이학석사 학위논문

선형 Uniform Group CA로부터 유도되는 여원 CA에 대한 특성화

2007 년 8월

부경대학교 대학원

응 용 수 학 과

김 경 자

이학석사 학위논문

선형 Uniform Group CA로부터 유도되는 여원 CA에 대한 특성화

지도교수 조 성 진

이 논문을 이학석사 학위논문으로 제출함

2007 년 8월

부경대학교 대학원

응 용 수 학 과

김 경 자

김경자의 이학석사 학위청구논문을 인준함

2007년 8월 30일

주 심 이학박사 표 용 수 ㊞

위 원 이학박사 박 진 한 ㊞

위 원 이학박사 조 성 진 ㊞

< 차 례 >

Characterization of a class of the Complemented CA derived from Linear Uniform Group CA

Kyung-Ja Kim

Department of Applied Mathematics, Graduate School.
Pukyoung National University

Abstract

In this paper, we analyze several complemented Cellular Automata(CA) derived from a linear uniform group CA with rule 60 or 102 according to the complement vector. These CA rules referred to as functions determining the state transition of the CA divide the entire state space into smaller cycles of equal maximum lengths. We analyze cycle properties of these CA. Also we extend and generalize the results of Mukhopadhyay et al.

1.서론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 Von Neumann과 Ulam에 의해서 스스로 조직화하고 재생산할 수 있는 모델로 처음 소개되었다([1]). Wolfram([2])은 각 셀이 0과 1, 두 상태를 가지고 다음 상태가 자기 자신과 인접한 두 이웃에 의해 갱신되는 3-이웃(3-neighbourhood) CA를 제안하였다. Das 등([3]~[5])은 행렬을 이용하여 CA를 분석하는 방법을 도입하였다. CA는 테스트 패턴 생성, 의사난수생성기, 오류정정부호기, 암호, 시그니처 분석 등 많은 분야에 응용되었다([6]~[9]). Cho 등([10]~[13])은 해쉬함수, 데이터 저장, 암호 등에 CA를 적용한 연구를 하였다.

그룹 CA의 상태전이행렬은 정칙행렬이고, 상태전이그래프는 사이클들로 이루어져 있다. 그룹 CA를 이용하면 아주 긴 주기의 의사난수를 생성할 수 있다. 최대 길이를 갖지 않는 그룹 CA의 상태들은 여러 사이클들로 이루어져 있는데, Das([3])는 선형 그룹 CA C의 전이규칙 R의 주기가 m이면 C로부터 유도된 전이규칙 $\overline{R}$의 주기가 m 또는 $2m$일 것이라고 예측했다.

무선 통신의 출현과 PDA, 스마트카드와 같은 휴대용 장치의 발전으로 인해 이에 대한 보안과 개인 정보보호에 대한 필요성이 대두되면서 암·복호화를 공유할 수 있는 하드웨어 구현이 주목을 받고 있다. CA는 전용 하드웨어를 사용하지 않고 실행가능하도록 프로그램화 될 수 있어 여기에 이용할 수 있다. Mukhopadhyay 등([7])은 전이규칙 102에서 셀 상태가 모두 1인 여원벡터에 의해 유도된 여원 uniform group CA를 분석하고, 이러한 성질을 이용하여 키 공유 프로토콜에 적용하였다.

본 논문에서는 이러한 키 공유 프로토콜에 적용 가능한 특별한 전이규칙을 갖는 선형 uniform group CA(이하 LUGCA)와 각각에 대응하는 여원벡터에 의해 유도된 여원 CA를 분석했다. 또한 Das 의 예측이 참임을 밝혔다. 그리고 전이규칙 60 또는 102를 갖는 LUGCA로부터 유도된 여원 CA의 상태전이 연산자의 주기를 구체적으로 밝혔다. 또한 Mukhopadhyay 등([7])의 결과를 일반화한 연구를 하였다.

2. 정의 및 기초이론

2.1. CA의 정의

셀룰라 오토마타(Cellular Automata, 이하 CA)는 Von Neumann과 Ulam에 의해 스스로 조직화하고 재생산할 수 있는 모델로 소개되었다.

CA란 동역학계(dynamical system)를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루고, 이산적인 공간을 셀룰라 공간(cellular space)의 기본 단위인 각 셀이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. CA는 그 후 Wolfram에 의하여 처음으로 암호학에 도입되었다. 이후 Das 등에 의해서 행렬 대수학으로 분석이 이루어졌으며 Chaudhuri, Nandi 등이 많은 분야에 CA를 폭넓게 활용하였다. 오류검출 및 정정 부호는 메모리 시스템 설계, 디지털 데이터 통신 등에 널리 적용된다.

가장 간단한 구조를 가지는 1차원 CA에서는 모든 셀들이 선형으로 배열되어 있고 국소적 상호 작용이 세 개의 셀, 즉 자기 자신과 인접한 두 셀에 의해 이루어지는 3-이웃(3- neighbourhood) CA이다.

CA를 설명하기 위해서는 다음 기호들이 사용된다.

i	일차원으로 배열되어 있는 각 셀들의 위치
t	시간단계
$q_i(t)$	시간 t에서 i번째 셀의 상태
$q_i(t+1)$	시간 $t+1$에서 i번째 셀의 상태

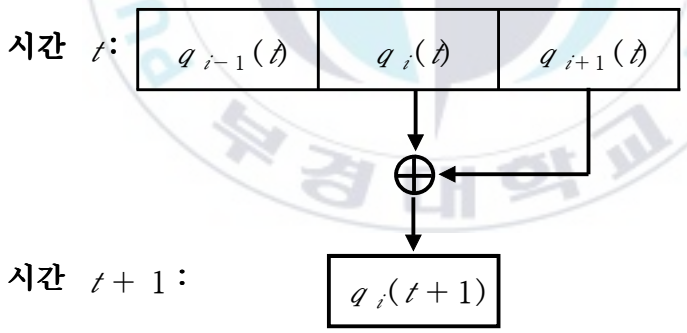
<표 2.1> CA의 기호

2.2. CA Rule

3-이웃 CA의 다음 상태전이 함수(state-transition function)는 다음과 같다.

$$q_i(t+1) = f[q_{i-1}(t), q_i(t), q_{i+1}(t)] \quad (16.1)$$

여기서 3-이웃 다음상태전이 함수에서 f는 결합논리를 가지는 국소 전이 함수이다. f는 3개의 변수를 가지는 Boolean 함수이며 따라서 $2^{2^3}(256)$개의 상태전이 함수로 되어있고, 이것을 CA Rule이라 한다. 예를 들어 rule 60은 왼쪽 셀과 자기 자신에 영향을 받고, rule 102는 자기 자신과 오른쪽 셀에 영향을 받아 다음상태가 만들어진다. <그림 2.1>은 rule 102 선형 셀 구조이다.



<그림 2.1> Rule 102의 선형Cell 구조

3-이웃 CA에서 rule 60과 rule 102의 상태배열의 예를 살펴보면 다음과 같다.

이웃상태	(1,1,1)	(1,1,0)	(1,0,1)	(1,0,0)	(0,1,1)	(0,1,0)	(0,0,1)	(0,0,0)	rule
다음상태	0	1	1	0	0	1	1	0	rule 60
다음상태	0	1	1	0	0	1	1	0	rule 102

<표2.1>은 CA Rule 이다.

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

<표2.1> Additive CA Rules

2.3. CA의 분류

1차원 CA는 셀들에 적용되는 rule의 논리의 종류에 따라 linear CA, additive CA, nonadditive CA로 분류된다.

<정의 2.1> 모든 셀들의 rule이 XOR논리로만 이루어진 CA를 linear CA, XOR과 XNOR의 조합으로 이루어진 CA를 additive CA, AND-OR논리로 이루어진 CA를 nonadditive CA라 한다.

모든 같은 rule이 적용되었으나 여부에 따라 uniform CA, hybrid CA로 분류된다.

<정의 2.2> 모든 CA의 셀들이 같은 rule을 따르는 CA를 uniform CA, 같은 rule을 따르지 않는 CA를 hybrid CA라 한다.

셀들이 rule에 의해 변화되는 상태에 따라 group CA, nongroup CA로 분류된다.

<정의 2.3> T가 CA에 대한 상태전이행렬 일 때, $\det(T)=1$인 CA를 그룹 CA(group CA)라고 한다.

그룹 CA의 상태전이그래프는 사이클들로 이루어진다.

<보조정리 2.2> 상태전이행렬 T를 갖는 CA로부터 여원벡터 F에 의해 유도된 CA의 연산자를 $\overline{T}$라 하면, X의 p번째 다음 상태는

$$\overline{T^p}X = T^pX \oplus (T^{p-1} \oplus \cdots \oplus T^2 \oplus T \oplus I)F$$

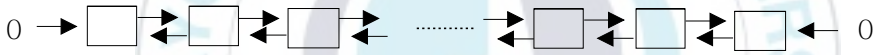
이다.

CA에서 가장 왼쪽과 가장 오른쪽 셀은 2개의 이웃만을 가지므로 이들의

세 번째 이웃을 결정해 주는 일은 매우 중요하며 이들 세 번째 이웃을 결정해 주는 것을 CA의 경계조건이라 한다. 일반적으로 CA를 경계조건에 따라 다음 세 가지로 분류한다.

<정의 2.4> 가장 왼쪽과 가장 오른 쪽의 셀들이 0상태에 연결되어 있는 경우를 NBCA(Null boundary CA), 양 끝의 셀들이 연결되어 있는 경우를 PBCA(Periodic boundary CA), 가장 왼쪽(오른 쪽)셀의 다음 상태가 그 자신과 그것의 오른 쪽(왼쪽) 이웃, 두 번째 오른 쪽(왼쪽) 이웃의 상태에 의존하는 경우를 IBCA(Intermediate boundary CA)라 한다.

<그림 2.2>는 CA의 경계조건을 나타낸 것이다.



(1)1-D NBCA

(2) 1-D PBCA

(3) 1-D IBCA

<그림 2.2> 1-D CA의 경계조건

2.4. CA의 전이행렬과 특성다항식

n개의 셀을 가지는 1-D CA에서는 현재 상태를 다음 상태로 전이시키는 작용소를 $n \times n$ 행렬로 나타낼 수 있는데 이것을 CA의 전이행렬이라 한다.

전이 행렬 T에서 i번째 행은 i번째 셀에 적용되는 rule이며 그 셀의 다음 상태가 현재 상태에 의존하면 1, 그렇지 않으면 0으로 쓴다.

$f_t(x)$ 가 시간 t에서 CA의 상태를 나타내면 시간 $t+1$ 에서의 상태는 다음과 같다.

$$f_{t+1}(x) = T \cdot f_t(x) \tag{2.2}$$

<예 2.4.1> 4-셀의 1차원 PBCA의 rule이 <102, 102, 102, 150>이라면 전이 행렬은 다음과 같다.

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

그리고 이 CA의 현재 상태가 $f_t(x) = [0\ 1\ 0\ 1]^T$ 이면 다음상태는 다음과 같다.

$$f_{t+1}(x) = T \cdot f_t(x) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

CA의 전이행렬이 T일 때, T의 특성다항식(Characteristic Polynomial) $\Delta(x)$ 은 다음과 같다. 여기서 I는 n차 단위행렬이다.

$$\Delta(x) = |T + xI| \tag{2.3}$$

<예 2.4.2> 위의 <예 2.4.1>에서 사용한 T 행렬에 대한 특성다항식을 구해보자.

$$\Delta(x) = |T + xI| = \begin{vmatrix} x+1 & 1 & 0 & 0 \\ 0 & x+1 & 1 & 0 \\ 0 & 0 & x+1 & 1 \\ 1 & 0 & 1 & x+1 \end{vmatrix}$$

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

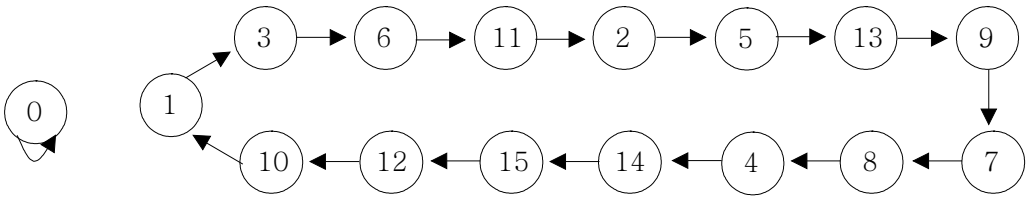
$$= x^4 + x^2 + 1$$

CA의 전이행렬 T가 $|T| = 1$이면 그 CA는 group CA이다. 즉 임의의 상태에 대하여 이전 상태를 알 수 있다. group CA는 최대길이를 갖는 CA와 최대길이를 갖지 않는 CA로 구별할 수 있다.

n개의 셀로 이루어진 CA에서 모든 셀의 상태가 0인 경우를 제외한 $2^n - 1$개의 상태가 하나의 사이클 안에 있을 때 최대 길이를 가진다고 한다.

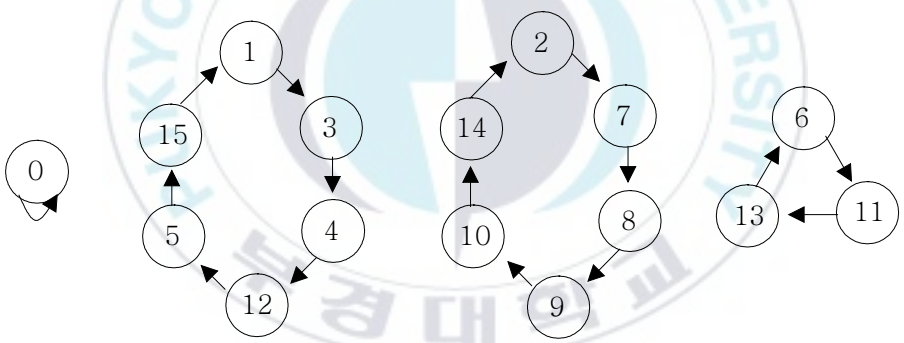
아래 그림은 rule <90, 150, 90, 150>인 4개의 cell로 구성된 최대길이를 가지는 NBCA이다.

<그림 2.3>은 최대길이를 갖는 group CA의 상태 전이 그래프이다.



<그림 2.3> 최대 길이를 갖는 Group CA

<그림 2.4>는 최대길이를 가지지 않는 선형 CA로써 rule <102, 102, 102, 150>을 갖는 PBCA의 상태 전이 그래프이다.

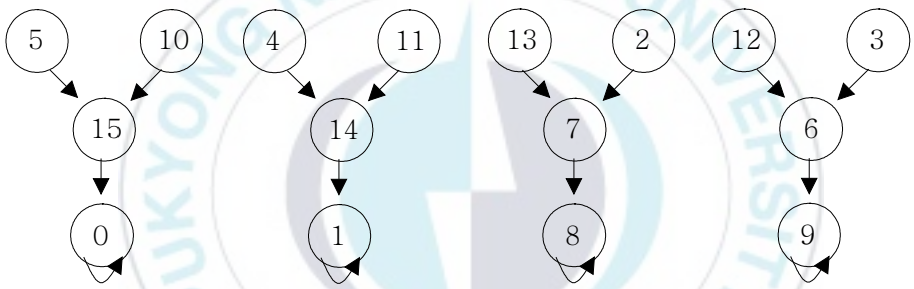


<그림 2.4> 최대 길이를 갖지 않는 Group CA

그림에서 알 수 있듯이 0을 제외한 다른 상태들이 몇 개의 서로 다른 사이클로 분리되어 있다. 이 사이클 길이의 최소공배수가 이 CA의 주기가 된다. 즉, rule이 <102, 102, 102, 150>인 PBCA는 0을 제외한 각 사이클의 길이가 3과 6이다. 따라서 이 CA의 주기는 6이 된다.

CA의 전이행렬 T가 $|T|=0$ 이면 그 CA는 nongroup CA이다. nongroup CA는 전이행렬에 대한 역행렬이 존재하지 않으므로 임의의 상태에 대하여 이전 상태를 명확하게 알 수 없다.

아래 그림은 rule <102, 102, 60, 60>을 갖는 NBCA의 상태 전이 그래프이다. 이 CA의 전이행렬 $T=\begin{bmatrix}1&1&0&0\\0&1&1&0\\0&1&1&0\\0&0&1&1\end{bmatrix}$의 행렬식 값 $|T|=0$이므로 nongroup CA이다. 아래 그림은 이 CA의 상태 전이 그래프이다.



<그림 2.5> Nongroup CA

2.5. 상태 전이 행동의 특성화와 CA의 그룹성질

$f_t(x)$ 가 i번째 시간에서의 셀의 상태를 나타낸다면 다음 순간에서의 상태는 상태 전이 방정식에 의해서 다음과 같이 나타내어질 수 있다.

$$f_{t+1}(x)=T\cdot f_t(x)$$

$$f_{t+2}(x) = T \cdot f_{t+1}(x)$$
$$= T^2 \cdot f_t(x)$$

같은 방법으로 m번째 후에는

$$f_{t+m}(x) = T^m \cdot f_t(x) \tag{2.4}$$

와 같이 나타낼 수 있다.

XNOR논리를 가지는 여원 CA(Complemented CA)를 편리하게 행렬로써 나타내는 방법을 알아보자.

rule 105는 rule 150의 additive complement이다. 그러나 XNOR함수는 곱셈의 표기법으로 나타낼 수 없으므로, 그것을 $\overline{T}$로 나타내기로 한다면 여원 CA 는 다음과 같이 나타낼 수 있다.

$$f_{t+1}(x) = \overline{T} \cdot f_t(x) = F(x) \oplus T \cdot f_t(x) \tag{2.5}$$

여기서 $F(x)$ 는 n차원 벡터이고(n은 셀의 개수), 그것의 원소는 XNOR논리가 XOR논리로 바뀌면 1, 그렇지 않으면 0으로 표시한다. 따라서 $F(x)$ 는 0이 아닌 원소를 반드시 가진다.

<예 2.5.1> Additive complemented rule 105 를 가지는 4-셀의 NBCA 의 상태전이행렬은 다음과 같이 쓸 수 있다.

$$\overline{T} \cdot f_t(x) = f_{t+1}(x) = \begin{bmatrix}1\\1\\1\\1\end{bmatrix} \oplus \begin{bmatrix}1100\\1110\\0111\\0011\end{bmatrix} \cdot f_t(x)$$

여기서 T는 rule 150 에 대응하는 상태전이행렬이다.

<예 2.5.2> Rule <204, 60, 153, 153>을 가지는 4-셀의 NBCA의 상태전이행렬은 다음과 같다.

$$\overline{T} \cdot f_t(x) = f_{t+1}(x) = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1000 \\ 1100 \\ 0011 \\ 0001 \end{bmatrix} \cdot f_t(x)$$

여기서 T는 rule <204, 60, 102, 102>에 대응하는 상태전이행렬이다.

상태 전이행렬 T를 가지는 CA가 cyclic group을 이룬다면

$$f_{t+m}(x) = T^m \cdot f_t(x) = f_t(x) \tag{2.6}$$

인 자연수 m이 존재한다.

그런 성질을 가지는 CA를 특별히 group CA라 한다.

$$T^m = I \tag{2.7}$$

(I : 단위행렬)

<정리 2.5.3> T가 CA의 전이행렬일 때, 이 CA가 group CA이기 위한 필요충분조건은 $|T|=1$ 이다.

(증명) ($\Rightarrow$) $T^m = I$ 인 m이 존재하고

$$1 = |I| = |T^m| = |T|^m$$

이므로, $|T| = 1$ 이다.

($\Leftarrow$) T의 멱승에 의해 생성된 commutative subgroup을 고려해 보자.

이 멱 그룹은 I를 가진 cyclic subgroup을 형성하고 또한 이 그룹은

가환이다. 이 그룹의 order는 $n \times n$ T에 대해서 $m \leq 2^n$ 이다. 왜냐하면

T는 어떤 n-bit벡터를 다른 n-bit 벡터로 변환시키는 변환 행렬이고 그러한 벡터는 기껏해야 2^n 개이기 때문이다. □

<보조정리 2.5.4> $\overline{T^p}$가 $\overline{T}$를 p번 적용한 것이라 한다면

$$\overline{T^p}(f(x)) = (I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1})F \oplus T^p \cdot f(x) \tag{2.8}$$

로 나타낼 수 있고 T는 여원이 아닌 CA에 대응되는 행렬이다.

(증명) 수학적 귀납법을 이용해서 증명하자.

1) p=1 일 때 (2.5)에 의해서

$\overline{T} \cdot f(x) = F(x) \oplus T \cdot f(x)$

2) $p = k$ 일 때

$\overline{T^k}(f(x)) = (I \oplus T \oplus T^2 \oplus \cdots \oplus T^{k-1})F \oplus T^k \cdot f(x)$ 라고 가정하자.

그러면, $p = k+1$ 일 때 다음이 성립한다.

$$\begin{aligned}
&\overline{T^{k+1}}(f(x)) \\
&= (I \oplus T \oplus T^2 \oplus \cdots \oplus T^k)F \oplus T^{k+1} \cdot f(x) \\
&= F(x) \oplus (T \oplus T^2 \oplus \cdots \oplus T^k)F \oplus T^k \cdot T \cdot f(x) \\
&= F(x) \oplus (I \oplus T \oplus T^2 \oplus \cdots \oplus T^{k-1})T \cdot F \oplus T^k \cdot T \cdot f(x) \\
&= F(x) \oplus T[(I \oplus T \oplus T^2 \oplus \cdots \oplus T^{k-1})F \oplus T^k \cdot f(x)]
\end{aligned}$$

□

<보조정리 2.5.5> R이 group CA의 rule이면 여원 $\overline{R}$도 또한 group CA의 rule이다.

(증명) Rule R 을 가진 CA가 T 에 의해 특성화된다면 여원인 rule $\overline{R}$를 가진 CA는 $\overline{T}$ 에 의해 특성화되고 <보조정리 2.5.4> 에 의해

$$\overline{T^k} \cdot f(x) = [I \oplus T \oplus T^2 \oplus \cdots \oplus T^{k-1}]F \oplus T^k \cdot f(x)$$

로 쓸 수 있다.

R이 group rule 이므로 $T^m = I$인 자연수 m이 존재한다.

$\overline{T}$도 group CA를 형성한다는 것을 보이기 위해서는

$$I \oplus T \oplus T^2 \oplus \cdots \oplus T^{r-1} = 0$$

이고, $T^r = I$ 인 자연수 r이 존재한다는 것을 보인다.

$r = 2m$ 이면,

1) $I \oplus T \oplus T^2 \oplus \cdots \oplus T^{m-1} \oplus T^m \oplus T^{m+1} \oplus \cdots \oplus T^{2m-1}$

$= [I \oplus T \oplus T^2 \oplus \cdots \oplus T^{m-1}] \oplus [I \oplus T \oplus T^2 \oplus \cdots \oplus T^{m-1}]T^m$

$= 0$

2) $T^m = I$ 이고, $T^{2m} = [T^m]^2 = I$ 이다. 따라서

$r = 2m$ 이면 $I \oplus T \oplus T^2 \oplus \cdots \oplus T^{r-1} = 0$ 이고, $T^r = I$ 이다. □

rule $\overline{R}$에 의해 생성된 order는 m이 rule R에 대응하는 그룹의 order일 때 $2m$을 넘지 못한다. 또한 그러한 그룹의 order는 $2m$ 또는 m이거나 그것의

약수이다.

<정의 2.5.6> Uniform group CA에 적용된 rule을 group rule 이라 한다.

<정의 2.5.7> R_1과 R_2가 두 개의 group rule 이라 하면 $\langle R_1, R_2\rangle$는 CA의 길이 위에서 공간적인 permutation을 가지는 CA를 나타낸다.

<보조정리 2.5.8> R이 group rule 이면 $\langle R, \overline{R}\rangle$은 group CA이다.

(증명) $\langle R, \overline{R}\rangle$가 길이 n위에서 R과 $\overline{R}$의 어떤 permutation으로써 n-셀의 hybrid CA라 하자. 어떤 특별한 permutation $T_1 = < R, \overline{R} >$ 는 일반적으로 다음과 같은 형태로 나타낼 수 있다.

$$T_1^r \cdot f(x) = [I \oplus T \oplus T^2 \oplus \cdots \oplus T^{r-1}] F \oplus T^r \cdot f(x)$$

여기서 T는 모든 셀에 uniform하게 적용되는 R에 대응하는 특성행렬이며 $F(x)$는 0아닌 원소를 반드시 가진다. R이 group rule이므로 $T^m = I$인 자연수 m이 존재하며 $I \oplus T \oplus T^2 \oplus \cdots \oplus T^{r-1} = 0$ 이고, $T^r = I$인 또 다른 자연수 r이 존재한다. □

<정리 2.5.9> Group CA가 0이 아닌 상태로 시작하면서 길이가 p또는 p의 인수인 cycle을 가지는 필요충분조건은 $|T^p \oplus I| = 0$ 이다.

(증명) ($\Rightarrow$)상태 $A(x)$에 대해서 길이가 p인 cycle이 존재한다면

$$T^p f(x) = f(x)$$
$$\Rightarrow (T^p \oplus I) f(x) = 0$$
$$\Rightarrow |T^p \oplus I| = 0$$

($\Leftarrow$) $|T^p \oplus I| = 0$ 이면 $(T^p \oplus I) f(x) = 0$ 인 영 아닌 상태 $f(x)$ 가 적어도 한 개 존재하므로 $T^p f(x) = f(x)$ 이다. □

<정리 2.5.10> T에 의해 특성화된 그룹CA의 order가 소수가 아니면 사이클의 길이는 그것의 인수들뿐이다.

(증명) 그룹CA의 order를 m이라 하고, p가 m을 나누지 않는 사이클 길이, 즉, $m = p \times q + r$ (q, r은 정수이고, $0 < r < p$) 라고 가정하자. 길이가 p 인 싸이클이 존재하므로 즉, $T^p = I$ 이므로 가장 작은 정수 p에 대해서 $T^p f(x) = f(x)$ 인 영 아닌 상태 $f(x)$ 가 있다. 그러면

$$\begin{aligned}
T^m f(x) &= T^{pq} \cdot T^r f(x) \\
&= T^r \cdot T^{(q-1)p}(T^p f(x)) \\
&= T^r \cdot T^{(q-1)p} f(x) \\
&= T^r \cdot T^{(q-2)p}(T^p f(x)) \\
&= T^r \cdot T^{(q-2)p} f(x) \\
&\quad \vdots \\
&= T^r \cdot T^p f(x) = T^r f(x)
\end{aligned}$$

다시 말해서, $T^m \cdot \Lambda(x) = T^r \cdot \Lambda(x)$ 이다.

가정에서 p는 가장 작은 정수이고 $r < p$이므로, 그러한 r은 존재할 수 없다. 따라서 p는 m의 약수이어야 한다. □

3. LUGCA로부터 유도되는 여원 CA의 분석

이번 장에서는 전이규칙 60 또는 102를 갖는 LUGCA로부터 유도되는 여원 CA를 분석한다.

<보조정리 3.1> C를 전이규칙 60 또는 102를 갖는 n-셀 LUGCA라 하면, C의 상태전이행렬 T의 최소다항식 $m(x) = (x+1)^n$ 이다.

$(T \oplus I)^n = O$ **(증명)** C를 전이규칙 60을 갖는 n-셀 LUGCA라 하면 이고 $(T \oplus I)^{n-1} = (a_{ij})$이다. 여기서 $a_{ij} = \begin{cases} 1, & i = n, \quad j = 1, \\ 0, & o/w \end{cases}$ 이다. 따라서 $m(x) = (x+1)^n$이다. 전이규칙 102를 갖는 n-셀 LUGCA에 대한 증명도 전이규칙 60의 경우와 유사하다.

<보조정리 3.2> C를 전이규칙 60 또는 102를 갖는 n-셀 LUGCA라 하고 T를 C의 상태전이행렬이라 하자. 그러면 T의 주기 $\mathrm{ord}(T)$는 $2^a (a = 0,1,2,\cdots)$이다. 여기서 $2^{a-1} < n \leq 2^a$ 이다.

<보조정리 3.3> C를 전이규칙 60 또는 102를 갖는 n-셀 LUGCA라 하고

T를 C의 상태전이행렬이라 할 때 여원벡터 F가 $F=(1,\cdots,1)^t$이면 $(T\oplus I)^a F\neq O$이다. 여기서 $0\leq a\leq n-1$이다.

(증명) $(T\oplus I)^{n-1}F\neq O$ 임을 보이면 된다. C를 전이규칙 60을 갖는 n-셀 LUGCA라 하면 보조정리 3.1의 증명에 의하여 $(T\oplus I)^{n-1}=(a_{ij})$이다. 여기서 $a_{ij}=\begin{cases}1, & i=n,\ j=1,\\ 0, & o/w\end{cases}$ 이다. 따라서 $(T\oplus I)^{n-1}F=(0,\cdots,0,1)^t$ 이므로 $(T\oplus I)^{n-1}F\neq O$ 이다. 전이규칙 102를 갖는 n-셀 LUGCA에 대한 증명도 전이규칙 60의 경우와 유사하다. □

<보조정리 3.4> C를 상태전이행렬 T를 갖는 선형 그룹 CA라고 하자. 여원벡터가 $F\neq O$이고 $\mathrm{ord}(T)=m$이면 $\mathrm{ord}(\overline{T})=m$ 또는 $\mathrm{ord}(\overline{T})=2m$이다.

(증명) $\mathrm{ord}(T)=m$ 이므로, $T^m=I$이다. 그러므로

$$\begin{aligned}\overline{T}^{2m}X &= T^{2m}X\oplus\left(T^{2m-1}\oplus\cdots\oplus T^m\oplus T^{m-1}\oplus\cdots\oplus T\oplus I\right)F\\ &= T^{2m}X\oplus\left\{T^m\left(T^{m-1}\oplus\cdots\oplus T\oplus I\right)\oplus\left(T^{m-1}\oplus\cdots\oplus T\oplus I\right)\right\}F\\ &= T^{2m}X\oplus\left\{\left(T^{m-1}\oplus\cdots\oplus T\oplus I\right)\oplus\left(T^{m-1}\oplus\cdots\oplus T\oplus I\right)\right\}F\\ &= X\oplus O=X \text{ 이다. 즉, } \mathrm{ord}(\overline{T})\text{는 } 2m \text{ 의 약수이다.}\end{aligned}$$

$\mathrm{ord}(\overline{T})=p$라 두면, 모든 상태 X에 대하여

$X=\overline{T}^pX=T^pX\oplus\left(T^{p-1}\oplus\cdots\oplus T\oplus I\right)F$이다.

그러므로 모든 상태 X에 대하여 $T^pX=X$이고, $\left(T^{p-1}\oplus\cdots\oplus T\oplus I\right)F=O$ 이다. $\mathrm{ord}(T)=m$이고 $T^pX=X$이므로 $p=m$ 또는 $p=2m$이다. □

다음 정리는 정리 4([7])의 확장이다.

<정리 3.5> C를 전이규칙 60(또는 102)를 n-셀 LUGCA라 하고 T를 C의 상태전이행렬이라 하자. C'을 C로부터 유도된 전이규칙 195(또는 153)을 갖는 n-셀 uniform group CA(이하 UGCA)라 하고 $\mathrm{ord}(T)=m$이라 하자. 그러면 다음이 성립한다.

$$\mathrm{ord}(\overline{T})=\begin{cases}2m, & n=2^a(a\in N),\\ m, & o/w.\end{cases}$$

$(T\oplus I)^{m-1}=T^{m-1}\oplus T^{m-2}\oplus\cdots\oplus I\neq 0$

(증명) i) $n=2^a$인 경우 : <보조정리 3.2>에 의하여 $\mathrm{ord}(T)=n=2^a=m$ 이다. $m(x)=(1+x)^m$ 이므로 $(T\oplus I)^m=(T\oplus I)^{2^n}=T^{2^a}\oplus I=O$이고 $(T\oplus I)^{m-1}=T^{m-1}\oplus T^{m-2}\oplus\cdots\oplus I\neq 0$이다. 그러므로 <보조정리 3.3>에 의해서 다음과 같다.

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

따라서, <보조정리 3.4>에 의하여 $\mathrm{ord}(\overline{T})=2m$ 이다.

ii) $2^{k-1}<n<2^k$ 인 경우 : <보조정리 3.2>에 의해서, $\mathrm{ord}(T)=2^k=m$ 이므로 $n<m$이다. 따라서 $(1+x)^n$는 $(1+x)^m$를 나눈다. 보조정리 3.1에 의해서 $m(x)=(1+x)^n$이므로

$(I\oplus T)^n=(I\oplus T)^{n+1}=\cdots=(I\oplus T)^m=O$ 이다. 그러므로

$(I\oplus T)^{m-1}=T^{m-1}\oplus T^{m-2}\oplus\cdots\oplus I=O$이고, 따라서 다음이 성립한다.

$\overline{T}^m X=T^m X\oplus(T^{m-1}\oplus\cdots\oplus I)F$ 그러므로 $\mathrm{ord}(\overline{T})=m$ 이다

$=X\oplus(T^{m-1}\oplus\cdots\oplus I)F=X$

□

[참고] <정리 3.5>는 전이규칙 60 또는 102를 갖는 LUGCA에 대하여 Das의 예측(conjecture)[3]이 참임을 보여준다.

<보조정리 3.2>와 <정리 3.5>로부터 다음 정리를 얻는다.

<정리 3.6> C를 전이규칙 60(또는 102)를 갖는 n-셀 LUGCA라 하고, T를 C의 상태전이행렬이라 하자. C'을 C로부터 유도된 전이규칙 195(또는 153)을 갖는 n-셀 UGCA라 하자. 그러면 C'의 상태전이그래프는 길이가 같은 사이클들로 구성된다.

(증명) i) $n=2^a$ 인 경우 : 보조정리 3.2와 정리 3.5에 의하여 $\mathrm{ord}(T) = 2^a$ 이고 $\mathrm{ord}(\overline{T}) = 2^{a+1}$ 이다. X를 C'에서 길이가 $l = 2^p (p \le a)$ 인 사이클에 놓인 상태라 하자. 그러면 $\overline{T}^{2^p} X = \overline{T}^{2^{p+1}} X = \cdots = \overline{T}^{2^a} X = \overline{T}^{2^{a+1}} X = X$이다. 보조정리 3.3에 의해서 $[T^{2^a-1} \oplus T^{2^a-2} \oplus \cdots \oplus T \oplus I] F \neq O$ 이므로, 모든 상태 X에 대하여 $\overline{T}^{2^a} X = T^{2^a} X \oplus (T^{2^a-1} \oplus T^{2^a-2} \oplus \cdots \oplus T \oplus I) F \neq X$ 이다. 이것은 모순이다. 따라서 C'의 모든 사이클의 길이는 모두 2^{a+1} 이다.

ii) $2^{a-1} < n < 2^a$ 인 경우 : 보조정리 3.2와 정리 3.5에 의해서 $\mathrm{ord}(T) = 2^a$ 이고, $\mathrm{ord}(\overline{T}) = 2^a (2^{a-1} < n < 2^a)$이다. 보조정리 3.1에 의해서 $m(x) = (1+x)^n$이므로 $(I \oplus T)^n = (I \oplus T)^{n+1} = \cdots = (I \oplus T)^{2^a} = O$이다. X가 C'에서 주기 2^p $(p < a)$인 사이클에 놓인 상태라 하면 $\overline{T}^{2^p} X = \overline{T}^{2^{p+1}} X = \cdots = \overline{T}^{2^{a-1}} X = T^{2^a} X = X$이다.

① X가 C에서 주기가 2^a보다 작은 사이클에 놓인 경우:

보조정리 3.3에 의하여

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

$$= X \oplus (T \oplus I)^{2^{a-1}-1} F \neq X$$

이므로 모순이다.

② X가 C'에서 주기가 2^a인 사이클에 놓인 경우:

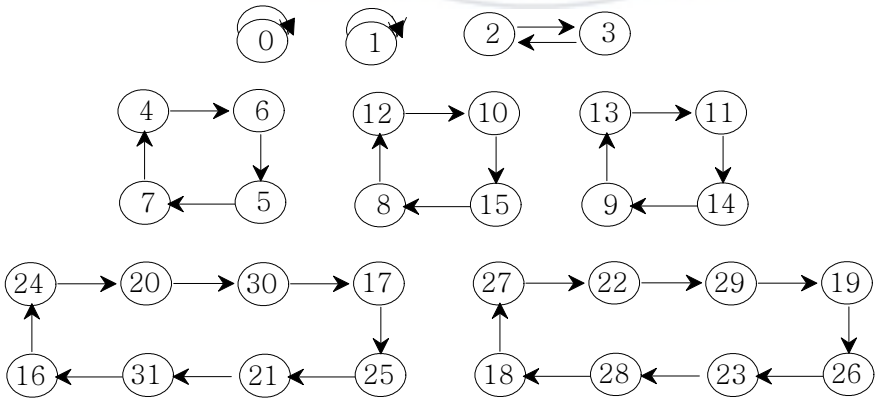
$X = (x_1, \cdots, x_n)^t$ 라 두면

$$\overline{T}^{2^{a-1}}X = T^{2^{a-1}}X \oplus (T \oplus I)^{2^{a-1}}F$$

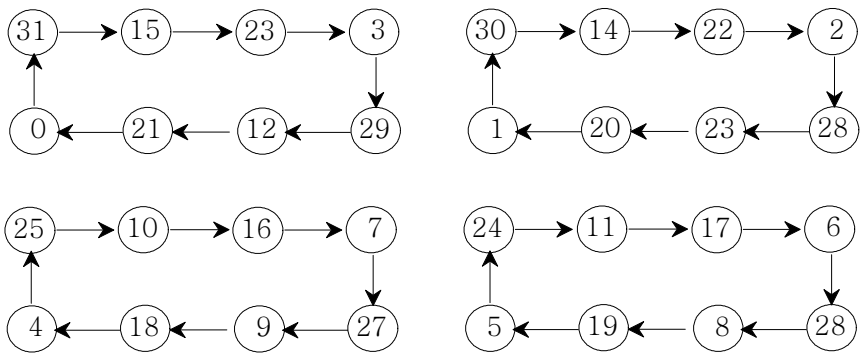
$$= \begin{pmatrix} x_1 \\ \vdots \\ 1 \oplus x_{2^{a-1}} \\ 1 \oplus x_1 \oplus x_{2^{a-1}+1} \\ \vdots \end{pmatrix} \neq \begin{pmatrix} x_1 \\ \vdots \\ x_{2^{a-1}} \\ 1 \oplus x_1 \oplus x_{2^{a-1}+1} \\ \vdots \end{pmatrix} = X$$

이므로 모순이 된다. 따라서 ①과 ②에 의하여 C'의 모든 사이클의 길이는 모두 2^a이다. 전이규칙 153에 대한 경우도 전이규칙 195에 대한 증명과 유사하다. □

<예제 3.7> C를 전이규칙 60을 갖는 5-셀 LUGCA라 하고, 여원벡터 $F=(1,1,1,1,1)^t$에 의해 C로부터 유도된 여원 CA를 C'이라 하면 C와 C'의 상태전이그래프는 그림 1과 그림 2와 같다.



<그림3-1> 전이규칙 60을 갖는 5-셀 LUGCA C



<그림 3-2> C에서 F에 의해 유도된 C'

다음 보조정리는 쉽게 증명할 수 있다.

<보조정리 3.8> C를 전이규칙 60(또는 102)를 갖는 n-셀 LUGCA라 하고, T(또는 S)를 C의 상태전이행렬이라 하자($2^{k-1} < n \le 2^k$). 그러면 $T^{2^k} = S^{2^k} = I$ 이고 $T^{2^{k-1}} = (t_{ij})$ 과 $S^{2^{k-1}} = (s_{ij})$ 은 다음과 같다.

$$t_{ij} = \begin{cases} 1, & i = j \quad \text{또는} \quad i = j + 2^{k-1}, \\ 0, & o/w \end{cases}$$

$$s_{ij} = \begin{cases} 1, & j = i \quad \text{또는} \quad j = i + 2^{k-1}, \\ 0, & o/w \end{cases}$$

<정리 3.9> C를 전이규칙 60(또는 102)를 갖는 n-셀 LUGCA라 하고, T(또는 S)를 C의 상태전이행렬이라 하자($2^{k-1} < n \le 2^k$). $X = (1, a_2, \cdots, a_n)^t$ (또는 $X = (a_1, a_2, \cdots, a_{n-1}, 1)^t$)라 두면 X는 C에서 길이가 가장 긴 사이클에 놓인다.

(증명) 보조정리 3.2에 의하여, $\mathrm{ord}(T) = 2^k$ 이므로 $T^{2^k}X = X$이다. 보조정리 3.8에 의하여,

$$T^{2^{k-1}}X=\begin{pmatrix}1\,0\,0\cdots 0\,0\,0\,0\\ 0\,1\,0\cdots 0\,0\,0\,0\\ 0\,0\,1\cdots 0\,0\,0\,0\\ \quad\ddots\\ 1\,0\,0\cdots 1\,0\cdots 0\\ \quad\vdots\\ 0\,1\,0\cdots 0\,0\,0\,1\end{pmatrix}\begin{pmatrix}1\\ a_2\\ a_3\\ \vdots\\ a_{2^{k-1}}\\ \underline{a_{2^{k-1}+1}}\\ \vdots\\ a_n\end{pmatrix}=\begin{pmatrix}1\\ a_2\\ a_3\\ \vdots\\ a_{2^{k-1}}\\ \underline{1\oplus a_{2^{k-1}+1}}\\ \vdots\\ a_n\end{pmatrix}$$ 이므로 $T^{2^{k-1}}X\neq X$ 이다.

그러므로 X는 C에서 길이가 가장 긴 사이클에 놓인다. 전이규칙 102인 경우의 증명도 전이규칙 60의 경우와 유사하다. □

다음 보조정리는 쉽게 증명할 수 있다.

<보조정리 3.10> C를 전이규칙 60 또는 102를 갖는 n-셀 LUGCA라 하고, T를 C의 상태전이행렬이라 하면 C의 임의의 상태 $X=(x_1,\cdots,x_n)^t$ 에 대하여 다음이 성립한다.

$$(T\oplus I)^{m-1}X=\begin{cases}(0,\ 0,\ \cdots\ \overset{m}{\ },\ x_1,\ x_2,\cdots,x_{n-m+1})^t,\\ \text{if } R=<60,60,\cdots>,\\ (x_m,\cdots,x_{n-1},x_n,\ 0,\cdots,0)^t,\\ \text{if } R=<102,102,\cdots>.\end{cases}$$

다음 정리는 n이 2의 거듭제곱일 때 전이규칙 60 또는 102를 갖는 n-셀 LUGCA로부터 유도된 여원 CA의 주기가 $2\cdot \mathrm{ord}(T)$ 또는 $\mathrm{ord}(T)$가 되는 조건을 알려준다. 여기서 T는 LUGCA의 상태전이행렬이다.

<정리 3.11> C를 전이규칙 60 또는 102를 갖는 n-셀 LUGCA라 하자. 여기서 $n=2^k$이라 하고 T를 C의 상태전이행렬이라 하자. C'을 C에서 여원벡터 $F(\neq O)$에 의해 유도된 여원 CA라 하면 다음이 성립한다.

$$\mathrm{ord}(\overline{T}) = \begin{cases} 2\,\mathrm{ord}(T), & \text{if } F=(1,a_2,\cdots,a_n)^t \\ & (\text{또는 } F=(a_1,a_2,\cdots,a_{n-1},1)^t) \\ \mathrm{ord}(T), & o/w \end{cases}$$

(증명) C'의 임의의 상태 X에 대하여 보조정리 3.2를 이용하면

$\overline{T}^{2^{k+1}} X$

$= T^{2^{k+1}} X \oplus (T^{2^{k+1}-1} \oplus \cdots \oplus T \oplus I)\ F$

$= X \oplus \mathrm{T}^{2^k}(\mathrm{T}^{2^k-1} \oplus \cdots \oplus \mathrm{T} \oplus \mathrm{I})$

이다. 따라서 $\mathrm{ord}(\overline{T})$는 2^{k+1}를 나눈다. $\mathrm{ord}(\overline{T}) = p$라 두면

$X = \overline{T}^p X = T^p X \oplus (T^{p-1} \oplus \cdots \oplus T \oplus I) F$ 이므로 $T^p X = X$이 되고, $(T^{p-1} \oplus \cdots \oplus T \oplus I)\ F = 0$ 이 된다. 따라서 $\mathrm{ord}(T) = 2^k$는 p를 나눈다. 그러므로 $p = 2^k$ 이거나 2^{k+1} 이다.

i) $F = (1, a_2, \cdots, a_n)^t$ 이라 두면 보조정리 3.10에 의하여

$\overline{T}^{2^k} X = T^{2^k} X \oplus (T \oplus I)^{2^k-1} F$

$= X \oplus (0,0,\cdots,1)^t \neq X$

이므로 $p = 2^{k+1}$이다.

ii) $F = (0, a_2, \cdots, a_n)^t$ 라 두면 보조정리 3.10에 의하여

$\overline{T}^{2^k} X = T^{2^k} X \oplus (T \oplus I)^{2^k-1} F$ 이므로

$= X \oplus (0,\cdots,0)^t = X$

$p = \mathrm{ord}(\overline{T}) = 2^k$ 이다 □

$X = \overline{T^p} X = T^p X \oplus (T^{p-1} \oplus \cdots \oplus T \oplus I) F$

<정리 3.12> C를 전이규칙 60 또는 102를 갖는 n-셀 LUGCA라 하고 T를 C의 상태전이행렬이라 하자($2^{k-1} < n \leq 2^k$). C'을 C에서 여원벡터 $F(\neq O)$에

의해 유도된 여원 CA라 하면 다음 각 경우에 대하여 C'에서 모든 사이클의 길이는 같다.

i) $R=<60,60,\cdots>,\ F=(1,\ a_2,\ \cdots,\ a_n)^t$

ii) $R=<102,102,\cdots>,\ F=(b_1,\ \cdots,\ b_{n-1},\ 1)^t$

여기서, $a_2,\cdots,a_n,b_1,\cdots,b_{n-1}\in\{0,\ 1\}$ 이다.

(증명) ① 먼저 $n=2^k$인 경우를 증명한다.

i) $\mathrm{ord}(\overline{T})=2^{k+1}$이므로 C'의 임의의 상태 X에 대하여 $\overline{T}^{2^{k+1}}X=X$이다. 또한 보조정리 3.10에 의하여 $\overline{T}^{2^k}X=T^{2^k}X\oplus(T\oplus I)^{2^k-1}F\neq X$이므로 X는 길이가 2^{k+1}인 사이클 위에 놓인다. 그러므로 C'에서 모든 사이클의 길이는 같다.

ii) i)의 증명과 같은 방법으로 증명할 수 있다.

② 다음에 $2^{k-1}<n<2^k$인 경우를 증명한다.

i) $\mathrm{ord}(\overline{T})=2^k$이므로 C'의 임의의 상태 X에 대하여 정리 3.5에 의하여 $\overline{T}^{2^k}X=X$이다. X가 C에서 길이가 $\mathrm{ord}(T)=2^k$ 미만인 사이클에 놓인다면, 보조정리 3.10에 의하여

$$\overline{T}^{2^{k-1}}X=T^{2^{k-1}}X\oplus(T\oplus I)^{2^{k-1}-1}F$$

$$=X\oplus(T\oplus I)^{2^{k-1}-1}F\neq X$$

이다. 만약 X가 C에서 길이가 가장 긴 사이클에 놓인다면,

$$\overline{T}^{2^{k-1}}X=T^{2^{k-1}}X\oplus(T\oplus I)^{2^{k-1}-1}F$$

$$=(x_1,\ x_2,\ \cdots,\ x_{2^{k-1}},\ x_{2^{k-1}+1}+x_1,\cdots)^t$$

$$\oplus\ (0,0,\cdots,\ \underbrace{0,\quad 1}_{2^{k-1}},\quad a_2,\ \cdots\ )^t$$

$$=(x_1,x_2,\cdots,\overline{x_{2^{k-1}}},\underline{a_2\oplus x_1\oplus x_{2^{k-1}+1}},\cdots)^t\neq X$$

이다. 따라서 $T^{2^{k-1}}X \neq X$이고, X는 C'에서 길이가 가장 긴 사이클에 놓인다.

ii) i)의 증명과 같은 방법으로 증명할 수 있다. □

4. 여원 그룹 CA의 사이클 관계의 특성

Mukhopadhyay 등([7])은 두 함수 R_1과 R_2를 구성하여 기본 변환의 상태 공간의 관계를 보였다. 이 장에서는 R_1과 R_2로부터 서로 다른 여러 개의 함수를 구성하고 이 함수들의 특성을 분석한다.

<정리 4.1> C를 전이규칙 60 (또는 102)를 갖는 n-셀 LUGCA라 하고 T를 C의 상태전이행렬이라 하자. C'을 C에 대응하는 전이규칙 195(또는 153)을 갖는 UGCA라 하면 C'의 임의의 상태 $X=(x_1, x_2, \cdots, x_n)^t$에 대하여 다음이 성립한다.$A = X \oplus \overline{T}^2 X \oplus \overline{T}^3 X$

(1) X와 $X \oplus \overline{T^2} X \oplus \overline{T^3} X$은 다른 사이클에 놓인다.

(2) X와 $X \oplus \overline{T^4} X \oplus \overline{T^5} X$은 다른 사이클에 놓인다.

(3) X와 $X \oplus \overline{T} X \oplus \overline{T^5} X$은 다른 사이클에 놓인다.

(증명) 전이규칙 102인 경우에 대하여 (1)만 증명하도록 한다.

$A = X \oplus \overline{T}^2 X \oplus \overline{T}^3 X$ 라 두면 $A = (T^3 \oplus T^2 \oplus I)X \oplus T^2 F = \begin{pmatrix} \vdots \\ x_{n-2} \oplus x_{n-1} \\ \overline{x_{n-1} \oplus x_n} \\ \overline{x_n} \end{pmatrix}$이고,

음이 아닌 정수 a에 대하여 $\overline{T}^a X = \begin{pmatrix} x_{n-2} \oplus C_1 x_{n-1} \oplus {}_aC_2 x_n \oplus a \oplus {}_aC_2 \oplus {}_aC_3 \\ x_{n-1} \oplus {}_aC_1 x_n \oplus a \oplus {}_aC_2 \\ x_n \oplus a \end{pmatrix}$이다.

$\overline{T}^a X = A$ 인 정수 a가 존재한다고 가정하자.

1. a가 짝수인 경우, $A = \begin{pmatrix} \vdots \\ \overline{x_n} \end{pmatrix}$이고 $\overline{T}^a X = \begin{pmatrix} \vdots \\ x_n \end{pmatrix}$이므로 $\overline{T}^a X \neq A$ 이다.

2. a가 홀수인 경우,

$a = 4n+1$ 이라면 $A = \begin{pmatrix} \vdots \\ \overline{x_{n-2} \oplus x_{n-1}} \\ \overline{x_{n-1} \oplus x_n} \\ \overline{x_n} \end{pmatrix}$이고 $\overline{T}^a X = \begin{pmatrix} \vdots \\ \overline{x_{n-2} \oplus x_{n-1}} \\ \overline{x_{n-1} \oplus x_n} \\ \overline{x_n} \end{pmatrix}$ 이므로 $\overline{T}^a X \neq A$

이다.

$a = 4n+3$이라면, $A = \begin{pmatrix} \vdots \\ \overline{x_{n-1} \oplus x_n} \\ \overline{x_n} \end{pmatrix}$이고 $T^a X = \begin{pmatrix} \vdots \\ x_{n-1} \oplus x_n \\ \overline{x_n} \end{pmatrix}$이므로 $\overline{T}^a X \neq A$ 이

다. 따라서 X 와 $X \oplus \overline{T^2} X \oplus \overline{T^3} X$는 다른 사이클에 놓인다. □

[함수의 구성]

함수 R_i를 다음과 같이 정의한다.

$$R_1(X) = X \oplus \overline{T} X \oplus \overline{T^2} X.$$

$$R_2(X) = X \oplus \overline{T} X \oplus \overline{T^3} X.$$

$$R_2(X) = X \oplus \overline{T^2} X \oplus \overline{T^3} X.$$

다음 보조정리는 수학적 귀납법으로 증명할 수 있다.

보조정리 4.2 C를 전이규칙 60 (또는 102)를 갖는 n-셀 LUGCA라 하고 T를 C의 상태전이행렬이라 하자. C'을 C에 대응하는 전이규칙 195(또는 153)을

갖는 UGCA라 하면 C'의 각 상태와 음이 아닌 정수 a에 대하여 다음이 성립한다.

(1) $R_1^{2^a}(X) = X \oplus \overline{T^{2^a}} X \oplus \overline{T^{2^{a+1}}} X.$

(2) $R_2^{2^a}(X) = X \oplus \overline{T^{2^a}} X \oplus \overline{T^{3 \cdot 2^a}} X.$

(3) $R_3^{2^a}(X) = X \oplus \overline{T^{2^{a+1}}} X \oplus \overline{T^{3 \cdot 2^a}} X.$

<정리 4.3> C를 전이규칙 60 (또는 102)를 갖는 n-셀 LUGCA라 하고 T를 C의 상태전이행렬이라 하자. C'을 C에 대응하는 전이규칙 195(또는 153)을 갖는 UGCA라 하면 음이 아닌 정수 a에 대하여 다음이 성립한다.

각 정수 $i(1 \le i \le 3)$에 대하여

$$\overline{T^{i \cdot 2^a}} R_i^{2^a}(X) = \left\{ (T \oplus I)^{3 \cdot 2^a} (T^i \oplus T \oplus I)^{2^a} \oplus I \right\} X \oplus$$

$$(T \oplus I)^{3 \cdot 2^a - 1} (T^i \oplus T \oplus I)^{2^a} F$$

(증명) $i = 1$인 경우: a에 대한 수학적 귀납법으로 증명하자. 일$a = 0$ 때

$$\begin{aligned} \overline{T} R_1(X) &= \overline{T}(X \oplus \overline{T} X \oplus \overline{T}^2 X) \\ &= \overline{T} X \oplus \overline{T}^2 X \oplus \overline{T}^3 X \\ &= (T^3 \oplus T^2 \oplus T) X \oplus (T^2 \oplus I) F \\ &= (T \oplus I)^3 \oplus I X (T \oplus I)^2 F \end{aligned}$$

이다. 그러므로 $a = 0$일 때 성립한다. $a = k$ 일 때 성립한다고 가정하자. 보조정리 4.3에 의하여

$\overline{T}^{2^{k+1}} R_1^{2^{k+1}}(X)$

$= \overline{T}^{2^k} R_1^{2^k}(\overline{T}^{2^k} R_1^{2^k}(X))$

$= \overline{T}^{2^k} R_1^{2^k}(\{(T\oplus I)^{3\cdot 2^k}\oplus I\}X\oplus (T\oplus I)^{3\cdot 2^k-1}F)$

$= \{(T\oplus I)^{3\cdot 2^k}\oplus I\}(\{(T\oplus I)^{3\cdot 2^k}\oplus I\}X$
$\oplus (T\oplus I)^{3\cdot 2^k-1}F)\oplus (T\oplus I)^{3\cdot 2^k-1}F$
$= (T\oplus I)^{3\cdot 2^k}(T\oplus I)^{3\cdot 2^k}X\oplus X\oplus (T\oplus I)^{3\cdot 2^k}$
$\oplus (T\oplus I)^{3\cdot 2^k-1}F$
$= \{(T\oplus I)^{3\cdot 2^{k+1}}\oplus I\}X\oplus (T\oplus I)^{3\cdot 2^{k+1}-1}F$

이므로 $a=k+1$일 때 성립한다.

$i=2$인 경우: a에 대한 수학적 귀납법으로 증명하자. $a=0$일 때

$$\begin{aligned}\overline{T}^2 R_2(X) &= \overline{T}^2(X\oplus \overline{T}X\oplus \overline{T}^3X)\\ &= \overline{T}^2X\oplus \overline{T}^3X\oplus \overline{T}^5X\\ &= (T^5\oplus T^3\oplus T^2)X\\ &\oplus (T^4\oplus T^3\oplus T\oplus I)F\end{aligned}$$

이다.

$T^5\oplus T^3\oplus T^2 = T^3(T^2\oplus I)\oplus (T^2\oplus I)\oplus I$
$= (T\oplus I)^2(T^3\oplus I)\oplus I$
$= (T\oplus I)^3(T^2\oplus T\oplus I)\oplus I$

이고

$T^4\oplus T^3\oplus T\oplus I = T^3(T\oplus I)\oplus (T\oplus I)$
$= (T^3\oplus I)(T\oplus I)$
$= (T\oplus I)^2(T^2\oplus T\oplus I)$

이므로

$\overline{T}^2 R_2(X) = \{(T\oplus I)^3(T^2\oplus T\oplus I)\oplus I\}X$

$\oplus (T\oplus I)^2(T^2\oplus T\oplus I)F$

이다. 그러므로 $a=0$일 때 성립한다. $a=k$일 때 성립한다고 가정하자. 보조정리

4.3에 의하여

$$\overline{T}^{2^{k+2}} R_2^{2^{k+1}}(X)$$
$$= \overline{T}^{2^{k+1}} R_2^{2^k}(\overline{T}^{2^{k+1}} R_2^{2^k}(X))$$
$$= \overline{T}^{2^{k+1}} R_2^{2^k}(\{(T\oplus I)^{3\cdot 2^k}(T^2\oplus T\oplus I)^{2^k}\oplus I\}X$$
$$\oplus (T\oplus I)^{3\cdot 2^k-1}(T^2\oplus T\oplus I)^{2^k}F)$$

$$= \{(T\oplus I)^{3\cdot 2^k}(T^2\oplus T\oplus I)^{2^k}\oplus I\}$$
$$(\{(T\oplus I)^{3\cdot 2^k}(T^2\oplus T\oplus I)^{2^k}\oplus I\}X$$
$$\oplus (T\oplus I)^{3\cdot 2^k-1}(T^2\oplus T\oplus I)^{2^k}F)$$
$$\oplus (T\oplus I)^{3\cdot 2^k-1}(T^2\oplus T\oplus I)^{2^k}F$$
$$= (T\oplus I)^{3\cdot 2^k}(T^2\oplus T\oplus I)^{2^k}(T\oplus I)^{3\cdot 2^k}(T^2\oplus T\oplus I)^{2^k}X$$
$$\oplus X\oplus \{(T\oplus I)^{3\cdot 2^k}\oplus (T^2\oplus T\oplus I)^{2^k}\}$$
$$\{(T\oplus I)^{3\cdot 2^k-1}(T^2\oplus T\oplus I)^{2^k}\}F$$
$$= \{(T\oplus I)^{3\cdot 2^{k+1}}(T^2\oplus T\oplus I)^{2^{k+1}}\oplus I\}X$$
$$\oplus (T\oplus I)^{3\cdot 2^{k+1}-1}(T^2\oplus T\oplus I)^{2^{k+1}}F$$

이므로 $a=k+1$일 때 성립한다.

$i=3$인 경우: a에 대한 수학적 귀납법으로 증명하자. $a=0$일 때

$$\overline{T}^3 R_3(X) = \overline{T}^3(X\oplus \overline{T}^2X\oplus \overline{T}^3X)$$
$$= \overline{T}^3X\oplus \overline{T}^5X\oplus \overline{T}^6X$$
$$= (T^6\oplus T^5\oplus T^3)X$$
$$\oplus (T^5\oplus T^2\oplus T\oplus I)F$$

아다.

$$T^5\oplus T^2\oplus T = T^2(T^3\oplus I)\oplus (T\oplus I)\oplus I$$
$$= (T\oplus I)\{T^2(T^2\oplus T\oplus I)\oplus I\}\oplus I$$
$$= (T\oplus I)(T^4\oplus T^3\oplus T^2\oplus I)\oplus I$$
$$= (T\oplus I)\{T^3(T\oplus I)\oplus (T\oplus I)^2\}\oplus I$$
$$= (T\oplus I)^2(T^3\oplus T\oplus I)\oplus I$$

이고

$T^6 \oplus T^5 \oplus T^3$

$= T^5(T \oplus I) \oplus (T \oplus I)(T^2 \oplus T \oplus I) \oplus I$

$= (T \oplus I)(T^5 \oplus T^2 \oplus T \oplus I) \oplus I$

$= (T \oplus I)(T \oplus I)^2(T^3 \oplus T \oplus I) \oplus I$

$= (T \oplus I)^3(T^3 \oplus T \oplus I) \oplus I$

이므로

$$\overline{T}^3 R_3(X) = \{(T \oplus I)^3(T^3 \oplus T \oplus I) \oplus I\} X$$

$$\oplus (T \oplus I)^2(T^3 \oplus T \oplus I) F$$

이다. 그러므로 $a = 0$일 때 성립한다. $a = k$일 때 성립한다고 가정하자. 보조정리 4.3에 의하여

$\overline{T}^{3 \cdot 2^{k+1}} R_3^{2^{k+1}}(X)$

$= \overline{T}^{3 \cdot 2^k} R_3^{2^k}(\overline{T}^{3 \cdot 2^k} R_3^{2^k}(X))$

$= \overline{T}^{3 \cdot 2^k} R_3^{2^k}(\{(T \oplus I)^{3 \cdot 2^k}(T^3 \oplus T \oplus I)^{2^k} \oplus I\} X$

$\oplus (T \oplus I)^{3 \cdot 2^k - 1}(T^3 \oplus T \oplus I)^{2^k} F)$

$= \{(T \oplus I)^{3 \cdot 2^k}(T^3 \oplus T \oplus I)^{2^k} \oplus I\}$

$[\{(T \oplus I)^{3 \cdot 2^k}(T^3 \oplus T \oplus I)^{2^k} \oplus I\} X$ 이므로 $a = k+1$일 때 성립한다.

$\oplus (T \oplus I)^{3 \cdot 2^k - 1}(T^3 \oplus T \oplus I)^{2^k} F]$

$\oplus (T \oplus I)^{3 \cdot 2^k - 1}(T^3 \oplus T \oplus I)^{2^k} F$

$= \{(T \oplus I)^{3 \cdot 2^{k+1}}(T^3 \oplus T \oplus I)^{2^{k=1}} \oplus I\} X$

$\oplus (T \oplus I)^{3 \cdot 2^{k+1} - 1}(T^3 \oplus T \oplus I)^{2^{k=1}} F$

□

5. 결 론

본 논문에서는 전이규칙 60 또는 102를 갖는 LUGCA로부터 유도되는 여원 CA의 상태전이 연산자의 주기와 사이클 구조를 연구하였으며, Das의 추측이 참임을 증명하였다. 또한 여원 CA의 상태전이 연산자로부터 생성되는 순환부분공간에서 다른 순환부분공간으로 이동하는데 사용되는 유용한 함수를 분석하였다. 이 분석은 새로운 암호와 키 분배 프로토콜을 발전시키는데 도움이 될 것이다.

참 고 문 헌

[1] J. Von Neumann, The theory of self-reproducing automata, A.W. Burks ed. (Univ. of Illinois Press, Urbana and London), 1996.

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

[3] A.K. Das, Additive cellular automata: theory and applications as a Built-In Self-Test structure, Ph. D. Thesis, I.I.T. Kharagpur, India, 1990.

[4] A.K. Das and P.P. Chaudhuri, Efficient characterization of cellular automata, Proc. IEE(Part E), 137(1), pp. 81-87, 1990.

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

[6] 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.

[7] D. Mukhopadhyay and D.R. Chowdhury, Characterization of a class of complemented group cellular automata, LNCS, 3305, pp. 775-784, 2004.

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

[9] S. Nandi and P.P. Chaudhuri, Analysis of periodic and intermediate boundary 90/150 cellular automata, IEEE Trans. Computers, 45(1), p.1-12, 1996.

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

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

[12] 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 Modelling, 36, pp. 979-986, 2002.

[13] S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim and Y.S. Pyo, Analysis of state-transition of SACA over $GF(2^p)$, J. Kor. Inst. Info. Security and Cryptology, 15, pp. 105-111, 2005.

[14] B. Elspas, The Theory of autonomous linear sequential networks, TRE Trans. on Circuits, CT-6(1), pp. 45-60, 1959.

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