Regular paper

Journal of the KIECS. pp. 293-302, vol. 11, no. 3, Mar. 31 2016, t. 71, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2016.11.3.293

Uniform CA와 90/150 Hybrid CA의 합성

김한두* · 조성진** · 최언숙*** · 권민정**** · 공길탁*****

Synthesis of Uniform CA and 90/150 Hybrid CA

Han-Doo Kim* · Sung-Jin Cho** · Un-Sook Choi*** · Min-Jeong Kwon**** · Gil-Tak Kong*****

요 약

본 논문에서는 전이규칙이 모두 102인 Uniform CA(Uniform Cellular Automata, UCA) $\mathbb{C}_u$와 특성다항식이 $(x+1)^m$인 m-셀 90/150 hybrid CA $\mathbb{C}_h$를 합성한 CA의 특성을 분석한다. 먼저 $\mathbb{C}_u$로부터 유도된 여원 그룹 CA의 사이클 구조를 분석하고 이를 통해 모든 사이클의 길이가 같아지는 여원 CA의 조건을 제시한다. 그리고 $\mathbb{C}_u$와 $\mathbb{C}_h$를 합성한 CA $\mathbb{C}$의 최소다항식이 $(x+1)^q$일 때 $(T+I)^{q-1}F \neq \mathbf{0}$을 만족하는 F를 여원벡터로 택하여 구성한 여원 그룹 CA $\mathbb{C}'$의 사이클 구조를 분석한다.

ABSTRACT

In this paper we analyze the CA formed by combining the uniform 102 CA $\mathbb{C}_u$ and the m-cell 90/150 hybrid CA $\mathbb{C}_h$ whose characteristic polynomial is $(x+1)^m$. We analyze cycle structures of complemented group CA derived from $\mathbb{C}_u$ and propose a condition of complemented CA dividing the entire state space into smaller cycles of equal lengths. And we analyze the cycle structure of complemented group CA $\mathbb{C}'$ derived from the CA $\mathbb{C}$ formed by combining $\mathbb{C}_u$ and $\mathbb{C}_h$ with complement vector F such that $(T+I)^{q-1}F \neq \mathbf{0}$ where $(x+1)^q$ is the minimal polynomial of $\mathbb{C}$.

키워드

Cellular Automata, Minimal Polynomial, Complemented CA, Cycle Structure
셀룰라 오토마타, 최소 다항식, 여원 CA, 사이클 구조

Ⅰ. 서 론

셀룰라 오토마타(Cellular Automata, 이하 CA)란 이산 시간의 동적 시스템으로 셀이라는 기본 단위 메모리의 배열로 이루어진다. 3-이웃 셀룰라 오토마타에서는 자기 자신과 인접 한 두 셀의 상태에 의해 정해진 규칙에 따라 셀의 다음 상태가 갱신된다. 이러한 CA는 간단하고 규칙적이며 작은 단위로 확장 연결할 수 있는 구조이기 때문에 VLSI 하드웨어 구현에 적절하다[1-6]. 가장 간단한 구조를 가지는 1차원 CA는

* 인제대학교 응용수학과 (mathkhd@inje.ac.kr)
** 교신저자 : 부경대학교 응용수학과
*** 동명대학교 정보통신공학과 (choies@tu.ac.kr)
**** 한국과학영재학교 (mjblack02@hanmail.net)
***** 부경대학교 응용수학과 (dieze@naver.com)
· 접 수 일 : 2016. 02. 24
· 수정완료일 : 2016. 03. 13
· 게재확정일 : 2016. 03. 24
· Received : Feb. 24, 2016, Revised : Mar. 13, 2016, Accepted : Mar. 24, 2016
· Corresponding Author : Sung-Jin Cho
Dept. of Applied Mathematics, Pukyong University,
Email : sjcho@pknu.ac.kr

모든 셀이 선형으로 배열되어 있고, CA의 상태전이에 적용되는 전이규칙의 종류에 따라 선형 CA와 비선형 CA로 나뉜다. 또한 CA의 모든 상태에 대하여 이전 상태가 유일하게 존재하는 CA를 그룹 CA라 한다. 그룹 CA는 주어진 상태가 일정한 주기 이후 원래의 상태로 돌아가는 특징을 가지고 있어서 상태전이가 반복되는 동안 정보가 보존되는 특성이 있으므로 암호시스템에서 암호화 및 복호하는데 사용할 수 있다[7-10]. 인터넷 기술의 발달로 멀티미디어 자료뿐만 아니라 중요한 금융 거래 자료들이 인터넷을 통해 이루어지고 있다. 영상은 민감하고 사적인 정보들을 포함하는 의학연구, 원격의료, 산업공정, 우주탐구 등 많은 분야에서 사용된다[11]. 따라서 데이터 전송 도중에 인증 받지 않은 사람의 도용을 피하기 위한 방법이 필요해졌다. Nandi 등[8]은 대칭키 영상 암호시스템의 암호 기법으로 그룹 CA 규칙을 이용하였다. 그리고 Roy 등[11]은 각각 전이규칙 204, 102, 60의 여원규칙인 51, 153, 195로 이루어진 그룹 CA를 이용한 대칭키 암호시스템을 제안하였다. 본 논문에서는 동일한 길이의 사이클로 구성된 더 긴 길이의 기계를 만들기 위하여 전이규칙이 모두 102인 UCA $\mathbb{C}_u$와 특성다항식이 $(x+1)^m$인 90/150 HCA $\mathbb{C}_h$를 합성한 CA의 특성을 분석한다. 먼저 $\mathbb{C}_u$로부터 유도된 여원 그룹 CA의 사이클 구조를 분석하고 이를 통해 모든 사이클의 길이가 같아지는 여원 CA의 조건을 제시한다. $\mathbb{C}_u$와 $\mathbb{C}_h$를 합성한 CA의 최소다항식이 $(x+1)^q$일 때 $(T+I)^{q-1}F \neq \mathbf{0}$을 만족하는 F를 여원벡터로 택하여 구성한 여원 그룹 CA의 사이클 구조를 분석한다. Nandi 등[8]의 영상 암호 기법에서 CA의 전이규칙과 여원벡터가 키의 역할을 하는데 [8]에서는 여원벡터가 한 개로 고정되나 본 연구에 의하면 더 많은 CA를 합성할 수 있고 다양한 여원벡터를 택할 수 있어 [8]의 방법보다 키 공간을 크게 할 수 있는 장점이 있으므로 안전성이 높아진다.

II. CA의 사전 지식

3개의 이웃을 가지는 CA의 다음 상태 전이함수는 3변수 부울함수 $f:\{0,1\}^3 \rightarrow \{0,1\}$이다. 그러므로 다음 상태 전이함수 f는 2^{2^3}개가 있으며 이것을 CA의 전이규칙(Transition rule)이라고 한다. n개의 셀로 이루어진 n-셀 CA의 각 셀에 사용되는 전이규칙으로 90과 150만 사용되는 CA를 90/150 HCA(: Hybrid CA)라 하고 표 1은 본 논문에서 사용되는 전이규칙을 부울식으로 나타낸 것이다. 같은 전이규칙으로 이루어진 CA를 UCA(: Uniform CA)라고 한다. 표 1과 같이 전이규칙을 부울식으로 표현했을 때 XOR 논리로만 이루어진 CA를 선형 CA(: Linear CA)라 한다. 이러한 CA는 상태전이함수를 $n \times n$ 행렬로 나타낼 수 있으며, 이를 상태전이행렬(State transition matrix)이라고 한다[12].

표 1. CA의 전이규칙의 부울식

Table 1. Boolean representation of the transition rules of CA

Transition Rule	State transition function
90	$q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
102	$q_i(t+1) = q_i(t) \oplus q_{i+1}(t)$
150	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$
204	$q_i(t+1) = q_i(t)$

주어진 n-셀 CA의 상태전이행렬 T의 특성다항식(Characteristic polynomial) $c_T(x)$는 $GF(2)$에서 $c_T(x) = |T \oplus xI|$ 이다. 여기서 I는 n차 단위행렬이다. 특성다항식의 인수 중 T를 근으로 갖는 가장 낮은 차수의 다항식을 최소다항식(Minimal polynomial)이라 하고 $m_T(x)$로 나타낸다. 그룹 CA의 상태전이 그래프에서 사이클의 구조는 CA의 최소다항식에 의하여 특성화된다. 90/150 CA는 특성다항식과 최소다항식이 같으므로 모든 크기의 CA에 대하여 최대주기 CA가 존재한다. 비선형 CA(: Nonlinear CA)는 셀에 선형이 아닌 규칙을 적용한 CA이며, 그룹 CA는 주어진 상태에 대한 이전 상태가 유일하게 존재하는 CA이다.

CA의 각 셀에 적용되는 규칙이 XOR 논리와 XNOR 논리의 조합으로 이루어진 CA를 여원 CA(: Complemented CA)라고 한다. 여원 CA의 다음 상태를 구하는 연산자를 $\overline{T}$라 하면 현재 CA의 상태 S_t에

대하여 다음 상태 S_{t+1}은 $S_{t+1}=\overline{T}S_t = TS_t \oplus F$로 나타낼 수 있으며, 여기서 F를 여원벡터(Complement vector)라고 한다. 일반적으로 $\overline{T}^p$를 여원 CA의 연산자인 $\overline{T}$를 p번 적용한 것이라 하면 현재 상태 S_t로부터 p시간 단계 후 여원 CA의 상태 S_{t+p}는 다음과 같다.

$$S_{t+p}=\overline{T}^pS_t=T^pS_t+(T^{p-1}+\cdots+T+I)F$$

여기서 $+$은 $GF(2)$에서 덧셈연산이다. n-셀 90/150 CA의 상태전이행렬 T_n은 다음과 같은 삼중대각행렬로 나타낼 수 있다.

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

단 $d_i \in \{0,1\}$ 이다. 본 논문에서는 간단히 $T_n=<d_1,d_2,\cdots,d_n>$ 으로 나타내기로 한다.

다음 정리 2.1은 본 논문에서 기본적으로 사용된다.

<정리 2.1> [13] 기약다항식 $p(x)$의 주기가 k이면 $[p(x)]^j$의 주기는 $k\cdot 2^r$ 이다. 단 $2^{r-1}<j\le 2^r$ 이다.

어떤 CA의 특성다항식인 다항식을 CA-다항식(CA-Polynomial)이라고 한다. 모든 기약다항식은 CA-다항식이다. Cho 등[3]은 유사변환(Similarity transformation)과 Lanczos 삼중대각 알고리즘(Lanczos tridiagonalization algorithm)을 이용하여 주어진 모든 CA-다항식에 대한 90/150 NBCA를 빠르게 합성하는 새로운 방법을 제안하였다. 또한 주어진 k차 기약다항식에 대하여 그것을 특성다항식으로 갖는 90/150 CA가 두 개($T_k=\langle r_1,r_2,\cdots,r_k\rangle$ 와 $T_k'=<r_k,\cdots,r_2,r_1>$) 존재한다는 것을 보였다.

III. 102 UCA의 분석

이 절에서는 특성다항식이 $(x+1)^n$인 n-셀 102 UCA를 분석하고 n-셀 102 UCA로부터 유도되는 여원 CA의 성질을 분석한다.

다음 보조정리는 행렬 곱셈의 성질로부터 알 수 있다.

<보조정리 3.1> n-셀 102 UCA $\mathbb{C}$의 상태전이행렬 T에 대하여 다음이 성립한다.

(i) 특성다항식과 최소다항식은 $(x+1)^n$이다.

(ii) 각 $k=1,2,\cdots,n-1$ 에 대하여 $(T+I)^k=(a_{ij})$ 라 하면 다음과 같다.

$$a_{ij}=\begin{cases}1, 1\le i\le n-k \text{ and } j=i+k\\ 0, otherwise\end{cases}$$

(iii) $F=(*,\cdots,*,1)^t$ 일 때 모든 $i=1,2,\cdots,n-1$에 대하여 $(T+I)^iF\neq \mathbf{0}$ 이다.

<정리 3.2> n-셀 102 UCA $\mathbb{C}_u$의 상태전이행렬 T에 대하여 여원벡터 $F=(*,\cdots,*,1)^t$ 에 대응하는 여원 그룹 CA $\mathbb{C}_u'$의 상태전이 함수 $\overline{T}$의 위수 $ord(\overline{T})$는 $ord(\overline{T})\ge ord(T)$ 이다.

(증명) $ord(T)=p$ 이고 $ord(\overline{T})=k$ 라 하자. 그러면 $p=2^r\ (2^{r-1}<n\le 2^r)$ 이다. $k=\frac{p}{2}=2^{r-1}$ 이라 가정하자. 그러면 $\mathbb{C}_u'$의 모든 상태 X에 대하여 식 (1)이 성립한다.

$$\overline{T}^kX=X \tag{1}$$

$X=\mathbf{0}$ 일 때 $\overline{T}^k\mathbf{0}=T^k\mathbf{0}+(T^{k-1}+\cdots+T+I)F=(T+I)^{k-1}F$ 이다. 그런데 $m_T(x)=(x+1)^n$이고 $k<n$ 이므로 $(T+I)^{k-1}\neq O$이다. 그러므로 보조정리 3.1에 의하여 $(T+I)^{k-1}F\neq\mathbf{0}$ 이다. 따라서 $\overline{T}^k\mathbf{0}\neq\mathbf{0}$ 이다. 이는 식 (1)에 모순이다. 따라서 $ord(\overline{T})>\frac{p}{2}$ 이므로 $ord(\overline{T})\ge ord(T)$ 이다.

<정리 3.3> n-셀 102 UCA $\mathbb{C}_u$의 상태전이행렬 T에 대하여 여원벡터 $F=(*,\cdots,*,1)^t$ 에 대응하는 여원 그룹 CA $\mathbb{C}_u'$의 상태전이 함수 $\overline{T}$의 위수

$ord(\overline{T})$ 는 $ord(T)$ 또는 $2 \cdot ord(T)$ 이다.

(증명) $ord(T)=p$ 라 하자. 그러면 $\mathbb{C}_u'$의 모든 상태 X에 대하여 다음이 성립한다.

$$\overline{T}^{2p}X = T^{2p}X+(T^{2p-1}+\cdots+T+I)F = X+\{T^p(T^{p-1}+\cdots+T+I)+(T^{p-1}+\cdots+T+I)\}F = X+\mathbf{0}=X .$$

그러므로 $ord(\overline{T})$ 는 $2p$의 약수이다. 정리 3.2에 의하여 $ord(\overline{T}) \geq p$ 이므로 $ord(\overline{T})$ 는 p 또는 $2p$이다.

<따름정리 3.4> 정리 3.3에서 $ord(\overline{T})$ 는 다음과 같다.

$$ord(\overline{T})=\begin{cases}2^r, & 2^{r-1}<n<2^r\\ 2^{r+1}, & n=2^r\end{cases}$$

(증명) (i) $n=2^r$ 일 때 $ord(T)=n$ 이다. 그러면 $\mathbb{C}_u'$의 모든 상태 X에 대하여 $\overline{T}^nX = T^nX+(T+I)^{n-1}F = X+(T+I)^{n-1}F$ 이 성립한다. $m_T(x)=(x+1)^n$ 이므로 보조정리 3.1에 의하여 $(T+I)^{n-1}F \neq \mathbf{0}$ 이다. 그러면 $\overline{T}^nX \neq X$ 이므로 $ord(\overline{T})=2n=2^{r+1}$ 이다.

(ii) $2^{r-1}<n<2^r$ 일 때 $ord(T)=p$ 라 하면 $p=2^r$ 이다. 그러면 $\mathbb{C}_u'$의 모든 상태 X에 대하여 $\overline{T}^pX = T^pX+(T+I)^{p-1}F = X+(T+I)^{p-1}F$ 이 고 $n \leq p-1$ 이므로 $(T+I)^{p-1}=O$이다. 따라서 $\mathbb{C}_u'$의 모든 상태 X에 대하여 $\overline{T}^pX=X$이므로 정리 3.2에 의하여 $ord(\overline{T})=p=2^r$ 이다.

<정리 3.5> n-셀 102 UCA $\mathbb{C}_u$의 상태전이행렬 T에 대하여 여원벡터 $F=(*,\cdots,*,1)^t$ 에 대응하는 여원 그룹 CA $\mathbb{C}_u'$의 상태전이그래프에서 모든 사이클의 길이는 주기와 같다.

(증명) (i) $n=2^r$ 일 때: 따름정리 3.4에 의하여 $\mathbb{C}_u'$의 상태전이그래프에서 모든 사이클의 길이는 주기 2^{r+1}과 같다.

(ii) $2^{r-1}<n<2^r$ 일 때: 따름정리 3.4에 의하여 $ord(\overline{T})=2^r$ 이다. 2^r보다 작은 l에 대하여 $\overline{T}^lX=X$인 $\mathbb{C}_u'$의 상태 X가 존재한다고 가정하자. 그러면

$$X=\overline{T}^lX=T^lX+(T+I)^{l-1}F$$
$$(T+I)^lX=(T+I)^{l-1}F$$
$$(T+I)^{n-l}(T+I)^lX=(T+I)^{n-l}(T+I)^{l-1}F$$
$$(T+I)^nX=(T+I)^{n-1}F$$

이고 $m_T(x)=(x+1)^n$이므로 $(T+I)^n=O$ 이다. 그러므로 $\mathbf{0}=(T+I)^{n-1}F$. 보조정리 3.1에 의하여 $F=(*,\cdots,*,1)^t$ 일 때 $(T+I)^{n-1}F \neq \mathbf{0}$ 이므로 모순이다. 그러므로 F에 대응하는 $\mathbb{C}_u'$의 상태전이그래프에서 모든 사이클의 길이는 주기와 같다.

<참고 A> 정리 3.5의 증명으로부터 최소다항식이 $(x+1)^n$인 $\mathbb{C}_u$로부터 유도된 $\mathbb{C}_u'$에 대하여 $(T+I)^{n-1}F \neq \mathbf{0}$ 을 만족하는 F를 여원벡터로 택하면 $\mathbb{C}_u'$의 상태전이그래프의 모든 사이클의 길이는 주기와 같다는 것을 알 수 있다.

<예제 3.6> 6-셀 102 UCA $\mathbb{C}_u$의 상태전이행렬을 T라 하면 T의 최소다항식은 $(x+1)^6$이다. $\mathbb{C}_u$와 여원벡터 $F=(*,\cdots,*,1)^t$ 에 대응하는 $\mathbb{C}_u'$의 상태전이그래프에서 모든 사이클의 길이는 주기와 같다. $\mathbb{C}_u$의 상태전이그래프의 사이클은 다음과 같다:

1-사이클의 개수: 2개, 2-사이클의 개수: 1개, 4-사이클의 개수: 3개, 8-사이클의 개수: 6개.

예를 들어 $F=(0,0,0,0,0,1)^t$ 일 때 $\mathbb{C}_u'$의 상태전이그래프는 8개의 동일한 8-사이클로 구성된다.

Ⅳ. 102 UCA와 90/150 HCA의 합성

102 UCA $\mathbb{C}_u$인 경우 언제든지 $c_T(x)=(x+1)^k$ 꼴인 T를 구성할 수 있으나[12] 90/150 HCA의 경우에는 다음 정리 4.1과 같이 T를 구성할 수 있다. 다음 정리는 최소다항식이 $(x+1)^n$인 n-셀 90/150 HCA를 합성할 수 있는 이론적 근거를 제시하며 이는 [14]의 정리 3.6과 3.8의 특별한 경우이다.

<정리 4.1> 최소다항식이 $(x+1)^k$인 90/150 HCA의 상태전이행렬이 $T_k = \langle r_1, r_2, \cdots, r_k \rangle$ 일 때 T_{2k}와 T_{2k+1}은 다음과 같다.

(i) $T_{2k} = < r_1, \cdots, r_{k-1}, \overline{r_k}, \overline{r_k}, r_{k-1}, \cdots, r_1 >$

(ii) $T_{2k+1} = < r_1, \cdots, r_k, 0, r_k, \cdots, r_1 >$

여기서 $T_1 = \langle 1 \rangle$ 이다.

<정리 4.2> [15] 최소다항식이 $m_{T_n}(x) = (x+1)^n$, $n = 2,3,\cdots$ 인 n-셀 90/150 HCA $\mathbb{C}_h$의 상태전이행렬 T_n에 대하여 $S_n = (T_n + I_n)^{n-1}$라 하면 S_{2n}과 S_{2n+1}은 다음과 같다.

$$S_{2n} = (T_{2n} + I_{2n})^{2n-1} = \begin{bmatrix} S_n & S_n \\ S_n & S_n \end{bmatrix},$$

$$S_{2n+1} = (T_{2n+1} + I_{2n+1})^{2n} = \begin{bmatrix} S_n & O & S_n \\ O & 0 & O \\ S_n & O & S_n \end{bmatrix}.$$

단, $S_2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, S_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ 이다.

표 2는 정리 4.1에 의해 합성할 수 있는 90/150 HCA의 몇 가지 상태전이행렬이다.

표 2. 90/150 HCA의 상태전이행렬
Table 2. State transition matrix of 90/150 HCA

State transition matrix	Characteristic Polynomial	Period
$T = <1>$	$x+1$	1
$T = <0,0>$	$(x+1)^2$	2
$T = <1,1,1>$	$(x+1)^3$	4
$T = <0,1,1,0>$	$(x+1)^4$	4
$T = <0,0,1,0,0>$	$(x+1)^5$	8
⋮	⋮	⋮

앞으로 90/150 HCA의 상태전이행렬은 표 2의 상태전이행렬을 택하기로 한다. 상태전이행렬이 T_{a_m}인 m-셀 $\mathbb{C}_u$와 상태전이행렬이 T_{b_n}인 n-셀 $\mathbb{C}_h$를 합성하는데 최소다항식이 $(x+1)^q$인 형태가 되도록 하기 위하여 $\mathbb{C}_u$의 마지막 전이규칙 102를 204로 바꾸거나 $\mathbb{C}_h$의 첫 번째 전이규칙을 90은 170으로 150은 102로 바꾸어야 할 경우가 있다. $\mathbb{C}_u$의 마지막 전이규칙 102를 204로 바꾼 CA를 $\mathbb{C}_{u^*}$, $\mathbb{C}_h$의 첫 번째 전이규칙을 90은 170으로 150은 102로 바꾼 CA를 $\mathbb{C}_{h^*}$라 하자.

4.1 $\mathbb{C} = < \mathbb{C}_{u^*} \| \mathbb{C}_h >$ 인 경우

m-셀 $\mathbb{C}_{u^*}$에 대한 최소다항식은 $(x+1)^m$이고 n-셀 $\mathbb{C}_h$에 대한 최소다항식은 $(x+1)^n$이다.

<정리 4.3> m-셀 $\mathbb{C}_{u^*}$와 n-셀 $\mathbb{C}_h$를 합성한 $(m+n)$-셀 CA $\mathbb{C} = < \mathbb{C}_{u^*} \| \mathbb{C}_h >$ 의 최소다항식은 다음과 같다.

$$m_T(x) = \begin{cases} (x+1)^m, & m > n \\ (x+1)^{n+1}, & n \geq m \end{cases}$$

(증명) $\mathbb{C}$의 상태전이행렬 T는

$$T = \left(\begin{array}{c|c} T_{a_m} & O \\ \hline \begin{matrix} 1 \\ 0 \\ O \\ 0 \end{matrix} \vdots & T_{b_n} \end{array}\right)$$ 이므로

$$T+I = \left(\begin{array}{c|c} T_{a_m} + I_m & O \\ \hline \begin{matrix} 1 \\ 0 \\ O \\ 0 \end{matrix} \vdots & T_{b_n} + I_n \end{array}\right)$$ 이다.

이 경우 각 자연수 l에 대하여 $(T+I)^l$은 다음과 같다.

$$(T+I)^l = \left(\begin{array}{c|c} (T_{a_m} + I_m)^l & O \\ \hline \begin{matrix} * \\ O \\ * \end{matrix} \vdots & (T_{b_n} + I_n)^l \end{array}\right)$$

(1) $m > n$ 인 경우:

$(T_{b_n} + I_n)^n = O$이므로

$(T+I)^{n+1} = (T+I)^n (T+I)$

$$= \left(\begin{array}{c|c} (T_{a_m}+I_m)^n & O \\ \hline & * \\ O & \vdots \\ & * \end{array}\right) \left(\begin{array}{c|c} T_{a_m}+I_m & O \\ \hline & 1 \\ & 0 \\ O & \vdots \\ & 0 \end{array}\right)$$

$$= \left(\begin{array}{c|c} (T_{a_m}+I_m)^{n+1} & O \\ \hline O & O \end{array}\right) \text{ 이다.}$$

그런데 $i < m$ 이면 $(T_{a_m}+I_m)^i \neq O$ 이고 $(T_{a_m}+I_m)^m = O$ 이므로 $m_T(x) = (x+1)^m$ 이다.

(2) $n \geq m$ 인 경우:

$(T_{a_m}+I_m)^m = O$ 이므로

$(T+I)^{m+1} = (T+I)^m (T+I)$

$$= \left(\begin{array}{c|c} (T_{a_m}+I_m)^m & O \\ \hline & * \\ O & \vdots \\ & * \end{array}\right) \left(\begin{array}{c|c} T_{a_m}+I_m & O \\ \hline & 1 \\ & 0 \\ O & \vdots \\ & 0 \end{array}\right)$$

$$= \left(\begin{array}{c|c} O & O \\ \hline * & \\ O \vdots & (T_{b_n}+I_n)^{m+1} \\ * & \end{array}\right)$$

이다. 정리 4.2에 의하면 $(T_{b_n}+I_n)^{n-1}$ 의 첫 열은 영벡터가 아니다. $(T_{b_n}+I_n)^n = O$ 이므로 $(T+I)^l$ 의 m 번째 열은 $l = n+1$ 일 때 영벡터가 될 수 있다. 그러므로 $(T+I)^n \neq O$ 이고 $(T+I)^{n+1} = O$ 이다. 따라서 $m_T(x) = (x+1)^{n+1}$ 이다.

<따름정리 4.4> $m_T(x) = (x+1)^q$ ($q = \max(m, n+1)$) 일 때 $F = (f_1, \cdots, f_m, \cdots, f_{n+m})^t$ 가 $(T+I)^{q-1}F \neq \mathbf{0}$ 을 만족하는 여원벡터라고 하면 $f_m = 1$ 이다.

참고 A와 따름정리 4.4에 의하여 m-셀 $\mathbb{C}_{u^*}$와 n-셀 $\mathbb{C}_h$를 합성한 $(m+n)$-셀 CA $\mathbb{C}$와 여원벡터 $F = (*, \cdots, *, \underline{1}, *, \cdots, *)^t$ (1의 위치는 m번째)에 대응하는 여원 그룹 CA $\mathbb{C}'$의 상태전이그래프의 모든 사이클의 길이는 주기와 같음을 알 수 있다.

<예제 4.5> 3-셀 $\mathbb{C}_{u^*}$와 3-셀 $\mathbb{C}_h$를 합성한 6-셀 CA $\mathbb{C}$의 최소다항식은 $m_T(x) = (x+1)^4$ 이다. $\mathbb{C}$의 상태전이그래프의 사이클은 다음과 같다:

1-사이클의 개수: 4개, 2-사이클의 개수: 6개, 2^2-사이클의 개수: 12개.

여원벡터 F를 $F = (0,0,1,0,0,0,0)^t$ 로 택하면 $(T+I)^3 F \neq \mathbf{0}$ 이고 $\mathbb{C}'$의 상태전이그래프는 8개의 동일한 8-사이클로 구성된다.

4.2 $\mathbb{C} = <\mathbb{C}_u \| \mathbb{C}_{h^*}>$ 인 경우

<정리 4.6> m-셀 $\mathbb{C}_u$와 n-셀 $\mathbb{C}_{h^*}$를 합성한 $(m+n)$-셀 CA $\mathbb{C}$의 최소다항식은 $m_T(x) = (x+1)^{m+n}$ 이다.

(증명) $\mathbb{C}$의 상태전이행렬은

$$T = \left(\begin{array}{c|c} T_{a_m} & O \\ \hline & 1\,0\cdots 0 \\ O & T_{b_n} \end{array}\right) \text{ 이다.}$$

(1) $m \geq n$ 인 경우:

$$(T+I)^n = \left[\begin{array}{c|c} & A_1 \\ (T_{a_m}+I_m)^n & \vdots \\ & A_{m-1} \\ & A_m \\ \hline O & O \end{array}\right] \text{ 이다.}$$

여기서 A_m은 $(T_{b_n}+I_n)^{n-1}$의 1행이고 정리 4.2에 의하여 $(T_{b_n}+I_n)^{n-1}$의 1행은 영벡터가 아니므로 $A_m \neq \mathbf{0}$ 이다.

$$(T+I)^{n+k}=\left[\begin{array}{c|c}(T_{a_m}+I_m)^{n+k} & \begin{matrix}A_{k+1}\\ \vdots\\ A_m\\ \mathbf{0}\end{matrix}\\ \hline O & O\end{array}\right]$$ 이므로

$k=m-1$ 이면

$$(T+I)^{m+n-1}=\left[\begin{array}{c|c}O & \begin{matrix}A_m\\ \mathbf{0}\\ \vdots\\ \mathbf{0}\end{matrix}\\ \hline O & O\end{array}\right]\neq O$$

(2) $m<n$ 인 경우:

$$(T+I)^{n}=\left[\begin{array}{c|c}O & \begin{matrix}A_1\\ \vdots\\ A_{m-1}\\ A_m\end{matrix}\\ \hline O & O\end{array}\right]$$ 이므로 (1)의 증명 방법과 같은 방법으로 증명할 수 있다.

<따름정리 4.7> 정리 4.6에서 $F=(f_1,\cdots,f_m,\cdots,f_{n+m})^t$ 를 여원벡터라고 하면 $m_T(x)=(x+1)^{m+n}$ 일 때 $(T+I)^{m+n-1}F\neq\mathbf{0}$ 을 만족하는 F는 다음과 같다.

$$F=(*,\cdots,*,f_{m+1},\cdots,f_{m+n})^t$$

단, $(f_{m+1},\cdots,f_{m+n})\cdot A_m\neq 0$.

여기서 크기 n에 따른 $(T_{b_n}+I_n)^{n-1}$의 1행인 A_m은 표 3과 같다.

표 3. $(T_{b_n}+I_n)^{n-1}$의 1행

Table 3. The 1st row of $(T_{b_n}+I_n)^{n-1}$

n	The 1st row of $(T_{b_n}+I_n)^{n-1}$
2	11
3	101
4	1111
5	11011
6	101101
⋮	⋮

표 3은 정리 4.2에 의하여 얻어지며 $(T_{b_n}+I_n)^{n-1}$의 1행을 구하는 계산복잡도는 $O(\log_2 n)$ 이고[15], F의 개수는 2^{m+n-1} 이다.

<예제 4.8> 3-셀 $\mathbb{C}_u$와 4-셀 $\mathbb{C}_{h^*}$를 합성한 7-셀 CA $\mathbb{C}$의 최소다항식은 $m_T(x)=(x+1)^7$ 이다. $F=(f_1,f_2,f_3,f_4,f_5,f_6,f_7)^t$ 라 하면 따름정리 4.7과 표 3에 의하여 $F=(*,*,*,f_4,f_5,f_6,f_7)^t$ 이다. 단, $\sum_{i=4}^{7} f_i\neq 0 \pmod 2$ 이다. 또한 $(T+I)^6F\neq\mathbf{0}$ 인 F의 개수는 2^6이다.

4.3 $\mathbb{C}=<\mathbb{C}_h\|\mathbb{C}_u>$ 인 경우

90/150 HCA $\mathbb{C}_h$ 다음에 102 UCA $\mathbb{C}_u$를 붙이는 경우를 생각해보자. $\mathbb{C}_h$의 상태전이행렬을 T_{b_n}, $\mathbb{C}_u$의 상태전이행렬을 T_{a_m}이라 하면 다음 정리 4.9는 정리 4.6과 유사한 방법으로 증명할 수 있다.

<정리 4.9> n-셀 90/150 HCA $\mathbb{C}_h$와 m-셀 102 UCA $\mathbb{C}_u$를 합성한 $(m+n)$-셀 CA $\mathbb{C}=<\mathbb{C}_h\|\mathbb{C}_u>$ 의 최소다항식은 $m_T(x)=(x+1)^{m+n}$ 이다.

<따름정리 4.10> $\mathbb{C}$와 여원벡터 F에 대응하는 여원 그룹 CA $\mathbb{C}'$의 상태전이그래프에서 모든 사이클의 길이는 주기와 같다. 여기서 F는 $F=(*,\cdots,*,1)^t$ 이다.

<참고 C> $\mathbb{C}=<\mathbb{C}_h,\mathbb{C}_u>$ 의 상태전이행렬 T에 대하여

$$(T+I)^{m+n-1}=\left(\begin{array}{c|c} O & \mathbf{0}\cdots\mathbf{0}\,B_n \\ \hline O & O \end{array}\right)$$

, 여기서 B_n은 $(T_{b_n}+I_n)^{n-1}$의 마지막 열이다. 정리 4.2에 의하여 $(T_{b_n}+I_n)^{n-1}$이 대칭행렬이므로 B_n은 $(T_{b_n}+I_n)^{n-1}$의 첫 행과 같다. 따라서 $(T+I)^{m+n-1}$의 마지막 열은 $(B_n 0\cdots 0)^t$ 이다.

<예제 4.11> 3-셀 90/150 HCA $\mathbb{C}_h$와 4-셀 102 UCA $\mathbb{C}_u$를 합성한 7-셀 CA $\mathbb{C}$의 $T=<150,150,150,102,102,102,102>$ 에 대하여 최소다항식은 $(x+1)^7$이다. 정리 4.2에 의하면 $T_{b_3}+I_3$가 대칭행렬이므로 $(T_{b_3}+I_3)^2$의 마지막 열은 첫 행과 같으므로 표 3에 의하여 101이다. 그러므로 $(T+I_7)^6$의 마지막 열은 $(1010000)^t$ 이다.

$$(T+I_7)^6=\left(\begin{array}{ccc|cccc} 0&0&0&0&0&0&1\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1\\ \hline 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0 \end{array}\right)\leftarrow (T_{b_3}+I_3)^2\text{의 마지막 열}$$

$F=(f_1,f_2,f_3,f_4,f_5,f_6,f_7)^t$ 일 때 $(T+I_7)^6F\neq\mathbf{0}$ 이기 위한 F의 조건은 $f_7=1$ 이다. 따라서 $\mathbb{C}'$의 상태전이그래프에서 모든 사이클의 길이를 같게 하는 F는 2^6개다.

전이규칙이 모두 102인 UCA $\mathbb{C}_u$와 최소다항식이 $(x+1)^m$인 90/150 HCA $\mathbb{C}_h$를 합성한 CA의 최소다항식이 $(x+1)^q$일 때 $(T+I)^{q-1}F\neq\mathbf{0}$을 만족하는 F를 여원벡터로 택하여 구성한 여원 그룹 CA의 상태전이그래프의 사이클들은 모두 동일한 길이이다. Nandi 등[8]의 영상 암호 기법에서 CA의 전이규칙과 여원벡터가 키의 역할을 하는데 [8]에서는 여원벡터가 한 개로 고정되나 본 연구에 의하면 더 많은 CA를 합성할 수 있고 다양한 여원벡터를 택할 수 있는 장점이 있으므로 [8]의 방법보다 키 공간을 크게 할 수 있어 안전성이 높아진다.

Ⅴ. 결론

본 논문에서는 동일한 길이의 사이클로 구성된 더 긴 길이의 기계를 만들기 위하여 전이규칙이 모두 102인 UCA $\mathbb{C}_u$와 특성다항식이 $(x+1)^m$인 90/150 HCA $\mathbb{C}_h$를 합성한 CA의 특성을 분석하였다. 먼저 $\mathbb{C}_u$로부터 유도된 여원 그룹 CA의 사이클 구조를 분석한 다음 모든 사이클의 길이가 같아지는 여원 CA의 조건을 제시하였다. $\mathbb{C}_u$와 $\mathbb{C}_h$를 합성한 CA의 최소다항식이 $(x+1)^q$일 때 $(T+I)^{q-1}F\neq\mathbf{0}$을 만족하는 F를 여원벡터로 택하여 구성한 여원 그룹 CA의 사이클 구조를 분석하였다.

References

[1] S. Cho, U. Choi, Y. Hwang, and H. Kim, "Analysis of hybrid group cellular automata," *International Conference on Cellular Automata for Research and Industry(ACRI) 2006, Lecture Notes in Computer Science 4173*, Perpignan, France, September, 2006, Proceedings, pp. 222-231.

[2] S. Cho, U. Choi, H. Kim, and Y. Hwang, "Analysis of complemented CA derived from linear hybrid group CA," *Computers Math. Appli.*, vol. 53, 2007, pp. 54-63.

[3] S. Cho, U. Choi, H. Kim, Y. Hwang, J. Kim, and S. Heo, "New synthesis of one-dimensional 90/150 linear hybrid group cellular automata," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Trans.*, vol. 26, no. 9, 2007, pp. 1720-1724.

[4] Y. Hwang, U. Choi, and S. Cho, "D1-MACA based Two-Class Pattern Classifier," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 3, no. 4, 2008, pp. 254-259.

[5] Y. Hwang, S. Cho, and U. Choi, "Multiple Attractor CA based Pattern Classifier," *J. of the Korea Institute of Electronic Communication*

Sciences, vol. 5, no. 3, 2010, pp. 315-320.
[6] S. Kwon, S. Cho, U. Choi, H. Kim, and N. Kim, "Generation of Pattern Classifier using LFSRs," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 9, no. 6, 2014, pp. 673-679.
[7] N. Ganguly, "Cellular automata evolution: theory and applications in pattern recognition and classification," Ph.D's Thesis, *Bengal Engineering College, India,* 2004.
[8] S. Nandi, S. Roy, S. Nath, S. Chakraborty, W. Karaa, and N. Dey, "1-D Group Cellular Automata based Image Encryption Technique," *IEEE Int. Conf. on Control, Instrumentation, Communication and Computational Technologies*, Kanyakumari, India, July, 2014, pp. 521-526.
[9] J. Jin, "Image Encryption Method based on Elementary Cellular Automata," *Optics and Lasers in Engineering,* vol. 50, no. 12, 2012, pp. 1836-1843.
[10] T. Nam, S. Kim, and S. Cho, "Image Encryption using Complemented MLCA based on IBCA and 2D CAT," *J. of The Institute of Electronics and Information Engineers,* vol. 46-SP, no. 4, 2009, pp. 34-41.
[11] S. Roy, S. Nandi, J. Dansana, and P. Pattnaik, "Application of Cellular Automata in Symmetric Key Cryptography," *IEEE Int. Conf. on Communication and Signal Processing, April 3-5, 2014, India*, pp. 572-576.
[12] P. Chaudhuri, D. Choudhury, S. Nandi, and S. Chattopadhyay, *Additive cellular automata theory and applications vol. 1.* California, IEEE Computer Society Press, 1997.
[13] B. Elspas, "The theory of autonomous linear sequential networks," *TRE Trans. Circuits, CT-6,* no. 1, 1959, pp. 45-60.
[14] U. Choi, S. Cho, and G. Kong, "Analysis of Characteristic Polynomial of Cellular Automata with Symmetrical Transition Rules," *Proc. of the Jangjeon Mathematical Society,* vol. 18, no. 1, 2015, pp. 85-93.
[15] M. Kwon, S. Cho, H. Kim, U. Choi, and G. Kong, "Analysis of Complemented Group CA derived from 90/150 Group CA," J. Appl. Math. & Informatics(accepted).

저자 소개

김한두(Han-Doo Kim)

1982년 2월 고려대학교 수학과 졸업 (이학사)
1984년 2월 고려대학교 대학원 수학과 졸업 (이학석사)
1988년 2월 고려대학교 대학원 수학과 졸업(이학박사)
1989년~현재 인제대학교 응용수학과 교수
※ 관심분야 : 전산수학, 셀룰라 오토마타론

조성진(Sung-Jin Cho)

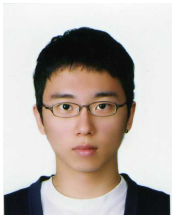
1979년 2월 강원대학교 수학교육과 졸업 (이학사)
1981년 2월 고려대학교 대학원 수학과 졸업 (이학석사)
1988년 2월 고려대학교 대학원 수학과 졸업 (이학박사)
1988년 ~ 현재 부경대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

최언숙(Un-Sook Choi)

1992년 2월 성균관대학교 산업공학과 졸업 (공학사)
2000년 8월 부경대학교 응용수학과 졸업 (이학석사)
2004년 8월 부경대학교 응용수학과 졸업 (이학박사)
2009년 8월 부경대학교 정보보호학과 졸업 (공학박사)
2009년~현재 동명대학교 정보통신공학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

권민정(Min-Jeong Kwon)

1997년 2월 부산대학교 수학교육과 졸업 (이학사)
20002년 8월 부산대학교 교육대학원 수학과 졸업 (교육학석사)
2014년 8월 부경대학교 응용수학과 졸업 (이학박사)
2014년~현재 한국과학영재학교 교원
※ 관심분야 : 셀룰라 오토마타론, 정보보호



공길탁(Gil-Tak Kong)

2013년 3월 부경대학교 응용수학과 졸업 (이학사)
2015년 2월 부경대학교 응용수학과 졸업 (이학석사)
※ 관심분야 : 셀룰라 오토마타론