교 육 학 석 사 학 위 논 문

90/150 TPNCA의 합성과 분석

2009년 8월

부경대학교 교육대학원

수 학 교 육 전 공

김 영 미

교 육 학 석 사 학 위 논 문

90/150 TPNCA의 합성과 분석

지도교수 조 성 진

이 논문을 교육학석사 학위청구논문으로 제출함.

2009년 8월

부경대학교 교육대학원

수 학 교 육 전 공

김 영 미

김영미의 교육학석사 학위논문을 인준함.

2009년 8월 26일

주 심 이학박사 표 용 수 (인)

위 원 이학박사 박 진 한 (인)

위 원 이학박사 조 성 진 (인)

목 차

표 목차

그림 목차

Synthesis and analysis of 90/150 two predecessor nongroup cellular automata

Young Mi Kim

Graduate School of Education

Pukyong National University

Abstract

In this thesis, using algorithm for finding 90/150 Two Predecessor Nongroup Cellular Automata(TPNCA) and analyzing 90/150 TPNCA. In particular we analyze n-cell 90/150 Two Predecessor Single Attractor CA(TPSACA) whose minimal polynomial is x^n and n-cell Two Predecessor Multiple Attractor CA(TPMACA) whose minimal polynomial is $x^{n-1}(x+1)$ which are useful to study hashing. Also we analyze two types of 90/150 TPNCA. One is TPNCA for the minimal polynomial whose type is of the form $xp(x)$, where $p(x)$ is a primitive polynomial of degree $n-2$. Another is TPNCA for the minimal polynomial whose type is of the form $x(x+1)p(x)$, where $p(x)$ is a primitive polynomial of degree $n-1$.

Ⅰ. 서론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 Von Neumann과 Ulam에 의해서 스스로 조직화하고 재생산할 수 있는 모델로 소개되었다[18, 22]. CA는 셀이라 불리는 메모리의 배열로 이루어진 이산 시간의 동적 시스템이다. 배열 속에서 셀의 상태는 다음의 규칙에 따라 갱신된다. 각 셀은 자기 자신의 상태와 이전단계의 이웃 셀의 상태에 의해 다음 상태가 결정된다. CA는 테스터 패턴 생성, 의사난수생성기, 암호학, 오류정정부호기, 압축치 분석과 같은 많은 분야에서 응용되고 있다[2, 4, 12, 13, 15, 16, 20, 21]. 그룹 CA의 상태전이행동의 분석은 많은 연구자들에 의해 연구되어왔다[1, 8, 11, 12, 15-17, 19, 20]. 그룹 CA의 연구는 연구자들로부터 상당한 주목을 받았지만 비그룹 CA의 연구는 그렇지 못했다. 그룹 CA의 상태전이행렬은 정칙(nonsingular)이다. 그러나 비그룹 CA의 상태전이행렬은 비정칙(singular)이다. 최근 비그룹 CA의 흥미로운 특성들이 여러 분야에서 사용되고있다[2, 5-7, 9, 10, 13]. 특히 D1*CA[2, 5]로 나타내는 특별한 부류의 비그룹 CA의 연구가 수행되었고, 이 연구에 기반을 두고 D1*CA가 합성 디자인의 테스트 능력을 강화하기 위하여 유한상태기계에 효율적으로 장착될 수 있는 이상적인 테스트 기계로서 제안되었다. 또한 [13]에서 그들은 $x(x+1)p(x)$형태의 최소다항식을 가지는 90/150 Two Predecessor Nongroup Cellular Automata(이하, TPNCA)를 연구했다. 여기서 $p(x)$는 원시다항식이다. 이런 CA를 사용하면 하드웨어 구현이 간단해지고 이 차함수와 관련된 행렬을 얻기 위한 여러 계산을 피할 수 있다. 따라서 그들은 CA길이가 다른 여러 가지 경우를 연구했지만 그들은 $n \geq 6$에 대해서 n-셀 90/150 TPNCA가 존재한다는 것은 보여주지는 못했다. 본 논문에서 90/150 TPNCA를 찾기 위한 알고리즘을 사용하여 90/150 TPNCA를 분석한다. 특히

최소다항식이 x^n인 n-셀 90/150 Two Predecessor Single Attractor CA(이하, TPSACA)과 해싱연구에 유용한 최소다항식이 $x^{n-1}(x+1)$인 n-셀 Two Predecessor Multiple Attractor CA(이하, TPMACA)를 분석한다[5]. 또한 두 가지 형태의 90/150 TPNCA를 분석한다. 하나는 depth가 1인 D1*CA[2] 과 같은 90/150 TPNCA연구에 유용한 최소다항식이 $xp(x)$형태인 TPNCA이다. 제시된 n-셀 90/150 TPNCA는 D1*CA보다 길이가 길며, 길이가 $2^{n-1}-1$인 최대길이 주기를 가진다. 또 다른 하나는 90/150 비그룹 CA[13]에 기초한 의사난수생성기 연구에 유용한 최소다항식이 $x(x+1)p(x)$의 형태인 90/150 TPNCA이다. 여기서 $p(x)$는 원시다항식이다.

Ⅱ. CA의 기본지식

2.1 CA 기본 지식

CA는 규칙적인 방법으로 배열되어진 관련 있는 셀의 수로 이루어져 있다 [22]. 각 셀의 상태전이는 그들의 이웃하는 상태에 의존한다. 만일 셀의 다음 상태함수가 진리표상태로 나타나 있다면 출력의 십진수의 대응은 셀에 대한 규칙수로 불린다.

이웃상태	111	110	101	100	011	010	001	000	전이규칙
다음상태	0	1	0	1	1	0	1	0	90
다음상태	1	0	0	1	0	1	1	0	150

<표 2.1> 전이 규칙 90과 150

2.2 CA의 전이행렬

n개의 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 i번째 셀의 규칙을 나타낸다. CA가 다음 상태로 전이될 때 i번째

셀이 j번째 셀에 영향을 받으면 $t_{ij}=1$이고 그렇지 않으면 $t_{ij}=0$이다. 3-이웃 NBCA의 전이행렬은 정방행렬의 주 대각선과 그 윗 대각선과 아래 대각선을 제외한 나머지가 0인 삼중 대각행렬(tridiagonal matrix)이다. 예를 들어 4-셀 NBCA의 규칙이 <102, 90, 150, 204>이면 전이행렬은 다음과 같다.

$$T=\begin{pmatrix}1&1&0&0\\1&0&1&0\\0&1&1&1\\0&0&0&1\end{pmatrix} \tag{2.1}$$

S_t가 시간 t에서 CA의 상태를 나타내면 시간 $t+1$에서 CA의 상태는 다음과 같다.

$$S_{t+1}=TS_t \tag{2.2}$$

또한 시간 $t+2$에서 CA의 상태는 다음과 같다.

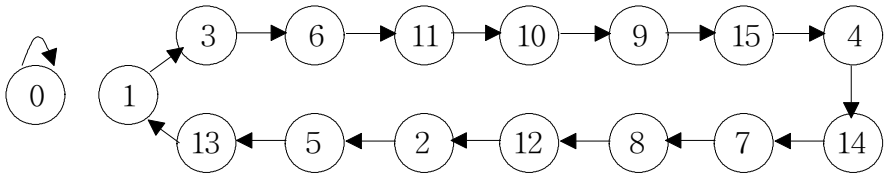
$$S_{t+2}=TS_{t+1}=T(TS_t)=T^2S_t \tag{2.3}$$

같은 방법으로 p 단계 후의 CA의 상태는

$$S_{t-1}=T^{-1}S_t \tag{2.4}$$

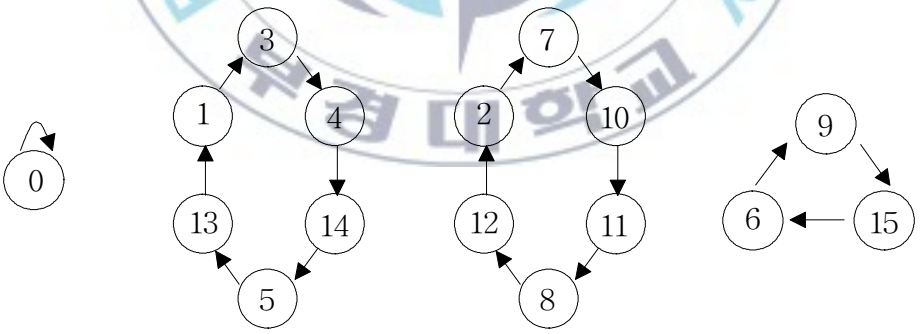
이다. 그룹 CA는 최대길이를 갖는 CA와 최대길이를 갖지 않는 CA로 구별할 수 있다. n개의 셀로 이루어진 CA에서 모든 셀의 상태가 0인 경우를 제외한

2^n-1개의 상태가 하나의 주기 안에 있는 CA를 최대길이 CA(Maximal length CA, 이하 MLCA)라 한다. 그림 2.1은 전이규칙이 <150, 150, 90, 150>인 4-셀 MLCA의 상태전이 그래프이다.



<그림 2.1> 최대길이를 갖는 CA

그림 2.2는 최대길이를 가지지 않는 선형 CA로 전이규칙이 <150, 150, 150, 150>인 uniform CA 이다. 그림에서 알 수 있듯이 0을 제외한 다른 상태들이 몇 개의 서로 다른 사이클로 분리되어 있다. 각 사이클 길이의 최소공배수 6이 CA의 주기가 된다.

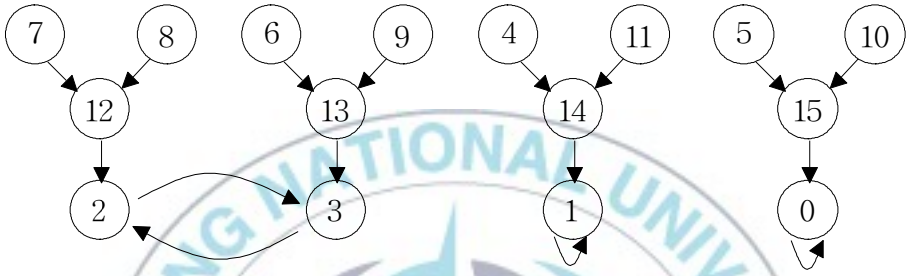


<그림 2.2> 최대길이를 갖지 않는 그룹 CA

그룹 CA가 아닌 비그룹 CA는 전이행렬 T 가 비정칙이다. 따라서 T 의 역행렬이 존재하지 않으므로 임의의 상태에 대하여 이전상태를 명확하게 알 수 없다. 그림 2.3은 전이규칙이 <150, 60, 60, 150>인 비그룹 CA의 상태전이 그

래프이다. 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 2.3> 비그룹 CA

선형 비그룹 CA는 다음 상태를 결정짓는 상태전이 함수가 XOR 논리로만 이루어진 CA로 그룹 CA가 아니 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 0이거나 2 이상이다. 어떤 상태의 이전상태 수가 0이면 도달 불가능한 상태이다. 이전상태 수가 2 이상이란 의미는 주어진 상태가 도달 가능한 상태이며, 2개 이상의 이전상태가 존재한다는 것을 말한다. 이처럼 비그룹 CA는 상태전이 함수가 일대일 대응 함수가 아니다. 그러므로 주어진 상태에 대하여 이전상태를 구하는 것이 불가능하다. 다음은 선형 비그룹 CA와 이 논문의 전개에 필요한 몇 가지 용어들을 정의한다.

<정의 2.1 [5, 7, 9, 10]> ⅰ) **Group CA** : 모든 셀들의 상태가 상태전이그래

프에서 싸이클을 이루면 그룹 CA, 그렇지 않다면 비그룹 CA이다.

ii) **Attractor** : 자기루프를 가진 상태를 attractor라 한다. attractor는 단위 순환 길이를 가진 순환의 상태를 보여준다.

iii) **Depth** : 비그룹 CA의 상태전이그래프에서 임의의 도달불가능 상태에서 가장 가까운 순환상태까지 전이되는데 걸리는 최소 상태전이 수를 말한다.

iv) **Multiple-attractor CA(MACA)** : 상태전이그래프가 각 attractor를 root로 하는 서로 분리된 트리들로 구성된 비그룹 CA를 multiple-attractor CA라 한다. Single Attractor CA(SACA)는 attractor가 하나인 MACA이다.

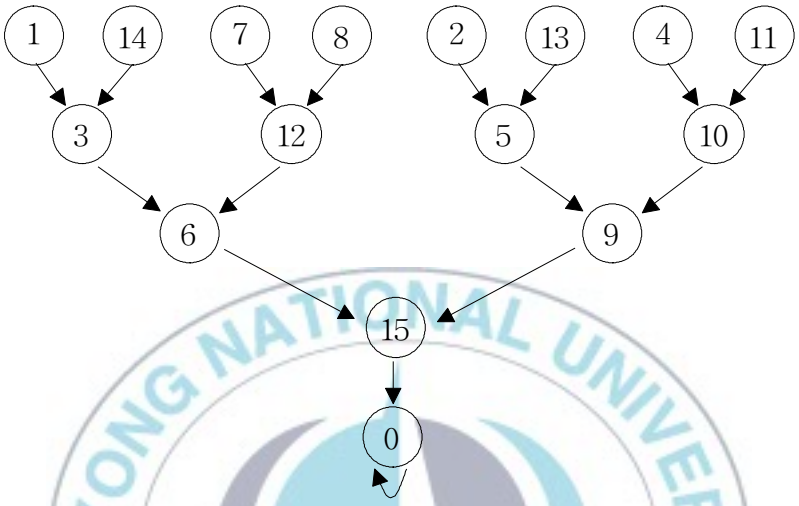
v) **TPMACA** : TPMACA는 상태전이그래프에서 도달가능한 상태의 직전자 수가 두 개인 MACA이다. TPSACA는 상태전이그래프에서 도달가능한 상태의 직전자 수가 두 개인 SACA이다. n-셀 TPSACA의 최소다항식은 x^n이다.

그림 2.3에서 순환상태는 0, 1, 2, 3 이다. 특히 상태 0과 1은 사이클의 길이가 1이므로 attractor이다. 상태 2, 3 은 사이클의 길이가 2 인 사이클이 존재한다. 그러므로 이 CA의 주기는 1과 2의 최소공배수인 2이다. 각 트리는 depth가 2이다. 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 2에 있는 상태들은 4, 5, 6, 7, 8, 9, 10, 11 이다. 다음은 4-셀 TPMACA의 예이다.

<예제 2.2> 4-셀 CA의 전이규칙이 <150, 90, 90, 150>일 때, 전이행렬은

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

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



<그림 2.4> 4-셀 TPSACA

그림 2.4는 예 2.1에서 주어진 CA에 대한 상태전이 그래프로 TPSACA이다.

Ⅲ. 90/150 TPNCA의 합성

이 장에서 90/150 TPNCA를 찾기 위한 알고리즘을 소개한다.

상삼각행렬 U를 다음과 같다고 하자.

$$U=\begin{pmatrix} 1 & a_1 & * & \cdots & * & * & * \\ 0 & 1 & a_2 & \cdots & * & * & * \\ 0 & 0 & 1 & \cdots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-2} & * \\ 0 & 0 & 0 & \cdots & 0 & 1 & a_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

90/150 삼중대각행렬 T를 다음과 같다고 하자.

$$T=\begin{pmatrix} d_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & d_2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & d_3 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & d_{n-1} & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & d_n \end{pmatrix}$$

이후로 우리는 행렬 T를 $T=<d_1, d_2, \cdots, d_n>$, $d_i \in \{0,1\}$로 나타낸다.

$f(x)=x^n+c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0$, $c_i \in GF(2)$라 할때, 다음과 같은 $n\times n$행렬 C를 $f(x)$의 동반행렬이라고 한다.

$$C=\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}$$

<정의 3.1 [14]> 주어진 n-벡터 x와 $n\times n$행렬 M에 대하여 $K(M, x)=(x; Mx; M^2x;\cdots M^{n-1}x)$라 하자. $K(M, x)$는 Krylov행렬 이라하고, x는 seed 벡터라 한다.

<정리 3.2 [11]> $T=<d_1, d_2, \cdots, d_n>$라 하고, C를 T의 특성다항식의 동반행렬이라 하자. U가 $TU=UC$를 만족하는 위와 같은 상삼각행렬이면 다음식이 성립한다.

$$\begin{cases} d_1 = a_1 \\ d_2 = a_1 \oplus a_2 \\ d_3 = a_2 \oplus a_3 \\ \quad\vdots \\ d_{n-1} = a_{n-2} \oplus a_{n-1} \\ d_n = a_{n-1} \oplus c_{n-1} \end{cases} \tag{3.1}$$

(증명) $$\begin{pmatrix} d_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & d_2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & d_3 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & d_{n-1} & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & d_n \end{pmatrix}\begin{pmatrix} 1 & a_1 & * & \cdots & * & * & * \\ 0 & 1 & a_2 & \cdots & * & * & * \\ 0 & 0 & 1 & \cdots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-2} & * \\ 0 & 0 & 0 & \cdots & 0 & 1 & a_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & a_1 & * & \cdots & * & * & * \\ 0 & 1 & a_2 & \cdots & * & * & * \\ 0 & 0 & 1 & \cdots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-2} & * \\ 0 & 0 & 0 & \cdots & 0 & 1 & a_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}$$

□

$f(x)$를 90/150 TPNCA에 대응하는 다항식이라 두면, $f(x)$는 90/150 TPNCA 다항식이라 한다.

<정리 3.3 [11]> B는 n차 다항식

$$x^{i-1}+x^{2i-1}+x^{2i} \pmod{f(x)} \quad (i=1,2,\cdots n) \tag{3.2}$$

를 풀어서 얻는 $n\times n$행렬이라 두자. $f(x)$는 가약다항식이다. 그리고 $\{v|\, Bv=(0,\cdots,0,1)^t\}$를 공집합이 아니라고 하면 집합 $\{v|\, Bv=(0,\cdots,0,1)^t\}$ 의 원소는 Krylov행렬에 대한 seed벡터가 된다. A^t는A 의 전치행렬이다.

다음의 알고리즘은 주어진 가약다항식에 대해 90/150 TPNCA를 찾는 알고리즘이다.

입력 : 특성다항식 $f(x)$

출력 : 90/150 TPNCA

단계1 : 식 (3.2)로부터 행렬 B를 구성한다.

단계2 : 방정식 $Bv = (0, \cdots, 0, 1)^t$을 푼다.

단계3 : 단계2에서의 방정식의 해r 인 seed벡터로부터 Krylov 행렬를 만들어라.

단계4 : 만일 H가 LU분해를 가지고 있지 않으면 멈춘다.

단계5 : LU분해 H=LU를 계산한다.

단계6 : (3.1)에 사용된 행렬 U에 의한 $f(x)$에 대해 90/150 TPNCA를 계산한다.

<표 3.1> 90/150 TPNCA의 합성 알고리즘

Ⅳ. 90/150 TPNCA의 분석

이 장에서 90/150 TPNCA를 분석한다.

<정리 4.1> Δ_{2m}이 $< d_1, d_2, \cdots, d_m, d_m, \cdots, d_2, d_1 >$의 특성다항식이라 두면, 다음 식이 성립한다.

$$\Delta_{i+1}\Delta_{2m-i-1} + \Delta_i\Delta_{2m-i-2} = \Delta_{i+2}\Delta_{2m-i-2} + \Delta_{i+1}\Delta_{2m-i-3}$$
$$(i = 1, \cdots, 2m-1,\ \Delta_{-1} = 0 \text{ 그리고 } \Delta_0 = 1)$$

(증명) $d_{2m} = d_1$이고 $d_1 = d_{2m}$이므로 $d_{2m-i} = d_{i+1}$이고 $d_{2m+1-i} = d_i$이다. 그러므로 각각의 $i = 1, \cdots, 2m-1$에 대하여 다음이 성립한다.

$$\begin{aligned}
&\Delta_{i+1}\{(x + d_{2m-i-1})\Delta_{2m-i-2} + \Delta_{2m-i-3}\} + \Delta_i\Delta_{2m-i-2} \\
&= \Delta_{i+1}\{(x + d_{i+2})\Delta_{2m-i-2} + \Delta_{2m-i-3}\} + \Delta_i\Delta_{2m-i-2} \\
&= \{(x + d_{i+2})\Delta_{i+1} + \Delta_i\}\Delta_{2m-i-2} + \Delta_{i+1}\Delta_{2m-i-3} \\
&= \Delta_{i+2}\Delta_{2m-i-2} + \Delta_{i+1}\Delta_{2m-i-3}
\end{aligned}$$

□

<정리 4.2> $f(x)$를 $< d_1, d_2, \cdots, d_m \oplus 1 >$의 특성다항식이고 Δ_m이 $< d_1, d_2, \cdots, d_m >$의 특성다항식이라 두자. 그러면 다음식이 성립한다.

$$\Delta_m + \Delta_{m-1} = f(x)$$

(증명) 정리 4.1에 의하여 다음 식을 얻을 수 있다.

$$\begin{aligned}\Delta_m+\Delta_{m-1}&=(x+d_m)\Delta_{m-1}+\Delta_{m-2}+\Delta_{m-1}\\&=(x+d_m+1)\Delta_{m-1}+\Delta_{m-2}\\&=\begin{vmatrix} x+d_1 & 1 & 0 & \cdots & 0 & 0 & 0\\ 1 & x+d_2 & 1 & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1 & x+d_{m-1} & 1\\ 0 & 0 & 0 & \cdots & 0 & 1 & x+d_m+1 \end{vmatrix}\\&=f(x)\end{aligned}$$

□

<따름정리 4.3> Δ_{2m}이 $< d_1, d_2, \cdots, d_m, d_m, \cdots, d_2, d_1 >$의 특성다항식이고, $f(x)$가 $< d_1, d_2, \cdots, d_m \oplus 1 >$의 특성다항식이라 하면 다음식이 성립한다.

$$\Delta_{2m}=f(x)^2$$

(증명) 정리 4.2에 의하여 성립한다.

□

<정리 4.4> $C_S^k =< d_1, \cdots, d_k >$를 k-셀 90/150 TPSACA라 하면 다음식이 성립한다.

(i) $C_S^{2k} =< d_1, \cdots, d_k \oplus 1, d_k \oplus 1, \cdots, d_2, d_1 >$는 최소다항식 x^{2k}를 가지는 $2k$-셀 TPSACA이다.

(ii) $C_S^{2k+1} =< d_1, \cdots, d_k, 0, d_k, \cdots, d_1 >$은 최소다항식 x^{2k+1}를 가지는 $(2k+1)$-

셀 TPSACA이다.

(증명) (i) Δ_k가 C_1^k의 특성다항식이라 두면 $\Delta_k = x^k$이다. 그러므로 따름정리 4.3에 의하여 C_1^{2k}의 특성다항식은 $\Delta_k^2 = x^{2k}$이다. 90/150 CA는 분리가 불가능한(nonderogatory)이므로, Δ_k^2는 C_1^{2k}의 최소다항식이다.

(ii) Δ_k가 C_1^{2k+1}의 특성다항식이라 두면 $\Delta_k = x^k$이다. 그러므로 C_1^{2k+1}의 특선다항식은 정리 4.1에 의하여 다음과 같다.

$$\begin{aligned}
\Delta_{2k+1} &= (x+a_1)\Delta_{2k} + \Delta_{2k-1} \\
&= (x+a_1)((x+a_2)\Delta_{2k-1} + \Delta_{2k-2}) + \Delta_{2k-1} \\
&= \Delta_2\Delta_{2k-1} + \Delta_1\Delta_{2k-2} \\
&\quad \vdots \\
&= \Delta_{k+1}\Delta_k + \Delta_{k-1}\Delta_k \\
&= \Delta_k(\Delta_{k+1} + \Delta_{k-1}) \\
&= \Delta_k(x+0)\Delta_k \\
&= \Delta_k^2 \bullet x \\
&= x^{2k+1}
\end{aligned}$$

따라서 90/150 CA는 분리가 불가능한(nonderogatory)이므로, Δ_k^2는 C_1^{2k+1}의 최소다항식이다.

□

<예제 4.5> <1, 0, 0, 1>은 4-셀 90/150 TPNCA이므로 정리 4.4에 의하여 <1, 0, 0, 1, 1, 0, 0, 1>은 8-셀 90/150 TPNCA 임을 알 수 있다. 그리고 <1, 0, 0, 1, 0, 1, 0, 0, 1>은 9-셀 TPNCA라는 것을 알 수 있다.

<정리 4.6> 모든 양의 정수에 대하여 n-셀 90/150 TPSACA가 존재한다.

(증명) $n=1$ 일때, <0>은 1-셀 90/150 TPSACA 이다. 그리고 $< d_1, d_2, \cdots, d_m >$이 m-셀 90/150 TPSACA 일때 따름정리 4.3에 의하여 각각의 $n=2m$ $(m \in \mathbb{N})$이면 $< d_1, \cdots, d_{m-1}, d_m+1, d_m+1, d_{m-1}, \cdots, d_1 >$이 $2m$-셀 90/150 TPSACA이다. 또한 각각의 $n=2m+1$ $(m \in \mathbb{N})$에 대하여 다음이 성립한다.

$$
\begin{aligned}
\Delta_{2m+1} &= (x+d_1)\Delta_{2m} + \Delta_{2m-1} \\
&= (x+d_1)\{(x+d_2)\Delta_{2m-1} + \Delta_{2m-2}\} + \Delta_{2m-1} \\
&= \Delta_2\Delta_{2m-1} + \Delta_1\Delta_{2m-2} \\
&= \Delta_3\Delta_{2m-2} + \Delta_2\Delta_{2m-3} \\
&\quad \vdots \\
&= \Delta_{m+1}\Delta_m + \Delta_{m-1}\Delta_m \\
&= \Delta_m(\Delta_{m+1} + \Delta_{m-1}) \\
&= \Delta_m(x+0)\Delta_m \\
&= \Delta_m^2(x+0)
\end{aligned}
$$

따라서 $< d_1, \cdots, d_{m-1}, d_m, 0, d_m, d_{m-1}, \cdots, d_1 >$은 $(2m+1)$-셀 90/150 TPSACA

이다.

□

<정리 4.7> $N(T_m)=\{(a_1,a_2,\cdots,a_m)^t \mid a_1,a_2,\cdots,a_m\in\{0,1\}\}(:=[(a_1,a_2,\cdots,a_m)^t])$을 m-셀 90/150 TPSACA의 상태전이행렬 T_m의 영공간(null space)이라 하면 다음이 성립한다.

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

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

(증명) $T_m=<d_1,d_2,\cdots,d_{m-1},d_m>$이고, $N(T_m)=[(a_1,\cdots,a_m)^t]$ 라 두자. 그러면 다음과 같은 방정식을 얻을 수 있다.

$$\begin{cases} a_1d_1+a_2=0 \\ a_1+a_2d_2+a_3=0 \\ \quad\vdots \\ a_{m-2}+a_{m-1}d_{m-1}+a_m=0 \\ a_{m-1}+a_md_m=0 \end{cases} \tag{4.1}$$

(ⅰ)정리 4.5의 증명에 의하여 $T_n=<d_1,d_2,\cdots,d_{m-1},d_m+1,d_m+1,d_{m-1},\cdots,d_2,d_1>$ (4.1)로부터 다음 방정식이 성립한다.

$$\begin{cases} a_1d_1+a_2=0 \\ a_1+a_2d_2+a_3=0 \\ \quad\vdots \\ a_{m-2}+a_{m-1}d_{m-1}+a_m=0 \\ a_{m-1}+a_m(d_m+1)+a_m=0 \\ a_{m-1}+a_m(d_m+1)+a_m=0 \\ a_{m-2}+a_{m-1}d_{m-1}+a_m=0 \\ \quad\vdots \\ a_1+a_2d_2+a_3=0 \\ a_1d_1+a_2=0 \end{cases} \tag{4.2}$$

(4.2)로부터 다음 방정식 얻을 수 있다.

$$T_n(a_1, a_2, \cdots, a_{m-1}, a_m, a_m, a_{m-1}, \cdots, a_2, a_1)^t = O$$

그러므로 $N(T_n)=[(a_1, a_2, \cdots, a_m, a_m, \cdots, a_2, a_1)^t]$이다.

(ii) 정리 4.5에 의하여 $T_n =< d_1, d_2, \cdots, d_{m-1}, d_m, 0, d_m, d_{m-1}, \cdots, d_2, d_1 >$이다.

(4.1)로부터 다음과 같은 방정식을 얻는다.

$$\begin{cases} a_1d_1+a_2=0 \\ a_1+a_2d_2+a_3=0 \\ \quad\vdots \\ a_{m-2}+a_{m-1}d_{m-1}+a_m=0 \\ a_{m-1}+a_md_m=0 \\ a_m \cdot 1+0 \cdot 0+a_m \cdot 1=0 \\ a_{m-1}+a_md_m=0 \\ a_{m-2}+a_{m-1}d_{m-1}+a_m=0 \\ \quad\vdots \\ a_1+a_2d_2+a_3=0 \\ a_1d_1+a_2=0 \end{cases} \tag{4.3}$$

(4.3)으로부터 다음과 같은 방정식을 얻는다.

$$T_n(a_1, a_2, \cdots, a_{m-1}, a_m, 0, a_m, a_{m-1}, \cdots, a_2, a_1)^t = O$$

그러므로 $N(T_n) = [(a_1, a_2, \cdots, a_m, 0, a_m, \cdots, a_2, a_1)^t]$ 이다. □

<정리 4.8> $C_S^n = < d_1, \cdots, d_n, 1, d_n, \cdots, d_1 >$이 n-셀 90/150 TPSACA이면 $C_M^{2n+1} = < d_1, \cdots, d_n, 1, d_n, \cdots, d_1 >$은 최소다항식 $x^{2n}(x+1)$를 가지는 $(2n+1)$-셀 90/150 TPMACA이다.

(증명) Δ_n은 C_S^n의 특성다항식이고 Δ_{2n+1}은 C_M^{2n+1}의 특성다항식이라 두자. 그러면 정리 4.1에 의하여 다음 방정식을 구할 수 있다.

$$\begin{aligned}
\Delta_{2n+1} &= (x+d_1)\Delta_{2n} + \Delta_{2n-1} \\
&= (x+d_1)\{(x+d_2)\Delta_{2n-1} + \Delta_{2n-2}\} + \Delta_{2n-1} \\
&= \Delta_2\Delta_{2n-1} + \Delta_1\Delta_{2n-2} \\
&= \Delta_3\Delta_{2n-2} + \Delta_2\Delta_{2n-3} \\
&\quad \vdots \\
&= \Delta_{n+1}\Delta_n + \Delta_{n-1}\Delta_n \\
&= \Delta_n(\Delta_{n+1} + \Delta_{n-1}) \\
&= \Delta_n(x+1)\Delta_n \\
&= \Delta_n^2(x+1)
\end{aligned}$$

따라서 90/150 TPNCA는 분리가 불가능한(nonderogatory)[19]이고, $\Delta_n = x^n$ 이므로 $\Delta_{2n+1} = x^{2n}(x+1)$는 C_M^{2n+1}의 최소다항식이다. $(2n+1)$-셀 90/150 TPMACA의 depth가 $2n$이므로 attractors의 수는 2이다. 따라서 정리가 성립한다.

□

<보조정리 4.9> n이 짝수인 경우, 최소다항식이 $f(x) = x^n + x^{n-1}$인 n-셀 90/150 TPMACA는 존재하지 않는다.

(증명) $f(x) = x^n + x^{n-1}$이므로 행렬B는 다음과 같은 형태이다.

$$B = \begin{pmatrix} 1 & 1 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 1 & * & \cdots & * & * & 0 \\ 0 & 0 & 1 & \cdots & * & * & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & * & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

B는 정칙(nonsingular) 이므로 $B_v = (0, \cdots, 0, 1)^t$는 유일한 해 $v = (0, \cdots, 0, 1)^t$를 가진다. 그러므로 $K(C^t, v) = \begin{pmatrix} 0 & 0 & * & \cdots & * & * & 1 \\ 0 & 0 & * & \cdots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & * & * \\ 0 & 1 & * & \cdots & * & * & * \\ 1 & * & * & \cdots & * & * & * \end{pmatrix}$이다. 따라서 $K(C^t, v)$는 LU인수분해를 가지지 않으므로 상삼각행렬 U가 존재하지 않는다. 즉 $f(x)$는 90/150 CA 다항식이 아니다. 그러므로 n이 짝수 일 때, n-셀 90/150 TPMACA는 존재하지 않는다. □

<정리 4.10> $N(T_m)=[(a_1,a_2,\cdots,a_m)^t]$이 m-셀 90/150 TPSACA C_S^m의 상태전이행렬 T_m의 영공간이면 C_S^m으로부터 얻어진 $(2m+1)$-셀 90/150 TPMACA C_M^{2m+1}의 영공간은 $N(T_{2m+1})=[(a_1,\cdots,a_{m-1},a_m,0,a_m,a_{m-1},\cdots,a_1)^t]$이다.

(증명) $C_S^m=<d_1,d_2,\cdots,d_m>$이라 두면 정리 4.6에 의하여

$$C_M^{2m+1}=<d_1,\cdots,d_n,1,d_n,\cdots,d_1>$$

$N(T_m)=[(a_1,a_2,\cdots,a_m)^t]$이므로 다음 방정식을 얻을 수 있다.

$$\begin{cases} a_1d_1+a_2=0 \\ a_1+a_2d_2+a_3=0 \\ \quad\vdots \\ a_{m-2}+a_{m-1}d_{m-1}+a_m=0 \\ a_{m-1}+a_md_m=0 \end{cases} \tag{4.4}$$

(4.4)로부터 다음 방정식을 얻을 수 있다.

$$\begin{cases} a_1d_1+a_2=0 \\ a_1+a_2d_2+a_3=0 \\ \quad\vdots \\ a_{m-2}+a_{m-1}d_{m-1}+a_m=0 \\ a_{m-1}+a_md_m+0\cdot 1=0 \\ a_m\cdot 1+1\cdot 1+1\cdot a_m=0 \\ a_{m-2}+a_{m-1}d_{m-1}+a_m=0 \\ \quad\vdots \\ a_1+a_2d_2+a_3=0 \\ a_1d_1+a_2=0 \end{cases} \tag{4.5}$$

(4.5)의 방정식으로부터 다음 방정식을 얻을 수 있다.

$$T_n(a_1, a_2, \cdots, a_{m-1}, a_m, 0, a_m, a_{m-1}, \cdots, a_2, a_1)^t = O$$

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

□

n	TPSACA	$N(T_S)$	TPMACA	$N(T_M)$	$N(T_M \oplus I)$
1	0	1	1	0	1
2	11	11			
3	000	101	010	101	111
4	1001	1111			
5	11011	11011	11111	11011	10101
6	001100	101101			
7	0000000	1010101	0001000	1010101	1101011
8	10000001	11111111			
9	100101001	111101111	100111001	111101111	101111101
10	1101001011	1101111011			
11	11011011011	11011011011	11011111011	11011011011	10111111101
12	001101101100	101101101101			
13	0011000001100	1011010101101	0011001001100	1011010101101	1101011101011
14	00000011000000	10101011010101			
15	000000000000000	101010101010101	000000010000000	101010101010101	110110111011011

<표 4.1> TPSACA와 TPMACA

<표 4.1>에서 $N(T_S)$는 n-셀 90/150 TPSACA의 영공간을 의미하고 $N(T_M)$은 n-셀 90/150 TPMACA의 영공간을 의미한다. 또한 $N(T_M \oplus I)$는 n-셀 90/150 TPMACA 각각에 대한 모든 attractors의 집합을 말한다. 101은 $[(1,0,1)^t]$를 의미한다. Chattopadhyay[4]는 모든 선형 규칙 (60, 90, 102, 150, 170, 204, 240)를 가지고 MACA를 찾는 알고리즘을 제시한다. 그러나 여기에서는 규칙 90과 규칙 150을 사용하여 TPMACA의 합성 방법을 제시한다.

$f(x)=xp(x)$ ($p(x)$는 $(n-1)$차 다항식) 일때 $f(x)$가 n-셀 90/150 TPNCA에 대응하는 최소다항식이 되는 원시다항식 $p(x)$가 많이 있고, $f(x)=x(x+1)p(x)$($p(x)$는 $(n-2)(n \geq 6)$차 다항식) 일때 $f(x)$가 n-셀 90/150 TPNCA에 대응하는 최소다항식이 되는 원시다항식 $p(x)$가 많이 있다. <표 4.2>는 각 $n \geq 4$에 대하여 $xp(x)$ 형태 ($p(x)$는 원시다항식)의 90/150 TPNCA 다항식에 대한 n-셀 90/150 TPNCA가 존재한다는 것을 보여준다. 여기서 320

은 $p(x)=x^3+x^2+1$을 나타낸다. 또한 <표 4.3>은 각 $n \geq 6$에 대하여 $x(x+1)p(x)$형태 ($p(x)$를 원시다항식)의 90/150 TPMACA 다항식에 대한 n-셀 90/150 TPMACA가 존재하는 것을 보여준다. 여기서 210은 $p(x)=x^2+x+1$을 나타낸다.

n	$p(x)$	CA Configuration	n	$p(x)$	CA Configuration
4	320	0111	14	13,8,5,3,0	01100110101000
5	430	00010	15	14,11,9,7,0	100010001010000
6	520	001001	16	15,12,4,3,0	1000010010101010
7	65320	0011111	17	16,15,12,10,0	11011110100010001
8	740	00000011	18	17,3,0	100011101011110001
9	86520	000010001	19	18,7,0	0001110111000101000
10	95320	0000100100	20	19,10,9,3,0	01010100110000000010
11	10,3,0	01011111110	21	20,3,0	001001010110100100100
12	11,2,0	011101000110	22	9,4,3,0	110010011001010001 0011
13	12,10,9,8,6,2,0	101101001000	23	12,7,3,0	00010100100001011101000

<표 4.2> $xp(x)$에 대한 90/150 CA

n	$p(x)$	CA Configuration	n	$p(x)$	CA Configuration
4	210	1100	13	11,9,7,5,2,1,0	1111101110111
6	410	100110	14	12,10,2,1,0	01000110010010
7	53210	0100101	15	13,12,10,5,2,1,0	000101010001101
8	610	00001110	16	14,12,10,1,0	11001100110100 11
9	73210	010000000	17	15,12,9,1,0	00000111110100111
10	85310	0001001001	18	16,14,12,1,0	101100100110001101
11	95410	10000110011	19	17,13,12,1,0	0100101010011011100
12	10,7,6,5,2,1,0	001111010101	20	18,17,12,10,9,1,0	00111100100000111000

<표 4.3> $x(x+1)p(x)$에 대한 90/150 CA

참 고 문 헌

[1] K. Cattell and J.C. Muzio, Synthesis of one-dimensional linear hybrid cellular automata, IEEE Trans. on Computer Aided Design of Circuits and Systems 15-3, pp. 325-335, 1996.

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

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

[4] S. Chattopadhyay and P.P. Chaudhuri, Theory and application of nongroup cellular automata in pattern classification, IEEE Trans. Computers, communicated.

[5] P.P. Chaudhuri, D.R. Chowdhury, S. Nandy and C. Chattopadhyay, Additive cellular automata theory and applications, vol. 1. IEEE Computer Society Press, California, 1997.

[6] S.J. Cho, U.S. Choi, Y.H. Hwang and H.D. Kim, Analysis of hybrid group cellular automata, In El Yacoubi, S., Chopard, B., Bandini, S. (eds.) ACRI 2006. LNCS, vol. 4173, pp. 222 - 231. Springer, Heidelberg, 2006.

[7] S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim and H.H. Choi, Behaviors of single attractor cellular automata over Galois Field $GF(2p)$. In El Yacoubi, S., Chopard, B., Bandini, S. (eds.) ACRI 2006. LNCS, vol. 4173, pp. 232 - 237. Springer, Heidelberg, 2006.

[8] S.J. Cho, U.S. Choi, Y.H. Hwang, Y.S. Pyo, H.D. Kim, K.S. Kim and S.H. Heo, Computing phase shifts of maximum-length 90/150 cellular automata sequences, In Sloot, P.M.A., Chopard, B., Hoekstra, A.G. (eds.) ACRI 2004. LNCS, vol. 3305, pp. 31 - 39. Springer, Heidelberg, 2004.

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

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

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

[12] A.K. Das and P.P. Chaudhuri, Vector space theoretic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation, IEEE Trans. Comput. 42, pp. 340 - 352, 1993.

[13] D. De la Guia Martinez and A. Peinado Dominguez, Pseudorandom number generation based on nongroup cellular automata, In Security Technology, 1999, Proceedings, IEEE 33rd Annual 1999 International Carnahan Conference, vol. 45, pp. 370 - 376, 1999.

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

[15] P.D. Hortensius, R.D. McLeod and H.C. Card, Parallel random number generation for VLSI systems using cellular automata, IEEE Trans.

Computers 38, pp. 1466 - 1473, 1989.

[16] P.D. Hortensius, R.D. McLeod, D.M. Miller and H.C. Card, Cellular automata based pseudorandom number generations for built-in self test. IEEE Trans. on CAD of Integrated Circuits ans Systems 8, pp. 842 - 859, 1989.

[17] S. Nandi, B.K. Kar and P.P. Chaudhuri, Theory and application of cellular automata in cryptography, IEEE Trans. Computers 43, pp. 1346 - 1357, 1994.

[18] J. Von Neumann, The theory of self-reproducing automata, In Burks, A.W. (ed.). University of Illinois Press, Urban, 1966.

[19] W. Pries, A. Thanailakis and H.C. Card, Group properties of cellular automata and VLSI applications, IEEE Trans. Computers 35, pp. 1013 - 1024, 1986.

[20] M. Serra, T. Slater, J.C. Muzio and D.M. Miller, The analysis of one dimensional linear cellular automata and their aliasing properties, IEEE Trans Computer-Aided Design 9, pp 767 - 778, 1990.

[21] P. Tsalides, T.A. York and A. Thanailakis, Pseudorandom number generators for systems based on linear cellular automata, IEE Proc(Part E) Computers Digital Techniques 138, pp. 241 - 249, 1991.

[22] S. Wolfram, Statistical mechanics of cellular automata, Rev. Mod. Phys. 55, pp. 601 - 644, 1983.