교 육 학 석 사 학 위 논 문

선형 $GF(2^p)$ 셀룰라 오토마타의 분석과 합성

2010년 8월

부경대학교 교육대학원

수 학 교 육 전 공

김 양 숙

교 육 학 석 사 학 위 논 문

선형 $GF(2^p)$ 셀룰라 오토마타의 분석과 합성

지도교수 조 성 진

이 논문을 교육학석사 학위논문으로 제출함.

2010년 8월

부경대학교 교육대학원

수 학 교 육 전 공

김 양 숙

김양숙의 교육학석사 학위논문을 인준함.

2010년 8월 25일

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

Analysis and Synthesis of Linear $GF(2^p)$ Cellular Automata

Yang-Suk Kim

Graduate School of Education

Pukyong National University

Abstract

Cellular Automata(CA) has been used as modeling and computing paradigm for a long time and it has been used to model many physical systems. While studying the models of systems, it is seen that as the complexity of the physical system increase, the CA based model is very complex and difficult to track analytically. Also such models fail to recognize the presence of inherent hierarchical nature of a physical system. So the study the linear $GF(2^p)$ multiple attractor cellular automata is needed. In this paper we analyze the linear $GF(2^p)$ multiple attractor cellular automata, synthesize the linear $GF(2^p)$ multiple attractor cellular automata and give the characterization of linear $GF(2^p)$ multiple attractor cellular automata.

Ⅰ. 서론

셀룰라 오토마타는 셀이라 불리는 간단한 메모리의 배열로서 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. 셀룰라 오토마타는 오랫동안 모델링과 컴퓨팅 패러다임에 사용되어왔다. 그리고 셀룰라 오토마타는 많은 물리적 시스템 모형을 만드는데 사용되었다. 그러한 시스템의 모델을 연구함에 있어서 물리계의 복잡성이 증가함에 따라 셀룰라 오토마타를 이용한 모델은 매우 복잡하고 분석적으로 추적하기가 어렵게 되었다.

$GF(2)$ 셀룰라 오토마타는 생물학적 자체 재생산 모델링하기 위하여 Von Neumann[14]에 의하여 처음으로 소개되었다. Von Neumann은 셀룰라 오토마타의 물리적 특성에 특히 많은 관심을 가지고 연구하였다. 그러다가 Wolfram[20]이 자체적으로 구성하는 통계적 시스템을 위한 수학적 모델로서 $GF(2)$ 셀룰라 오토마타를 연구하기 시작하였다. 또한 Wolfram은 일차원에서 선형적으로 배열된 셀들을 갖는 단순한 상태가 되는 0과 1 두 개인 3-이웃 셀룰라 오토마타의 사용을 제시하였다. 이와 같은 식으로 발전되어 오다가 $GF(2)$ 셀룰라 오토마타를 특성화 할 수 있는 행렬로 표현함으로써 행렬에 관한 연구로 발전하게 되었다[1, 4, 5, 8, 13~17]. 2007년에 Cho 등[9]은 선형 $GF(2)$ 셀룰라 오토마타 다항식에 대한 일차원 90/150 선형 하이브리드 그룹 셀룰라 오토마타의 획기적인 합성방법을 제안하였다. 이것은 이 분야의 연구에 커다란 도움을 주는 연구 결과이다. 또한 Cho 등과 많은 연구자들([2, 8, 9, 15, 19])은 해시 함수, 자료 저장 및 암호 등의 연구를 위하여 $GF(2)$ 셀룰라 오토마타를 분석하였다.

이러한 $GF(2)$ 셀룰라 오토마타는 물리적 시스템의 내재적인 계층성에 대한 분석에는 많은 어려움이 있지만 계층성은 자연에서의 복잡한 시스템의 중요한 요소이므로 복잡시스템의 이러한 내재적 계층적 성질을 알아내기 위한 모델링 도구가 반드시 필요하다. 본 논문에서는 이러한 계층적 시스템의 연구의 모델링 도구로서 $GF(2^p)$ 셀룰라 오토마타를 분석하고 합성하고자 한다.

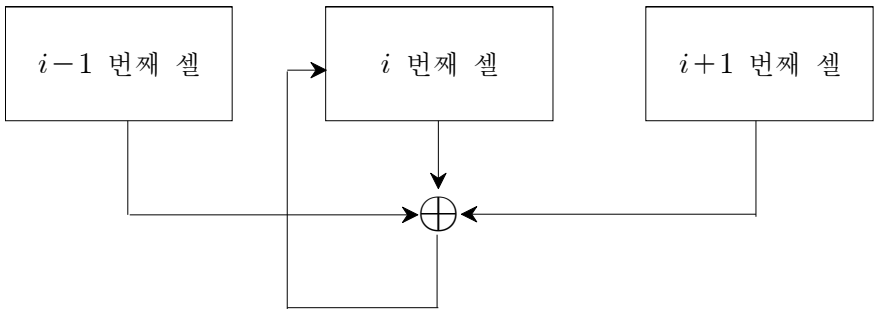
특히, $GF(2^p)$ 셀룰라 오토마타 중 특별한 클래스인 $GF(2^p)$ MACA와 $GF(2^p)$ SACA의 특성다항식의 점화관계를 분석하여 그 결과를 바탕으로 하여 $GF(2^p)$ SACA를 합성하고자 한다.

Ⅱ. 셀룰라 오토마타의 기본지식

2.1. 셀룰라 오토마타의 정의와 구조

셀룰라 오토마타(Cellular Automata, 이하 CA)란 이산시간의 동적 시스템으로 셀이라는 기본 단위 메모리의 배열로 이루어진다. 이 시스템에서 셀의 다음 상태는 어떤 규칙에 따라 정해진다. 즉, 각 셀들은 자기 자신과 이웃 셀의 함숫값에 의해 다음 상태가 결정되어 동시에 갱신된다. 셀룰라 오토마타는 간단하고, 규칙적이며, 작은 단위로 확장 연결할 수 있는 구조이기 때문에 VLSI 하드웨어 구현에 알맞다. Wolfram은 모든 셀이 선형으로 배열되어 있으며 각 셀이 0과 1, 두 상태를 가지고 다음상태가 자기 자신과 인접한 두 이웃에 의하여 갱신되는 3-이웃(3-neighbourhood) 셀룰라 오토마타는 제안하였다. [그림 Ⅱ-1]은 3-이웃 선형 셀룰라 오토마타의 셀의 구조를 나타낸 것이다.

[그림 Ⅱ-1] 3-이웃 선형 셀룰라 오토마타의 셀 구조



세 개의 이웃을 가지는 셀룰라 오토마타에 대한 상태전이함수(state transition function)는 다음과 같이 나타낸다.

$$q_i(t+1) = f(q_{i-1}(t), q_i(t), q_{i+1}(t))$$

여기서 $q_i(t)$는 시간 t에서 i번째 셀의 상태를 나타내고, f는 결합논리를 가지는 국소전이함수이다. f는 3개의 변수를 가지는 Boolean함수로 $f: \{000, 001, 010, \cdots, 110, 111\} \rightarrow \{0, 1\}$이다. 그러므로 다음 상태 전이함수 f는 2^{2^3}, 즉 256개가 있으며 이것을 셀룰라 오토마타의 전이규칙이라고 한다. 위의 규칙에 대한 결합논리는 다음 [표 Ⅱ-1]로 표현할 수 있고 $\oplus$는 XOR 논리를 나타낸다. 즉, 같은 수끼리 더하면 0이 되고 다른 수 끼리 더하면 1이 된다.

[표 Ⅱ-1] 전이규칙 90 / 150

전이규칙 90	$q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
전이규칙 150	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$

규칙 90은 자기 자신의 왼쪽 이웃과 오른쪽 이웃의 영향을 받아 다음 상태로 갱신되는 규칙을 의미하며 규칙 150은 자기 자신의 왼쪽 이웃과 오른쪽 이웃 그리고 자신의 영향을 받아 다음 상태로 갱신되는 규칙을 의미한다. 다음 [표 Ⅱ-2]를 보자.

[표 Ⅱ-2] 규칙 90과 150

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

[표 Ⅱ-2]의 첫 번째 줄은 시간 t에서 인접한 세 개의 셀들의 가능한 8가지 상태의 배열이고 다음 두 줄은 시간 $t+1$에서 i번째 셀의 갱신된 상태이다. 두 번째 줄의 첫 칸의 0은 $1 \oplus 1 = 0$이며 두 번째 칸의 1은 $1 \oplus 0 = 1$이다. 두 번째 줄을 이진수로 나열하여 십진수로 계산하면 $(01011010)_2 = 90$이므로 이 함수를 전이규칙 90이라 하고 세 번째 줄을 이진수로 나열하여 십진수로 계산하면 $(10010110)_2 = 150$이므로 이 함수를 전이규칙 150이라 한다.

2.2. 셀룰라 오토마타의 분류

셀룰라 오토마타는 셀의 배열된 구조에 따라, 적용된 규칙의 개수에 따라, 상태전이그래프의 형태에 따라, attractor의 수에 따라, 그리고 경계 조건에 따라 각각 아래와 같이 분류된다.

셀룰라 오토마타는 셀의 배열된 구조에 따라, 적용된 규칙의 개수에 따라, 상태전이그래프의 형태에 따라, attractor의 수에 따라, 그리고 경계 조건에 따라 각각 아래와 같이 분류된다.

가. 셀의 배열된 구조에 따른 분류

(1) 1차원 셀룰라 오토마타 : 셀이 선형으로 배열되어 있는 셀룰라 오토마타
(2) 2차원 셀룰라 오토마타 : 셀이 평면으로 배열되어 있는 셀룰라 오토마타
(3) 3차원 셀룰라 오토마타 : 셀이 공간으로 배열되어 있는 셀룰라 오토마타

나. 적용된 규칙의 개수에 따른 분류

(1) 유니폼 셀룰라 오토마타 (Uniform CA) : 모든 셀룰라 오토마타의 셀이 같은 규칙이 적용된 셀룰라 오토마타
(2) 하이브리드 셀룰라 오토마타 (Hybrid CA) : 2가지 이상의 서로 다른 규칙이 적용된 셀룰라 오토마타

다. 상태전이 그래프의 형태에 따른 분류

(1) 그룹 셀룰라 오토마타(Group CA) : 모든 셀의 상태가 몇 개의 사이클을 이루며 반복 되는 셀룰라 오토마타
(2) 비그룹 셀룰라 오토마타(Nongroup CA) : 그룹 셀룰라 오토마타가 아닌 셀룰라 오토마타

그룹 셀룰라 오토마타는 모든 셀의 상태가 몇 개의 사이클을 이루며 반복되는 셀룰라 오토마타로 임의의 한 상태에 대한 이전상태가 유일하다. 이와 달리 비그룹 셀룰라 오토마타는 상태전이그래프가 트리 구조를 이루고 있으며 상태전이함수에 의해 얻어질 수 있는 상태인 도달 가능한 상태와 상태전이함수에 의해 나타날 수 없는 도달 불가능한 상태로 나누어진다. 비그룹 셀룰라 오토마타는 임의의 한 상태에 대한 이전상태가 존재하지 않거나 2개 이상 존재한다. 이런 비그룹 셀룰라 오토마타 중 순환상태의 주기가 모두 1인 비그룹 셀룰라 오토마타를 MACA라 하며 특히 순환상태가 단 하나인 MACA를 SACA라한다.

라. attractor의 개수에 따른 분류

(1) MACA(Multiple Attractor CA) : 상태전이그래프가 각 attractor를 root로 하는 서로 분리된 트리들로 구성된 비그룹 셀룰라 오토마타를 MACA라한다.
(2) SACA(Single Attractor CA) : attractor가 한 개인 MACA를 SACA라한다.

여기서 attractor란 순환상태들 중 사이클의 길이가 1인 상태로 상태 x가 attractor이면 전이행렬 T에 대하여 $Tx = x$를 만족한다. 깊이(depth)는 비

그룹 셀룰라 오토마타의 상태전이 그래프에서 임의의 도달 불가능한 상태에서 가장 가까운 순환상태로 전이되는데 걸리는 최소 상태 전이 수를 말한다.

마. 경계조건에 따른 분류

1차원으로 배열된 셀룰라 오토마타의 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 끝 셀의 세 번째 이웃 셀을 정하는 기준에 따라 다음과 같이 분류된다.

(1) NBCA(Null Boundary CA) : 세 번째 이웃 셀의 상태를 0으로 정의한 셀룰라 오토마타
(2) PBCA(Periodic Boundary CA) : 양끝의 셀 들이 서로 연결되어 있는 셀룰라 오토마타
(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 셀룰라 오토마타

[그림 Ⅱ-2]는 서로 다른 경계조건을 가지는 셀룰라 오토마타의 구조를 나타낸 것이다.

[그림 Ⅱ-2] 서로 다른 경계조건을 가지는 셀룰라 오토마타

(1) NBCA

(2) PBCA

(3) IBCA

2.3. 선형 $GF(2^p)$ 셀룰라 오토마타에 대한 예비지식

일반적으로 n 셀 90/150 $GF(2)$에서 셀룰라 오토마타의 상태전이 행렬 U는 다음과 같은 $n \times n$ 행렬이다. 여기서 $GF(2)$는 원소가 0과 1로 이루어진 유한체이다.

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

이 행렬 U를 다음과 같이 나타내기도 한다.

$$U = < d_1, d_2, d_3, \cdots, d_i, \cdots, d_{n-1}, d_n >$$

여기서 $d_i \in GF(2)$이다. 이때 규칙이 90이면 $d_i = 0$으로 150이면 $d_i = 1$로 나타낸다. $GF(2)$ 위에서 90/150 셀룰라 오토마타를 생각해 보자. 예를 들어 4 셀 90/150 $GF(2)$ 셀룰라 오토마타 $\mathbb{C}$의 상태전이 규칙이 $< 0, 1, 0, 1 >$ 이라 하면 $\mathbb{C}$의 상태 전이행렬 U는 다음과 같다.

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

여기서 첫 번째 셀의 왼쪽 이웃이 없으므로 첫 번째 셀의 왼쪽 이웃을 0이라 두고 마찬가지로 마지막 셀의 오른쪽 이웃도 0이라 두기로 한다. U의 행렬식 $|U|=1$이므로 그룹 $GF(2)$ 셀룰라 오토마타이다.

$GF(2^p)$ 셀룰라 오토마타는 $GF(2)$ 셀룰라 오토마타와 마찬가지로 셀들의 배열로 이루어지며 규칙적으로 왼쪽 셀과 자기 자신 그리고 오른쪽 셀의 영향을 받아 다음 상태로 갱신되는 시스템이다. 여기서 $GF(2^p)$은 원소의 개수가 2^p인 유한체이다[12,13].

i번째 셀의 다음 상태는 $i-1$번째 셀, i번째 셀 그리고 $i+1$번째 셀의 현재 상태들의 가중치가 있는 일차결합을 나타내는 함숫값으로 주어진다. 여기서 가중치는 $GF(2^p)$의 원소이다. 그러므로 $q_i(t)$가 t번째 시각에서 i번째 셀의 상태라면

$$q_i(t+1)=\psi(d_{i-1}q_{i-1}(t),\ d_iq_i(t),\ d_{i+1}q_{i+1}(t))$$

이다. 여기서 ψ는 i번째 셀의 국소전이(local transition) 함수이며 d_{i-1}, d_i, $d_{i+1}\in GF(2^p)$은 영향을 미치는 정도를 나타내는 가중치이다.

3-이웃 $GF(2^p)$ 셀룰라 오토마타 셀에 대한 상태전이규칙(state transition rule)은 $<d_{i-1},\ d_i,\ d_{i+1}>$로 나타낸다. 여기서 d_{i-1}은 그것의 왼쪽 이웃에게 의존하는 정도이며 마찬가지로 d_i와 d_{i+1}은 각각 자기 자신과 오른쪽 이웃에게 의존하는 정도를 말한다. $GF(2)$ 셀룰라 오토마타와 마찬가지로 $GF(2^p)$ 셀룰라 오토마타의 모든 셀들에 적용되는 상태전이 규칙들이 모두 같으면 유니폼(uniform) $GF(2^p)$ 셀룰라 오토마타라 하고 그렇지 않으면 하이브리드(hybrid) $GF(2^p)$ 셀룰라 오토마타라 한다.

이웃의 가중치가 모두 같은 $GF(2^p)$ 셀룰라 오토마타는 90/150 $GF(2)$ 셀룰라 오토마타의 자연스러운 확장이다. 따라서 가중치가 $w \in \{1, 2, \cdots, 2^p-1\}$이고 상태전이 규칙이 $< d_1, d_2, \cdots, d_n >$ 인 n 셀 $GF(2^p)$ 셀룰라 오토마타를 $< d_1, d_2, \cdots, d_n >_w$라 쓰기로 한다.

n 셀 $GF(2^p)$ 셀룰라 오토마타 $\mathbb{C}$가 $< d_1, d_2, \cdots, d_n >_w$라면 $\mathbb{C}$의 상태전이행렬 U는 다음과 같다.

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

[참고] 앞으로는 행렬 U를 $U = < d_1, d_2, \cdots, d_j, \cdots, d_n >_w$로 표시한다. 여기서 $d_j \in GF(2^p)$이다.

$GF(2)$ 위에서 $-1 \equiv 1$이다. 예를 들어 $GF(2^2)$은 원소의 개수가 2^2인 유한체로서 생성다항식 $f(x) = x^2 + x + 1$에 의하여 생성된다. 즉, $\alpha^2 + \alpha + 1 = 0$라면 $\alpha^2 = \alpha + 1$이다. 물론 $\alpha^3 = 1$이다. 따라서

$$GF(2^2) = \{ 0, 1, \alpha, \alpha^2 \}, \qquad \alpha^2 = \alpha + 1$$

이다. $G = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$라 하면 G의 생성다항식 $c_G(x) = x^2 + x + 1$이 된다. 그러므로 G를 α로 간주할 수 있다. G의 2열을 십진수로 나타내면 $(1\,1)_2 = 3$

이 된다. 마찬가지로 $G^2=\begin{pmatrix}1&1\\1&0\end{pmatrix}$이므로 α^2은 $(1\,0)_2=2$로 간주하여 $GF(2^2)$ $=\{0,1,2,3\}$로 나타낼 수 있다. 이와 같은 방법으로 $GF(2^3)$도 다음과 같이 나타낼 수 있다.

$$GF(2^3)=\{0,1,\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta\}=\{0,1,2,3,4,5,6,7\},\quad \beta^3=\beta+1$$

n 셀 선형 $GF(2^p)$ 셀룰라 오토마타는 $n\times n$ 상태전이행렬 $U=(u_{ij})$로 나타낼 수 있다. 여기서 i번째 셀의 다음 상태가 가중치 $d_{ij}\in GF(2^p)$에 의하여 j번째 셀의 현재 상태에 의존하면 $u_{ij}=d_{ij}$라 하고 그렇지 않은 경우는 $u_{ij}=0$라한다. 예를 들어 3-이웃 $GF(2^2)$ 셀룰라 오토마타의 상태전이행렬 $U=<1,3,0,3>_2$는 다음과 같다.

$$U=\begin{pmatrix}1&\alpha^2&0&0\\\alpha^2&\alpha&\alpha^2&0\\0&\alpha^2&0&\alpha^2\\0&0&\alpha^2&\alpha\end{pmatrix},\qquad \alpha\in GF(2^2)$$

여기서 $\alpha=3$, $\alpha^2=2$, $\alpha^3=1$이므로 U를 다음과 같이 나타낼 수도 있다.

$$U=\begin{pmatrix}1&2&0&0\\2&3&2&0\\0&2&0&2\\0&0&2&3\end{pmatrix}=\left(\begin{array}{cc|cc|cc|cc}1&0&1&1&0&0&0&0\\0&1&1&0&0&0&0&0\\\hline1&1&0&1&1&1&0&0\\1&0&1&1&1&0&0&0\\\hline0&0&1&1&0&0&1&1\\0&0&1&0&0&0&1&0\\\hline0&0&0&0&1&1&0&1\\0&0&0&0&1&0&1&1\end{array}\right)$$

상태전이행렬이 U인 n 셀 선형 $GF(2^p)$ 셀룰라 오토마타의 현재 상태를 V라 하고 다음 상태를 V'라 하면 $V' = UV$가 성립한다. 여기서 V와 V'는 $n \times 1$ 행렬이다. 예를 들어 위의 U에 대하여 현재 상태 V가 $(0, \alpha^2, \alpha, \alpha^2)^t$라 하면 다음 상태 V'는 다음과 같이 된다.

$$V' = UV = \begin{pmatrix} 1 & \alpha^2 & 0 & 0 \\ \alpha^2 & \alpha & \alpha^2 & 0 \\ 0 & \alpha^2 & 0 & \alpha^2 \\ 0 & 0 & \alpha^2 & \alpha \end{pmatrix} \begin{pmatrix} 0 \\ \alpha^2 \\ \alpha \\ \alpha^2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + \alpha^2 \cdot \alpha^2 + 0 \cdot \alpha + 0 \cdot \alpha^2 \\ \alpha^2 \cdot 0 + \alpha \cdot \alpha^2 + \alpha^2 \cdot \alpha + 0 \cdot \alpha^2 \\ 0 \cdot 0 + \alpha^2 \cdot \alpha^2 + 0 \cdot \alpha + \alpha^2 \cdot \alpha^2 \\ 0 \cdot 0 + 0 \cdot \alpha^2 + \alpha^2 \cdot \alpha + \alpha \cdot \alpha^2 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

덧셈과 곱셈은 $GF(2^2)$ 하에서 다음 [표 Ⅱ-3]와 같이 덧셈과 곱셈 규칙을 따른다.

[표 Ⅱ-3] $GF(2^2)$ 위에서의 덧셈과 곱셈

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

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

< **예제 2.3.1** > 위의 U에 대하여 $V = (1, 2, 3, 2)^t$라 하면

$$V' = UV = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 3 & 2 & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 2 + 0 \cdot 3 + 0 \cdot 2 \\ 2 \cdot 1 + 3 \cdot 2 + 2 \cdot 3 + 0 \cdot 2 \\ 0 \cdot 1 + 2 \cdot 2 + 0 \cdot 3 + 2 \cdot 2 \\ 0 \cdot 1 + 0 \cdot 2 + 2 \cdot 3 + 3 \cdot 2 \end{pmatrix} = \begin{pmatrix} 1 + 3 + 0 + 0 \\ 2 + 1 + 1 + 0 \\ 0 + 3 + 0 + 3 \\ 0 + 0 + 1 + 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 0 \\ 0 \end{pmatrix}$$

< **정의 2.3.1** > $GF(2)$ 위에서의 차수가 n인 기약다항식 $f(x)$가 다음을 만족할 때 원시다항식(primitive polynomial)이라 한다.

$$\min\{ m: f(x) \mid x^m - 1 \} = 2^n - 1$$

< **예제 2.3.2** > $GF(2)$위에서 기약다항식은 [표 Ⅱ-4]와 같다.

[표 Ⅱ-4] $GF(2)$ 위에서의 기약다항식

	기약다항식
1차	$x, x+1$
2차	x^2+x+1
3차	x^3+x+1, x^3+x^2+1
4차	$x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$
5차	$x^5+x^2+1, x^5+x^4+x^3+x^2+1, x^5+x^3+x^2+x+1$ $x^5+x^3+1, x^5+x^4+x^3+x+1, x^5+x^4+x^2+x+1$

이 중에서 x와 $x^4+x^3+x^2+x+1$을 제외한 나머지 5차까지의 기약다항식들은 모두 원시다항식들이다.

[참고] $GF(2)$ 위에서의 n차 원시다항식의 개수는 $\frac{\phi(2^n-1)}{n}$ 이다. 여기서 ϕ는 Euler의 ϕ-함수이다. 따라서 2차의 원시다항식의 개수는 1개이고 4차의 원시다항식의 개수는 2이고 7차의 원시다항식의 개수는

$$\frac{\phi(2^7-1)}{7} = \frac{\phi(127)}{7} = \frac{126}{7} = 18$$

이다. 당연히 $GF(2^p)$ 위에서의 n차 원시다항식의 개수는 $\frac{\phi((2^p)^n-1)}{n}$이다. 예를 들어 $GF(2^2)$ 위에서의 2차의 원시다항식의 개수는 $\frac{\phi((2^2)^2-1)}{2} = \frac{\phi(15)}{2} = 4$이다. 실제로 $GF(2^2)$ 위에서의 2차의 원시다항식은 x^2+x+2, x^2+x+3, x^2+2x+2, x^2+3x+3이다. x^2+2x+1, x^2+3x+1은 주기가 5인 2차 기약다항식들이다.

< **예제 2.3.3** > 다항식 x^4+x+1은 $GF(2)$ 위에서 원시다항식이지만 $GF(2^2)$ 위에서는 다음과 같이 인수분해 된다.

$$x^4+x+1 = (x^2+x+2)(x^2+x+3)$$

< **정의 2.3.2** > $GF(2)$ 위에서 주어진 n차 다항식 $f(x)$에 대응하는 $GF(2)$ 셀룰라 오토마타가 존재할 때 $f(x)$를 셀룰라 오토마타 다항식(Cellular Automata polynomial)이라 한다.

< **예제 2.3.4** > $GF(2)$ 위에서 $f(x)=x^3+x+1$에 대하여 규칙 <90, 150, 150> 인 셀룰라 오토마타의 상태전이행렬은 다음과 같다.

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

U의 특성다항식 $c_U(x)=\begin{vmatrix}x&1&0\\1&1+x&1\\0&1&1+x\end{vmatrix}=x^3+x+1$이 되어 x^3+x+1은 셀룰라 오토마타 다항식이 된다. 그러나 x^3+1은 셀룰라 오토마타 다항식이 아니다.

[참고] 2007년 Cho 등 [9]은 주어진 기약다항식에 대응하는 $GF(2)$ 셀룰라 오토마타가 두 개가 존재한다는 것을 밝혔다. 사실 모든 기약다항식은 셀룰라 오토마타 다항식이다. $GF(2^2)$ 위에서 주어진 기약다항식에 대응하는 $GF(2^2)$ 셀룰라 오토마타 다항식을 찾는 알고리즘은 현재까지 존재하지 않는다.

< 정의 2.3.3 > $\mathbb{C}$가 다음과 같은 상태전이 행렬 U를 갖는 $GF(2^2)$ 셀룰라 오토마타라 하자.

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

그러면 $|U|=3\neq 0$이므로 $\mathbb{C}$는 그룹 $GF(2^2)$ 셀룰라 오토마타이다.

Ⅲ. 선형 $GF(2^p)$ 셀룰라 오토마타

3.1. 선형 $GF(2^p)$ 셀룰라 오토마타의 특성분석

이 절에서는 각 셀의 이웃이 다 같은 경우의 선형 $GF(2^2)$ 셀룰라 오토마타의 특성을 분석하고자 한다.

다음 정리는 잘 알려진 정리이다.

< 정리 3.1.1 > n 셀 $GF(2)$ 셀룰라 오토마타 $\mathbb{C}$의 상태전이행렬을 $U = < d_1, d_2, \cdots, d_n >$라 하고 $|U_{-1}| = 0$, $|U_0| = 1$이라 하면 다음이 성립한다.

$$|U_n| = d_n|U_{n-1}| + |U_{n-2}|$$

여기서 $|U_n|$은 U_n의 행렬식이다.

< 예제 3.1.1 > 4 셀 $GF(2)$ 셀룰라 오토마타 $\mathbb{C}$의 상태전이행렬을 $U_4 = <0,1,0,1>$라 하면

$$U_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

이므로

$$|U_4| = 1 \cdot |U_3| + |U_2| = \begin{vmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{vmatrix} + \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} = 1$$

이다.

다음 <보조정리 3.1.1>은 <정리 3.1.1>의 $GF(2^p)$ 위로의 확장이다.

< 보조정리 3.1.1 > n 셀 $GF(2^p)$ 셀룰라 오토마타 $\mathbb{C}$의 상태전이행렬을 $T_n = < d_1, d_2, \cdots, d_n >_w$라 하고 $|T_{-1}| = 0$, $|T_0| = 1$이라 하면 다음이 성립한다.

$$|T_n| = d_n |T_{n-1}| + w^2 |T_{n-2}|$$

여기서 $w \in \{1, 2, \cdots, 2^p - 1\}$이며 $|T_n|$은 T_n의 행렬식이다.

[증명] 수학적 귀납법에 의하여 증명 됨.

□

< 예제 3.1.2 > 4 셀 $GF(2^2)$ 셀룰라 오토마타 $\mathbb{C}$의 상태전이행렬을 $T_4 = < 1, 2, 3, 2 >_2$라 하면

$$T_4 = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 2 & 2 & 0 \\ 0 & 2 & 3 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}$$

이므로

$$|T_4| = 2 \cdot \begin{vmatrix} 1 & 2 & 0 \\ 2 & 2 & 2 \\ 0 & 2 & 3 \end{vmatrix} + 2^2 \cdot \begin{vmatrix} 1 & 2 \\ 2 & 2 \end{vmatrix} = 3$$

이다.

< 정리 3.1.2 > $\mathbb{C}$를 상태전이행렬이 $T_n = <0, 0, \cdots, 0>_w$인 n셀 유니폼 $GF(2^p)$ 셀룰라 오토마타라 하자. n이 짝수이면 $\mathbb{C}$는 그룹 $GF(2^p)$ 셀룰라 오토마타이고, n이 홀수이면 $\mathbb{C}$는 비그룹 $GF(2^p)$ 셀룰라 오토마타이다.

[증명] $j = 1, 2, \cdots, n$에 대하여 $w_j = 0$이므로 <보조정리 3.1.1>에 의하여 $|T_n| = w^2|T_{n-2}|$이다. n이 짝수이면 $|T_2| = w^2|T_0| = w^2$, $|T_n| = w^2|T_{n-2}| = w^n$이다. 그러므로 n이 짝수이면 $\mathbb{C}$는 그룹 셀룰라 오토마타이다. 마찬가지로 n이 홀수이면 $|T_1| = w^2|T_{-1}| = 0$, $|T_n| = w^2|T_{n-2}| = 0$이다. 그러므로 n이 홀수이면 $\mathbb{C}$는 비그룹 셀룰라 오토마타이다.

□

< 정리 3.1.3 > $\mathbb{C}$가 상태전이행렬이 $T_n = <w, w, \cdots, w>_w$인 n 셀 유니폼 $GF(2^p)$ 셀룰라 오토마타라 하자. $n(\mathrm{mod}3) \neq 2$이면 $\mathbb{C}$는 그룹 $GF(2^p)$

셀룰라 오토마타이고, $n(\mathrm{mod}3)=2$이면 $\mathbb{C}$는 비그룹 $GF(2^p)$ 셀룰라 오토마타이다.

[증명] <보조정리 3.1.1>에 의하여 $|T_0|=1$, $|T_1|=w$이고 $|T_2|=0$이다.

$$\begin{aligned}|T_{3k+2}| &= w|T_{3k+1}|+w^2|T_{3k}| \\ &= w(w|T_{3k}|+w^2|T_{3k-1}|)+w^2|T_{3k}| \\ &= w^3|T_{3k-1}| \\ &= w^3|T_{3(k-1)+2}|\end{aligned}$$

이므로

$$|T_n| = \begin{cases}(w^3)^k|T_0|, & n=3k \\ (w^3)^k|T_1|, & n=3k+1 \\ (w^3)^k|T_2|, & n=3k+2\end{cases}$$

이다. 그러므로 $n(\mathrm{mod}3)\neq 2$이면 $\mathbb{C}$는 그룹 $GF(2^p)$ 셀룰라 오토마타이며 $n(\mathrm{mod}3)=2$이면 $\mathbb{C}$는 비그룹 $GF(2^p)$ 셀룰라 오토마타이다.

□

< 정리 3.1.4 > $\mathbb{C}$를 n 셀 하이브리드 $GF(2^p)$ 셀룰라 오토마타라 하고 그것의 상태전이 행렬이 $T_n = <0, d, 0, d, \cdots>_w$라 하자. 여기서 $d \in GF(2^p)$이다. n이 짝수이면 $\mathbb{C}$는 그룹 $GF(2^p)$ 셀룰라 오토마타이고, n이 홀수이면 $\mathbb{C}$는 비그룹 $GF(2^p)$ 셀룰라 오토마타이다.

[증명] $n=2m+1$일 때와 $n=2m$일 때로 나누어 증명한다. 여기서 $m=0, 1, 2, \cdots$ 이다.

(i) $n=2m+1$이라 하자. 그러면 <보조정리 3.1.1>에 의하여

$$|T_{2m+1}| = 0 \cdot |T_{2m}| + w^2|T_{2m-1}| = w^2|T_{2(m-1)+1}|$$

이므로 $|T_{2m+1}| = (w^2)^m|T_1| = 0$이다. 따라서 $\mathbb{C}$는 비그룹 $GF(2^p)$ 셀룰라 오토마타이다.

(ii) $n=2m$이라 하자. 그러면 <보조정리 3.1.1>에 의하여

$$|T_{2m}| = d|T_{2m-1}| + w^2|T_{2m-2}|$$

이고 (i)에 의하여 $|T_{2m-1}| = 0$이므로 $|T_{2m}| = w^2|T_{2m-2}|$이다. 따라서

$$|T_{2m}| = (w^2)^m|T_0| = w^{2m}$$

이다. 그러므로 $\mathbb{C}$는 그룹 $GF(2^p)$ 셀룰라 오토마타이다.

□

< 정리 3.1.5 > n 셀 하이브리드 $GF(2^p)$ 셀룰라 오토마타 $\mathbb{C}$의 상태전이 행렬이 $T_n = < d, 0, d, 0, \cdots >_w$라 하자. 여기서 $w \in \{1, 2, \cdots, 2^p-1\}$이다. n이 $n(\mathrm{mod}\,4) \neq 3$이면 $\mathbb{C}$는 그룹 $GF(2^p)$ 셀룰라 오토마타이고,

$n(\mathrm{mod}\,4)=3$이면 $\mathbb{C}$는 비그룹 $GF(2^p)$ 셀룰라 오토마타이다.

[증명] <보조정리 3.1.1>에 의하여 $|T_0|=1$이고 $|T_3|=0$이므로 다음 두 개의 방정식을 얻는다.

$$\begin{aligned}|T_{4k+3}| &= d|T_{4k+2}| + w^2|T_{4k+1}| \\ &= d\{0\cdot|T_{4k+1}|+w^2|T_{4k}|\} + w^2\{d|T_{4k}|+w^2|T_{4k-1}|\} \\ &= w^4|T_{4k-1}|\end{aligned}$$

$|T_{4k+3}|=|T_{4(k-1)+3}|$ 이므로

$$\begin{aligned}|T_{4k+3}| &= w^4|T_{4(k-1)+3}| \\ &= (w^4)^2|T_{4(k-2)+3}| \\ &\vdots \\ &= (w^4)^k|T_3| \\ &= 0\end{aligned}$$

$$\begin{aligned}|T_{2m}| &= 0\cdot|T_{2m-1}| + w^2|T_{2m-2}| \\ &= w^2|T_{2(m-1)}| \\ &= (w^2)^m|T_0| \\ &= w^{2m}\end{aligned}$$

위의 두 방정식에 의하여

$$\begin{aligned}|T_{4k+1}| &= d|T_{4k}| + w^2|T_{4k-1}| \\ &= dw^{4k} + w^2|T_{4(k-1)+3}| \\ &= dw^{4k}\end{aligned}$$

을 얻는다. 그러므로 $n \pmod 4 \neq 3$ 이면 $\mathbb{C}$는 그룹 $GF(2^p)$ 셀룰라 오토마타이고, $n \pmod 4 = 3$ 이면 $\mathbb{C}$는 비그룹 $GF(2^p)$ 셀룰라 오토마타이다.

□

3.2. 선형 $GF(2^p)$ 셀룰라 오토마타의 특성다항식과 상태전이행렬과의 관계

이 절에서는 선형 $GF(2^p)$ 셀룰라 오토마타의 특성다항식과 상태전이행렬과의 관계를 분석하고자 한다. 주어진 $GF(2)$위에서의 기약다항식이나 원시다항식에 대응하는 90/150 $GF(2)$ 셀룰라 오토마타는 반드시 두 개만이 존재한다는 것을 2007년에 Cho 등[9]이 밝혔다. 그러나 $GF(2^p)$ 기약다항식이나 원시다항식에 대응하는 $GF(2^p)$ 셀룰라 오토마타는 [표 Ⅲ-1]에서 보듯이 여러 개인 경우가 있다.

[표 Ⅲ-1] $GF(2^2)$ 위에서의 셀룰라 오토마타 룰

특성다항식	CA 룰		
x^3+x^2+x+2	$(032)_1$	$(023)_2$	$(203)_3$
x^3+x^2+x+3	$(023)_1$	$(203)_2$	$(032)_3$
x^3+x^2+2x+3		$(133)_2$	
x^3+x^2+3x+2			$(122)_3$
x^3+2x^2+x+3			$(112)_3$
x^3+2x^2+2x+2	$(233)_1$		
x^3+2x^2+3x+2	$(103)_1$	$(013)_2$	$(031)_3$
x^3+2x^2+3x+3	$(013)_1$	$(031)_2$	$(103)_3$
x^3+3x^2+x+2		$(113)_2$	
x^3+3x^2+2x+2	$(012)_1$	$(102)_2$	$(021)_3$
x^3+3x^2+2x+3	$(102)_1$	$(021)_2$	$(012)_3$
x^3+3x^2+3x+3	$(223)_1$		

< **예제 3.2.1** > 3 차 $GF(2^2)$ 원시다항식 x^3+3x^2+2x+2에 대응하는 3

셀 $GF(2^2)$ 셀룰라 오토마타는

$$<0,1,2>_1=\begin{pmatrix}0&1&0\\1&1&1\\0&1&2\end{pmatrix},\quad <1,0,2>_2=\begin{pmatrix}1&2&0\\2&0&2\\0&2&2\end{pmatrix},\quad <0,2,1>_3=\begin{pmatrix}0&3&0\\3&2&3\\0&3&1\end{pmatrix}$$

이다. 또한 4차 $GF(2^2)$ 원시다항식 $x^4+3x^3+2x^2+3x+2$에 대응하는 4 셀 $GF(2^2)$ 셀룰라 오토마타는

$$<0,3,2,2>_1=\begin{pmatrix}0&1&0&0\\1&3&1&0\\0&1&2&1\\0&0&1&2\end{pmatrix},\quad <1,1,1,2>_1=\begin{pmatrix}1&1&0&0\\1&1&1&0\\0&1&1&1\\0&0&1&2\end{pmatrix},\quad <1,3,2,3>_3=\begin{pmatrix}1&3&0&0\\3&3&3&0\\0&3&2&3\\0&0&3&3\end{pmatrix}$$

이다.

선형 $GF(2^p)$ 셀룰라 오토마타의 특성다항식과 상태전이행렬과의 관계를 분석하기에 앞서 90/150 $GF(2)$ 셀룰라 오토마타의 특성다항식과 상태전이행렬과의 관계를 알아보기로 한다.

다음 정리는 잘 알려진 정리이다.

< 정리 3.2.1 > n 셀 90/150 $GF(2)$ 셀룰라 오토마타 $\mathbb{C}$의 상태전이행렬이 $U_n=<d_1, d_2, \cdots, d_n>$이며 특성다항식이 Δ_n이라 하자. $\Delta_{-1}=0$이고 $\Delta_0=1$이라 하면 다음이 성립한다.

$$\Delta_k = (x+d_k)\Delta_{k-1} + \Delta_{k-2}$$

여기서 $k = 1, 2, \cdots, n$ 이다.

< **예제 3.2.2** > 4 셀 90/150 $GF(2)$ 셀룰라 오토마타 $\mathbb{C}$의 상태전이행렬을 $U_4 = < 0, 1, 0, 1 >$라 하면

$$\Delta_4 = \begin{vmatrix} x & 1 & 0 & 0 \\ 1 & x+1 & 1 & 0 \\ 0 & 1 & x & 1 \\ 0 & 0 & 1 & x+1 \end{vmatrix}$$

이다. <정리 3.2.1>에 의하여

$$\Delta_4 = (x+1)\Delta_3 + \Delta_2$$

$$= (x+1)\begin{vmatrix} x & 1 & 0 \\ 1 & x+1 & 1 \\ 0 & 1 & x \end{vmatrix} + \begin{vmatrix} x & 1 \\ 1 & x+1 \end{vmatrix}$$

$$= x^4 + x + 1$$

이다.

다음 <정리 3.2.2>은 <정리 3.2.1>의 확장이다.

< **정리 3.2.2** > n 셀 $GF(2^p)$ 셀룰라 오토마타 $\mathbb{C}$의 상태전이행렬이 $T_n = < d_1, d_2, \cdots, d_n >_w$이며 특성다항식이 Δ_n이라 하자. $\Delta_{-1} = 0$이라 하

고 $\Delta_0 = 1$이라 하면 다음이 성립한다.

$$\Delta_k = (x+d_k)\Delta_{k-1} + w^2\Delta_{k-2}$$

여기서 $k = 1, 2, \cdots$ 이며 $w \in \{1, 2, 3, \cdots, 2^p - 1\}$이다.

[증명] $\Delta_1 = x + d_1 = (x+d_1)\cdot 1 + w^2 \cdot 0 = (x+d_1)\Delta_0 + w^2\Delta_{-1}$이므로 $n=1$일 때 성립한다. $n=k$일 때 성립한다고 하자. 그러면

$$\Delta_{k+1} = \begin{vmatrix} x+d_1 & w & 0 & \cdots & 0 & 0 \\ w & x+d_2 & w & \cdots & 0 & 0 \\ 0 & w & x+d_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x+d_k & w \\ 0 & 0 & 0 & \cdots & w & x+d_{k+1} \end{vmatrix}$$

이므로

$$\Delta_{k+1} = (x+d_{k+1}) \begin{vmatrix} x+d_1 & w & 0 & \cdots & 0 & 0 \\ w & x+d_2 & w & \cdots & 0 & 0 \\ 0 & w & x+d_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x+d_{k-1} & w \\ 0 & 0 & 0 & \cdots & w & x+d_k \end{vmatrix}$$

$$+w^2\begin{vmatrix} x+d_1 & w & 0 & \cdots & 0 & 0 \\ w & x+d_2 & w & \cdots & 0 & 0 \\ 0 & w & x+d_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x+d_{k-2} & w \\ 0 & 0 & 0 & \cdots & w & x+d_{k-1} \end{vmatrix}$$

$$= (x+d_{k+1})\Delta_k + w^2\Delta_{k-1}$$

이므로 모든 자연수 n에 대하여 성립한다.

□

[참고] <정리 3.2.2>은 가중치가 동일한 선형 $GF(2^p)$ 셀룰라 오토마타의 특성다항식을 구하는 효율적인 알고리즘을 제공한다.

< 예제 3.2.3 > $\mathbb{C}$를 상태전이행렬이 $<1,3,2,3>_3$인 4 셀 $GF(2^2)$ 셀룰라 오토마타라 하자. 그러면 다음을 얻는다.

$$\Delta_{-1} = 0$$
$$\Delta_0 = 1$$
$$\begin{aligned}\Delta_1 &= (x+d_1)\Delta_0 + 3^2 \cdot \Delta_{-1} \\ &= (x+1)\cdot 1 + 3^2 \cdot 0 \\ &= x+1\end{aligned}$$

$$\begin{aligned}\Delta_2 &= (x+d_2)\Delta_1 + 3^2 \cdot \Delta_0 \\ &= (x+3)(x+1) + 3^2 \cdot 1 \\ &= x^2+2x+1\end{aligned}$$

$$\begin{aligned}\Delta_3 &= (x+d_3)\Delta_2 + 3^2 \cdot \Delta_1 \\ &= (x+2)(x^2+2x+1) + 2(x+1) \\ &= x^3\end{aligned}$$

$$\begin{aligned}\Delta_4 &= (x+d_4)\Delta_3 + 3^2 \cdot \Delta_2 \\ &= (x+3)x^3 + 2(x^2+2x+1) \\ &= x^4+3x^3+2x^2+3x+2\end{aligned}$$

위의 예제에서 Δ_4부터 시작하여 Δ_1까지의 몫을 차례로 쓰면 $<3, 2, 3, 1>_3$을 얻는다. 그러면 어떻게 하면 "주어진 $GF(2^p)$ 기약다항식이나 원시 다항식에 대응하는 가중치가 동일한 $GF(2^p)$ 셀룰라 오토마타를 구할 수 있을까?" 라는 질문을 가질 수 있다. 나눗셈 알고리즘의 변형된 형태인 다음 나눗셈 알고리즘을 생각해 보자. a를 b로 나누었을 때 몫을 q라 하고 나머지가 r이라 하면

$$a = b \cdot q + w^2 \cdot r_1$$

이다. 여기서 $w \in \{1, 2, 3, \cdots, 2^p-1\}$이며 $w^2 \cdot r_1 = r$이다.

[참고] 위의 형태의 알고리즘을 변형된 나눗셈 알고리즘이라 한다.

< 예제 3.2.4 > <예제 3.2.3>에서 $\Delta_4 = x^4+3x^3+2x^2+3x+2$에 대하여 $w=3$이고 $\Delta_3 = x^3$라면

$$\begin{aligned}\Delta_4 &= (x+3)\Delta_3 + 3^2 \cdot \Delta_2 \\ \Delta_3 &= (x+2)\Delta_2 + 3^2 \cdot \Delta_1 \\ \Delta_2 &= (x+3)\Delta_1 + 3^2 \cdot \Delta_0 \\ \Delta_1 &= (x+1)\Delta_0 + 3^2 \cdot \Delta_{-1}\end{aligned}$$

을 얻게 된다. Δ_1의 몫부터 차례로 올라가면서 순서대로 읽어서 가중치가 3인 4 셀 $GF(2^2)$ 셀룰라 오토마타 $<1, 3, 2, 3>_3$을 얻는다.

위의 <예제 3.2.4>에서 Δ_4는 4차의 원시다항식이며 Δ_3는 3차, Δ_2는 2차 그리고 Δ_1은 1차 다항식임을 알 수 있다. 이와 같이 Δ_3을 안다고 해서 $w \in \{1, 2, 3\}$를 바로 알 수는 없다. 하나씩 대입해서 Δ_k $(k = 1, 2, 3)$가 k차 다항식일 때만 Δ_4에 대응하는 셀룰라 오토마타를 구할 수 있다.

< 정의 3.2.3 > $GF(2^p)$ 위에서 주어진 n차 다항식 $f(x)$에 대하여 대응하는 가중치가 $w \mathit{IN} \{1, 2, 3, \cdots, 2^p - 1\}$인 선형 $GF(2^p)$ 셀룰라 오토마타가 존재할 때 $f(x)$를 $GF(2^p)$ 셀룰라 오토마타 다항식이라 한다.

< 예제 3.2.5 > $GF(2^2)$ 위에서의 4차 원시다항식 $x^4 + x^2 + 2x + 3$에 대응하는 선형 $GF(2^2)$ 셀룰라 오토마타는 $<0, 0, 3, 3>_2$이다. 또한 $x^4 + x^3 + x + 2$에 대응하는 선형 $GF(2^2)$ 셀룰라 오토마타는 $<0, 3, 1, 3>_3$과 $<2, 2, 3, 2>_3$이다.

앞의 <예제 3.2.4>에서 Δ_3를 알지 못하고는 Δ_4에 대응하는 $GF(2^2)$ 셀룰라 오토마타를 구하는 것은 아주 어려운 문제이다. 이와 같은 이유로 앞에서도 언급한 바와 같이 주어진 n차 $GF(2^p)$ 기약다항식이나 원시다항식에 대응하는 n 셀 $GF(2^p)$ 셀룰라 오토마타를 구하는 방법이 존재하지 않는다.

< **예제 3.2.6** > 상태전이행렬 T가 다음과 같을 때, T에 의한 $GF(2^2)$ MACA 상태전이는 [표 Ⅲ-2]과 같다.

$$T = \begin{pmatrix} 0 & \alpha^2 & 0 \\ \alpha^2 & 1 & 0 \\ 0 & \alpha^2 & 0 \end{pmatrix} = < 0, 1, 0 >_{\alpha^2}$$

[표 Ⅲ-2] $GF(2^2)$ MACA 상태전이

221	023	122	320	031	332	130	233	012	311	113	210
101				202				303			
000											

003	102	201	300	032	133	230	331	011	110	213	312
020				222				323			
121											

001	100	203	302	022	123	220	321	013	112	211	310
030				131				333			
232											

002	103	200	301	021	120	223	322	033	132	231	330
010				111				212			
313											

[표 Ⅲ-2]에서 색칠한 부분의 상태들은 주기가 1인 순환상태이고 이런 순환상태를 attractor라 한다. attractor가 121인 트리는 상태 003, 102, 201, … , 121로 이루어졌다. 주어진 3-셀 $GF(2^2)$ MACA의 상태전이그래프는 모두 깊이가 2인 4개의 독립된 트리로 구성되며 각 순환상태들은 모두 attractor이다. 상태 221은 시간의 변화에 따라 221→101→000으로 상태가

전이된다. 따라서 000-트리의 깊이는 2이다. 일반적으로 MACA의 최소 다항식은 $x^d(x+1)$이며 여기서 d는 MACA의 상태전이그래프에서 트리의 깊이가 된다[18]. 또한 n-셀 SACA의 최소다항식은 x^n이며 이러한 SACA의 상태전이그래프는 깊이가 n인 트리가 된다[8]. 가중치가 $w(\in GF(2^p))$인 $GF(2^p)$인 셀룰라 오토마타는 90/150 셀룰라 오토마타의 확장으로 특성다항식과 최소다항식이 같다. T에 의한 3-셀 $GF(2^2)$ MACA의 최소다항식은 $x^3+x^2=x^2(x+1)$이므로 상태전이그래프의 트리의 깊이는 2이다.

3.3. 선형 $GF(2^p)$ MACA 전이규칙

가중치가 w인 m-셀 $GF(2^p)$의 전이규칙이 $T = < d_1, d_2, \cdots, d_m >_w$ $(w \in GF(2^p))$일 때, 이 셀룰라 오토마타의 특성다항식을 Δ_m이고, 주어진 셀룰라 오토마타의 i번째 셀에서 j번 째 셀까지의 부분 셀룰라 오토마타의 특성다항식을 Δ_{ij}라 하자. 그리고 $\Delta_{1,m-1}$은 간단히 Δ_{m-1}라 하자. 그러면 특성다항식 Δ_m에 대한 점화식은 다음과 같다[21].

$$\Delta_k = (x + d_k)\Delta_{k-1} + w^2\Delta_{k-2}, \ (k > 0)$$
$$\Delta_{-1} = 0, \quad \Delta_0 = 1$$

주어진 셀룰라 오토마타의 전이규칙을 mirror image를 이용하여 합성한 $2m$-셀 $GF(2^p)$ 셀룰라 오토마타의 전이규칙을 다음과 같이 정의한다.

$$T = < d_1, d_2, \cdots, d_m + w, d_m + w, \cdots, d_2, d_1 >_w$$

그리고 합성된 셀룰라 오토마타의 특성다항식을 Δ_{2m}라 표현하도록 하자. 다음 정리는 mirror image를 이용하여 합성된 $GF(2^p)$ 셀룰라 오토마타의 특성다항식 사이의 점화관계를 특성화 한다.

< 정리 3.3.1 > $2m$-셀 $GF(2^p)$ 셀룰라 오토마타의 전이규칙이

$$T = < d_1, d_2, \cdots, d_m, d_m, \cdots, d_2, d_1 >_w$$

라 할 때, 부분 행렬의 특성다항식은 다음과 같은 두 점화식을 만족한다.

(1) $\Delta_{i-1}\Delta_{2m-i-1} + w^2\Delta_i\Delta_{2m-i-2}$
$= \Delta_{i+2}\Delta_{2m-i-1} + w^2\Delta_{i+1}\Delta_{2m-i-3}$

(2) $\Delta_{2m} = (\Delta_m + w\Delta_{m-1})^2$

[증명] 주어진 전이 규칙 T의 각 셀에 대한 규칙이 $d_{2m-i-1} = d_{i+2}$이므로 다음 식을 만족한다.

(1) $\Delta_{i+1}\Delta_{2m-i-1} + w^2\Delta_i\Delta_{2m-i-2}$
$= \Delta_{i+1}((x+d_{2m-i-1})\Delta_{2m-i-2} + w^2\Delta_{2m-i-3}) + w^2\Delta_i\Delta_{2m-i-2}$
$= \Delta_{i+1}((x+d_{i+2})\Delta_{2m-i-2} + w^2\Delta_{2m-i-3}) + w^2\Delta_i\Delta_{2m-i-2}$
$= ((x+d_{i+2})\Delta_{i+1} + w^2\Delta_i)\Delta_{2m-i-2} + w^2\Delta_{i+1}\Delta_{2m-i-3}$
$= \Delta_{i+2}\Delta_{2m-i-2} + w^2\Delta_{i+1}\Delta_{2m-i-3}$

(2)의 증명은 다음과 같다.

$$\begin{aligned}\Delta_{2m} &= (x+d_{2m})\Delta_{2m-1} + w^2\Delta_{2m-2}\\ &= (x+d_1)\Delta_{2m-1} + w^2\Delta_0\Delta_{2m-2}\\ &= \Delta_1\Delta_{2m-1} + w^2\Delta_0\Delta_{2m-2}\end{aligned}$$

<정리 3.3.1>의 식(1)에 의해 위 식은 다음을 만족한다.

$$\begin{aligned}\Delta_{2m} &= \Delta_{1+m-1}\Delta_{2m-1-m+1} + w^2\Delta_{m-1}\Delta_{2m-2-m+1} \\ &= \Delta_m\Delta_m + w^2\Delta_{m-1}\Delta_{m-1} \\ &= (\Delta_m + w\Delta_{m-1})^2\end{aligned}$$

□

다음 정리들은 $GF(2^p)$ 셀룰라 오토마타의 SACA와 MACA를 합성하는 근거가 되는 매우 중요한 정리이다.

< **정리 3.3.2** > 가중치가 w인 m-셀 $GF(2^p)$ 셀룰라 오토마타의 전이규칙

$$T = < d_1, d_2, \cdots, d_m + w >_w$$

의 특성다항식을 $f(x)$라 할 때, $2m$-셀 $GF(2^p)$ 셀룰라 오토마타의 전이규칙 $T_{2m} = < d_1, d_2, \cdots, d_m, d_m, \cdots, d_2, d_1 >_w$의 특성다항식은 $\Delta_{2m} = \{f(x)\}^2$이다.

[증명] 주어진 T_{2m}의 특성다항식은 <정리 3.3.1>의 식 (2)에 의해 $\Delta_{2m} = (\Delta_m + w\Delta_{m-1})^2$이다. 그리고

$$\begin{aligned}\Delta_m + w\Delta_{m-1} &= (x+d_m)\Delta_{m-1} + w^2\Delta_{m-2} + w\Delta_{m-1} \\ &= (x+d_m+w)\Delta_{m-1} + w^2\Delta_{m-2}\end{aligned}$$

이다. 그런데 $(x+d_m+w)\Delta_{m-1} + w^2\Delta_{m-2}$는 T_m의 특성다항식 $f(x)$의 점화식이다. 그러므로 $\Delta_{2m} = \{f(x)\}^2$이다.

□

< **정리 3.3.3** > 가중치가 w인 m-셀 $GF(2^p)$ 셀룰라 오토마타의 전이규칙 $T_m = < d_1, d_2, \cdots, d_m >_w$의 특성다항식을 $f(x)$라 할 때, $(2m+1)$-셀 $GF(2^p)$ 셀룰라 오토마타 전이규칙 $T_{2m+1} = < d_1, d_2, \cdots, d_m, 0, d_m, \cdots, d_2, d_1 >_w$의 특성다항식은 $\Delta_{2m} = x\{f(x)\}^2$이다.

[증명] 주어진 T_{2m+1}의 특성다항식은 다음을 만족한다.

$$\begin{aligned}
\Delta_{2m+1} &= (x+d_1)\Delta_{2m} + w^2\Delta_{2m-1} \\
&= \Delta_1\Delta_{2m} + w^2\Delta_0\Delta_{2m-1} \\
&= \Delta_2\Delta_{2m-1} + w^2\Delta_1\Delta_{2m-2} \\
&\quad\vdots \\
&= \Delta_{m+1}\Delta_m + w^2\Delta_{m-1}\Delta_m \\
&= \Delta_m(\Delta_{m+1} + w^2\Delta_{m-1}) \\
&= \Delta_m((x+d_{m+1})\Delta_m + w^2\Delta_{m-1} + w^2\Delta_{m-1}) \\
&= \Delta_m^2(x+d_{m+1})
\end{aligned}$$

그런데 $d_{m+1} = 0$이므로 $\Delta_{2m+1} = x\Delta_m^2$이고 T_{2m+1}의 Δ_m은 T_m의 특성다항식 $f(x)$와 같다. 그러므로 $\Delta_{2m} = x\{f(x)\}^2$이다.

□

$T_1 = <0>_w$의 특성다항식은 $c_1(x) = x$로 1-셀 SACA이다. 따라서 <정리 3.3.2>에 의해 2셀 SACA는 mirror image를 사용한 $T_2 = < w, w >_w$로 합성되고 3-셀 SACA는 <정리 3.3.3>에 의해 $T_3 = < w, 0, w >_w$로 합성

된다. 같은 방법으로 합성하면 모든 크기의 셀에 대한 $GF(2^p)$ SACA를 합성할 수 있다. 이제 가중치가 w인 m-셀 $GF(2^p)$ SACA가 주어졌을 때, 이로부터 유도되는 $GF(2^p)$ MACA를 합성하는 방법을 제안한다.

< 정리 3.3.4 > 가중치가 w인 m-셀 $GF(2^p)$ SACA의 전이규칙 $T_m = < d_1, d_2, \cdots, d_m >_w$이라 할 때, $(2m+1)$-셀 $GF(2^p)$ 셀룰라 오토마타의 전이규칙이 다음과 같은 셀룰라 오토마타는 MACA이다.

$$T_{2m+1} = < d_1, d_2, \cdots, d_m, 1, d_m, \cdots, d_2, d_1 >_w$$

[증명] 주어진 T_{2m+1}의 d_{m+1}의 값이 1이므로 특성다항식은 $\Delta_{2m+1} = \Delta_m^2(x + d_{m+1}) = \Delta_m^2(x+1)$이다. 부분 특성다항식 Δ_m은 주어진 m-셀 SACA T_m의 특성다항식과 같으므로 $\Delta_{2m+1} = x^{2m}(x+1)$이다.

□

[표 Ⅲ-3]은 <정리 3.3.2>와 <정리 3.3.3>에 의해 합성된 $GF(2^p)$ SACA와 <정리 3.3.4>에 의해 합성된 $GF(2^p)$ MACA의 전이규칙에 관한 표이다. 이렇게 합성된 $(2m+1)$-셀 $GF(2^p)$ MACA 특성다항식이 $x^{2m}(x+1)$이므로 트리의 깊이가 $2m$이다. 따라서 하나의 트리를 이루고 있는 상태의 수는

$$(2^p)^{2m+1} = 2^{2mp+p}$$

이다. 따라서 attractor의 수는 $2^{2mp+p}/2^{2mp} = 2^p$ 이다.

[표 Ⅲ-3] 합성된 $GF(2^p)$ SACA와 MACA

n	SACA	MACA
1	$<0>_w$	$<1>_w$
2	$<w, w>_w$	
3	$<0, 0, 0>_w$	$<0, 1, 0>_w$
4	$<w, 0, 0, w>_w$	
5	$<w, w, 0, w, w>_w$	$<w, w, 1, w, w>_w$
6	$<0, 0, w, w, 0, 0>_w$	
7	$<0, 0, 0, 0, 0, 0, 0>_w$	$<0, 0, 0, 1, 0, 0, 0>_w$
8	$<w, 0, 0, 0, 0, 0, 0, w>_w$	
9	$<w, 0, 0, w, 0, w, 0, 0, w>_w$	$<w, 0, 0, w, 1, w, 0, 0, w>_w$
10	$<w, w, 0, w, 0, 0, w, 0, w, w>_w$	
11	$<w, w, 0, w, w, 0, w, w, 0, w, w>_w$	$<w, w, 0, w, w, 1, w, w, 0, w, w>_w$
12	$<0, 0, w, w, 0, w, w, 0, w, w, 0, 0>_w$	
13	$<0, 0, w, w, 0, 0, 0, 0, 0, w, w, 0, 0>_w$	$<0, 0, w, w, 0, 0, 1, 0, 0, w, w, 0, 0>_w$

Ⅳ. 결론

비트단위로 처리하는 $GF(2)$ 위에서의 셀룰라 오토마타 보다 복잡한 시스템을 모델링하기에 적합한 $GF(2^p)$ 셀룰라 오토마타 중 특별한 클래스인 MACA와 SACA의 특성다항식의 점화관계를 분석하여 그 결과를 바탕으로 하여 $GF(2^p)$ SACA를 합성하였다. 또한 얻어진 m-셀 $GF(2^p)$ SACA로부터 $(2m+1)$-셀 $GF(2^p)$ MACA를 합성하였다. $GF(2)$ 위에서 90/150 TPSACA와 90/150 TPMACA 보다 2^p배 이상 많은 $GF(2^p)$ SACA와 MACA가 존재함을 보였다. 또한 가중치가 동일한 n-셀 $GF(2^p)$ 셀룰라 오토마타에 관하여 n 셀 90-150 $GF(2)$ 셀룰라 오토마타와 비교하여 분석하였다. 그리고 주어진 n차 기약다항식과 원시다항식과 그에 대응하는 n 셀 $GF(2^p)$ 셀룰라 오토마타와 관계에 대하여 분석하였다.

참 고 문 헌

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

[2] K. Cattell and J.C. Muzio, Analysis of one-dimensional linear hybrid cellular automata over $GF(q)$, IEEE Trans. Comput. Vol. 45, No. 7, pp. 782-792, 1996.

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

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

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

[6] S.J. Cho, U.S. Choi, Y.H. Hwang , Y.S. Pyo, H.D. Kim, S.H. Heo , Computing Phase Shift of Maximum-Length 90/150 Cellular Automata Sequences, LNCS, Vol. 3305, pp. 31-39, 2004.

[7] S.J. Cho, U.S. Choi, Y.H. Hwang and H.D. Kim, Analysis of hybrid group cellular Automata, ACRI 2006, LNCS, 4137, pp. 222-231, 2006.

[8] 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 $GF(2^p)$", LNCS 4173, pp. 232-237, 2006.

[9] S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim, J.G. Kim, S.H. Heo, New synthesis of one-dimensional 90/150 linear hybrid group cellular automata, IEEE Trans. Comput.-Aided Design Inter. Circuits Syst., Vol. 25, No. 9, pp. 1720-1724, 2007.

[10] U.S. Choi, S.J. Cho, H.D. Kim, Y.H. Hwang and S.T. Kim, Nonlinear Pseudorandom Sequences Based on 90/150 LHGCA, H.Umeo et al. (Eds): ACRI 2008, LNCS 5191, pp. 471-477, 2008.

[11] 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.

[12] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press 1994.

[13] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press 1997.

[14] J. Von Neumann, The Theory of Self-Reproduction Automata, In: Burks, A.W. (ed.) University of Illinois Press, 1966.

[15] K. Paul, Theory and application of $GF(2^p)$ Cellular automata, Ph.D Thesis, Department of Computer Science and Technology, Bengal Engineering College (A Deemed University), 2002.

[16] 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. Comput-Aided Desig, 9, pp. 767-778, 1990.

[17] A.F. Sabater and P.C. Gil, Synthesis of cryptographic interleaved sequence by means of linear cellular automata, Applied Mathematics Letters, 22(10), pp. 1518-1524.

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

[19] B.K. Sikdar, P. Maiumder, M. Mukherjee, N. Ganguly, D.K. Das and P.P. Chaudhuri, Hierarchical Cellular automata as an on-chip test pattern generator, In: VLSI Design, Fourteenth International Conference on 2001, pp. 403-408, 2001.

[20] S. Wolfram, Statistical Mechanics of Cellular Automata, Rev. Mod. Phys. 55, pp. 601-644, 1983.

[21] 최언숙, 조성진, 최향희 "계층적 셀룰라 오토마타의 특성에 관한 연구", 한국해양정보통신학회눈문지, Vol. 12(3), pp. 493-499, 2008.