한다.

$$\begin{aligned}
 \overline{T}\overline{S}_{1,0}^\beta &= \overline{T}(\overline{S}_{1,0} \oplus \beta) \\
 &= T(\overline{S}_{1,0} \oplus \beta) \oplus F \\
 &= T\overline{S}_{1,0} \oplus T\beta \oplus F \\
 &= \overline{T}^{i-1}F \oplus \beta
 \end{aligned}$$

$$\begin{aligned}
\overline{T} \overline{S}_{l,0}^\beta &= \overline{T}(\overline{S}_{l,0} \oplus \beta) \\
&= T(\overline{S}_{l,0} \oplus \beta) \oplus F \\
&= (T \overline{S}_{l,0} \oplus F) \oplus \beta \\
&= \overline{T} \overline{S}_{l,0} \oplus \beta \\
&= \overline{S}_{l-1,0} \oplus \beta \\
&= \overline{S}_{l-1,0}^\beta
\end{aligned}$$

□

5.2.2 여원 TPNCA의 트리 구성

이 절에서는 앞 절에서 얻어진 각 트리의 기본경로와 선형 TPMACA의 0-트리의 기본경로로부터 각 트리의 기본경로를 제외한 나머지 트리를 구성한다.

<정리 5.10> 선형 TPMACA의 0-트리에 대응하는 트리인 여원 TPNCA에서 상태 0이 속한 $\overline{T}^{i-1} F$ -트리의 각 level l 의 $(k+1)$ 번째 상태 $\overline{S}_{l,k}$ 는 다음 두 식을 만족한다.

$$\sum_{k=0}^{2^{l-1}-1} \overline{S}_{l,k} = 2^{l-1} \overline{S}_{l,0} \oplus 2^{l-2} (S_{1,0} \oplus S_{2,0} \oplus \cdots \oplus S_{l-1,0}) \quad (5.15)$$

(단, $l \leq \text{depth}$ 이고 kS 는 S 를 k 번 XOR한 값이다.)

$$\overline{S}_{l,k} = \overline{S}_{l,0} \oplus \sum_{i=1}^{l-1} b_i S_{i,0} \quad (5.16)$$

여기서 b_i 는 $k (\leq 2^{l-1} - 1)$ 를 이진수로 표현했을 때 각 bit의 값이고, $\overline{S_{l,0}}$ 는 여원벡터의 위치에 따라 식 5.10, 5.11, 5.13에서 얻은 기본경로이다.

<증명> 정리 5.1의 증명과 유사하다.

(1) 먼저 식 5.15이 성립함을 보이기 위하여 수학적 귀납법을 이용한다.

$l = 1$ 일 때, $\overline{T}^{j-1} F$ -트리의 level 1에 있는 상태는 $\overline{S_{1,0}}$ 뿐이므로 $l = 2$ 일 때부터 보인다.

i) $l = 2$ 일 때, 정리 4.18에 의해 $\overline{S_{2,1}} \oplus \overline{S_{2,1}} = S_{1,0}$ 이므로

$$\sum_{k=0}^1 \overline{S_{2,k}} = 2 \overline{S_{2,0}} \oplus S_{1,0}$$

이다. 그러므로 $l = 2$ 일 때 식 5.15은 성립한다.

ii) $l = m$ 일 때, 다음이 성립한다고 가정하자.

$$\sum_{k=0}^{2^{m-1}-1} \overline{S_{m,k}} = 2^{m-1} \overline{S_{m,0}} \oplus 2^{m-2} (S_{1,0} \oplus S_{2,0} \oplus \cdots \oplus S_{m-1,0})$$

iii) $l = m + 1$ 에 대하여

C' 의 상태전이 그래프에서 각 트리의 level m 에 놓인 비순환상태의 수는 대응하는 C 의 0-트리의 level m 에 있는 상태의 수와 같으므로 정리 4.4에 의해 2^{m-1} 이다. $2^{r-1} \leq k \leq 2^r - 1$ 인 정수 k 에 대하여 다음이 성립한다.

$$\min \{ j \mid \overline{T}^j \overline{S_{m+1,k}} = \overline{T}^j \overline{S_{m+1,0}} \} = r$$

그러므로

$$\begin{aligned}
 \overline{T}^r \overline{S}_{m+1,k} &= \overline{T}^r \overline{S}_{m+1,0} \\
 \langle \rangle T^r \overline{S}_{m+1,k} \oplus (T^{r-1} \oplus \cdots \oplus T \oplus I) F \\
 &= T^r \overline{S}_{m+1,0} \oplus (T^{r-1} \oplus \cdots \oplus T \oplus I) F \\
 \Leftrightarrow T^r \overline{S}_{m+1,k} &= T^r \overline{S}_{m+1,0} \\
 \Leftrightarrow T^r (\overline{S}_{m+1,k} \oplus \overline{S}_{m+1,0}) &= 0
 \end{aligned}$$

이고, $T^{r-1} (\overline{S}_{m+1,k} \oplus \overline{S}_{m+1,0}) \neq 0$ 이므로 $\overline{S}_{m+1,k} \oplus \overline{S}_{m+1,0}$ 는 \mathbb{C} 의 0-트리의 level r 상태 중 하나이다 ($2^{r-1} \leq k \leq 2^r - 1$). 또한 다음이 성립한다.

$$\begin{aligned}
 &\overline{S}_{m+1,2^{r-1}} \oplus \overline{S}_{m+1,2^{r-1}+1} \oplus \cdots \oplus \overline{S}_{m+1,2^r-1} \\
 &= (\overline{S}_{m+1,0} \oplus \cdots \oplus \overline{S}_{m+1,0}) \oplus (\overline{S}_{m+1,2^{r-1}} \oplus \overline{S}_{m+1,2^{r-1}+1} \oplus \\
 &\quad \cdots \oplus \overline{S}_{m+1,2^r-1}) \\
 &\quad (\text{단, } \overline{S}_{m+1,0} \text{의 개수는 } 2^{r-1} \text{이다.}) \\
 &= (\overline{S}_{m+1,0} \oplus \overline{S}_{m+1,2^{r-1}}) \oplus (\overline{S}_{m+1,0} \oplus \overline{S}_{m+1,2^{r-1}+1}) \oplus \\
 &\quad \cdots \oplus (\overline{S}_{m+1,0} \oplus \overline{S}_{m+1,2^r-1}) \\
 &= \overline{S}_{r,0} \oplus \overline{S}_{r,1} \oplus \cdots \oplus \overline{S}_{r,2^{r-1}-1}
 \end{aligned}$$

그러므로

$$\begin{aligned}
& \sum_{k=0}^{2^m-1} \overline{S}_{m+1,k} \\
&= (\overline{S}_{m+1,0} \oplus \overline{S}_{m+1,1}) \oplus (\overline{S}_{m+1,2} \oplus \overline{S}_{m+1,2^2-1}) \oplus \\
&\quad (\overline{S}_{m+1,2^2} \oplus \cdots \oplus \overline{S}_{m+1,2^3-1}) \oplus \cdots \oplus (\overline{S}_{m+1,2^m} \oplus \cdots \oplus \overline{S}_{m+1,2^m-1}) \\
&= S_{1,0} \oplus (S_{2,0} \oplus S_{2,1}) \oplus (S_{3,0} \oplus S_{3,1} \oplus S_{3,2^2-1}) \oplus \cdots \\
&\quad \oplus (S_{m,0} \oplus S_{m,1} \oplus \cdots \oplus S_{m,2^{m-1}-1}) \\
&= S_{1,0} \oplus \{2^{2-1}S_{2,0} \oplus 2^{2-2}S_{1,0}\} \oplus \{2^{3-1}S_{3,0} \oplus 2^{3-2}(S_{2,0} \oplus S_{1,0})\} \\
&\quad \oplus \{2^{4-1}S_{4,0} \oplus 2^{4-2}(S_{3,0} \oplus S_{2,0} \oplus S_{1,0})\} \\
&\quad \oplus \cdots \oplus \{2^{m-2}S_{m-1,0} \oplus 2^{m-3}(S_{m-2,0} \oplus \cdots \oplus S_{1,0})\} \\
&\quad \oplus \{2^{m-1}S_{m,0} \oplus 2^{m-2}(S_{m-1,0} \oplus \cdots \oplus S_{1,0})\} \\
&= (1+2^{2-2}+2^{3-2}+2^{4-2}+\cdots+2^{m-3}+2^{m-2})S_{1,0} \\
&\quad \oplus (2^{2-1}+2^{3-2}+2^{4-2}+\cdots+2^{m-3}+2^{m-2})S_{2,0} \\
&\quad \oplus (2^{3-1}+2^{4-2}+\cdots+2^{m-3}+2^{m-2})S_{3,0} \oplus \cdots \\
&\quad \oplus (2^{(m-1)-1}+2^{m-2})S_{m-1,0} \oplus 2^{m-1}S_{m,0} \\
&= \left(1 + \frac{2^{m-1}-1}{2-1}\right)S_{1,0} \oplus \left(2^1 + \frac{2^1(2^{m-2}-1)}{2-1}\right)S_{2,0} \\
&\quad \oplus \left(2^{3-1} + \frac{2^2(2^{m-3}-1)}{2-1}\right)S_{3,0} \oplus \cdots \oplus (2^{m-2}+2^{m-2})S_{m-1,0} \oplus 2^{m-1}S_{m,0} \\
&= 2^{m-1}S_{1,0} \oplus 2^{m-1}S_{2,0} \oplus \cdots \oplus 2^{m-1}S_{m,0} \\
&= 2^{m-1}(S_{1,0} \oplus S_{2,0} \oplus \cdots \oplus S_{m,0}) \\
&= 2^m \overline{S}_{m+1,0} \oplus (S_{1,0} \oplus \cdots \oplus S_{m,0}) \quad (\because 2^m: \text{ 짝수})
\end{aligned}$$

따라서 $l = m+1$ 일때도 성립한다.

(2) 임의의 level $l (\leq \text{depth})$ 에 대하여 식 5.16이 성립함을 보이기 위해 수학적 귀납법을 이용한다.

i) $k = 1$ 일 때,

정리 4.18에 의하여 $\bar{S}_{l,1} \oplus \bar{S}_{l,0} = S_{1,0}$ 이므로 $\bar{S}_{l,1} = \bar{S}_{l,0} \oplus S_{1,0}$ 이다.

ii) $k = n$ 일 때, 다음이 성립한다고 가정하자.

$$\bar{S}_{l,n} = \bar{S}_{l,0} \oplus \sum_{i=1}^{(n-1)} b_i S_{i,0}$$

iii) $k = n + 1$ 일 때 성립함을 보이기 위해 $n + 1$ 이 홀수일 때와 짝수일 때로 나누어 보인다.

(a) $n + 1$ 이 홀수일 때:

b_i^n 을 n 을 이진수로 표현했을 때 i 번째 비트 값이라 하자. n 이 짝수이므로 $b_1^n = 0$ 이고, $b_1^{n+1} = 1$ 이다. 즉, $b_1^{n+1} \oplus b_1^n = 1$ 이다. 또한 $2 \leq j \leq l-1$ 인 j 에 대하여 $b_j^{n+1} = b_j^n$ 이다.

$T \bar{S}_{l,n} = T \bar{S}_{l,n+1}$ 이므로 $T(\bar{S}_{l,n} \oplus \bar{S}_{l,n+1}) = 0$ 이다. 그러므로 정리 4.18에 의해 $\bar{S}_{l,n} \oplus \bar{S}_{l,n+1} = S_{1,0}$ 이다. 그러므로 다음이 성립한다.

$$\begin{aligned} \bar{S}_{l,n+1} &= \bar{S}_{l,n} \oplus S_{1,0} \\ &= \left(\bar{S}_{l,0} \oplus \sum_{i=1}^{(n-1)} b_i^n S_{i,0} \right) \oplus S_{1,0} \\ &= \bar{S}_{l,0} \oplus b_{l-1}^n S_{l-1,0} \oplus \cdots \oplus b_2^n S_{2,0} \oplus S_{1,0} \quad (\because b_1^n = 0) \\ &= \bar{S}_{l,0} \oplus b_{l-1}^{n+1} S_{l-1,0} \oplus \cdots \oplus b_2^{n+1} S_{2,0} \oplus b_1^{n+1} S_{1,0} \\ &\quad (\because b_1^{n+1} = 1, b_j^{n+1} = b_j^n) \\ &= \bar{S}_{l,0} \oplus \sum_{i=1}^{(n-1)} b_i^{n+1} S_{i,0} \end{aligned}$$

(b) $n + 1$ 이 짝수일 때:

$n + 2$ 가 홀수이므로 위의 (a)에 의해 $\bar{S}_{l,n+2} = \bar{S}_{l,0} \oplus \sum_{i=1}^{l-1} b_i^{n+1} S_{i,0}$ 이다. 또한

$$\begin{aligned} \bar{S}_{l,n+1} &= \bar{S}_{l,n+2} \oplus S_{1,0} \\ &= \bar{S}_{l,0} \oplus \sum_{i=1}^{l-1} b_i^{n+2} S_{i,0} \oplus S_{1,0} \end{aligned}$$

이다. 여기서 $b_i' = \begin{cases} b_1 \oplus 1 & , \quad i = 1 \\ b_i & , \quad i > 1 \end{cases}$

이다. 그런데 b_i^{n+2} 와 b_i^{n+1} 은 $i > 1$ 일 때 $b_i^{n+2} = b_i^{n+1}$ 이고 $b_1^{n+1} = 0$, $b_1^{n+2} = 1$ 이므로 $b_i^{n+1} = b_i^{n+2} \oplus 1$ 이다. 그러므로

$$\bar{S}_{l,n+1} = \bar{S}_{l,0} \oplus \sum_{i=1}^{l-1} b_i^{n+1} S_{i,0}$$

이다. (a), (b)에 의해 $k = n + 1$ 일 때도 성립한다. □

위 정리로부터 다음의 따름정리를 얻는다.

<따름정리 5.11> $\min \{ p: \bar{T}^p \bar{S}_{l,n+1} = \bar{T}^p \bar{S}_{l,n} \} = r \ (2 \leq r \leq l-1)$ 이라

하면 $\bar{S}_{l,n+1} \oplus \bar{S}_{l,n} = S_{r,2^{r-1}-1}$ 이다.

<증명> $\min \{ p: \bar{T}^p \bar{S}_{l,n+1} = \bar{T}^p \bar{S}_{l,n} \} = r \ (2 \leq r \leq l-1)$ 이라 하면

$$\begin{aligned}
& \overline{T}^r \overline{S}_{l,n+1} = \overline{T}^r \overline{S}_{l,n} \\
\Leftrightarrow & T^r \overline{S}_{l,n+1} \oplus (T^{r-1} \oplus \cdots \oplus I)F = T^r \overline{S}_{l,n} \oplus (T^{r-1} \oplus \cdots \oplus I)F \\
\Leftrightarrow & T^r \overline{S}_{l,n+1} = T^r \overline{S}_{l,n} \\
\Leftrightarrow & T^r(\overline{S}_{l,n+1} \oplus \overline{S}_{l,n}) = 0
\end{aligned}$$

이므로 $\overline{S}_{l,n+1} \oplus \overline{S}_{l,n}$ 는 정리 4.8에 의해 \mathbb{C} 의 0-트리의 level r 에 있는 상태 중 하나이다. 그리고

$$b_i^{n+1} \oplus b_i^n = \begin{cases} 1 & , 1 \leq i \leq r \\ 0 & , r+1 \leq i \leq l-1 \end{cases} \quad (*)$$

이므로 다음이 성립한다.

$$\begin{aligned}
& \overline{S}_{l,n} \oplus S_{r,2^{r-1}-1} \\
&= \left(\overline{S}_{l,0} \oplus \sum_{i=1}^{l-1} b_i^n S_{i,0} \right) \oplus \left(S_{r,0} \oplus \sum_{i=1}^{r-1} b_i^{2^{r-1}-1} S_{i,0} \right) \\
&= \left(\overline{S}_{l,0} \oplus \sum_{i=1}^{l-1} b_i^n S_{i,0} \right) \oplus (S_{r,0} \oplus S_{r-1,0} \oplus \cdots \oplus S_{1,0}) \\
&= \overline{S}_{l,0} \oplus \sum_{i=1}^r (b_i^n + 1) S_{i,0} \oplus \sum_{i=r+1}^{l-1} b_i^n S_{i,0} \\
&= \overline{S}_{l,0} \oplus \sum_{i=1}^r b_i^{n+1} S_{i,0} \oplus \sum_{i=r+1}^{l-1} b_i^{n+1} S_{i,0} \quad ((*)\text{에 의해}) \\
&= \overline{S}_{l,0} \oplus \sum_{i=1}^{l-1} b_i^{n+1} S_{i,0} = \overline{S}_{l,n+1}
\end{aligned}$$

□

다음 정리에 의해 여원 TPNCA의 나머지 트리들의 상태를 구할 수 있다.

<정리 5.12> 선형 TPMACA의 α -트리에 대응하는 트리인 여원 TPNCA에서 상태 α 가 속한 트리의 각 level l 의 $(k+1)$ 번째 상태 $\overline{S}_{l,0}^\alpha$ 는 다음을 만족한다.

$$\overline{S}_{l,k}^\alpha = \overline{S}_{l,0}^\alpha \oplus \sum_{i=1}^{k-1} b_i S_{i,0} \quad (5.17)$$

여기서 b_i 는 $k (\leq 2^{l-1} - 1)$ 를 이진수로 표현했을 때 각 bit의 값이고, $\overline{S}_{l,0}^\alpha$ 는 여원벡터의 위치에 따라 식 5.12와 5.14에서 얻은 기본경로이다.

<증명>

$$\begin{aligned} \overline{S}_{l,k}^\alpha &= \overline{S}_{l,k} \oplus \alpha && \text{(보조정리 5.8에 의해)} \\ &= \left(\overline{S}_{l,0} \oplus \sum_{i=1}^{k-1} b_i S_{i,0} \right) \oplus \beta && \text{(정리 5.10의 식 5.16에 의해)} \\ &= \left(\overline{S}_{l,0} \oplus \beta \right) \oplus \sum_{i=1}^{k-1} b_i S_{i,0} \\ &= \overline{S}_{l,0}^\alpha \oplus \sum_{i=1}^{k-1} b_i S_{i,0} \end{aligned}$$

□

5.2.3 트리 구성 알고리즘

이 절은 앞서 서술한 내용을 정리하여 알고리즘으로 제안한다. 선형 TPMACA의 트리 구성과 이 CA로부터 유도된 여원 CA의 트리 구성 알고리즘이다.

Step 1. 주어진 전이행렬이 T 일 때 $(T \oplus I)x = 0$ 을 만족하는 attractor x 를 찾는다.

Step 2. T 의 최소다항식 $m(x)$ 를 나누는 x^k 중 최대정수 k 를 찾아 CA의 depth d 를 구한다.

Step 3. $T^d y = 0$ 이고 $T^{d-1} y \neq 0$ 인 0-트리의 도달 불가능한 상태 y 하나를 찾는다.

Step 4. y 를 시작으로 하는 0-트리의 0-기본경로 $y \rightarrow Ty \rightarrow \dots \rightarrow 0$ 를 찾는다.

Step 5. $S_{l,k} = S_{l,0} \oplus \sum_{i=1}^{k-1} b_i S_{i,0}$ 에 의하여 0-트리를 구성한다.

Step 6. $S_{l,0}^\alpha = S_{l,0} \oplus \alpha$ 에 의하여 α -트리의 α -기본경로를 찾는다.

Step 7. $S_{l,k}^\alpha = S_{l,0}^\alpha \oplus \sum_{i=1}^{k-1} b_i S_{i,0}$ 에 의하여 나머지 α -트리를 구성한다.

/* 여원을 갖는 CA C' 트리의 구성 */

Step 8. 여원벡터 F 가 0이 아닌 attractor이면 C' 의 0-기본경로를

$$\overline{S_{l,0}} = \begin{cases} S_{l,0} & l: \text{짝수} \\ S_{l,0} \oplus \beta & l: \text{홀수} \end{cases}$$

에 의하여 구하고 Go To Step 10.

Step 9. 여원벡터 F 가 선형 TPMACA의 비순환상태이고 도달 불가능한 상태 이면 $0 \rightarrow \overline{T^0}(=F) \rightarrow \dots \rightarrow \overline{T^d}(= \overline{T^{d-1}} F)$ 를 $\overline{T^{d-1}} F$ -트리의 기본경로로 하고, 도달 가능한 상태이면 선형 TPMACA의 0-트리의 도달

불가능한 상태 y 에 대하여 $y \rightarrow \overline{T}y \rightarrow \dots \rightarrow \overline{T}^d y (= \overline{T}^{j-1} F)$ 를 $\overline{T}^{j-1} F$ -트리의 기본경로로 한다.

Step 10. $\overline{S}_{l,k} = \overline{S}_{l,0} \oplus \sum_{i=1}^{l-1} b_i S_{i,0}$ 에 의하여 $\overline{T}^{j-1} F$ -트리를 구성한다.

Step 11. $\overline{S}_{l,0}^a = \overline{S}_{l,0} \oplus \alpha$ 에 의하여 또 다른 트리의 기본경로를 구성한다.

Step 12. $\overline{S}_{l,k}^a = \overline{S}_{l,0}^a \oplus \sum_{i=1}^{l-1} b_i S_{i,0}$ 에 의하여 트리의 나머지 부분을 구성한다.

5.2.4 선형 TPNCA로부터 유도된 여원 TPNCA의 트리 구성

본 절에서는 일반적인 선형 TPNCA에서 여원벡터가 0-트리의 비순환상태인 경우에 한해서 여원 TPNCA의 트리를 구성한다.

<정리 5.13> 선형 TPNCA를 \mathbb{C} 라 하고 \mathbb{C} 로부터 유도된 여원 TPNCA를 \mathbb{C}' 라 하자. 이때 여원벡터는 \mathbb{C} 에서 0-트리의 level j 의 비순환상태이다. $O_{j,0}$ 를 \mathbb{C} 의 0-트리의 기본경로의 level j 상태라 하고 $X_{j,0}'$ 를 \mathbb{C}' 에서 X' -트리의 기본경로의 level j 상태라 하면 X' -트리의 level j 의 $(k+1)$ 번째 상태 $X_{j,k}'$ 는 다음을 만족한다.

$$\begin{aligned} X_{j,k}' &= X_{j,0}' \oplus \sum_{l=1}^{k-1} b_l O_{l,0} \\ &= O_{j,0} \oplus U_j \oplus \sum_{l=1}^{k-1} b_l O_{l,0} \end{aligned} \tag{5.18}$$

여기서 $b_{i-1} b_{i-2} \cdots b_1$ 는 $k(\leq 2^{i-1} - 1)$ 의 이진법 표현의 수이며 U_j' 는 X' 의 순환하는 j -직전자이다.

<증명> 정리 5.12에 의하여 $X_{j,k}' = X_{j,0}' \oplus \sum_{l=1}^{k-1} b_l O_{k,0}$ 이 되고 또한

$$\begin{aligned} X_{j,0}' &= \overline{T}(X_{j+1,0}) = T(X_{j+1,0}) \oplus F \\ &= T(O_{j+1,0} \oplus U_{j+1}) \oplus F \quad (\text{정리 5.4에 의해}) \\ &= O_{j,0} \oplus T(U_{j+1}) \oplus F \\ &= O_{j,0} \oplus \overline{T}(U_{j+1}) = O_{j,0} \oplus U_j' \end{aligned}$$

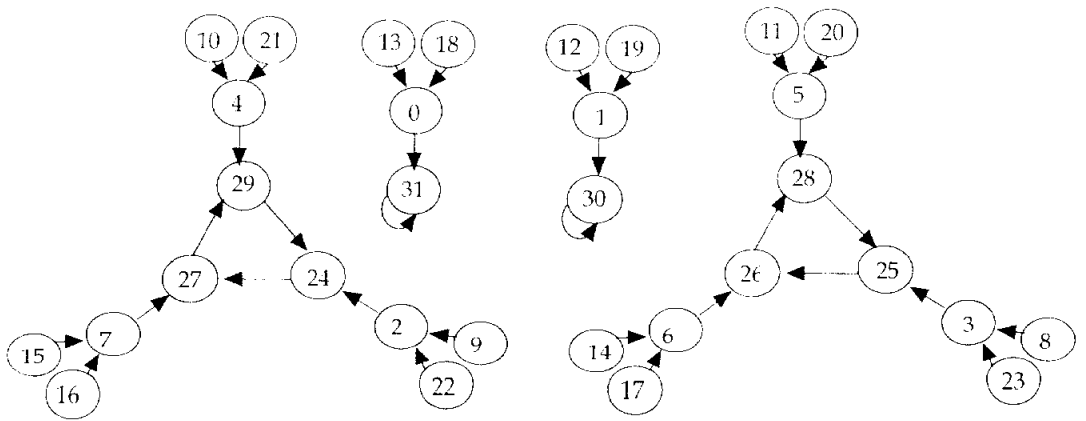
이므로 식 5.18을 얻는다.

위에서 얻은 여원 TPNCA C' 의 분석 결과를 통해 선형 TPNCA C 의 0-트리
의 비순환상태를 여원벡터로 갖는 C' 은 C 와 그 구조가 같다는 것을 알 수 있
다. 또한 C' 의 모든 상태들을 C 의 0-트리의 기본경로와 C' 의 순환상태를 이
용하여 상태들의 합으로 표현할 수 있음을 보임으로써 분석이 어려운 비선형인
 C' 을 C 와 관련지어 보다 효율적으로 분석할 수 있다. 다음의 예는 주어진 선
형 TPNCA C 의 사이클 구조와 0-트리의 기본경로를 이용하여 여원 TPNCA의
상태전이 그래프를 구성하는 예이다.

<예 5.3> 예 5.2의 5-셀 선형 TPNCA에서 여원벡터 F 가 0-트리의 level 1의 상
태 31인 여원 TPNCA의 상태전이 그래프는 그림 5.3과 같다.

$\overline{T}^{-1}F = \overline{T}^0F = 31$ 이 상태 0가 속한 트리의 attractor가 되고 상태 1이 선

형 TPNCA C 에서 attractor이므로 $31 \oplus 1 = 30$ 이 C' 에서 attractor가 된다. C 의 사이클이 $2 \rightarrow 7 \rightarrow 4 \rightarrow 2$ 이므로 $2, 7, 4, 2$ 에 $\overline{T}^{i-1}F = \overline{T}^0F = 31$ 를 더한 $2 \oplus 31 \rightarrow 7 \oplus 31 \rightarrow 4 \oplus 31 \rightarrow 2 \oplus 31$ 즉, $29 \rightarrow 24 \rightarrow 27 \rightarrow 29$ 가 C' 에서 사이클을 이루고 또 $29 \rightarrow 24 \rightarrow 27 \rightarrow 29$ 의 각 상태에 C 의 attractor인 상태 1을 더해서 얻은 사이클 $29 \oplus 1 \rightarrow 24 \oplus 1 \rightarrow 27 \oplus 1 \rightarrow 29 \oplus 1$ 즉, $28 \rightarrow 25 \rightarrow 26 \rightarrow 28$ 도 C' 에서 또 하나의 사이클을 이룬다. 순환상태 29를 root로 하는 29-트리를 구성하기 위하여 먼저 29-트리의 기본경로를 C 의 0-트리의 기본경로와 상태 29의 i -직전자를 이용하여 얻는다. 29-트리의 기본경로의 level 2의 상태는 $13 \oplus 24 = 21$ 이고, 29-트리의 기본경로의 level 1의 상태는 $31 \oplus 27 = 4$ 이다. 그러므로 29-트리의 기본경로는 $21 \rightarrow 4 \rightarrow 29$ 이다. 29-트리의 나머지 상태인 level 2의 두 번째 상태는 식 5.18을 이용하여 $21 \oplus 31 = 10$ 로 얻는다.



<그림 5.3> 5-셀 여원 TPNCA

5.3 TPSACA를 기반으로 하는 완전 해싱기술

5.3.1 TPSACA를 기반으로 하는 완전 해싱이론 및 MRT 계산

본 장에서는 여원 TPSACA와 선형 TPSACA의 성질을 이용해서 설계된 CA를 기반으로 하는 완전 해싱기술에 관해 서술한다. n -비트 선형 TPSACA의 상태 전이 그래프는 상태 0을 attractor로 하는 한 개의 트리로 구성되고 임의의 한 도달 가능한 상태의 직전자는 2개이다. 그러므로 이 CA의 모든 가능한 상태의 수가 2^n 이고 depth를 d 라 하면 다음 식을 만족한다.

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

그러므로 트리의 depth는 항상 n 이다. 따라서 n 셀 선형 TPSACA의 최소다항식은 $x^d \Phi(x) = x^n \Phi(x) = x^n$ 이다.

(1) TPSACA를 기반으로 하는 완전 해싱이론

k 개의 키를 갖는 n -비트 키 집합을 k' 비트 주소($\log_2 k \leq 2^{k'} < n$)로 완전히 해시하는 기초 기술은 다음과 같다:

1. 선형 TPSACA와 여원 TPSACA의 기본경로를 이용하여 해시하기 위한 키 값 x 의 위치를 찾는다.
2. 키 값 x 에 대하여 완전 해시된 주소인 k' 비트들이 그 CA에 의해서 생성

된 연속적인 상태들의 특정한 비트 위치로부터 얻어진다. 임의의 키들의 쌍에 대한 해시된 주소가 적어도 한 비트 위치에서 달라지므로 생성된 주소의 유일성을 보장한다.

보다 자세한 서술을 위해 다음을 정의한다.

<정의 5.2> 한 트리에 속한 임의의 두 상태 x_i 와 x_j 가 l 단계 후 처음으로 상태 y 로서 같아지는 위치에 있다고 하자. 즉, $l = \min \{k | T^k x_i = T^k x_j = y\}$ 이다. 이때 l 을 **MRT**(minimal running time)이라 한다.

위에서 언급한 기술을 상세하게 기술하면 다음과 같다. $X = \{x_1, x_2, \dots, x_k\}$ 를 주어진 k 개의 키를 원소로 갖는 집합이라 하고 W 를 완전 해시주소를 생성하기 위하여 사용된 특성행렬 T 를 갖는 TPSACA라 하자. 집합 X 의 각 원소가 W 의 상태전이 그래프의 제일 위쪽 level에 속한다고 하자. x_i 와 x_j 를 X 에 있는 두 개의 키 값이고, MRT가 l 이라 하자. 그러면 $T^l(x_i) = T^l(x_j) = y$ 이다. 또한 $T^{l-1}(x_i)(:= p_1)$ 과 $T^{l-1}(x_j)(:= p_2)$ 는 y 의 서로 다른 직전자이다. 따라서 $p_1 \oplus p_2(= z)$ 는 상태 0의 0이 아닌 직전자이다. 그러므로 만일 z 의 r 번째 비트($r=0, 1, 2, \dots, (n-1)$)가 1이면 p_1 과 p_2 중 한 상태만 r 번째 비트가 1이 되어야 하며, z 의 r 번째 비트가 0이면 p_1 과 p_2 의 r 번째 비트가 서로 같아야 한다. 이러한 이유로 pivot 비트 위치의 개념이 필요하다.

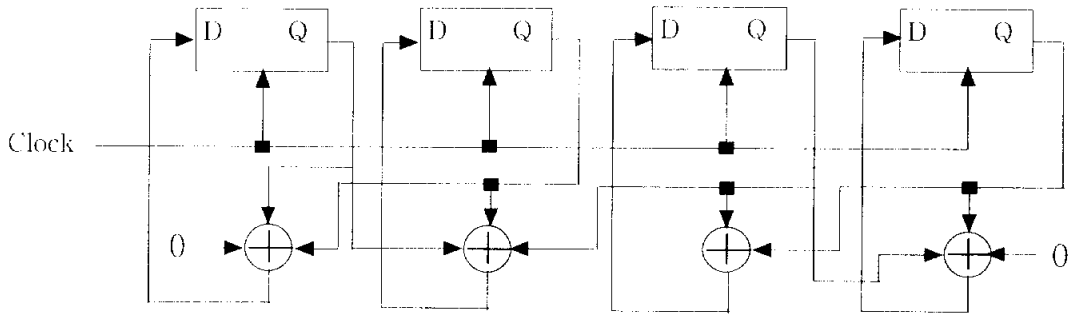
<정의 5.3> TPSACA의 상태전이 그래프에서 상태 0의 0이 아닌 직전자의 이진 표현에서 가장 오른쪽에 있는 1의 비트 위치를 **PB**(Pivot Bit) 위치라 한다.

p_1 과 p_2 는 PB 위치에서 서로 구별될 수 있다. x_i 의 해시된 주소는 p_1 로부터 얻어진 PB 위치의 비트 값을 가지며 x_j 의 해시된 주소는 p_2 로부터 얻어진 PB 위치의 비트 값을 가지게 된다. 결국 x_i 와 x_j 는 서로 다른 해시된 주소로 전달된다.

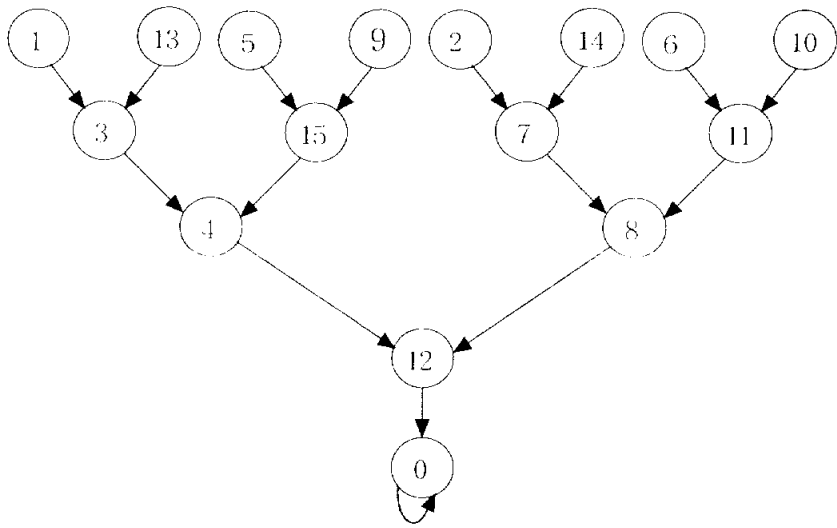
<예 5.4> 4-셀 선형 CA의 전이규칙이 <150, 150, 102, 150>인 CA를 W 라 할때 W 의 전이행렬 T 는 다음과 같다.

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

T 의 계수는 3이며 $(T \oplus I)$ 의 계수는 4이다. 또한 W 의 특성다항식과 최소다항식은 모두 x^4 이다. 그러므로 W 는 TPMACA의 특별한 부류인 TPSACA이다. 5.2.3에서 제안한 트리 구성 알고리즘에 따라 0-트리의 기본경로 $1 \rightarrow 2 \rightarrow 5 \rightarrow 8 \rightarrow 0$ 를 구하고 (Step 1~Step 4), Step 5에 의하여 0-트리의 나머지 부분을 구성한다. 그림 5.4은 W 의 상태전이 그래프 및 구조이다. 그림 5.4에서 0의 0이 아닌 직전자는 12(1100)이므로 PB 위치는 두 번째 비트이다. 1과 5가 키로 주어진다면 두 키의 MRT는 2이다. 4장 3절에 제안된 트리 구성 알고리즘을 이용하여 0-트리의 기본경로로부터 키 1과 5의 위치가 level 4의 0번째와 2번째이므로 상태 1은 level 3에서 0번째 상태가 되고, 상태 5는 level 3의 1번째 상태가 된다. 0-트리의 기본경로를 이용하여 해당 상태를 구하면 level 3의 0번째 상태는 3(0011)이고 첫 번째 상태는 15(1111)이므로 PB위치의 값을 기준으로 하여 1과 5의 해시된 주소를 0과 1로 한다.



(a) 구조



(b) 상태전이 그래프

<그림 5.4> 4-셀 TPSACA의 구조 및 상태전이 그래프

(2) MRT의 계산

집합 X 에 있는 주어진 원소 x 에 대한 완전 해시된 주소는 주어진 TPSACA에 x 를 로드하여 기본경로를 이용하여 원소 x 의 위치를 정확히 알아내고 또한 이로써 다음상태의 위치를 알아내어 그 결과의 상태들로부터 PB 번째 비트를 추출함으로써 함으로써 생성될 수 있다. 결과는 $(n-1)$ -비트 주소를 생성한다. 그러나 만일 집합 $Z = \{z = x_1 \oplus x_2 \mid x_1, x_2 \in X, x_1 \neq x_2\}$ 가 상태전이 그래프의 레벨 l 의 어떤 상태도 갖지 않는다면, 키 집합 X 의 가능한 모든 키의 순서쌍 중 MRT가 l 인 순서쌍은 없다. $(n-l+1)$ 번째 레벨에 대응하는 주소 비트를 얻을 필요가 없다. 이렇게 함으로써 주소비트가 $(n-2)$ 비트로 2비트가 줄어든다. 그러므로 주어진 키 집합에 대하여 임의의 키 순서쌍의 MRT를 구하는 것은 해시되는 주소의 비트수를 결정하는데 중요한 요인이 된다.

TPSACA의 같은 트리에서 동일한 레벨에 놓여있는 두 상태의 키 순서쌍 (x_i, x_j) 의 MRT는 기본경로에 의하여 구해진 두 상태의 위치를 XOR하여 얻을 수 있다. x_i 와 x_j 가 최상위 레벨 d 에 놓여있는 두 상태라 하자. 그리고 $b_i (i=1, \dots, d-1)$ 를 x_i 상태의 레벨 d 에서 위치를 이진표현으로 나타내었을 때의 각각의 위치 비트라 하고, $b'_i (i=1, \dots, d-1)$ 를 x_j 상태의 레벨 d 에서 위치를 이진표현으로 나타내었을 때의 각각의 위치 비트라 하면 c_i 를 다음과 같이 구한다.

$$c_i = b_i \oplus b'_i, (i=1, \dots, d-1) \quad (5.19)$$

식 5.19에서 구한 c_i 값 중 1인 최소 i 를 찾는다. 이때 두 순서쌍의 MRT는 $(d-i)$ 이다.

<예 5.5> 그림 5.4의 TPSACA W 에 대하여 주어진 키 집합이 $X = \{1, 13, 2, 14\}$ 이라 하면 모든 키들은 최상위 레벨(도달 불가능한)의 상태이다. 상태 0의 0이 아닌 직전자가 12(1100)이므로 PB의 위치는 두 번째 비트이다. 0-트리의 기본경로를 이용하여 키 집합의 각 원소들의 최상위 레벨에서 위치가 각각 0, 1, 4, 5 번째 상태이다. 이 상태들이 1단계 상태변화 후 level 3에서 위치는 각각 0, 0, 2, 2이다. 이는 키 순서쌍 (1, 13)과 (2, 14)의 MRT가 1임을 나타내므로 각 상태의 PB위치의 비트에서 구별이 된다.

다시 위의 과정을 반복하여 각 키가 2단계 상태변화 후 즉 level 2에서 위치가 0, 0, 1, 1이고 3단계 상태변화 후 모든 상태들은 level 1에서 모두 0 번째 상태인 상태 0의 0이 아닌 직전자 12가 된다. 그러므로 나머지 가능한 키의 순서쌍은 (1, 2), (1, 14), (13, 2), (13, 14)이고 이 순서쌍의 MRT는 모두 3이다. 그러므로 2단계 상태 변화 후 각 상태의 PB 위치에서 비트 값을 선택한다. 각 순서쌍은 MRT가 2인 경우가 없으므로 해시되는 주소의 비트수를 하나 줄일 수 있다. 그러므로 X 에 속한 모든 키를 2 비트로 해시된 주소를 생성할 수 있다. 다음 표 5.1은 주어진 키를 해시하는 과정이다. 한 상태의 현재 레벨의 위치에서 다음 상태의 한 단계 아래의 레벨의 위치는 현재 위치를 2로 나눈 몫과 같다.

Level 4		Level 3		Level 2		Level 1		해시된 주소
상태	위치	상태	위치	상태	위치	상태	위치	
1 (0001)	0	3 (0011)	0	4 (0100)	0	12	0	01
13 (1101)	1	3 (0011)	0	4 (0100)	0	12	0	11
2 (0010)	4	7 (0111)	2	8 (1000)	1	12	0	00
14 (1110)	5	7 (0111)	2	8 (1000)	1	12	0	10

<표 5.1> 주어진 키의 해시 과정

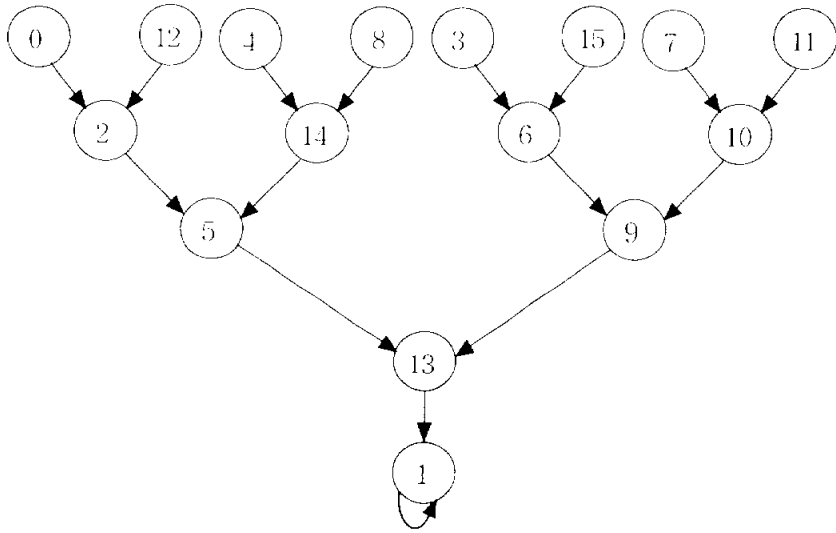
지금까지는 집합 X 의 각 원소들이 주어진 TPSACA의 상태전이 그래프에서 가장 위쪽 레벨에 있는 경우만을 언급하였다. 이것은 일반적이지 못한 방법이다. 이제부터는 완전히 일반적인 경우에 대하여 언급하고자 한다.

주어진 집합 X 가 주어진 부분집합 X_1 과 X_2 로 이루어졌다고 하자. 여기서 X_1 의 원소들은 주어진 TPSACA의 상태전이 그래프에서 최상위 레벨에 위치하고 X_2 의 원소들은 나머지 레벨에 위치한다. 여기서 W 의 도달 불가능한 상태 중 하나인 F 를 여원벡터로 취함으로써 얻어진 여원 $CA(=V)$ 의 상태전이 그래프에서 상태 0이 도달 불가능한 상태가 된다. 또한 여원 CA V 에서 W 의 도달 불가능한 상태는 도달 가능한 상태가 되고 도달 가능한 상태는 도달 불가능한 상태가 된다. 5.2.3절의 트리 구성 알고리즘으로부터 여원 TPSACA의 기본경로와 선형 TPSACA의 기본경로를 이용하여 선형 TPSACA로 해시할 수 없었던 X_2 의 키들을 해시한다. 이때 해시된 주소는 주어진 키가 선형 TPSACA로 해시

된 것인지, 아니면 여원 TPSACA로 해시된 것인지를 구별하는데 한 비트가 소요된다.

<예 5.6> 그림 5.4(b)에 대하여 주어진 키 집합이 $X = \{1, 13, 2, 14, 3, 15, 12, 0\}$ 이라 하면 키 집합 X 를 키가 선형 TPSACA의 상태전이 그래프에서 놓여있는 위치에 따라 최상위 레벨인 경우 $X_1 = \{1, 13, 2, 14\}$ 과 그렇지 않은 경우 $X_2 = \{3, 15, 12, 0\}$ 로 나눌 수 있다. 집합 X_2 의 키를 해시하기 위해 그림 5.4(b)로부터 여원벡터가 2인 여원 TPSACA를 이용한다. 그림 5.5은 예 5.4의 선형 TPSACA로부터 유도된 여원 TPSACA의 상태전이 그래프이다. 키 3, 15, 12, 0을 해시하는 방법은 선형 TPSACA를 이용하여 해시하는 방법과 동일하다. 이때 사용되는 여원 TPSACA의 기본경로는 $0 \rightarrow 2 \rightarrow 5 \rightarrow 13 \rightarrow 1$ 이다. 표 5.2는 주어진 키 집합 X_2 를 해시하는 과정이다. 그러므로 주어진 키 집합의 해시된 주소는 다음과 같다. 여기에서 해시된 주소의 맨 마지막 비트의 값이 0인 경우는 키가 선형 TPSACA를 이용하여 해시된 것임을, 비트 값이 1인 경우는 여원 TPSACA를 이용하여 해시된 경우임을 나타낸다.

1 : 010	13 : 110	2 : 000	14 : 100
3 : 001	15 : 101	12 : 111	0 : 011



<그림 5.2> 여원벡터가 2인 4-셀 여원 TPSACA의 상태전이 그래프

Level 4		Level 3		Level 2		Level 1		해시된 주소
상태	위치	상태	위치	상태	위치	상태	위치	
3 (0011)	4	6 (0110)	2	9 (1001)	1	13	0	00
15 (1111)	5	6 (0110)	2	9 (1001)	1	13	0	10
12 (1100)	1	2 (0010)	0	5 (0101)	0	13	0	11
0 (0000)	0	2 (0010)	0	5 (0101)	0	13	0	01

<표 5.2> 주어진 키 집합 X_2 를 해시하는 과정

5.3.2 TPSACA를 기반으로 하는 완전 해싱 알고리즘

본 절에서는 5.2.3절의 트리 구성 알고리즘과 5.3.1절에서 언급한 TPSACA를 기반으로 하는 완전 해싱이론과 MRT 계산법을 이용하여 TPSACA를 기반으로 하는 완전 해싱 알고리즘을 서술한다.

Step 1. 선형 TPSACA의 기본경로로부터(트리구성 알고리즘: Step 1 ~ Step 4) 최상위 레벨의 상태를 구하고(트리구성 알고리즘: Step 5) 주어진 키 집합 (X)에서 선형 TPSACA의 최상위 레벨에 해당하는 키의 부분집합 (X_1)을 찾고 각 키의 위치를 찾는다.

Step 2. 선형 TPSACA에서 상태 0의 0이 아닌 직전자로부터 PB위치를 찾는다.
 $X = X_1$ 이면 Go To Step 4.

Step 3. $X_2 = X - X_1$ 라하고 선형 TPSACA의 임의의 도달 불가능한 상태가 여원벡터 F 가 되는 선형 TPSACA로부터 유도된 여원 TPSACA의 기본 경로 $0 \rightarrow \overline{T}0 (= F) \rightarrow \dots \rightarrow \overline{T^d}0 (= \overline{T}^d F)$ 를 구하고(트리구성 알고리즘: Step 9), 여원 TPSACA의 최상위 레벨의 상태를 구한다(트리구성 알고리즘: Step 10). 키 부분집합 X_2 의 각 원소에 대하여 여원 TPSACA의 최상위 레벨에서의 위치를 찾는다.

Step 4. X_1 과 X_2 의 각각의 모든 키 순서쌍 (x_i, x_j) 의 MRT를 계산하여 MRT집합 M 을 구한다.

Step 5. X_1 과 X_2 의 각 원소의 위치를 나타내는 $b_i (i=1, \dots, d-1)$ 에 대하여 오른쪽에서부터 한 비트씩 줄여가면서 해당 하위 레벨에서의 상태들을 구하고 M 의 원소 $m_i (1 \leq i \leq d-1)$ 에 대하여 $(d+1-m_i)$ 레벨에서 각 상태의 PB 위치의 비트를 추출한다.

Step 6. $X = X_1$ 또는 $X = X_2$ 이면 Stop.

Step 7. X_1 에 속한 키의 해시된 주소의 맨 오른쪽에 0을, X_2 에 속한 키의 해시된 주소의 맨 오른쪽에 1을 부여한다.

6. 결론

CA는 LFSR과 비교하여 랜덤성이 우수하다는 것이 알려지면서 LFSR의 대안으로 의사 랜덤 패턴 생성기, 해쉬 함수, 스트림 암호 알고리즘, 오류 정정 부호의 설계 등의 고속화 응용에 많이 활용되고 있다. Nongroup CA는 group CA에 비하여 그 응용분야가 적은 것이 사실이지만 최근 부울 방정식의 해법, 해쉬 함수, 이미지 처리 등 그 응용분야가 넓어지고 있다. 그러나 CA를 이용하여 암호 알고리즘이나 해쉬함수를 생성함에 앞서 CA에 대한 안전성 분석과 CA의 상태전이 행동분석이 먼저 이루어져야 할 것이다. 본 논문은 가산 CA를 group CA와 nongroup CA로 나누어 각각 분석하였다. 먼저 group CA의 사이클 구조를 주어진 전이행렬의 최소다항식과 관련지어 특성화함으로 다양한 주기를 갖는 group CA에 대한 분석이 이루어졌다. 또한 여원 nongroup CA가 비선형이므로 선형 nongroup CA보다 분석에 어려움이 있으므로 이러한 CA를 선형 nongroup CA로부터 유도된 CA로 전이행렬과 여원벡터를 이용하여 여원 CA의 상태전이 행동을 선형 nongroup CA와 관련지어 분석하였다. 이러한 분석의 결과물의 하나인 TPNCA의 트리 구성 알고리즘을 이용하여 TPSACA를 기반으로 하는 완전 해싱알고리즘을 제안하였다.

참 고 문 헌

- [1] S. Bhattacharjee, U. Raghavendra, D.R. Chowdhury and 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 and 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 and 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 and 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 and 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. Chakraborty, D.R. Chowdhury and P.P. Chaudhuri, *Theory and application of non-group cellular automata for synthesis of easily testable finite state machines*, IEEE Transactions of Computers, Vol. 45, No. 7, 1996, pp. 769-781.
- [7] S. Chattopadhyay, D.F. Chowdhury, S. Bhattacharjee and P.P. Chaudhuri, *Cellular-automata-array-based diagnosis of board level faults*, IEEE Transactions of Computers, V. 47, No. 8, 1998, pp. 817-828

- [8] S. Chattopadhyay, *Some studies on theory and applications of additive cellular automata*, Ph.D. Thesis, I.I.T., Kharagpur, India, 1996.
- [9] P.P. Chaudhuri, D.P. Chowdhury, S. Nandi and S. Chattopadhyay, *Additive cellular automata theory and applications*, Vol. 1, IEEE Computer Society Press, California, USA, 1997.
- [10] 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.
- [11] S.J. Cho, U.S. Choi and H.D. Kim, *Analysis of complemented CA derived from a linear TPMACA*, Comput. & Math. Appl., Vol. 45, 2003, pp. 689-698.
- [12] S.J. Cho, H.D. Kim and U.S. Choi, *Behavior of complemented cellular automata derived from a linear cellular automata*, Mathematical and Computer Modelling, Vol. 36, 2002, 979-986.
- [13] D.R. Chowdhury, S. Basu, I.S. Gupta and P.P. Chaudhuri, *Design of CAECC-cellular automata based error correcting code*, IEEE Transactions of Computers, Vol. 43, No. 6, 1994, pp. 759-764.
- [14] D.R. Chowdhury, I.S. Gupta and P.P. Chaudhuri, *CA-based byte error-correcting code*, IEEE Transactions of Computers, Vol. 44, No. 3, 1995, pp. 371-382.
- [15] D.R. Chowdhury, S. Basu, I.S. Gupta and P.P. Chaudhuri, *A novel scheme for designing error correcting codes using cellular automata*, TENCON '91.1991 IEEE Region 10 International Conference on EC3-Energy, Computer, Communication and Control Systems , Volume: 3 , Aug. 28-30, 1991, pp. 231-235
- [16] D.R. Chowdhury, I.S. Gupta and P.P. Chaudhuri, *A programmable*

- cellular automata structure for built-in self-test*, TENCON '91.1991 IEEE Region 10 International Conference on EC3-Energy, Computer, Communication and Control Systems , Volume: 3 , Aug. 28-30, 1991, pp. 166-170
- [17] A.K. Das and P.P. Chaudhuri, *Efficient characterization of cellular automata*, Proc. IEE(part E), Vol. 137, No. 1, 1990, pp. 81-87.
- [18] 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.
- [19] A.K. Das, D. Saha, A.R. Chowdhury, S. Misra and P.P. Chaudhuri, *Signature analysers based on additive cellular automata*, Fault-Tolerant Computing, FTCS-20. Digest of Papers., 20th International Symposium , 26-28 June 1990, pp. 265-272
- [20] P. Dasgupta, S. Chattopadhyay, P.P. Chaudhuri and I. Sengupta, *Cellular automata-based recursive pseudoexhaustive test pattern generator*, IEEE Transactions of Computers, Vol. 50, No. 2, 2001, pp. 177-185.
- [21] P.D. Hortensius, R.D. McLeod and H.C. Card, *Cellular automata based pseudorandom number generators for built-in self test*, IEEE Trans. on DAS of Integrated Circuits and System, Vol. 8, 1989, pp. 842-859.
- [22] M. Mihaljevic and 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.
- [23] M. Mihaljevic, Y. Zheng and H. Imai, *A fast and secure stream cipher based on cellular automata over $GF(q)$* , IEEE Global Telecommu-

- nications Conference, GLOBECOM '98, Vol. 6, 1998, pp. 3250-3255.
- [24] J. Von Neumann, *Theory of self-reproducing automata*, University of Illinois Press Urbana, 1966.
- [25] M. Tomassini, M. Sipper and M. Perrenoud, *On the generation of high-quality random numbers by tow-dimensional cellular automata*, IEEE Transactions of Computers, Vol. 49, No. 10, 2000, pp. 1146-1151.
- [26] S. Wlofram, *Cellular automata and complexity*, Addison-Welsly Publishing Company, 1994.
- [27] S. Wolfram, *Statistical mechanics of cellular automata*, Rev. Modern Physics, Vol. 55, No. 3, 1983.
- [28] C.N. Zhang, M. Deng and R. Mason, *Two improved algorithms and hardware implementations for key distribution using extended programmable cellular automata*, Computer Security Applications Conference, Proceedings, 14th Annual , 7-11 Dec. 1998, pp. 244 -249

감사의 글

6년 간의 대학원 생활은 힘들 때도 있었지만, 학문의 연구하는 기쁨을 알게된 행복한 시간이었으며 축복의 시간이었습니다. 무엇보다도 「꿈을 계속 간직하고 있으면 반드시 실현할 때가 온다 -괴테」는 말을 실감할 수 있었던 시간이었습니다. 지금까지 나의 가는 길을 인도하시며 힘이 되신 하나님께 감사와 영광을 돌려드립니다.

이 논문을 완성하기까지 주위의 모든 분들로부터 수많은 도움을 받았습니다. 늘 가까이서 부족한 제자를 이해해 주시고, 저에게 칭찬과 격려를 아끼지 않으셨던 조성진 지도교수님께 머리 숙여 감사 드립니다. 보다 나은 논문을 완성할 수 있도록 조언해 주시고, 마지막까지 최선을 다할 수 있도록 지도해 주신 심사위원 이경현 교수님, 박지환 교수님께 감사의 마음을 전합니다. 항상 인자함과 끊임없는 관심으로 지도해 주신 표용수 교수님과 인제대 김한두 교수님께도 감사 드립니다. 오며 가며 늘 격려해주셨던 박용범 교수님, 신준용 교수님, 박진한 교수님 그리고 수리과학부 모든 교수님들께 감사 드립니다.

아울러 아낌없는 성원을 보내주며 즐거운 대학원 생활이 되게 해준 응용수학과 대학원의 여러 선배님들, 동기들, 후배들에게 고마움을 전합니다. 그리고 항상 격려해주며 의지가 되어준 CA연구실의 후배 성훈씨, 윤희, 성가, 귀자, 세영이와 최향희선생님께 감사의 마음을 전합니다. 논문이 통과되는 마지막 순간까지 기도로 힘이 되어준 사랑하는 가야교회 고등부의 박영삼 전도사님과 여러 선생님들 그리고 고3 우리 반 친구들에게도 고마움을 전합니다.

삶에 대한 열정과 성실함을 어릴 때부터 길러주신 친정부모님, 부족한 며느리를 위해 늘 기도하시고 아이들을 돌보아 주신 사랑하는 시부모님께 깊은 감사 드립니다. 공부를 다시 시작할 수 있도록 곁에서 힘이 되어주며, 외조를 아끼지 않은 사랑하는 믿음의 동역자인 남편 광석씨와 하나님께서 주신 귀한 선물인 보석 같은 옥찬이와 의찬이에게 감사하며 이 작은 결실을 바칩니다.